**D9.4**

**Pilot of Cyber training & exercise Framework**

|  |  |
| --- | --- |
| ****Project number**** | **830892** |
| ****Project acronym**** | **SPARTA** |
| ****Project title**** | **Strategic programs for advanced research and technology in Europe** |
| ****Start date of the project**** | **1st February 2019** |
| ****Duration**** | **36 months** |
| ****Programme**** | **H2020-SU-ICT-2018-2020** |

|  |  |
| --- | --- |
| ****Deliverable type**** | **Report** |
| ****Deliverable reference number**** | **SU-ICT-03-830892 / D9.1 / V1.0** |
| ****Work package contributing to the deliverable**** | **WP9** |
| ****Due date**** | **July 2021 – M30** |
| ****Actual submission date**** | **31st July, 2021** |

|  |  |
| --- | --- |
| ****Responsible organisation**** | **KTU** |
| ****Editor**** | **Algimantas Venčkauskas** |
| ****Dissemination level**** | **PU** |
| ****Revision**** | **V1.0** |

|  |  |
| --- | --- |
| ****Abstract**** | **…………………….** |
| ****Keywords**** | **…………………….** |

**Editor**

**Algimantas Venčkauskas** (KTU)

**Contributors** (ordered according to beneficiary numbers)

Tomas Lieskovan, Jan Hajny (BUT)

Giorgio Bernardinetti, Giuseppe Bianchi (CNIT)

Šarūnas Grigaliūnas, Stasys Maciulevičius, Nerijus Morkevičius (KTU)

………………………….. (UBO)

**Reviewers** (ordered according to beneficiary numbers)

…………… (XXX)

…………….. (YYY)

**Disclaimer**

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Executive Summary

Various hackers can attack today organizations and users. The attackers become more organized, and they are using more advanced and automated techniques and tools. One solution to problem detection of these attacks and building adequate protection against them is to enhance cybersecurity education and training for university students, cybersecurity professionals and IT staff to gain more knowledge and skills in tackling cyber threats and their consequences.

This report presents the study of cybersecurity exercises and training. Chapter 2 provides an overview of cybersecurity training target groups (Section 2.1), knowledge areas (Section 2.2), and mapping of target groups to knowledge areas (Section 2.3). Next (Section 2.4) is noted that training and exercises are essential for deeper mastering of teaching materials essential and preparing the cybersecurity workforce of both for today and tomorrow. Different activities – exercises and competitions (Section 2.5) – are analyzed, and mapping of training & exercise activities to knowledge areas is presented (Section 2.6). The chapter concludes with an analysis of cybersecurity platforms and training environments (Section 2.7) and cyber ranges, which are a popular environment for experiencing real-world threats in a virtual environment, learning how to identify potential threats and know how to deal with them (Section 2.8).

The architecture of cyber training & exercise framework is presented in Section 3.1 (Chapter 3). It includes tools presented by partners (KTU, BUT, CNIT, and UBO) and federated by SPARTA JCCI integrator. Presented by partners, training & exercise tools cover knowledge areas, as shown in Section 3.2.

KTU Pilot of Cyber Security Training Platform is presented in Chapter 4. A short description of this platform follows by presenting an example of using it in playing an attack according to a storyline-based scenario.

CNIT Cyber Range – the Nautilus Platform – is presented in Chapter 5. It represents a reliable training tool to advance cybersecurity skills at all levels, enables quick deployments and configurations as well as effective sharing, among different parties ant stakeholders, of the information gathered about cyber security threats and corresponding defense strategies. In this Chapter core design and principles are in short explained, as well as a pilot storyline based on an Attack&Defense CTF competition is presented.

BUT Pilot of KYPO Cyber Range Platform is presented in Chapter 6. Here, we describe the purpose and architecture of one of the first open-source cyber ranges on the European market, show the installation requirements, provide full installation manual, describe the deployment at BUT premises and demonstrate the sample training scenario. Furthermore, we present the description and results of the first pilot using the KYPO cyber range tools that took place at BUT premises with real students. We finish the section with the description of next activities, in particular concerning the further extension of the KYPO deployment and the connection to the cyber-physical lab.

UBO – a framework to measure IT-Security Awareness within working staff is presented in Chapter 7. It can be used to quantify the training effect of an awareness exercise, while the framework facilitates the comparison of different exercises based on effectiveness.

Table of Contents

[Executive Summary II](#_Toc70508177)

[Table of Contents III](#_Toc70508178)

[List of Figures 6](#_Toc70508179)

[List of Tables 8](#_Toc70508180)

[Chapter 1 Introduction 9](#_Toc70508181)

[Chapter 2 Structure of Cyber training & exercise Framework 11](#_Toc70508182)

[2.1 The target groups 11](#_Toc70508183)

[2.2 Knowledge areas 12](#_Toc70508184)

[2.3 Mapping of target groups to knowledge areas 16](#_Toc70508185)

[2.4 Training & exercise activities 17](#_Toc70508186)

[2.5 Cybersecurity Competitions 20](#_Toc70508187)

[2.6 Mapping of training & exercise activities to knowledge areas 23](#_Toc70508188)

[2.7 Cybersecurity Platforms and Training Environments 24](#_Toc70508189)

[2.8 Cyber Range as training&exercise platform 26](#_Toc70508190)

[2.8.1 Taxonomy of Cyber Ranges 27](#_Toc70508191)

[2.8.2 Benefits of a Cyber Range 30](#_Toc70508192)

[2.8.3 Cyber Range Mission – Capabilities – Advantages 31](#_Toc70508193)

[Chapter 3 Pilot of Cyber training & exercise Framework 32](#_Toc70508194)

[3.1 Architecture of Cyber training & exercise Framework 32](#_Toc70508195)

[3.2 Mapping of training & exercise activities to knowledge areas 35](#_Toc70508196)

[Chapter 4 KTU Pilot of Cyber Security Training Platform 36](#_Toc70508197)

[4.1 Description of KTU Cyber training & exercise Framework 36](#_Toc70508198)

[4.2 Pilot of KTU Cyber training & exercise Framework 38](#_Toc70508199)

[4.2.1 Description of KTU Cyber training & exercise Platform 38](#_Toc70508200)

[4.2.2 Installation of KTU Cyber training & exercise Platform 39](#_Toc70508201)

[4.2.3 Pilot of Red Team / Blue Team exercise on KTU Platform 39](#_Toc70508202)

[4.2.4 How to play storyline? 42](#_Toc70508203)

[4.2.5 The benefits of using the Cyber training & exercise Framework 44](#_Toc70508204)

[Chapter 5 CNIT – own platform with a storyline 46](#_Toc70508205)

[5.1 The Nautilus Platform 46](#_Toc70508206)

[5.1.1 Core Design and Principles 46](#_Toc70508207)

[5.2 The Pilot: CTF platform for cyber competition 50](#_Toc70508208)

[5.2.1 How to play 51](#_Toc70508209)

[5.2.2 CTF challenges 52](#_Toc70508210)

[5.2.3 Benefits of using the Nautilus Cyber Range 52](#_Toc70508211)

[Chapter 6 BUT Pilot of KYPO Cyber Range Platform 53](#_Toc70508212)

[6.1 Deploying KYPO CRP 53](#_Toc70508213)

[6.1.1 Requirements 53](#_Toc70508214)

[6.1.2 Recommendations 55](#_Toc70508215)

[6.1.3 Deployment at BUT 56](#_Toc70508216)

[6.1.4 Installation 58](#_Toc70508217)

[6.1.5 Troubleshooting 61](#_Toc70508218)

[6.2 Using KYPO 62](#_Toc70508219)

[6.2.1 Example Scenario 63](#_Toc70508220)

[6.2.2 Creating New Scenarios 64](#_Toc70508221)

[6.3 Piloting Cyber training Exercise 65](#_Toc70508222)

[6.3.1 Laboratory Settings 65](#_Toc70508223)

[6.3.2 Training Scenario 66](#_Toc70508224)

[6.3.3 Pilot Evaluation 69](#_Toc70508225)

[Chapter 7 UBO – a framework to measure IT-Security Awareness within working staff 72](#_Toc70508226)

[7.1 Description 72](#_Toc70508227)

[7.1.1 Artifact-based Assessment of IT security Awareness 72](#_Toc70508228)

[7.1.2 itsape: IT-Security Awareness Penetration Testing Environment 74](#_Toc70508229)

[7.2 Installation Procedure 74](#_Toc70508230)

[7.2.1 Requirements 75](#_Toc70508231)

[7.2.2 Clients 75](#_Toc70508232)

[7.2.3 Server 75](#_Toc70508233)

[7.3 Use Case 76](#_Toc70508234)

[7.3.1 Preparation 76](#_Toc70508235)

[7.3.2 Pre-test 78](#_Toc70508236)

[79](#_Toc70508237)

[7.3.3 Intervention 80](#_Toc70508238)

[7.3.4 Post-test 80](#_Toc70508239)

[7.4 Test Pilot 80](#_Toc70508240)

[Chapter 8 Summary and Conclusion 82](#_Toc70508241)

[Chapter 9 List of Abbreviations 83](#_Toc70508242)

[Chapter 10 Bibliography 86](#_Toc70508243)

[Annex No. 1. Summary information about Cyber Ranges 89](#_Toc70508244)

[Annex No. 2. The installation of a virtual machine image 97](#_Toc70508245)

[Annex No. 3. The infrastructure of an attack model of a typical organization and its functions 101](#_Toc70508246)

[Annex No. 4. An attack model in an IT infrastructure of typical organization with attack scenarios and an attack map 103](#_Toc70508247)

[Annex No. 5. Storyline A1 – bruteforce attack 106](#_Toc70508248)

[Annex No. 6. Storyline A2 – sql injection attack 111](#_Toc70508249)

[Annex No. 7. Storyline A3 – exploiting WP vulnerability 116](#_Toc70508250)

[Annex No. 8. Storyline B1 – distant workplace attack 119](#_Toc70508251)

[Annex No. 9. Trainers Manual. Description of the Attacks 122](#_Toc70508252)

[Annex No. 10. OpenStack installation manual for KYPO 146](#_Toc70508253)

List of Figures

[Figure 2.1: Mapping of target groups to knowledge areas 15](#_Toc67913608)

[Figure 2.2: Learning pyramid 16](#_Toc67913609)

Figure 2.3: Covering of Knowledge Areas by Exercises, Training and Competitions 23

Figure 2.4: Cyber Range taxonomy [16] 27

[Figure 3.1: Federated infrastructure of Cyber training & exercise Framework 31](#_Toc67913610)

Figure 3.2: Acquisition of knowledge and practical skills using KTU Cyber training & exercise platform 33

[Figure 4.1: The typical topology of institution 35](#_Toc67913611)

[Figure 4.2: Infrastructure of KTU Pilot of Cyber training & exercise Framework 38](#_Toc67913612)

[Figure 4.3: Attacks vectors based on story line scenarios 42](#_Toc67913613)

[Figure 5.1: Creating a new Scenario 46](file:///D:\SPARTA\Kovas\D9.4%20KTU_final%2003.28.docx#_Toc67912941)

[Figure 5.2: Creating a Scenario with 3 VMs 46](file:///D:\SPARTA\Kovas\D9.4%20KTU_final%2003.28.docx#_Toc67912942)

[Figure 5.3: Adding a CVE to a Virtual Machine 47](#_Toc67912943)

[Figure 5.4: Nautilus Console 48](file:///D:\SPARTA\Kovas\D9.4%20KTU_final%2003.28.docx#_Toc67912944)

[Figure 5.5: Scenario Report 48](#_Toc67912945)

[Figure 5.6: CTF Architecture 49](#_Toc67912946)

[Figure 5.7: Services in PROD and DEV environment 50](#_Toc67912947)

[Figure 5.8: Automatic deploy pipeline 50](#_Toc67912948)

[Figure 6.1: KYPO CRP User Interface 52](#_Toc67912949)

[Figure 6.2: Network Infrastructure needed for KYPO 54](#_Toc67912950)

[Figure 6.3: BUT KYPO CRP Rack 57](#_Toc67912951)

[Figure 6.4: KYPO Portal 61](#_Toc67912952)

[Figure 6.5: BUT Laboratory with running KYPO 64](#_Toc67912953)

[Figure 6.6: First task 65](#_Toc67912954)

[Figure 6.7: Second task 66](#_Toc67912955)

[Figure 6.8: Third task 66](#_Toc67912956)

[Figure 6.9: Fourth task 67](#_Toc67912957)

[Figure 6.10: Scoring board 67](#_Toc67912958)

[Figure 6.11: Feedback 68](#_Toc67912959)

[Figure 6.12: Automation laboratory 69](#_Toc67912960)

[Figure 6.13: Critical Infrastructure Equipment Laboratory 69](#_Toc67912961)

[Figure 6.14: Critical Infrastructure Equipment Laboratory 70](#_Toc67912962)

Figure 7.1: Situation model of terminal work 72

Figure 7.2: Classes of possible artifacts 73

Figure 7.3: Combinations of user reaction classes 73

Figure 7.4: Preparation phase within the artifactomat 77

Figure 7.5: Test execution within the artifactomat 79

List of Tables

[Table 2.1: Brief description of CyBOK Knowledge Areas 12](#_Toc66868584)

[Table 2.2: Correspondence of ACM CSEC 2017 and CyBOK Knowledge Areas 14](#_Toc66868585)

[Table 2.3: Use of different cyber security exercises in different Knowledge Areas 22](#_Toc66868586)

Table 3.1: Information exchange between Cyber training & exercise Framework and the JCCI platform 33

Table 3.2: Covering of different Knowledge Areas by partners’ platforms 34

[Table 4.1: Methodology of choosing practical and organizational measures 39](#_Toc66868587)

[Table 4.2: Additional information to be provided by the relevant staff 43](#_Toc66868588)

Table 6.1: Minimal hardware requirements for 10 players 54

Table 6.2: Recommended hardware requirements for 10 players 54

Table 6.3: Recommended Operation Systems 56

Table 6.4: BUT Deployment Specification 57

Table 7.1: System requirements of the server 75

Table 7.2: System requirements of the clients 75

Table 7.3: Decomposition of the IT security awareness components 81

# Introduction

All of us are living in age of global communication, the Internet. This also means that the possibilities of violating the computer networks and our computers are increasing, while all devices connected to the Internet can be hacked. In our everyday life we can be attacked from various hackers, even from state attackers in other countries. The attackers become more organized and they are using more advanced and automated techniques and tools.

Computers and online repositories have a huge amount of information. Much of it is important to information owners and theft or disclosure information would do great harm to the owners of the information.

The purpose of these cyber attacks can be different:

* Cyber attack can cause major damage to business. It can affect your business' standing and consumer trust. The impact of a security breach can be financial, reputational and legal.
* Development projects and research results are other important sources of information that can be a target of cyber attacks. This is a kind of industrial espionage, which can boost own industry of attackers and generate competitive advantages.
* Cyber-attacks organized by states usually aim to steel information that is important for the security of the country.

Human errors often allow attacks to be carried out. Recent research shows that such errors are responsible for more than 80% of data breaches. Every organization faces the risk of a cyber-attack. One mistake by a single employee could compromise an entire network. So if you want to keep your organization secure, every employee should know what he is doing.

Information theft is the most expensive and fastest growing segment of cybercrime. Cybercriminals are becoming more sophisticated, changing methods of attack for computers, networks, and repositories. They exploit factors such as:

* World wide networking of servers and personal computers.
* The ability to attack targets anywhere in the country or in another country.
* The spread of the Internet of mobile devices and things.
* The spread of the social networking and e-commerce.

One study shows that 60% of small businesses go under within 6 months of a successful attack1. It takes on average more than 7 months to identify and recover from a successful cyber-attack, and the typical disruption to business operations cost approximately 1 million USD.

According to ENISA (The European Union Agency for Cybersecurity) Threat Landscape Report 2018 [1], the main trends in the 2018’s cyber threat landscape were:

* Mail and phishing messages have become the primary malware infection vector.
* Exploit Kits have lost their importance in the cyber threat landscape.
* Crypto miners have become an important monetization vector for cyber-criminals.
* State-sponsored agents increasingly target banks by using attack-vectors utilized in cyber-crime.
* Skill and capability building are the focus of defenders. Public organizations struggle with staff retention due to strong competition with industry in attracting cybersecurity talents.
* The technical orientation of most cyber threat intelligence produced is considered an obstacle towards awareness raising at the level of security and executive management.
* Cyber threat intelligence needs to respond to increasingly automated attacks through novel approaches to utilization of automated tools and skills.
* The emergence of IoT environments will remain a concern due to missing protection mechanisms in low-end IoT devices and services. The need for generic IoT protection architectures/good practices will remain pressing.
* The absence of cyber threat intelligence solutions for low-capability organizations/end-users needs to be addressed by vendors and governments.

Preventing such attacks requires an increase cyber security awareness in public, as well as the development of security skills for security professionals so that they are prepared to deal with threats and are aware of the latest threats. This requires training programs that use cyber security labs for training and exercises.

ENISA also recommends – much more training offerings need to be developed in order to satisfy the current market needs in cyber threat intelligence training.

Detection of these attacks and building effective protection against them is very important, so we need to increase our knowledge of cybersecurity. Corresponding education and practice are critical also for the security professionals who should improve their strategies, tactics, and technology for defense. It is important for the growing number of cybersecurity students in university programs too.

ENISA in ECSC 2019 Analysis Report [2] highlights estimates that more than 3.5 million cybersecurity professionals will be needed worldwide by 2021 in order to be able to prevent, react and protect their citizens against cyber threats.

# Structure of Cyber training & exercise Framework

## The target groups

In relation to cyber security, we distinguish four groups in our society:

1. Academics.
2. Professionals.
3. Employees.
4. Public.

**Academics**

To protect organization from cyber crimes in modern-day society, you need trained cyber security professionals. Such professionals can be educated and trained at universities and colleges. Cyber Security study programmes teach students how to protect computer operating systems, networks, and data from cyber attacks. Universities are striving to create degree programs from within their existing computer science, business and engineering departments. New cybersecurity courses are developed by academics in response to real world needs both in the public and private sectors. Cybersecurity courses of study offer classes in different areas of computer science, engineering, management and law [3].

**Professionals**

Another path is possible. Some computer and information technology professionals additionally gain knowledge from cyber security.

Professional training in cybersecurity should focus on real-world applications and be taught by professionals able to relate to current and concrete issues. These trainings usually include practical sessions (case studies for organizational topics and human sciences, hands-on courses for technical topics).

One of the best ways to supplement your existing skills and experience is to earn cyber security certifications. Some professional certifications can help you establish yourself in the field cyber security, but most certifications and credentials are designed to help you further in your career.

Certifications are specialized credentials that professionals earn in a focused area to demonstrate their expertise and exact skill set, and generally require passing an exam. These are generally offered by companies or professional associations and agencies.

Certificates are some types of condensed degree or diploma program that students earn in order to first enter the field. You could find certificate programs at most colleges or universities.

**Employees**

Today employees are typically your greatest source of vulnerability. Some experts argue that the number one threat to cyber security is still workers leaving laptops and mobile devices unattended in vulnerable places, such as public transport, cars and restaurants.

Organizations and companies cannot achieve their cyber security goals through hardware and information technology workers alone, so all employees who use computers and computer networks must be trained on the knowledge, skills and policies related to cyber security. One of the most important tools in the fight against cyber threats is educating employees at all levels of organization or company about identity theft, fraud, data breaches, and the risks of social engineering and common social engineering scams like phishing emails.

**Public**

Now people whose work is quite far from information technology use them at home when communicate by e-mail with friends or acquaintances, use online banking, e-shop services.

In our time of information and technology, when we spend a lot of time at computers or other smart devices, we need to have a good understanding not only of how to use them in a general sense, but also how to use them safely. One mistake, one careless click on the email attachment – and your personal information is already available for malicious use.

Cyber threats can affect the entire population, depending on the goals of the cyber criminals, which can include espionage, disruption, and misappropriation of data or money. Thus, the public must also acquire at least a minimum knowledge of secure using computers at home.

## Knowledge areas

Cyber Sciences refers to all disciplines that involve technology, people, and processes to enable assured operation in the presence of risks and adversaries. In particular, it includes all those activities concerning the creation, operation, analysis, and testing of secure computer systems as well as reasonable risk taking, and risk mitigation [3, 4, 5].

According to Cybersecurity Curricula 2017 Curriculum Guidelines, **knowledge area** represents critical knowledge with broad importance within and across multiple computing-based disciplines. Collectively, knowledge areas represent the full body of knowledge within the field of cybersecurity.

1. **Data Security** focuses on the protection of data at rest, during processing, and in transit. The essential concepts covered by this KA and its learning goals are: Basic cryptography concepts, Digital forensics, End-to-end secure communications, Data integrity and authentication, Information storage security.
2. **Software Security** focuses on the development and use of software that reliably preserves the security properties of the information systems. The essential concepts covered by this KA and its learning goals are: Fundamental design principles including least privilege, open design, and abstraction, Security requirements and their role in design, Implementation issues, Static and dynamic testing, Configuring and patching, Ethics, especially in development, testing and vulnerability.
3. **Component Security** focuses on the design, procurement, testing, analysis and maintenance of components integrated into larger systems. The essential concepts covered by this KA and its learning goals are: Vulnerabilities of system components, Component lifecycle, Secure component design principles, Supply chain management security, Security testing, Reverse engineering.
4. **Connection Security** focuses on the security of the connections between components including both physical and logical connections. The essential concepts covered by this KA and its learning goals are: Systems, architecture, models, and standards, Physical component interfaces, Software component interfaces, Connection attacks, Transmission attacks.
5. **System Security** focuses on the security aspects of systems that are composed of components and connections and use software. The essential concepts covered by this KA and its learning goals are: Holistic approach, Security policy, Authentication system, Access control, Monitoring, Recovery, Testing, Documentation.
6. **Human Security** focuses on protecting individuals’ data and privacy in the context of organizations (i.e., as employees) and personal life. In addition, it also addresses human behaviour as it relates to cybersecurity. The essential concepts covered by this KA and its learning goals are: Identity management, Social engineering, Awareness and understanding, Social behavioral privacy and security, Personal data privacy and security.
7. **Organizational Security** focuses on protecting organizations from cybersecurity threats and managing risks. The essential concepts covered by this KA and its learning goals are: Risk management, Governance and policy, Laws, ethics, and compliance, Strategy and planning.
8. **Societal Security** focuses on those aspects of cybersecurity that broadly impact society as a whole for better or for worse. The essential concepts covered by this KA and its learning goals are: Cybercrime, Cyber law, Cyber ethics, Cyber policy, Privacy.

CyBOK defines 19 Knowledge Areas [5, 6], a brief description of which is given in Table 2.1.

Table 2.1: Brief description of CyBOK Knowledge Areas

|  |  |
| --- | --- |
| ***Knowledge Area*** | ***Description*** |
| **Human, Organisational, and Regulatory Aspects** | |
| Risk Management & Governance | Security management systems and organisational security controls, including standards, best practices, and approaches to risk assessment and mitigation. |
| Law & Regulation | International and national statutory and regulatory requirements, compliance obligations, and security ethics, including data protection and developing doctrines on cyber warfare. |
| Human Factors | Usable security, social & behavioural factors impacting security, security culture and awareness as well as the impact of security controls on user behaviours. |
| Privacy & Online Rights | Techniques for protecting personal information, including communications, applications, and inferences from databases and data processing. It also includes other systems supporting online rights touching on censorship and circumvention, covertness, electronic elections, and privacy in payment and identity systems. |
| **Attacks and Defences** | |
| Malware & Attack Technologies | Technical details of exploits and distributed malicious systems, together with associated discovery and analysis approaches. |
| Adversarial Behaviours | The motivations, behaviours, & methods used by attackers, including malware supply chains, attack vectors, and money transfers. |
| Security Operations & Incident Management | The configuration, operation and maintenance of secure systems including the detection of and response to security incidents and the collection and use of threat intelligence. |
| Forensics | The collection, analysis, & reporting of digital evidence in support of incidents or criminal events. |
| **Systems Security** | |
| Cryptography | Core primitives of cryptography as presently practised & emerging algorithms, techniques for analysis of these, and the protocols that use them. |
| Operating Systems & Virtualisation Security | Operating systems protection mechanisms, implementing secure abstraction of hardware, and sharing of resources, including isolation in multiuser systems, secure virtualisation, and security in database systems. |
| Distributed Systems Security | Security mechanisms relating to larger-scale coordinated distributed systems, including aspects of secure consensus, time, event systems, peer-to-peer systems, clouds, multitenant data centres, & distributed ledgers. |
| Authentication, Authorisation, & Accountability | All aspects of identity management and authentication technologies, and architectures and tools to support authorisation and accountability in both isolated and distributed systems. |
| **Software and Platform Security** | |
| Software Security | Known categories of programming errors resulting in security bugs, & techniques for avoiding these errors—both through coding practice and improved language design—and tools, techniques, and methods for detection of such errors in existing systems. |
| Web & Mobile Security | Issues related to web applications and services distributed across devices and frameworks, including the diverse programming paradigms and protection models. |
| Secure Software Lifecycle | The application of security software engineering techniques in the whole systems development lifecycle resulting in software that is secure by default. |
| **Infrastructure Security** | |
| Network Security | Security aspects of networking & telecommunication protocols, including the security of routing, network security elements, and specific cryptographic protocols used for network security. |
| Hardware Security | Security in the design, implementation, & deployment of general-purpose and specialist hardware, including trusted computing technologies and sources of randomness. |
| Cyber-Physical Systems Security | Security challenges in cyber-physical systems, such as the Internet of Things & industrial control systems, attacker models, safe-secure designs, and security of large-scale infrastructures. |
| Physical Layer & Telecommunications Security | Security concerns and limitations of the physical layer including aspects of radio frequency encodings and transmission techniques, unintended radiation, and interference. |

Analysis of ACM CSEC 2017 and CyBOK Knowledge Areas allows such a correspondence to be observed (see Table 2.2).

Table 2.2: Correspondence of ACM CSEC 2017 and CyBOK Knowledge Areas

|  |  |
| --- | --- |
| ***ACM CSEC 2017 Knowledge Areas*** | ***CyBOK Knowledge Areas*** |
| Data Security | 8. Forensics  9. Cryptography  12. Authentication, Authorisation, & Accountability |
| Software Security | 13. Software Security  14. Web & Mobile Security  15. Secure Software Lifecycle |
| Component Security | 17. Hardware Security  18. Cyber-Physical Systems Security |
| Connection Security | 16. Network Security  19. Physical Layer & Telecommunications Security |
| System Security | 10. Operating Systems & Virtualisation Security  11. Distributed Systems Security  12. Authentication, Authorisation, & Accountability |
| Human Security | 3. Human Factors  4. Privacy & Online Rights |
| Organizational Security | 1. Risk Management & Governance  2. Law & Regulation |
| Societal Security | 2. Law & Regulation  4. Privacy & Online Rights  5. Malware & Attack  6. Adversarial Behaviours |

In this report, as in the SPARTA report *D9.2. Curriculum descriptions* [3], we will use the ACM CSEC 2017 [4] knowledge areas.

## Mapping of target groups to knowledge areas

The relationship of target groups to knowledge areas is depicted on this picture (Figure 2.1):

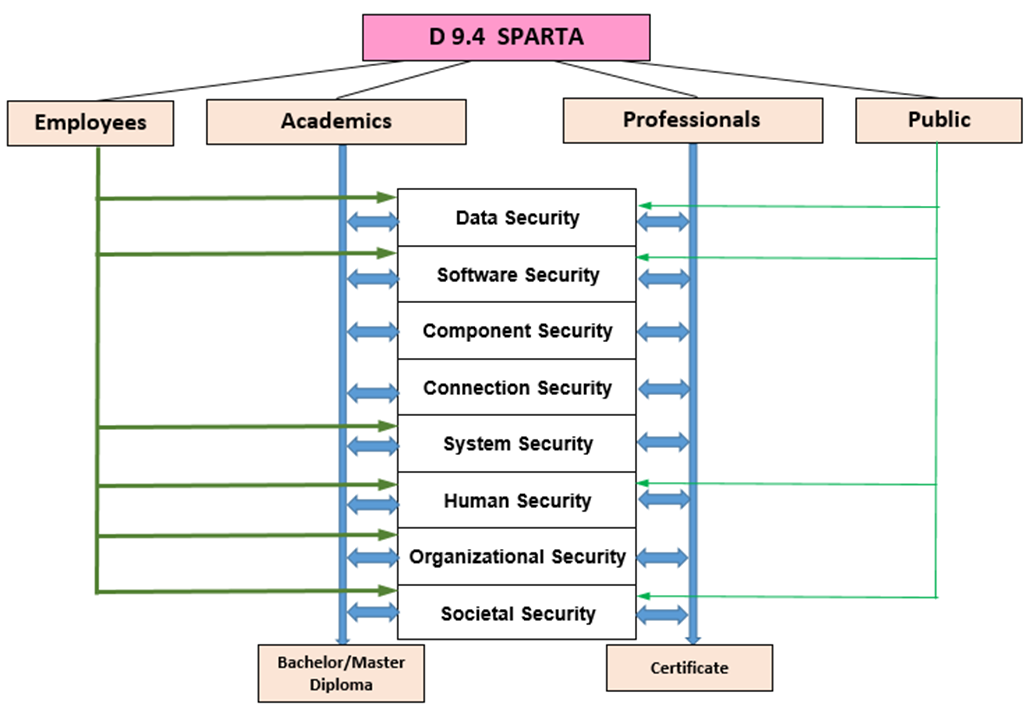


Figure 2.1: Mapping of target groups to knowledge areas

University bachelor and master students have relationships to all knowledge areas, but not every bachelor and master level study program has relationships (at least at same level) to all knowledge areas – it depends on study program curricula. For instance, some topics in study program are voluntary, so students have opportunity choose for themselves some topics of cyber security. An exhaustive analysis of university bachelor and master study programs is presented in [3].

Professionals earn certifications in a special area of cyber security. Usually, they take short courses and pass the appropriate exam.

Employees are not right cyber security professionals, but they should have general understanding about cyber security problems, which can arise in their everyday work in organization or company. Their area of interest usually includes basics of data security, software security, system security. Some aspects of human security (social engineering, social behavioral privacy and security, personal data privacy and security), organizational security (laws, ethics), societal security (cyber threats, privacy) also is important for them.

Public should have a good understanding how to use computers and information technologies safely. They should have general understanding about data security, software security, human security (social engineering, social behavioral privacy and security, personal data privacy and security), societal security (cyber threats, privacy).

## Training & exercise activities

Exercises as training tools have been well known to military and security personnel for many centuries. Conducting exercises can help with validating policies, plans and procedures, as well as with training, improving current tools or rolling out new equipment, testing information and communications technology (ICT) and identifying gaps in resources [7].

Training is essential to preparing the cybersecurity workforce of tomorrow, and for keeping current cybersecurity workers up to date on skills and evolving threats.

Training and exercises are important for deeper mastering of teaching materials. This is confirmed by the learning pyramid [8]. This piramide (Figure 2.2) shows the importance of practical activities in acquiring new knowledge or raising qualifications.

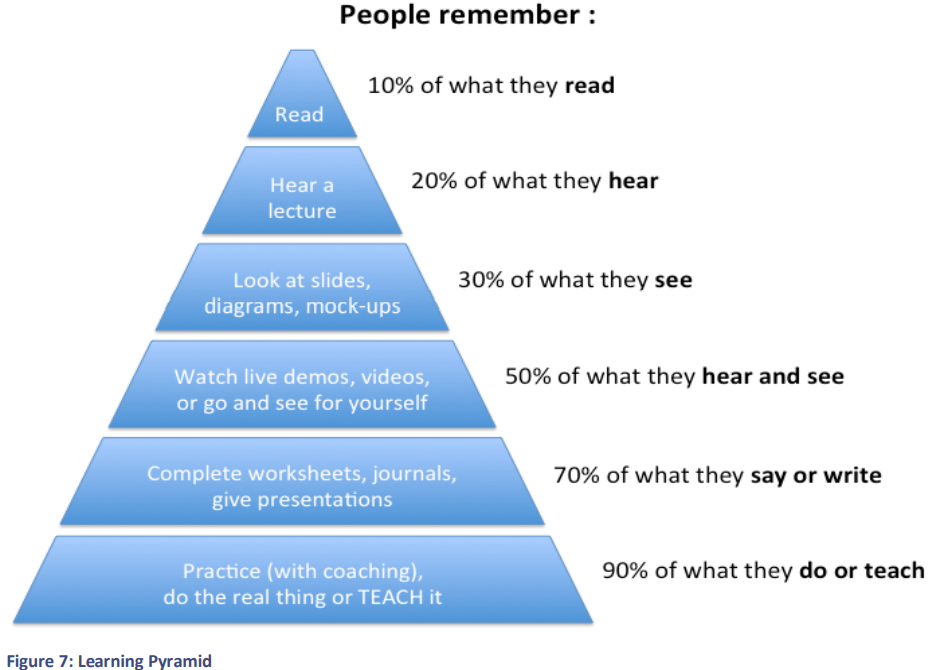


Figure 2.2: Learning pyramid

Analysis of current curriculum shows that though the practical education including hands-on experience plays an important role in the design of curricula, though only 30%-40% of existing courses have some form of practical education [3].

The cyber security exercises (CSE) are a critical component in the process of transferring theoretical knowledge to practical skills useful in the workforce. They demonstrate the important of the students’ practical understanding of security issues.

The cyber security exercises (or cyber defense exercises – CDX) can be used also as testbed platforms to test and assess IT and OT systems [9] while they have been playing a very important role in testing the technical cyber capacity of nations or organizations, cyber training, and cyber awareness raising.

CDX can increase the ability to test and develop common and coordinated technical and strategic mobility against the cyberattacks that may occur both on a national and an international basis, strengthening cooperation and coordination between public and private sectors in the cyberspace, gathering empirical data related to cybersecurity research.

The international standard ISO-22398 and experts have singled out the following types of exercises [10]:

* + Capture the flag
  + Discussion based game
  + Drill
  + Red team / blue team
  + Seminar
  + Simulation
  + Table-top
  + Workshop

**Capture the flag** **exercises**

According to Merriam-Webster Dictionary, capture the flag is “a game in which players on each of two teams seek to capture the other team's flag and return it to their side without being captured and imprisoned”.

Capture The Flag (CTF) is a kind of information security competition that challenges contestants to solve a variety of tasks of cyber security. These events consist of a number of challenges, which vary according to their difficulty and for which the participants need to use different skills. After solving an individual challenge, a “flag” is given to the player; he presents this “flag” to the CTF server to earn points. Players can attempt the various challenges individual by themselves, or they can work with others in a team to attempt to score the highest number of points.

CTF events are usually timed, and the points are totaled once the time has expired. The winning player / team will be the one that solved the most challenges and thus secured the highest score.

CTF is a form of wargaming where participants are divided into two teams, with one team playing the part of the aggressor or hacker and other team defending. In the game, teams are awarded points based on how deeply one penetrates the defended network or how quickly the other responds to an incident or attack and eliminates its consequences.

Like many competitions, the skill level for CTFs varies between the events. Some are targeted towards the high school and college students, other events target professionals with experience operating on cyber security teams.

There are different types of CTF:

* Jeopardy style CTFs provide a list of challenges and award points to individuals or teams that complete the challenges. The challenges can be in several categories: web exploits, binary exploitation, reverse engineering, forensics, and cryptography.
* Attack/Defense style CTFs focus on either attacking an opponent's servers or defending one's own. These CTFs are typically aimed at those with more experience and are conducted at a specific physical location.

**Discussion based games**

Game based learning allows students have fun whilst learning by actively learning and practicing. Studies show that the brain is 68% more involved when having fun. Often, the game is started on a slow pace gradually advancing gain in skill until the student is able to successfully navigate the difficult levels. Game-based learning provides many of these opportunities; one of them is that you can gradually improve your skills by immersing people in real life situations and rewarding them with their results.

It is important to develop a learning platform for the next generation of cyber security professionals to learn and be further equipped by introducing cybersecurity with the concept of gaming. Some of the games developed offer some challenges and a higher level of thinking. Learning through this system introduces an immersive, learner-centered experience with effectiveness on cybersecurity awareness training and practical skill acquisition for learners from diverse backgrounds.

**Drills**

A drill is a coordinated, supervised activity usually employed to test a single, specific operation or function within a single entity (e.g., a fire department conducts a decontamination drill). This term is used to describe systematic training in particular techniques or tools through multiple repetition.

The cyber drills are based on fictitious scenarios to assess the capabilities of cyber incident management. The exercise is based on scenarios covering several incidents related to the most common types of attacks. Scripts are submitted simultaneously to all participating teams. All resources must be available to all teams. The drill facilitator explains and instructs the teams to analyze the scenarios. The teams present the solution to the organizing group as an advisory report.

**Red team / blue team exercises**

Red team/blue team exercise is a cybersecurity assessment technique that uses simulated attacks to gauge the strength of the organization’s existing security capabilities and identify areas of improvement in a low-risk environment. This exercise, modeled on military exercises, is a clash of two teams of high-level cyber security professionals.

Red team is the entity brought in to test the effectiveness of a security program. They should emulate the behaviors and techniques of likely attackers to make it as realistic as possible. The blue team is the internal security team that is charged with stopping these simulated attacks.

The ultimate goal of such a test is to test an organization’s security maturity as well as its ability to detect and respond to an attack. Such an exercise can take up to three or four weeks, depending on the simulation, the people involved, and the attacks being tested.

**Seminars**

A seminar is a form of academic training in an academic institution or offered by a commercial or professional organization. Its function is to bring together small groups for recurring meetings, focusing each time on a specific subject in which everyone present is asked to actively participate. A seminar is an informal discussion in which participants discuss new or updated plans, policies, or procedures.

**Simulation based exercises**

A simulation-based exercise is a practice activity that places participants in a simulated situation requiring them to function in the capacity expected of them in a real event. Its purpose is to promote readiness by testing policies and plans, standard operating procedures, and personnel training.

Main benefits of simulation-based exercises are that they allow people to practice their roles, gain experience in their roles without an actual disaster.

**Table-top exercises**

This is paper-driven exercise with scripts prepared by exercise planners and delivered via paper. Table-top exercises are discussions in which team members get together and talk about their roles during an emergency situation and how they might react in various scenarios. This type of exercise can be planned and executed quickly, depending on the number of organizations involved.

Table-top exercises received their name because, in most cases, the planners and players of the exercise sit down at one table and execute the exercise. A table-top exercise should have a small training audience and very well-defined objectives. This type of environment opens communications between different players and aids in establishing the business processes associated with planning, executing, and training during an exercise. The injects are hypothetical, entirely pre-coordinated, and written down.

**Workshops**

The workshops at universities offer high school students an opportunity to explore computer and network security concepts and skills through on and offline hands-on activities. The purpose of the cybersecurity workshop on the national level is to share best practices on running national cyber drills and elaborating national cybersecurity strategies.

A workshop is like a seminar, but it is used to develop specific products, such as a draft plan (for example, a Training and Exercise Plan) or policy.

## Cybersecurity Competitions

Today’s university and college teachers are seeking to use new technologies and hands-on activities to help students master complex STEM (science, technology, engineering and math) and cybersecurity concepts. Students should be engaged to learn and practice in cybersecurity not only in the classroom but also outside of the classroom. One way is to form a team and bring students together to solve real-world cybersecurity challenges in cybersecurity competition.

Cybersecurity competitions are interactive events or exercises, where individuals or teams engage in cybersecurity activities including methods, practices, strategy, policy and ethics.

Using a cybersecurity competition provides an opportunity for students to test their skills and develop team-based management skills in an operational business environment. Cybersecurity challenges are also a fun and attractive way for learners.

Challenges are a great way to develop and practice a range of important skills including:

* cyber security and network defence,
* teamwork and professional communication,
* creative and critical thinking,
* risk management techniques,
* adaptability and change management.

The goal is to promote cybersecurity competitions as a focal point for [14]:

* awareness of the need for cybersecurity and threat intelligence;
* benchmarking for young people, in schools or universities;
* the early discovery of young people with a talent for IT security;
* understanding of the range and diversity of jobs in cyber security;
* the development of structures to sustain IT security excellence in the education sector;
* the attraction of IT and IT security for young people;
* national and European networks of excellence and establishing professional IT security excellence in Europe.

There are multiple cybersecurity competitions at the local and national levels. They each have the goal of encouraging professional development and cybersecurity education outside of the traditional classroom. Most of them start at the middle school level and continue up through the ranks of cybersecurity professionals.

**Capture the Flag** **competitions** are some of the most popular forms of cybersecurity competitions. This is because of the spectator-friendly of capture the flag events, in which score boards often highlight the number of points held by all of the competing teams.

The most popular formats for CTF competitions are:

* + ***Jeopardy[[1]](#footnote-1)***: this is a simple and common model of different difficulty in such domains as networking, cryptography, reverse engineering, web exploitation, forensic analysis, steganography, hardware, hacking, programming, mobile-centered challenges, etc. Each task is evaluated by a certain number of points depending on task complexity and difficulty. The goal is to get the highest number of points.
  + ***Attack and defense***: here each team will have to defend an infrastructure (a range of virtual machines which are hosted on an isolated network) with vulnerabilities while trying to penetrate the infrastructure of the rest of the competitors.

In **Cyber Defense** **competitions**, student teams are asked to take on administrative and security responsibilities for an existing “commercial” network – typically a small company with more than 50 users, up to 12 servers, and shared Internet services such as a web server, mail server, and e-shopping site. In competition will be assessed team's ability to detect and respond to external threats, maintain the availability of existing services, respond to business requests, for example, by creating a new e-commerce site that combines best security practices with business needs, service availability, network protection against attacks.

In **Network security competition** competitors seek to control shared resources and the most important services for those resources. When a competitor takes over a resource, he must protect it from attacks by other competitors and maintain the most important services provided to the resource. Competitors earn points for managing important services such as SMTP, DNS, HTTP, HTTPS, SSH, and so on.

**Cyber Quests** are exciting but challenging online competitions where participants have to demonstrate their knowledge in various areas of information security. Each quest provides an artifact for analysis and series of quiz questions. Some tasks focus on a potentially vulnerable web server, other quests include forensics, package capture analysis, and more.

In **Digital Forensics competition** for participants simulated scenario are provided, which involve the infiltration and attack of the system of some company, which led to the theft of personal and financial data. Participants should gather digital evidence, analyse data from digital devices, and reconstruct the facts of the case.

In **Research Paper competitions** research papers and publications submitted by participants on various cyber security issues are evaluated.

**Cybersecurity Policy competition** challenge students to propose public policy solutions to real-world computer security challenges. Students are invited to think critically about major cybersecurity policy issues affecting society.

Some examples of cybersecurity competitions:

* Global CyberLympics[[2]](#footnote-2) is an online cyber security competition, which pits teams from all over the world to compete in a series of challenges in the areas of digital forensics, web application exploitation, system exploitation, malware analysis, reverse engineering, cryptography. At first teams compete against players from all over the world in a 12-hour online elimination round. The two teams with the highest score from each continent will then be invited to compete at the Global CyberLympics World Finals event.
* The European Cyber Security Challenge[[3]](#footnote-3) (ECSC) is an initiative by the ENISA and aims at enhancing cybersecurity talent across Europe. The competition is promoted by the European Commission. European countries host their national cybersecurity competitions, ant the winners of the national contests represent their countries in the ECSC. Contestants have to solve security related tasks from domains such as web security, mobile security, crypto puzzles, reverse engineering and forensics.
* The National Cyber League[[4]](#footnote-4) (NCL) arranges NCL Games for individual students and teams, where students can prepare and validate their skills with practical challenges they will likely face in real-world cybersecurity roles. There are challenges in each category at three difficulty levels (easy, medium and hard) so players with different levels of cybersecurity expertise can measure their progress. Players can also receive feedback from the games that highlight their personal strengths within industry-relevant challenges. This feedback is a great resource for those entering the industry and is part of what helps competition participants stand out when seeking IT and cybersecurity jobs.
* CyberPatriot's National Youth Cyber Defense Competition[[5]](#footnote-5) is the world's largest cybersecurity competition, where teams of high school and middle school students challenge to find and fix cybersecurity vulnerabilities in virtual operating systems. Competitions take place on specified weekends throughout the school year.
* Every year, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Estonia invites over 1,000 cyber experts from 30 countries to participate in Locked Shields[[6]](#footnote-6). Locked Shields is an incredibly valuable and useful exercise, while it gives cyber defenders the opportunity to learn, practice and improve important skills such as teamwork and flexibility, gain experience confronting realistic cyber incidents that mirror attacks that have already taken place, demonstrates the importance of collaboration between NATO Allies and reaffirms that the transnational nature of technology makes cybersecurity a collective task.

## Mapping of training & exercise activities to knowledge areas

Different training & exercise activities can be used to deeper mastering of teaching materials in cyber security. Following table (see Table 2.3) shows passible use of different cyber security exercises.

Table 2.3: Use of different cyber security exercises in different Knowledge Areas

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Exercises***  ***Knowledge Areas*** | ***Capture the flag*** | ***Discussion based game*** | ***Drill*** | ***Red team / blue team*** | ***Simulation*** | ***Table-top*** | ***Seminar*** | ***Workshop*** |
| Data Security | x |  | x | x |  | x | x | x |
| Software Security |  |  | x |  |  | x | x | x |
| Component Security |  |  |  |  |  | x | x | x |
| Connection Security | x | x | x | x | x |  | x | x |
| System Security |  | x | x | x | x | x | x | x |
| Human Security | x |  |  |  |  | x | x | x |
| Organizational Security |  |  |  |  |  | x | x | x |
| Societal Security | x |  |  |  |  | x | x | x |

The competitions helps to deepen various cybersecurity aspects, invigorating the training process and making it more attractive. This is shown in Figure 2-3.

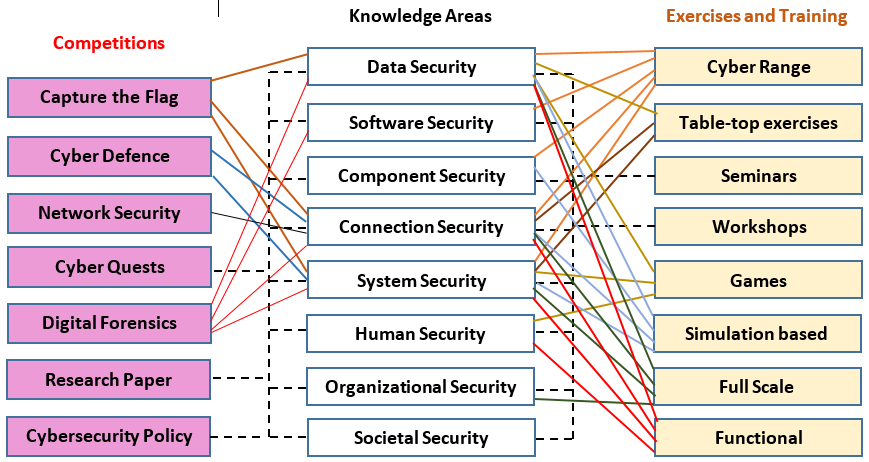


Figure 2.3: Covering of Knowledge Areas by Exercises, Training and Competitions

## Cybersecurity Platforms and Training Environments

What is the actual definition of term ***Cybersecurity platform***? In general, vendors use the word “platform” to describe an integrated consolidation of products that creates a common and interoperable architecture.

What general requirements must be met by cybersecurity platform? Here is a short list of such requirements [11]:

1. **Coverage from endpoints to data centers to clouds.** Platforms must provide coverage of components that includes endpoints (i.e. PCs, mobile devices, etc.) and networks, as well as physical servers, virtual servers, VMs, containers, etc. The best platforms should also offer strong integration with common threat vectors such as email security and web security.
2. **Prevention and detection capabilities.** Each individual tool should provide the best level of security, and the platform should ensure that the use of more tools increases the protection against threats accordingly. In addition to threat prevention, each tool should also act as a sensor when collecting security telemetry. Platforms should be complemented by some type of security analysis tools that process and analyze an increasing amount of security data.
3. **Hybrid deployment options.** Individual security tools and the platform management plane should be offered in on-premises and/or cloud-based form factors. Customers can then choose how they want to shape the entire system without losing the benefits of functionality or technology integration.
4. **Cloud-based services.** Security technology platforms should include cloud-based services for things like threat intelligence analysis/sharing, static/dynamic file analysis, reputation list compilation/distribution, machine learning modeling, etc.
5. **Central management and reporting.** All individual tools must also be managed centrally, providing role-based access, tailored to different users and functions. Management functionality must include policy management, configuration management, and detailed reporting from individual tools, from groups of tools, or across the entire architecture.
6. **Openness**. While security technology vendors want customers to buy their whole set of components, customers may wish to purchase and install tools gradually, depending on their budget capabilities. Given this reality, security technology platforms must be open for easy third-party technology integration by offering developer support, technology partnerships, and well-documented and standards-based APIs.
7. **Choices**. Finally, major security platform vendors offer their technology along with a range of services. Customers should be able to choose which parts of the platforms they purchase, which parts they outsource, and where and how much they need to improve staff skills.

The biggest challenge facing businesses and various organizations today is to protect themselves from modern, complex security challenges. As the digital transformation drives innovation, threats come with it, and your team needs to be prepared not only for the threats we face now, but also for the future threats.

The cyber security training environment is a cyber security training tool that allows you to practice and improve your cyber security skills, develop and learn new knowledge, and test older and emerging cyber threat concepts in the field of information security.

Cybersecurity training develops cognition needs, integration, communication and co-operation of team members.

Several types of cyber security training environments are currently known – cybersecurity labs (physical and virtual), cybersecurity platforms, and cyber ranges.

**Cybersecurity labs**

Cybersecurity lab usually is equipped with reconfigurable furniture to facilitate student collaboration, can also provide a dedicated place for student exercises in computer forensics and other hands-on activities.

The lab also hosts its own servers configured to provide a self-service private cloud for students. This private cloud allows students to fully experience cloud computing and create test/practice labs of their own choosing. Students also can have access to scalable compute resources and ready-to-use virtual machines to carry out a variety of tasks.

**Cybersecurity Virtual labs**

Virtual cybersecurity labs are a great way to give students and other learners access to the latest cyber security product demonstrations and training. The advantages of these laboratories are:

* Virtual lab is available from anywhere, enable encounter real-world scenarios and work through them, it is cheaper and ensure high quality training.
* A virtual lab removes the need for travel costs or high-end hardware on the client side since training is conducted primarily through an Internet browser on the learners terminal. The simulation is centralized and accessible from anywhere at any time with nothing but an Internet connection.
* Upgrading a lab to keep up with ever-changing technology and security trends is inexpensive and can be done quickly.
* Feedback between instructors and learners is instant and convenient. Instructors can offer help at any point, monitor user participation, and perform other relevant analysis.

Virtual labs are more than just basic cybersecurity training. They can also be designed to provide the latest certifications from world known companies like Cisco or Microsoft.

**Cybersecurity training** **platforms**

Most organizations are realizing only 25% or less of the capabilities of the cybersecurity tools they have already have in organization. Cybersecurity training platform will enable organizations to gain more knowledge about the use of cyber security tools, rationalize their cybersecurity tools thus increasing the effectiveness of existing cyber security system.

Cybersecurity training platform will make it easier to teach cybersecurity professionals how to maximize investments in cybersecurity tools using simulations based on real-life attacks that the company has incorporated into the curriculum.

This kind of cybersecurity training environment is often found speaking about security awareness training.

Security awareness training platforms provide online portals for end-users to access training materials on cyber security. They allow administrators to create training using interactive tests to encourage users to learn intensively and use training materials [12]. Many security awareness training platforms also provide the ability to simulate phishing to test how users are able to detect phishing attacks.

Security awareness training platforms provide online portals for end users to access training materials about cybersecurity issues. They allow admins to create training campaigns, with interactive quizzes and tests to ensure that users are learning and engaging with materials.

Other wide known type of security training platforms is cyber range.

**Cyber Ranges**

European Cyber Security Organisation (ECSO) defines cyber range as “*a platform for the development, delivery and use of interactive simulation environments. A simulation environment is a representation of an organisation’s ICT, OT, mobile and physical systems, applications and infrastructures, including the simulation of attacks, users and their activities and of any other Internet, public or third-party services which the simulated environment may depend upon. A cyber range includes a combination of core technologies for the realisation and use of the simulation environment and of additional components which are, in turn, desirable or required for achieving specific cyber range use cases”* [17].

The involvement of cyberranges for practical trainings played a significant role during the design of good-practice curricula. The virtualization technologies and gamified training methods, involving CTF, Red Blue teaming or table-top exercises should be considered a significant enhancement of existing training methods and could provide a hands-on experience [3].

## Cyber Range as training&exercise platform

From ordinary computer users to cyber experts and executives preparing to respond to cyber incidents, we can all improve our cyber defense skills at a special training facilities. One kind or such facility is cyber range.

Cyber ranges were initially developed by government agencies for training their cyber operators on skills and techniques.  Cyber range providers built representations of actual networks, systems, and tools that helped cyber professionals safely train in virtual, secure environments insted of using the agency’s operational network infrastructure which can might be compromised during such training.

Today, cyber ranges are used in the cyber security sector to effectively train IT professionals in all industries and help improve defenses against cyber–attacks. As technology advanced, cyber range training advanced as well, both in scope and potential.

A **cyber range** is a virtual environment that companies can use for cyber warfare training and software development2. Cyber ranges are interactive representations of an organization’s local network, system, tools, and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing.

A cyber range may include actual hardware and software or may be a combination of actual and virtual components. The Internet level piece of the range environment includes not only simulated traffic, but also replicates network services such as webpages, browsers, and email as needed by the customer.

A Cyber Range is a training center for cyber defense that allows organizations to increase the skills of their teams in the defense of their network infrastructures.

These environments allow companies to train employees and customers on the latest threats, practice handling specific real-world scenarios.

Cyber ranges are being actively used by the military and government agencies, private corporations, universities, which focus on cybersecurity:

* Professionals from information technology, cybersecurity, and others use cyber ranges to improve individual and team knowledge and capabilities.
* Students can use cyber ranges to apply knowledge in networking, develop cyber skills.
* Educators can use cyber ranges as a classroom.
* Organizations can use cyber ranges to evaluate their capability to defend cyber threats, train personnel on cyber defense and solving complex cyber problems.

Key features of a Cyber Range are [3]:

* Assess the effectiveness of the organization's exercise through exhaustive incident reporting and analysis guidelines for remedying deficiencies.
* Assess the organization's capability to determine operational impacts of cyberattacks and implement proper recovery procedures during the exercise.
* Understand the implications of losing trust in IT systems and create workarounds for such losses.
* Assess the ability of the technical team to detect and adequately react to hostile activity during the exercise.
* Expose and correct weaknesses in cybersecurity systems.
* Expose and correct weaknesses in cyber operations policies and procedures.
* Enhance cyber awareness, readiness, and coordination.
* Determine the effectiveness of the cyber education provided to the training audience before the start of the exercise.

### Taxonomy of Cyber Ranges

Exhaustive study of Cyber Ranges is presented in paper [10]. Authors proposed an initial taxonomy to classify cyber ranges (see Figure 2-4).

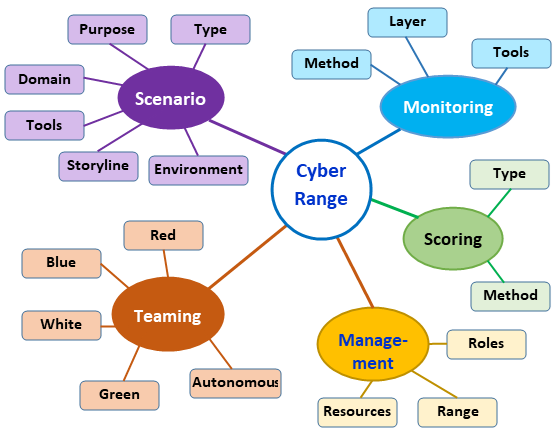


Figure 2.4: Cyber Range taxonomy [16]

1. A **scenario** defines following elements:

* the ***purpose*** explains what are the objectives of the scenario (the execution of a cyber security training exercise or the experimentation validation of new cyber security tools and techniques);
* the ***type*** of the scenario indicates whether the scenario is static (such scenario includes a static environment, and no changes are applied during the execution of the exercise) or dynamic (besides the static environment, scenario includes a dynamic component that will make changes during the execution of the scenario);
* the execution ***environment*** – the topology where the scenario is executed; in an operation-based exercise the environment will be a technical infrastructure (i.e., computer based, physical, virtualized or hybrid), if the exercise is a table-top or discussion based – the environment can be non computer based;
* the ***storyline*** indicates how the exercise will be executed; this allows the overall understating and controlling of a scenario, and gives the ability to evaluate the exercise, or test, outcome;
* the domain indicates the application domain of the scenario (e.g., Internet of Things, network, cloud etc.);
* the ***tools*** indicates the tools which are needed for the creation of the environment of the scenario, or the tools which are used in the development of a storyline.

1. **Monitoring** includes the methods, the tools and the layers at which real time monitoring of cyber security exercises and tests are performed:

* the ***methods*** employed for monitoring the cyber security exercise, or the test, is employed to monitor the cyber security exercise and tests, can be classified as automatically (with the use of tools that gather data for analysis), or manually (by human observers);
* the ***tools*** classifies the software and hardware tools that can be used for monitoring of cyber security exercises and tests; they may include security information and event management solutions and intrusion detection systems etc.;
* the ***layers*** classifies the layer at which monitoring is being performed; depending on the type of an exercise, monitoring can be performed at multiple TCP/IP layers (in case of an operation-based exercise) or at an abstract social layer (in case of a table-top exercise).

1. **Teaming** includes an individual and a group of individuals that design, develop, manage and participate in a cyber security exercise or a test. Depending on a team’s role in a cyber security exercise different colors are assigned to them:

* the ***red team*** is responsible to identify and exploit potential vulnerabilities that are present in the exercise environment;
* the ***blue team*** is responsible to identify and patch potential vulnerabilities that can be exploited by a red team;
* the ***white team*** designs the exercise and experiment scenario, objectives, rules and evaluation criteria;
* the ***green team*** is responsible for the development, monitoring and maintenance of the exercise infrastructure designed by the white team;
* the ***autonomous teams*** are teams which roles are being automated by different tools and techniques;

In some cyber security exercises, additional teams are included, which are exercise/specific:

* the ***orange team*** members assign different technical tasks to blue team members during the exercise;
* the ***purple teams*** perform the communication and information sharing between multiple exercises teams to increase the exercise effectiveness;
* the ***yellow team*** members simulate the behavior of normal users that are using the infrastructure created by the green team.

1. **Scoring** uses data from monitoring systems in order to give performance related semantics to the low level technical events observed during monitoring of cyber security exercises and tests. The scoring mechanism is also used to measure the teams and test progress during an exercise, or a test. The methods and tools used in the scoring mechanism are:

* the ***methods*** shows whether the scoring is done based upon achieving a specific objective, or it is done by analyzing logs that are generated during cyber security exercises or test;
* the ***tools*** classifies the software and hardware tools that are used for scoring of cyber security exercises or tests.

1. **Management i**nvolves the assignment of roles and duties to individuals and teams, allocation of computational and other resources required for conducting a cyber security exercise, or a test, and the overall management:

* ***Role management*** classifies the methods, tools and techniques with which the identities and roles of individuals and teams involved in a cyber security exercise, or a test, are managed;
* ***Range management*** classifies the methods, tools and techniques with which the holistic view of overall cyber security exercise, or a test, is presented in portals and dashboards;
* ***Resource management*** classifies the computational resources like processing frequency, memory and disk space required for conducting cyber security exercise, or a test.

### Benefits of a Cyber Range

Cyber ranges offer many advantages that can help your organization prepare itself to deal with potential cyber threats. These advantages include:

* Cyber ranges allow employees and customers to experience real-world threats in a virtual environment. You can test advanced cyberspace tactics, techniques, and procedures that require isolated environments of complex networked systems.
* You can perform testing that cannot occur on open operational networks due to potential catastrophic consequences, for example execution of extremely malicious threats on realistic representations of systems and networks.
* You can control these experiments, determine the parameters an individual will experience, rapidly and realistically represent operational environments at different levels of security, and/or scale.
* You can also repeat the experiment, using precise control of the test environment, reconfiguration, and rapid reconstitution of environment to a baseline checkpoint. This would allow rapid variation of conditions to quickly evaluate hundreds of scenarios.
* Cyber ranges allow employees and customers to learn how to identify potential threats, and know how to deal with them.
* Software developers can use cyber range applications to validate new ideas, testing market viability, and more. Cyber ranges allow test how applications will function in live environments, how these items will integrate with and act within that domain.
* Cyber range may help users develop concept of operations, set-up procedures and training materials, as well as assist them in determining how resilient a system is to a cyberattack.
* Cyber range may make sure products are compliant. Vendors can use the cyber range to see if their products are compliant with security standards (e.g. with NIST Risk Management Framework).
* Cyber ranges allow speed up time to production. Using the cyber range gives the opportunity to address vulnerabilities during the design phase, to certify that the product meets all operational requirements.
* Cyber ranges are easy to deploy, require less capital expenditure, so they allow save your business time and money.
* A virtual cyber range is always up to date and ready to help test against whatever threats they want.
* Cyber range training environments are accessible from anywhere. This accessibility makes them a great option for keeping your employees and customers trained, certified, and prepared to deal with cybersecurity threats.
* You can upgrade your existing virtual environments whenever you want, scale them up as you grow. With a virtual environment, you only pay for the resources you need.

### Cyber Range Mission – Capabilities – Advantages

Until now a dozens of Cyber Ranges were developed in universities [18], military organizations and other institutions around the world.

We reviewed some Cyber Ranges and presented the summary of the review in Annex No. 1. Table contains following information:

* Platform name
* Mission – destination and possibilities of use in education, training and research
* Capabilities to work in different environments (virtual, large network, cloud), visualization, different levels of expertise, flexibility etc.
* Advantages which distinguishe them from other Cyber Ranges
* Short information about organization where Cyber Range were developed.

# Pilot of Cyber training & exercise Framework

## Architecture of Cyber training & exercise Framework

During this project, KTU and partners developed or adapted several Security Training and Awareness Tools which are presented in following sections. The federated infrastructure of Pilot of Cyber training & exercise Framework is deployed using SPARTA JCCI (<https://www.sparta.eu/JCCI/nexus.html>), see Figure 3-1.

KTU presents its own training platform and Red Team / Blue Team training scenario ("storyline") as pilot of using this framework in training.

CNIT presents its own platform along with its usage in a CTF competition.

BUT presents the use case on the KYPO platform, one of the first open-source cyber range platforms available on the market.The full deployment procedure and pilot results are described.

UBO presents a framework to measure IT-Security Awareness within working staff.



Figure 3.1: Federated infrastructure of Cyber training & exercise Framework

**KTU.** The world has gone digital. In developed information societies, such as EU, this is a fact so profound that without functioning data networks and computer systems the well-being of humans and even the security of the nation is at risk.

In this complex world where the boundaries of the digitalized infrastructure and the physical realm are blurred the interconnected environment of physical and electrical systems is often described as a cyber domain.

In today’s world where the cyber domain is an integral part of people’s lives, the need for training against different types of cyber-related threats is ever-growing. KTU has arranged a vast number of different types of cyber training (Figure 3‑2). The training against threats should take place in a controlled environment because there is a need for realistic simulated attacks, and the risks for breaking laws or harming outsiders by making mistakes in the open internet are simply put too big and actual. Also, not many organizations are willing to take the risks of harming their production environment or continuity of business.

For this purpose, the cybersecurity exercises are held in closed cyber ranges isolated from the internet; however, they mimic the services and structures of the real internet. Nevertheless, it makes no difference if one is training in simulations or struggling with real Cyber Security incidents in one’s production systems, the need for accurate situational awareness is always paramount.

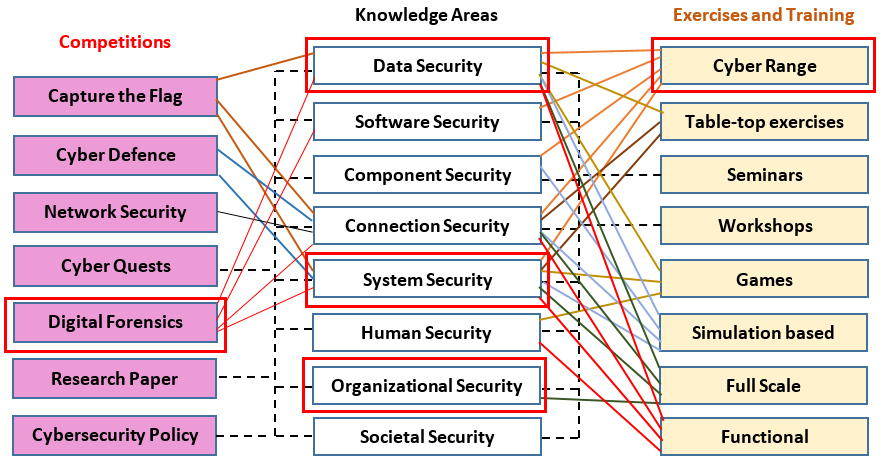


Figure 3.2: Acquisition of knowledge and practical skills using KTU Cyber training & exercise platform

The Table 3.1 shows the integration and information exchange between the KTU-proposed Cyber training & exercise Framework and the SPARTA JCCI platform.

The outcome of this KTU proposed Cyber Range platform can be used as a high-level requirement specification for a cybersecurity situational awareness system for the defender in cybersecurity exercises. It should be possible to design and develop a demonstration system that visualizes and helps in understanding what the current overall cybersecurity status and situation of incident handling is for a defending team.

Table 3.1: Information exchange between Cyber training & exercise Framework and the JCCI platform

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***Incident No. in KTU Cyber training & exercise Framework*** | | | ***SPARTA Joint Competence Centre Infrastructure (JCCI)*** | | | | |
| ***Data*** | ***Description*** | ***Interaction*** | ***Services*** | ***Tools*** |
| A1 |  |  | **X** | **X** | **X** | **X** | **X** |
|  | A1.1 |  | **X** | **X** | **X** |  | **X** |
|  |  | A1.1.1 | **X** | **X** |  |  |  |
|  |  | A1.1.2 | **X** | **X** |  |  | **X** |
| A1.2 |  |  | **X** | **X** | **X** |  | **X** |
|  | A1.2.1 |  | **X** | **X** |  | **X** |  |
|  | A1.2.2 |  | **X** | **X** |  | **X** |  |
| A2 |  |  | **X** | **X** | **X** |  | **X** |
|  | A2.1 |  | **X** | **X** |  | **X** |  |
|  | A2.2 |  | **X** | **X** |  | **X** |  |
| A3 |  |  | **X** | **X** | **X** | **X** | **X** |
|  | A3.1 |  | **X** | **X** |  |  |  |
|  | A3.2 |  | **X** | **X** | **X** |  | **X** |
|  |  | A3.2.1 | **X** | **X** |  | **X** |  |
|  |  | A3.2.2 | **X** | **X** | **X** | **X** | **X** |

**CNIT**

CNIT is piloting a Cyber Range infrastructure built internally, called Nautilus Cyber Range. We believe that joining forces among different stakeholders is the most effective way to address one of the most challenging issues which trainers encounter while deploying new scenarios: vulnerable components reuse. With Nautilus and its Marketplace, trainers are allowed to compose trainings in a drag-and-drop manner, using basic blocks from other scenarios (if they were published to the Marketplace). Components that can be shared are vulnerable software, misconfigurations, CVEs (e.g. how to download, install and configure either one or a set of software to make a system vulnerable to that particular CVE), etc. In this way, known threats – and their countermeasures too – can be applied easily to new scenarios. The most valuable advantage of this knowledge sharing approach is the ease in creating new content for trainees.

The other main feature of Nautilus is its ability to semi-automatically deploy training testbeds to remote machines via a Web Interface. Indeed, it is possible to install Nautilus Deployment Framework on any machine where training scenarios should be deployed; then, thanks to the webapp which securely communicates with the distributed Deployment Framework, scenarios can be launched/terminated and monitored remotely.

Currently, Nautilus is used by CNIT and a local University in Rome in an Ethical Hacking course, in order to provide practical exercises to the students. The infrastructure was also used in an Italian national CTF competition. A detailed description of the Nautilus architecture and its components is provided in Chapter 5.

**BUT**

BUT is piloting a cyber-range infrastructure built using the open-source package called KYPO Cyber Range Platform (KYPO CRP) available at [https://www.kypo.cz](https://crp.kypo.muni.cz/). This activity is part of the inter-pilot collaboration between SPARTA and CONCORDIA, where BUT plays the role of an early adopter and tester of the platform.

To the best of our knowledge, KYPO CRP is the first open-source cyber range platform that is actively maintained and suitable for the deployment at universities for a practical training of students. It is built on the OpenStack cloud platform, that is a set of freely available tools that allow users to create a cloud platform offering computing and storage services using virtualization. OpenStack is IaaS (Infrastructure as a Service), where it is possible to use computing and storage resources without the need for physical management of these resources and redistribution of resources. The KYPO CRP allows the simulation of devices, networks, and computers with any operating system. KYPO CRP provides a graphical user interface through which the entire training is available. Such trainings can be available both locally and remotely via the HTTPS interface. For further details please follow KYPO CPR documentation available at <https://docs.crp.kypo.muni.cz/>.

KYPO CRP utilizes an open approach for the content to encourage creating a community of trainers and supporting the sharing of training definitions, sandbox definitions, and its building blocks. Training and sandbox description are defined in human-readable data-serialization languages (JSON, YAML) and use open-source software to build virtual machines and describing machine content (Ansible, Packer).

Currently, KYPO CRP is used by the Brno University of Technology (SPARTA) and Masaryk University (CONCORDIA) in cybersecurity-related courses to provide hands-on experience to students of both Bachelor and Master programs. Using the platform, the students may safely execute cybersecurity attacks in virtual environments, study their principles, see the consequences and deploy countermeasures. The infrastructure is also used by students in semestral projects, in which students are asked to design and deploy their own training scenarios. Detailed description of the pilot design, deployment and results is provided in Chapter 6.

**UBO**

## Mapping of training & exercise activities to knowledge areas

Different training & exercise activities can be used to deeper mastering of teaching materials in cyber security. Following table (Table 3.2) shows passible use of different cyber security exercises.

Table 3.2: Covering of different Knowledge Areas by partners’ platforms

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Partner***  ***Knowledge***  ***Areas*** | ***Kaunas University of Technology (KTU)*** | ***National Consortium for Telecommuni-cations (CNIT)*** | ***Brno University of Technology (BUT)*** | ***UBO*** |
| ***SPARTA JCCI Integrator*** | ***KTU Cyber training & exercise Framework*** | ***Cyber security training platform*** | ***KYPO (Cyber range)*** | ***IT-Security Awareness Measure*** |
| Data Security | **X** | **X** | **X** |  |
| Software Security |  | **X** | **X** |  |
| Component Security |  |  | **X** |  |
| Connection Security |  |  | **X** |  |
| System Security | **X** | **X** | **X** |  |
| Human Security |  |  |  |  |
| Organizational Security | **X** |  |  |  |
| Societal Security |  |  |  |  |

# KTU Pilot of Cyber Security Training Platform

## Description of KTU Cyber training & exercise Framework

Our decision to propose Pilot of KTU Security Training and Awareness Platform is based on following:

* our experience in conducting cyber training exercises show importance of such training and exercises in the public and education sectors;
* our desire to provide an opportunity for a wide range of exercises, using all available tools and those that may appear in the near future.

A typical institution network topology is proposed in in Figure 4.1.

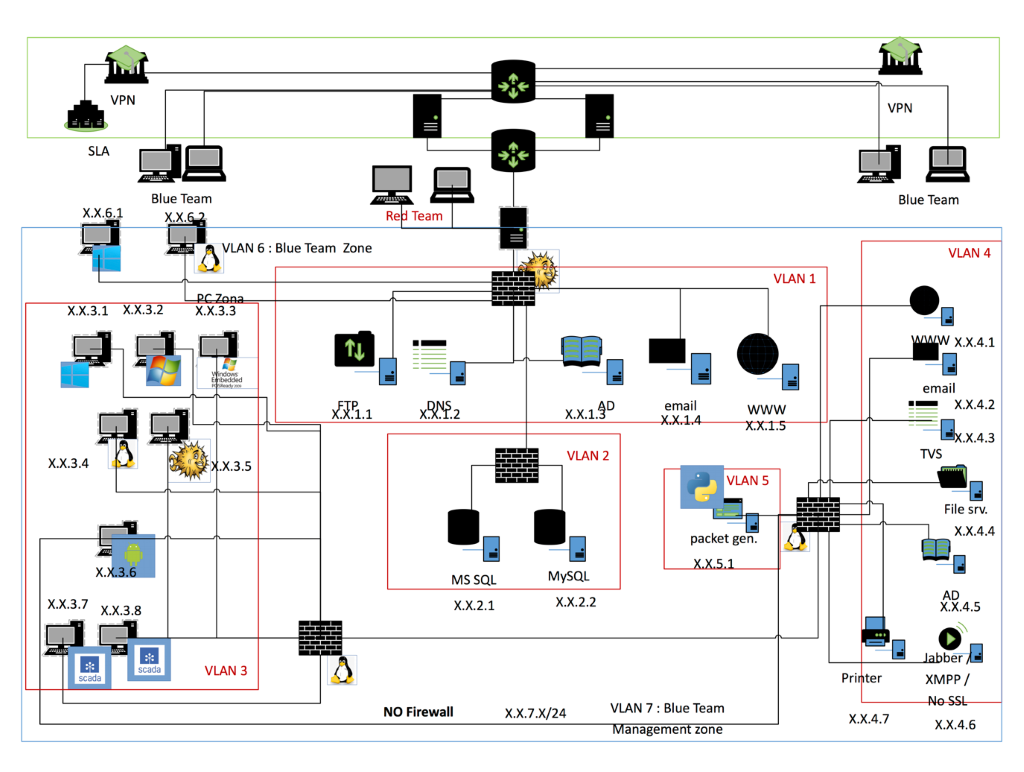


Figure 4.1: The typical topology of institution

Network segmentation with virtual local area networks (VLANs 1-6) creates a collection of isolated networks within the Cyber Range Platform. Each network is a separate broadcast domain. When properly configured, VLAN segmentation severely hinders access to system attack surfaces. It reduces packet-sniffing capabilities and increases threat agent effort. Finally, authorized users only “see” the servers and other devices necessary to perform their daily tasks. Another advantage of segmentation is protocol separation. Network architects can limit certain protocols to certain segments of the Cyber Range. In the specific case, we see that the segmentation performed makes it very difficult for an attacker to gain access to the internal network. At the same time, it explains the weaknesses of the network.

A group of people authorized and organized to train a potential adversary’s attack or exploitation capabilities against an organization security posture. The Red Team’s objective is to improve attacks vectors by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. The group responsible for defending (the Blue Team) or to go thru procedure an organization use of information systems by maintaining its security posture against a group of mock attackers (i.e., the Red Team). Typically, the Blue Team and its supporters must defend against real attacks. They can be over a significant period of time or in a representative operational context (e.g., as part of an operational exercise) and according to rules established and monitored with the help of an IT staff. The term Blue Team is also used for defining a group of individuals that conduct operational network vulnerability evaluations and provide mitigation techniques to customers who have a need for an independent technical review of their network security posture. The Blue Team identifies security threats and risks in the operating environment, and in cooperation with the customer, analyses the network environment and its current state of security readiness. Based on the Blue Team findings and expertise, they provide recommendations that integrate into an overall community security solution to increase the organization's cybersecurity readiness posture. Often times a Blue Team is employed by the organization or prior to a Red Team employment to ensure that the simulated information systems are as secure as possible before having the Red Team test the systems. Also, a common approach is to give the Blue team a full description of the information systems, the attacks carried out (Red teams) and ask them to find out and apply measures to increase cybersecurity.

**Objectives**

The main objectives of the KTU Security Training and Awareness Platform are:

1. Transfer of knowledge and experience between the partners in respect to educational and awareness raising activities, but also the establishment, management and operation of security testbeds.
2. Strengthen sustainable collaboration among the partners in respect to educational and awareness activities, but also towards talent identification, recruitments and mobility.
3. Enhance research-based knowledge and knowledge development among the partners, by providing a platform suitable both for the objectives of the platform, but also for further studies on research topics across the investigated sectors (e.g. Web platforms, network and telecommunications, hardware security, etc.).
4. Strengthen multilateral relations and the development of a regional competence network, with the aim of stimulating long-term cooperation, capacity, and competence–building, also towards future collaborative research projects on EU and regional level.

**Platform sustainability**

The developed training platform will be structured in a modular manner, aiming for each of the partners to provide interoperable modules dedicated to a specific sector.

**Case studies and widespread dissemination**

They should demonstrate its results with a multitude of case studies, aiming towards widespread dissemination. These currently include:

1. Selection and training of the national teams towards their participation to the European Cyber Security Challenge.
2. Summer school on cyber-security awareness and training.
3. Common development of educational material and tutorial lectures and integration into the currently offered curricula.
4. “Security Awareness and Training Day” workshops, targeted towards undergraduate students, secondary school students, educators and parents.

**Key anticipated activities**

1. Investigation and development of novel scientific methods in respect to:
   1. cyber-security training of digital natives,
   2. security awareness of key stakeholders such as educators and parents,
   3. young talent identification and recruitment.
2. Development of a collaborative and modular cyber-security training platform that, in addition to the aforementioned objectives, provides the technical depth and is suitable for parallel and future research activities in contemporary topics related with cyber-security across the integrated sectors.
3. Enhancement of the educational offering across the participating institutions, through the development of tailored and hands-on curricula components based on the developed platform.
4. Dissemination of results through scientific publications towards the scientific community, but also targeted security awareness activities towards the digital natives and key stakeholders (see Case studies and widespread dissemination).

## Pilot of KTU Cyber training & exercise Framework

We propose to use Pilot of Cyber training & exercise Framework while:

1. The basis for such a decision follows from the analysis already performed.
2. This will reach more users and get more benefits.
3. We are providing a framework which will be based on the storyline (scenario templates).
4. Partners can provide their own knowledge-based framework, which will cover the organizational and technical means.

Hands-on cybersecurity education and training activities are critical given that cyberattacks occur nowadays on an ever-increasing scale. Only such practical activities can ensure that trainees will acquire the actual skills necessary to promptly deal with security incidents in real-life situations. However, current programs rely significantly on the manual setup and configuration of the learning and/or training environments used, which is a tedious, inefficient and storyline approach.

### Description of KTU Cyber training & exercise Platform

In Figure 4.2, we present an integrated cybersecurity training framework, that we designed and implemented to address such the choosing training content and environment setup tasks. Our results show that Cyber training & exercise Framework is well-suited for actual training activities in terms of features, usability and execution performance.

Diagram

Description automatically generated

Figure 4.2: Infrastructure of KTU Pilot of Cyber training & exercise Framework

### Installation of KTU Cyber training & exercise Platform

Have you ever tried to install Windows operating system on Apple / Windows computer? You can install and run disk image in OS X or Windows for free using VirtualBox. Because this installs Windows into a virtual machine atop existing operating system software, running Windows is basically like running any other application, which makes it much easier than configuring Apple Boot Camp or Windows Hyper-V for a native Windows experience.

More information about installation see in Annex No.2.

### Pilot of Red Team / Blue Team exercise on KTU Platform

To demonstrate the capabilities of the KTU Cyber training & exercise Framework, we will provide a description of the Red Team/Blue Team exercise.

The main goal of Red Team/Blue Team exercise is to develop practical cybersecurity skills of the participants, including technical staff and responsible for organizational measure, to improve cooperation between cyber incident management and/or investigation centres, University technical staff and responsible for organizational measure, state institutions and cybersecurity entities, to:

1. focus on coordinating the actions of all participating institutions;
2. achieve greater efficiency in decision-making;
3. strengthen Lithuania's cybersecurity and defence.

An organization can use a Cyber training & exercise Framework in a typical organization's IT infrastructure as the template to identify and build the scenarios, which should be simulated during the exercise, and how deeply these scenarios will.

Four storylines are presented in Table 4.1:

* A1 – using of CMS brute force attack for malicious scanning of network and encryption of files;
* A2 – attack using the SQL injection method;
* A3 – attack by exploiting the WordPress vulnerability;
* B1 – attack by exploiting the user's insufficient care about security in social network.

First three columns in Table 4.1 represent incidents steps. Column ***Incident*** contain brief description of the steps of the incident. Two next columns show, what measures (organizational and practical) are involved in incident handling. The las column indicates what systems (servers, websites, workstations, etc.) are affected by incident.

Table 4.1: Methodology of choosing practical and organizational measures

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| *Incident No.* | | | *Incident* | *In organization* | | *The organizational system affected* |
| ***Organizational part*** | ***Technical part*** |
| A1 |  |  | Use of CMS brute force (password selection) | **+** | **+** | WWW 3 |
|  | **A1.1** |  | Review a malicious file | **+** | **+** | WS 1 |
|  |  | **A1.1.1** | received a phone call | **+** |  | WS 1 |
|  |  | **A1.1.2** | received an email | **+** | **+** | WS 1 |
| A1.2 |  |  | Reverse shell | **+** | **+** | WS 1 |
|  | **A1.2.1** |  | Malware synchronization | **+** | **+** | FS, WS 1, WS 2, WS 3 |
|  | **A1.2.2** |  | Internal network scanning, SMB vulnerability |  | **+** | WS 1, AD |
| A2 |  |  | SQL query | **+** | **+** | WWW, FS |
|  | **A2.1** |  | Malware synchronization | **+** |  | FS, WS 1, WS 2, WS 3 |
|  | **A2.2** |  | Transfer of a ransomware | **+** | **+** | FS, WS 2 |
| A3 |  |  | A CMS plugin that will allow you to view the full content tree | **+** |  | WWW 2 |
|  | **A3.1** |  | Public and private keys are used | **+** | **+** | FS |
|  | **A3.2** |  | Reverse shell |  | **+** | WWW 2, WS 3 |
|  |  | **A3.2.1** | Remote connection with saved settings (RDP, VPN client certificates) |  | **+** | WS 3, AD |
|  |  | **A3.2.2** | WWW 2 and data leakage to the outside | **+** | **+** | AD, WWW 2 |
| B1 |  |  | Social network | **+** | **+** | WS 3 |
|  | **B1.1** |  | Reverse shell | **+** | **+** | WS 3 |
|  | **B1.2** |  | The consequence of an attack (AD) is access to all policies | **+** | **+** | AD |
|  | **B1.3** |  | WWW1 and data leakage to the outside | **+** | **+** | AD, WWW 1 |
|  |  | **B1.3.1** | Data theft | **+** |  | WWW 1 |
|  | **B1.4** |  | Access from AD to FS and later to WS2 | **+** | **+** | FS, WS 2 |

Now we will expline each storyline in more detail.

**Storyline A1** (Additional information see in Annex No.5)

1. Using the password selection method, Attacker A hacks into the WWW3 site and places a malicious file there.
2. (A1.1) The employee responsible for the content of the public website (WWW3) receives an email. After that he logs in with his access profile (username / password) and views the file uploaded by the "service provider" (as attachment), giving Attacker access control to the organization's workstation (WS 1) (initiated by Windows powershell reverse-shell).
3. (A1.2.1) Attacker A moves malicious files (8.1.2\_AdbeRdr812\_en\_US.exe, Win32.exe) to a directory whose file synchronization (FS) is performed continuously, and the file is also distributed throughout the organization's workstations (WS 2, WS 3, WS n). WS 1 creates a new system user who will have Administrator rights. The internal network scan starts.
4. (A1.2.2) The Attacker launches malicious code files. One file is for network scanning, the other file is for workstation encryption.
5. Three CMS images required to complete the task: Wordpress (on Windows OS), Wordpress (on Linux OS).

**Storyline A2** (Additional information see in Annex No.6)

1. Using the SQL injection method, Attacker attacks WWW1 and obtains usernames and passwords required to access the WWW1 CMS.
2. (A2.1) AD usernames / passwords are synchronized with the CMS authentication database. A ransomware file is placed in a directory that is automatically synchronized by the File Exchange Server (FS).
3. (A2.2) The ransomware file is distributed to the organization's workstations, including WS2. Its user receives a message about file sharing. The user downloades the file and opens it. Encryption of this workstation starts.
4. The disk image can be fully encrypted, disk image is suspended. It can be used for different goals.
5. A website WWW1 (in Windows) is required to complete the task.

**Storyline A3** (Additional information see in Annex No.7)

1. In this case Attacker exploits WordPress vulnerability in WWW2. Using the brute-force attack, Attacker gets access to CMS to obtain administrator’s password and get access to the DB. Attacker connects to the site CMS. The CMS user “Insider” (which will be used later for data leakage) is created.
2. The malicious file "remote work order.pdf" is placed in the CMS. The document is uploaded to an automatically synchronized directory. File will be synchronized to WS2 and WS3 and opened there.
3. Attacker performs export of DB (sql\_dump) and download sql\_dump (data leak).
4. Attacker connects to WS3, launches Meterpreter (reverse shell), launches keyboard spyware Keystrokes (keylogger).
5. Attacker intercepts WS3-stored login data (VPN certificates, RDP settings). Waits for connection of network administrator to the organization's network (to receive a username / password).
6. Using VPN certificates stored in WS3, Attacker connects to the organization's AD server.
7. Because access to the organization's network requires not only certificates but also passwords, Attacker waits until the administrator connects to the organization's network by entering the login name / password, which is taken over by keyloger (input from keyboard).
8. The attacker enters the organization's network. Connects to the active directory system AD, exports user data to the user-list.txt file. Triggered to WWW2 from there and picked up.
9. A website WWW2 (in Linux) is required to complete the task.

**Storyline B1** (Additional information see in Annex No.6)

1. Attacker interacts with the child of a WS 3 user (who is the organization’s IT administrator) in chat room of the game platform STEAM (online game platform).
2. The child complains that the computer is too weak for games. Attacker promises to send information on how to boost game settings in child’s computer.
3. Attacker sends to child a link to the document "instruction.pdf". The child opens the document. The document is empty. Thus, Attacker takes over WS3 (using reverse-shell). Attacker creates user with administrator rights and enables keyloger.
4. Using VPN certificates stored in WS3, Attacker connects to the organization's Active Directory System (AD) server.
5. Because not only certificates but also passwords are required to connect to an organization's network, Attacker waits until the administrator connects to the organization's network by entering a login / password that is scanned by keyboard spyware.
6. The list of Active Directory users with password hashes is exported to the file, which is uploaded to WWW2 and downloaded by Attacker. The file is uploaded for public viewing on the Internet.
7. A file (system-update.exe) with redeemable software is uploaded to the synchronized directory.

### How to play storyline?

One of these possible storyline-based scenarios (Figure 4.3) is described below. We see how participants need to play during the exercise. An expanded version, with timing and actions, see in annexes.

An organization chooses a scenario in which its WEB site is hosted on a server. It is normal practice for an organization to purchase hosting services.

A picture containing text, black, close

Description automatically generated

Figure 4.3: Attacks vectors based on story line scenarios

Attack scenarios (storylines) are presented in Annex No. 2.

Below we explain in more detail one of the incidents – Incident A1.

Information about scenarios presented in Table 4.1 should be interpreted in such a way.

Incident A1 starts with cyber-attack using the password brute-force method. Attacker A hacks into the WWW3 website and places a malicious file there to prepare to phishing attack. The employee responsible for the content of the public website (WS1) receives an e-mail informing about the uploaded information, logs in with its access profile (username / password) and views the file uploaded by the "service provider" (attachmentNo1.xlsm) thus giving the Attacker A access control to the organization's workstation (WS 1) (initiated by reverse-shell which is write for Windows).

Step A.1.1. Attacker A moves malicious files (8.1.2\_AdbeRdr812\_en\_US.exe, Win32.exe) to a directory whose file synchronization (FS) is performed continuously, and the file is also distributed throughout the organization's workstations (WS 2, WS 3). WS 1 creates a new system user with Administrator rights and the internal network scan starts.

Step A.1.1.1. (Optional. Phishing over phone) The user WS1 calls the provider to discuss the contents of the uploaded file and learns that the provider actually did not upload the information. The user suspects that the site was hacked yesterday and became a victim of social engineering.

Step A.1.1.2. The user informs his IT (security) department about the received e-mail.

In order for the task to be successful, the relevant staff should provide the following additional information (Table 4.2):

Table 4.2: Additional information to be provided by the relevant staff

|  |  |
| --- | --- |
| *IT administrator* | *Procedure to get and deliver a WS1 image* |
| Hosting provider | Request data (LOGs, disk image, etc.) |
| Security Representative | Information on the situation and planned actions |
|  | Evaluation: risk, damage |
| IT (security) department | The IT administrator provides the image of WS1 |
|  | **Starts a WS1 forensics** |
| IT | Provides requested WWW3 files without discussion |
| IT | Provides requested WWW3 files but not in accordance with the term specified in the contract |
|  | **Starts a WWW3 forensics** |
| IT (security) department | Ask for more information on the progress and results of the WS1 and possibly WWW3 forensics |

Press release about the incident and possible damage to all who downloaded file attachment No.1.xlsx. Information has appeared in the public domain (IT security community forums) that an infected \*.xlsx file could be downloaded from your site yesterday. A screenshot of the site is attached and request for a comment is added. Information is needed quickly; an article is prepared to be published in two hours. If no information is received after an hour re-inject: Do, we have preliminary investigatory.

One full working day is allocated for the whole A1 scenario. Roles can also be added (for example director, department head, data protection position, public sector). For each of these roles, it is possible to prepare messages that will expand the analysis of the incident, check the procedures in place, and involve more departments and other responsible persons.

Trainers Manual, where the Attacks are explained in form of questions and answers, is presented in Annex No. 9.

### The benefits of using the Cyber training & exercise Framework

Our experience in conducting cyber training exercises allows to draw the following conclusions about using the Cyber training & exercise Framework:

* Cyber training & exercise Framework can be used for conducting a wide range of exercises.
* Topology of platform used in exercises provides an opportunity of creating a collection of isolated networks within the platform; this reduces packet-sniffing capabilities and limits users possibility to access only the servers and other devices necessary to perform their daily tasks.
* Network segmentation limits attacker possibility to gain access to the internal network.
* Framework provides possibility to expand using tools including those that may appear in the near future.
* Cyber training & exercise Framework can be used both for training of the national cyber-security team and educating undergraduate a graduate students at universities.
* Cyber training & exercise Framework can be used for future research activities in contemporary topics related with cyber-security.
* Awareness campaigns used in the majority of cybersecurity education programs typically employ lectures or presentations to state the issues to teach students and employees. Learning methods using this approach are often designed from the perspective of the presenter and focused on delivering information within a minimum amount of time, instead of paying attention to the effective transfer of information.
* Using games is aimed to improve cybersecurity awareness and training. This framework is based on existing frameworks addressing the complexity of the cyber domain, unique characteristics of participants, and pedagogic potential of the designed games.
* It was shown how the integration of these frameworks can help to increase the effectiveness, coverage, engagement, and the ability to reflect in the practice of games.
* In order to realize the full potential of this framework and achieve effective guideline for implementation of serious games, you need to install infrastructure on-site and start to play.
* KTU Cyber training & exercise framework quantifies the skill and motivation of the cybersecurity workforce and analyzes how cybersecurity stakeholders should build a robust and sustainable set of skills. Learning by experience provides technicians, IT managers and board members with an adequate level of training to bridge the training gaps at all levels of the organizations and governments.

# CNIT – own platform with a storyline

## The Nautilus Platform

**Nautilus** - CNIT Cyber Range - delivers a cyber range platform with extended capabilities. The platform represents a reliable training tool to advance cybersecurity skills at all levels, enables quick deployments and configurations (by leveraging recent advances in hybrid-cloud technologies) as well as effective sharing, among different parties ant stakeholders, of the information gathered about cyber security threats and corresponding defence strategies. In that sense, we propose a cyber range framework with a strong orientation towards a knowledge sharing platform.

**Nautilus** was designed in order to fulfil a number of very challenging requirements, of both technical and non-technical nature. For instance, it has to support the effortless configuration and deployment of virtual scenarios, the continuous monitoring and adaptation of the ongoing sessions, and the automation of actions and events, guaranteeing at the same time the possibility to test the most recent cyber menaces to match the fast pace at which the cyber security landscape changes. The approach of choice addresses such requirements incorporating one foundational concept: community.

The community component plays a fundamental role in establishing a common knowledge sharing platform, creating the framework for sharing the newly identified threats, protection strategies, as well as complete training scenarios and best practices among the members of our cyber range community.

### Core Design and Principles

The Cyber Range was designed with the following core principles:

* Easy configuration of dynamic scenarios and cyber threats
* Marketplate and Community
* Scalable Virtualized Platform and Hybrid Cloud deployment
* Monitoring, reproducibility and reporting

Creating a realistic scenario is the first step for building an effective training experience. The tools available in Nautilus to instructors for the definition of scenarios are flexible, embedding a variety of different components, and proposing a design experience as simple and intuitive as possible. Indeed, a cyber range with poor design tools hinders the capability of instructors to replicate agilely the emerging threats and the novel systems under evaluation, harming thus the temporal sustainability of the cyber range itself. An intuitive graphical web-interface based on drag-and-drop functionalities is the main Human-Machine Interface (HMI) for scenario developers and administrators. The HMI allows the quick and effortless configuration of the training scenario, which may be assembled from specific repositories dedicated to store the elements required for setting up the simulation, Nautilus is able to provision, orchestrate, compose and configure very specific components compared to classic IaaS platforms that are limited to VM images, including the descriptors, the templates and the executables for: i) known and zero-days vulnerabilities, ii) base images for exploitation systems, iii) vulnerable applications identified by means of a CVE, iv) network services, and v) advanced cyber threats and cyber defence mechanisms. By composing together these components enriched by the virtual network(s) topology for the training session, it is possible to deliver very accurate scenarios.

The graphical web interface is shown in Figures 5.1 and 5.2.

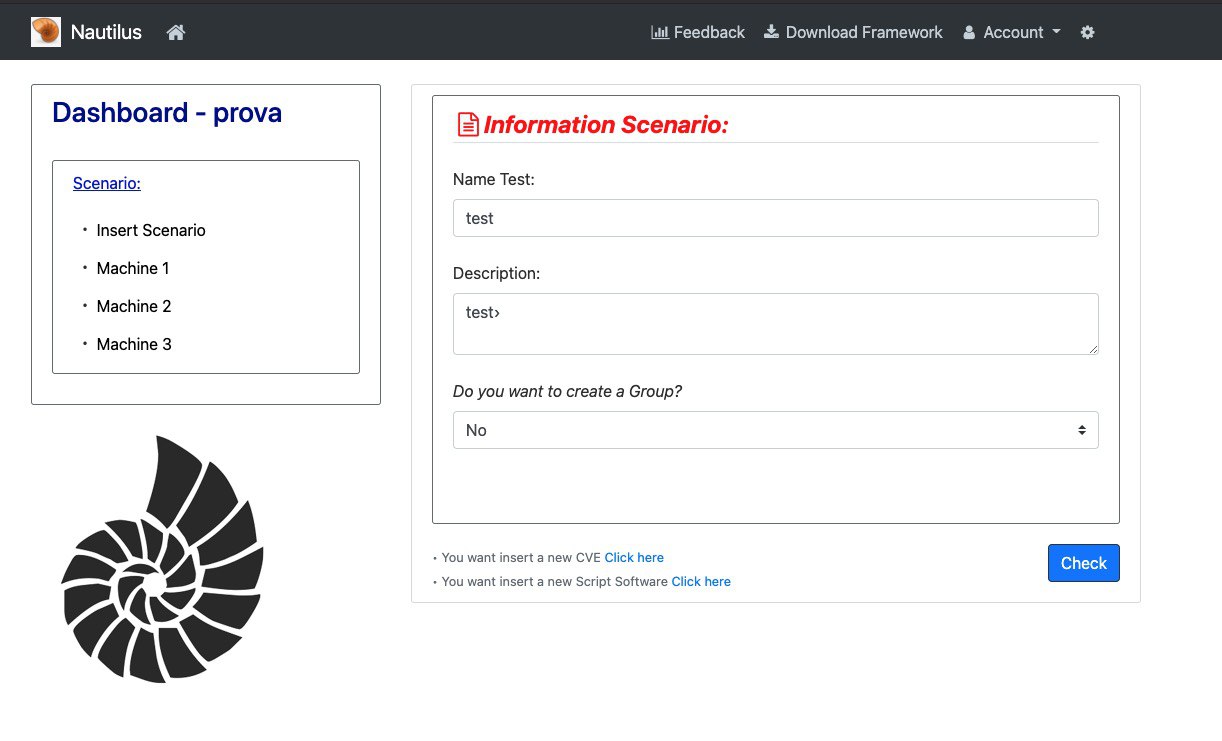
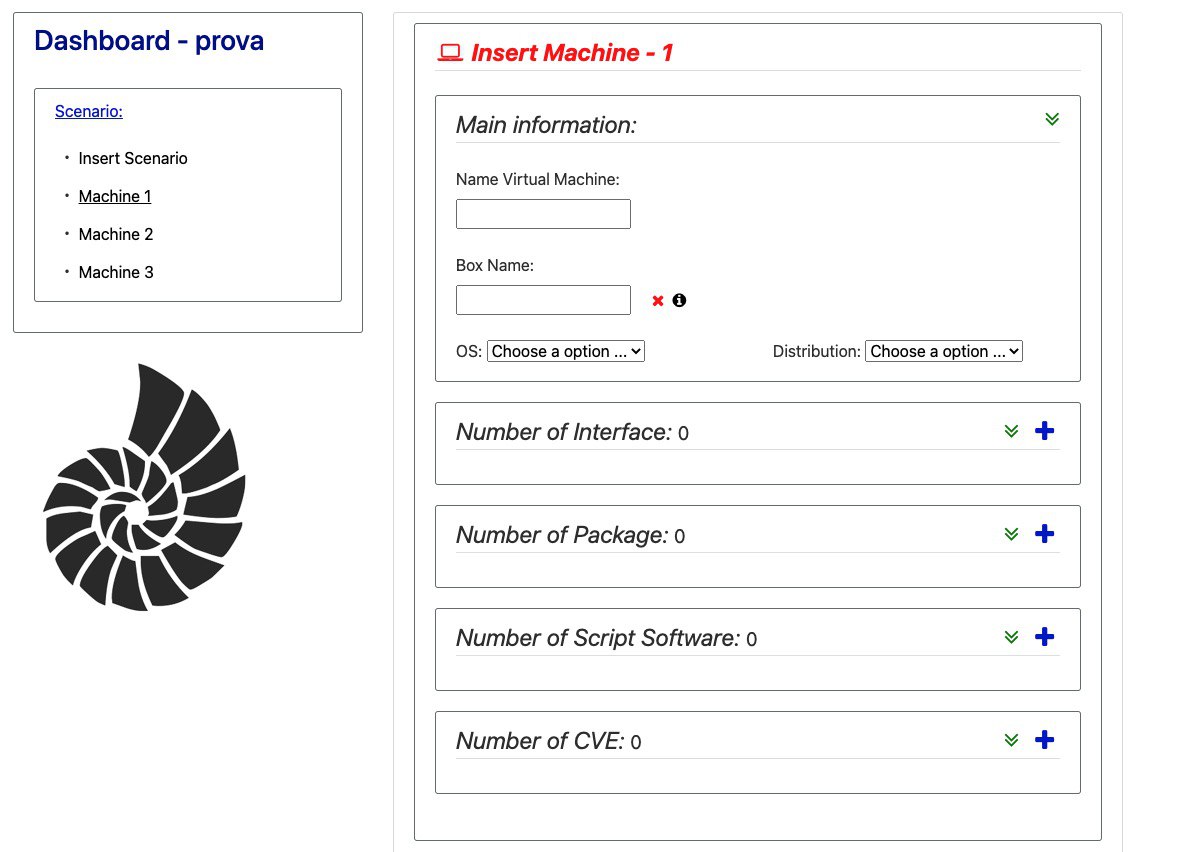
In addition, trainers and/or administrators, have the ability to build scenarios using the more advanced scenario-description language. This language is basically a set of yaml files, each describing a core component of the scenario; when a scenario is built using the web interface, it is then stored inside Nautilus database as a set of yaml files, thus providing a one-to-one mapping between these two methods.

Figure 5.2: Creating a Scenario with 3 VMs

Figure 5.1: Creating a new Scenario

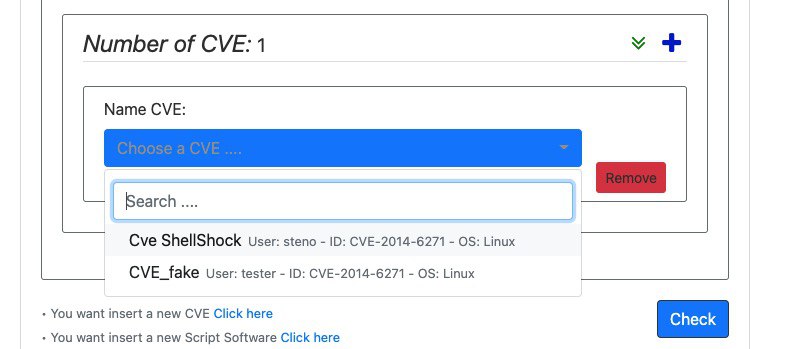
The core functionality of Nautilus here is the ability to assemble a scenario by using specific repositories, in particular the Nautilus repository, where specific training blocks are stored. As an example, a scenario may consist of a particular CVE to allow for privilege escalation. Once a scenario has the block corresponding to that particular CVE, that block can be pushed to the Nautilus repository so that other trainers can use it in their scenarios by simply drag-and-dropping it. In this example, the yaml file containing the configuration to make a system vulnerable to that particular CVE is the block which is shared among scenarios made by different trainers. This example is shown in Figure 5.3.

Figure 5.3: Adding a CVE to a Virtual Machine

In other words, once the scenario assembled and deployed, its recipe and constituent entities (e.g., from the file descriptors and the image templates for VMs, to the configuration files for software to be deployed, the threats and vulnerabilities that will be present in the scenario, up to the attack and defence patterns for automated opponents) are stored inside the Nautilus repositories, from where they can be uploaded to the marketplace. In the consortium view, Nautilus benefits enormously by the engagement of a community of end-users to its platform via the novel business model based on the sharing of vulnerabilities, attack vectors, and scenario definitions. By hosting this sharing economy ecosystem, Nautilus provides a way for specialized security firms and universities to monetize their researches, increasing at the same time the overall value of the platform and guaranteeing thus its sustainability beyond the end of the project itself. The marketplace can also be seen as a catalyst for economic growth and employment, as it incentivizes the creation of new businesses specialized in supplying those assets, as well as a source of certification and promotion for professional services.

Finally, the Nautilus platform leverages on established and emerging virtualization technologies to enable fast and automated system and network configuration deployments. This allows the platform to take advantage of both managed infrastructure services, such as Amazon AWS, Microsoft Azure, and of local deployments, e.g. based on VMWare vSphere, OpenStack, Kubernetes. In effect, Nautilus can deploy its virtual training environments on hybrid-cloud infrastructures by using tools like Vagrant. A scenario yaml configuration file may contain the information about the underlying virtualization platform to use and, during the deploy phase, Vagrant will take care of it. In this way, a scenario is completely decoupled from the underlying infrastructure where it will be deployed, and this allows faster and easier sharing.

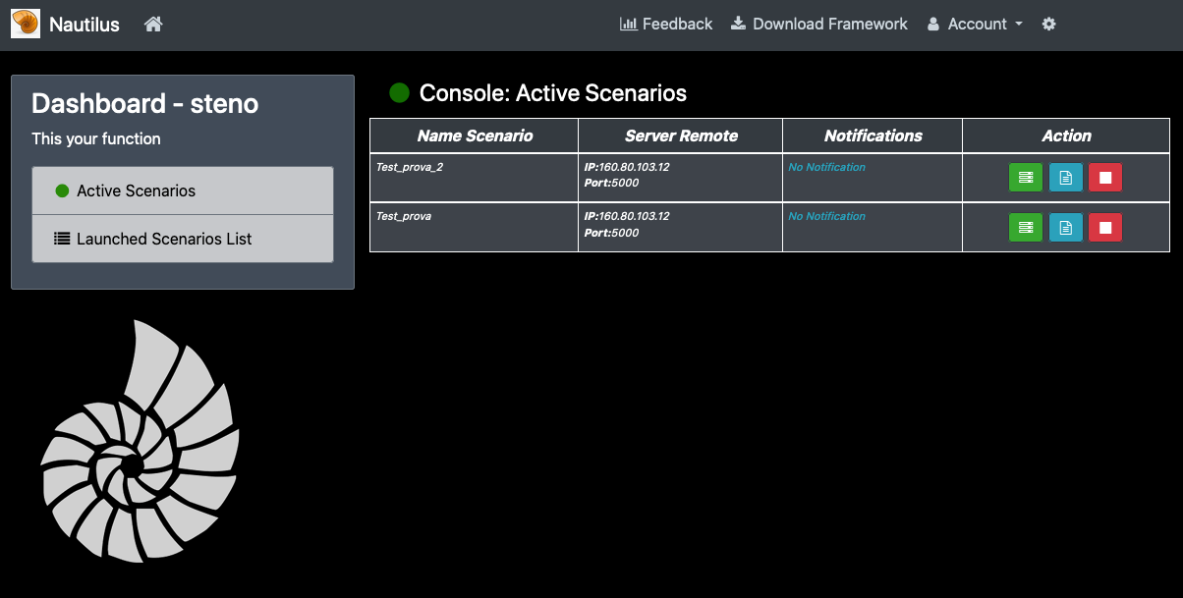
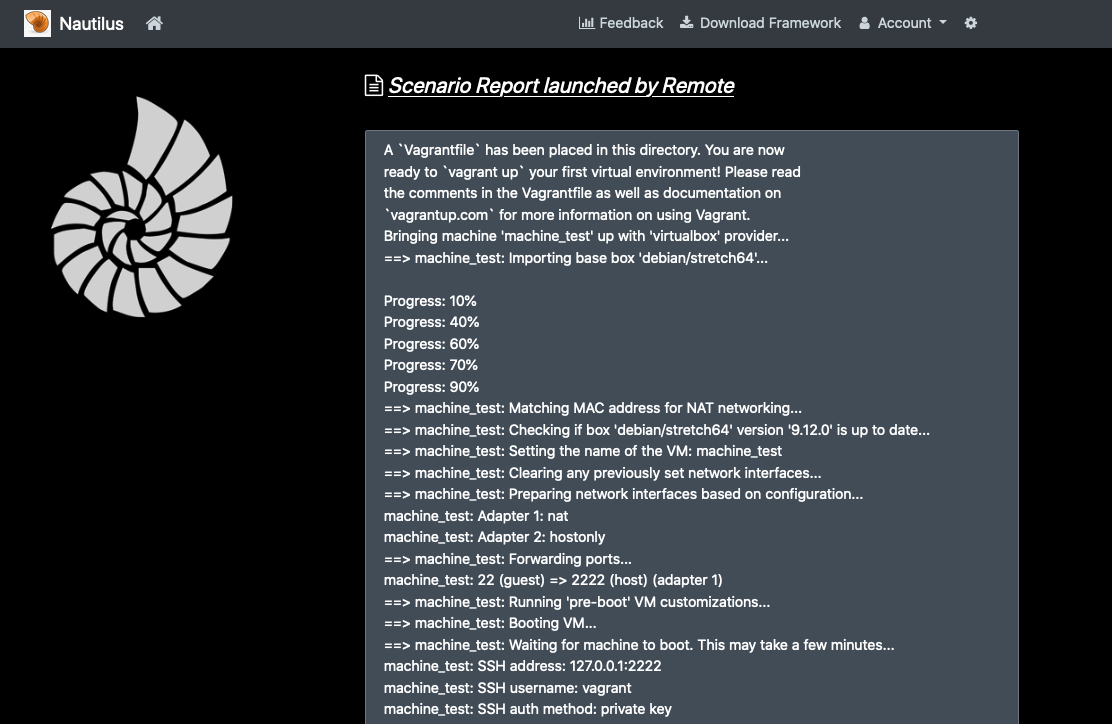
In addition, scenarios deployment can be monitored from the Nautilus web interface. A console allows to start/stop each scenario, view the corresponding logs, and deploy to a specific server (Figure 5.4). Deploying to a remote server allows for decoupling the scenario creation step from the deployment step. Figure 5.5 shows the report of execution of an example scenario deployed on a remote server.

Figure 5.5.4: Nautilus Console

Figure 5.5: Scenario Report

## The Pilot: CTF platform for cyber competition

The storyline we present is based on an Attack&Defense CTF competition. In this kind of competition, each team has a set of vulnerable environments which it has to protect from other teams; at the same time, the team is supposed to attack the same vulnerable environments belonging to other teams. This way, each team plays both the role of a Red Team and a Blue Team.

The proposed architecture is shown in Figure. Each team has a DEV environment and a PROD environment (Figure 5.4). The PROD environment contains the deployed challenges; in other words, this is the environment which is attacked by the other teams. The DEV environment contains the source code of the deployed challenges in form of a git repository (Figure 5.5). Access to this environment is isolated, meaning that each team can access only its own DEV machine, while each team can connect to all the PROD environments.

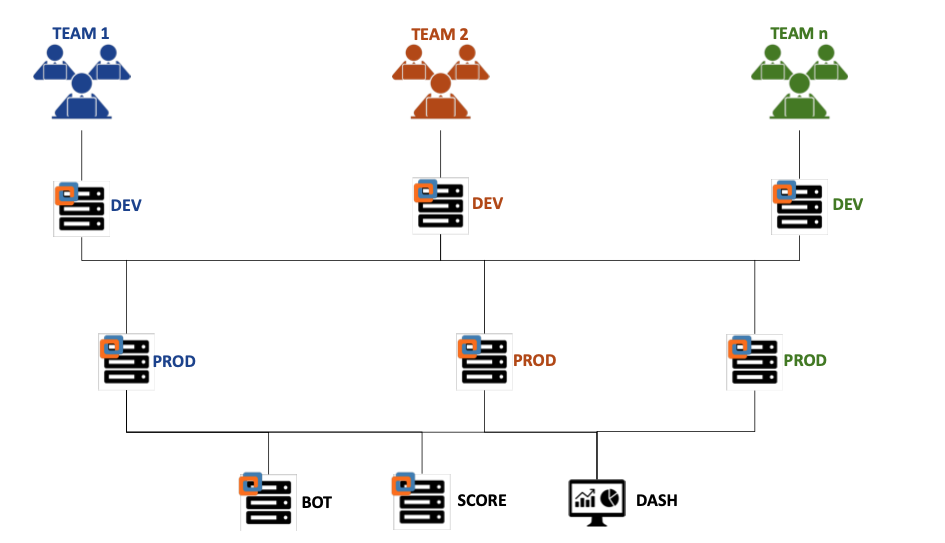
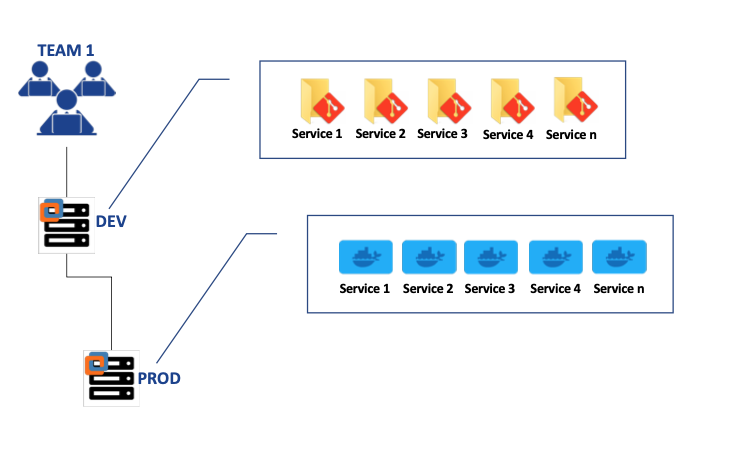
By analyzing the source code in the DEV environment, each team can find vulnerabilities. Once these vulnerabilities have been identified, the team must patch them by fixing the source code; an automatic pipeline (Gitlab CI) will deploy the new challenge to the team’s corresponding PROD environment (Figure 5.6). Fixing a Service means that other teams will not be able to exploit it.

Figure 5.6: CTF Architecture

Finally, there are 3 other components: the dashboard, responsible for showing the current rankings; the “score” component, where each team submits the flags in order to get points, and the bot component, which is responsible to control all the environments and make sure each team is behaving legit.



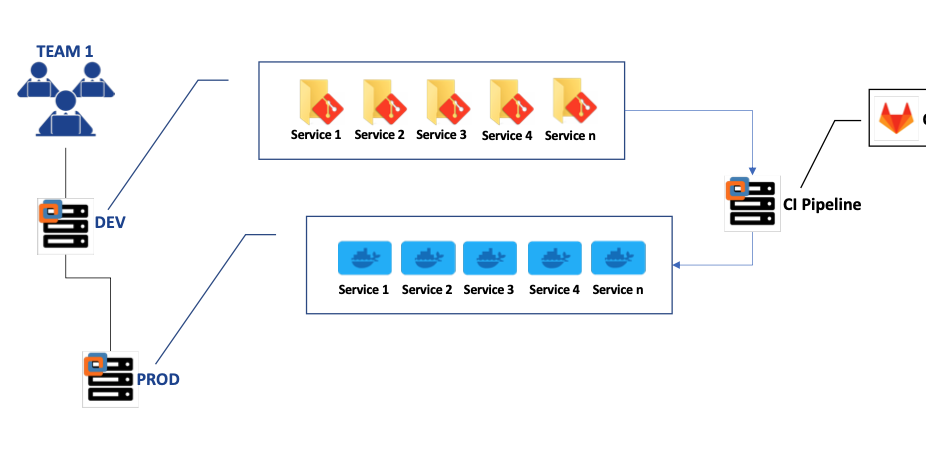
Figure 5.7: Services in PROD and DEV environment

Figure 5.8: Automatic deploy pipeline

### How to play

Access to the team environment is provided through WiFi. Each team connects to a shared WiFi network using a pre-defined set of credentials. Based on the credentials used to login to the network, a firewall isolates the team from the others by allowing connections only to their environment.

When the game starts, the firewall allows each team to connect to their own DEV environment, and to all the PROD environments.

### CTF challenges

Each PROD environment is composed of 5 containerized services, whose source code is available in the corresponding DEV environment:

1. Vending machine Web Interface, vulnerable to Command Injection; by exploiting this vulnerability it is possible to get a remote shell on the service container and get the flag.
2. Simple Blog web application, written using the Flask Framework (python), and vulnerable to Server Side Template Injection; by exploiting this vulnerability it is possible to arbitrarily read files on the underlying filesystem, thus reading the flag.
3. Patents managing application, which allows to submit new patents in docx form. This application is vulnerable to Blind XXE by submitting hand-crafted docx files composed of malicious xml payloads. By exploiting the blind XXE vulnerability, it is possible to read files on the filesystem, provided that the attacker knows the exact name and path of the file.
4. Custom Web Server written in C and vulnerable to buffer overflow; this is probably the most difficult challenge, not because of the vulnerability but because of the environment. The web server is a 64 bit application, with NX enabled and canaries enabled; on the kernel side, ASLR is enabled. This challenge requires creative thinking in order to gain a remote shell on the target container and read the flag.
5. Printer managing application with a Random Oracle vulnerability. The Printer queue stores the undergoing jobs by encrypting them, but the encryption process is a Random Oracle. By exploiting this vulnerability, a team is able to read the content of all the Printer undergoing jobs and one of them contains the flag.

### Benefits of using the Nautilus Cyber Range

* Marketplace of CVEs, vulnerable softwares, …
* Knowledge sharing
* As the marketplace grows, more complex scenarios can be easily created
* Easy configuration of dynamic scenarios, with an intuitive web interface
* Deploy on any Virtualization environment

# BUT Pilot of KYPO Cyber Range Platform

KYPO Cyber Range Platform (KYPO CRP) is an open-source platform developed at Masaryk University in Brno (https://crp.kypo.muni.cz). It is an open-source platform for cyber exercises, which is built on the OpenStack cloud platform. It allows the simulation of devices, networks, and computers with any operating system. KYPO CRP provides a graphical user interface (see Figure 6.1) through which the entire training is available. These trainings can be available both locally and remotely. For further details please follow KYPO CPR documentation (available at https://docs.crp.kypo.muni.cz/).

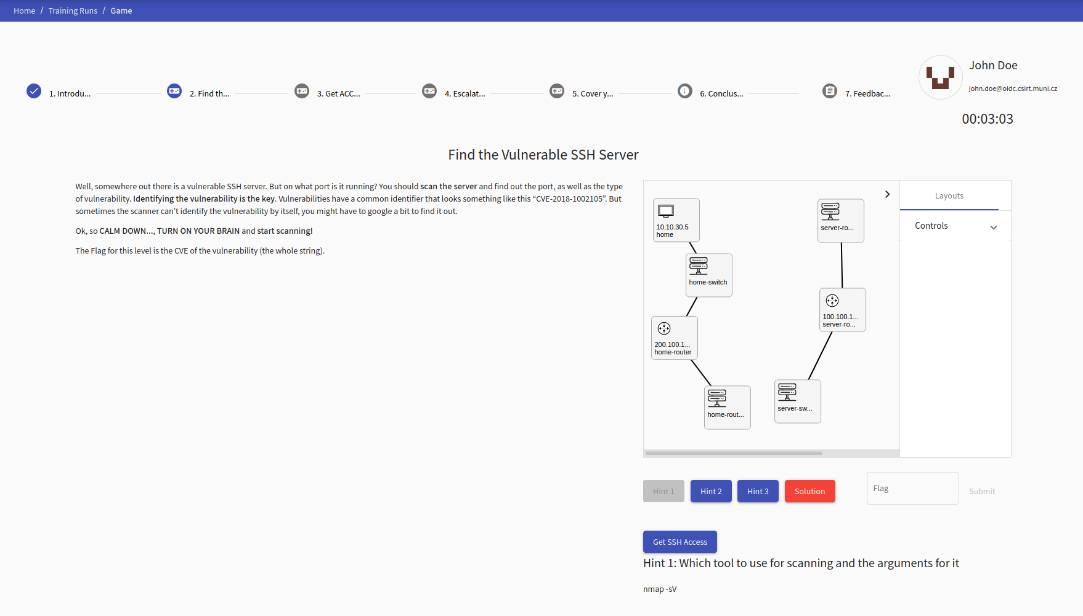


Figure 6.1: KYPO CRP User Interface

## Deploying KYPO CRP

KYPO CRP can be used in many ways and differently for each application. Next, we will deal with the recommended installation to meet the requirements of most institutions interested in the KYPO CRP platform evaluation.

### Requirements

This section describes what resources are needed for a successful KYPO CRP deployment. For successful KYPO CRP deployment is needed:

* fast Internet connection (at least 10Mbps),
* sufficient hardware resources,
* network Infrastructure,
* virtual or hardware appliance prepared KYPO,
* OpenStack installation in accordance with KYPO CRP requirements,
* KYPO CRP Proxy Jump Server (accessible from outside).

All the necessary software is downloaded from the Internet and a slow Internet connection prolongs the whole installation process.

Hardware recommendations are different for every server, Table 6.1 shows minimal requirements for running 10 average trainings.

Table 6.1: Minimal hardware requirements for 10 players

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Node** | **CPUs** | **RAM (GB)** | **Storage (GB)** | **Number of NICs** |
| KYPO | 4 | 16 | 50 | 2 |
| Controller | 10 | 16 | 50 | 2 |
| Compute | 20 | 128 | 1500 | 2 |

These requirements are sufficient, but not recommended. Recommended hardware requirements for 10 average trainings are shown in Table 6.2:

Table 6.2: Recommended hardware requirements for 10 players

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Node** | **CPUs** | **RAM (GB)** | **Storage (GB)** | **Number of NICs** |
| KYPO | 8 | 32 | 100 | 2 |
| Controller | 20 | 32 | 100 | 2 |
| Compute | 64 | 256 | 3000 | 2 |

In case using KYPO CRP for more users, it is recommended to increase hardware requirements proportionally.

KYPO CRP and OpenStack need two separate networks connected to the Internet (see Figure 6.2). One network is dedicated to management. Second network is dedicated as provider network for virtual appliances.

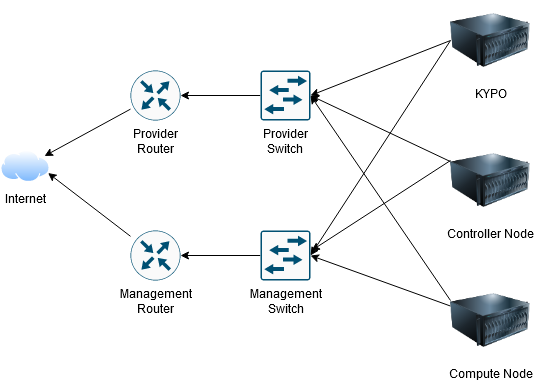


Figure 6.2: Network Infrastructure needed for KYPO

KYPO CRP Portal can be installed on physical or virtual server, it depends on the possibilities. Installing KYPO CRP on a virtual server has the advantage of being able to take snapshots of the entire machine if the administrator plans to modify the platform, for example. On the other hand, the installation of KYPO CRP on a physical server has the advantage that the operation of the KYPO CRP portal does not affect the compute node in any way.

It is necessary for the successful installation of KYPO CRP that the installation of OpenStack complies with the requirements of KYPO. Otherwise, the functionality could be reduced or the entire KYPO CRP platform could malfunction. The procedure for installing OpenStack in accordance with KYPO CRP requirements is included in the Appendix.

The KYPO CRP proxy jump server is absolutely necessary for the functionality of KYPO. Without this proxy server, KYPO CRP is not able to communicate with virtual machines. The procedure for installing the KYPO CRP Proxy Jump Server is part of the Installation chapter.

### Recommendations

Recommendations for the installation of KYPO CRP will be described in this chapter. In addition to the hardware recommendations described in the previous chapter, the recommendations will cover:

* Operation System Recommendation
* Disk controller recommendations
* RAID recommendation
* Network Infrastructure Recommendation

Table 6.3: Recommended Operation Systems

|  |  |
| --- | --- |
| **Node** | **Operation System** |
| Controller | Linux CentOS 8 |
| Compute | Linux CentOS 8 |
| KYPO | Linux Ubuntu 20.04.1 LTS |
| KYPO Proxy Jump | Linux Ubuntu 20.04.1 LTS |

For storage controller is recommended to use modern controllers. It is always necessary to verify the compatibility of the controller with the target operating system. For example, CentOS 8 no longer supports previously popular SAS controllers. This will cause drives and logical volumes not to be detected.

Regarding RAID recommendations, it is always recommended to choose the type of RAID (either hardware or software) to meet the redundancy condition. It is always recommended to reserve at least one disk in each disk array as a spare. For two disks it is necessary to select RAID1 (mirroring), for more disks at least RAID5. When selecting disks in a disk array, it is important to select disks that are designed to be in such a disk array. For example, hard disks with Shingled Magnetic Recording (MSR) technology are not suitable for use in a disk array.

It is also inappropriate to use an SSD of the same manufacturer and type in a RAID1 array. Each SSD has a limited number of overwrites before it fails, so theoretically when using RAID1, overwrites on both disks will be exhausted at the same time, so redundancy is not ensured.

The entire KYPO CRP architecture uses a network infrastructure for communication. In order for this infrastructure not to create the bottleneck of the whole system, it is necessary to design it appropriately. Due to the ever-increasing size of images and the complexity of configuration individual virtual machines, it is recommended to create the fastest possible connection between the machines, according to the current situation. It is recommended to use at least 10Gbps Ethernet to avoid network bottlenecks.

### Deployment at BUT

KYPO CRP was successfully deployed at BUT within the activities of the SPARTA project. KYPO CRP has been subjected to a stress test to verify that it can easily run many scenarios at once.

The following requirements were considered when designing the entire KYPO CRP deployment at BUT premises:

* long-term operation requirement,
* high load operation support,
* design for 50+ participants at once,
* requirement for future extensibility,
* local and remote access,
* readiness for integration with SPARTA JCCI (https://www.sparta.eu/JCCI/jcci\_home.html).

In order to meet all the requirements, we had for this solution, it was necessary to carry out the entire proposal. To meet the requirement for long-term operation, it was necessary to purchase hardware that will be fast enough for a few years. At the same time, it was decided that the controller node would be separated from the computer node, so that the whole solution could be extended to another computer node in the future.

The requirement for network operations requiring high network speed was solved by choosing 10Gbps ethernet as the standard. If the network caused bottleneck due to the speed of 10Gbps, all servers have twice as many interfaces than they need due to the possibility of a future upgrade, consisting in the creation of a 20Gbps bond to both the provider network and the management network. Of course, it is possible to choose, for example, 3 interfaces to the network provider and 1 interface to the management network, depending on the load, which would create a 30Gbps bond.

Due to the current pandemic situation, one of the requirements was the possibility of local and remote access to training. This requirement is ensured by the KYPO CRP platform, which is completely accessible via a web browser thanks to the use of the SPICE web console in the portal. Students' access to the laboratory will be provided by BUT VPN.

The whole KYPO CRP solution is relatively time-consuming to start, so in case of power outages, a backup power supply was purchased, which should be able to power all equipment for the time necessary to ensure electricity recovery.

These devices are used to run KYPO CRP at BUT (Figure 6.3):

Table 6.4: BUT Deployment Specification

|  |  |
| --- | --- |
| **Purpose** | **Device + Technical Specification** |
| Controller Server | SuperMicro Server (*X11SPi-TF Motherboard, Intel Xeon Bronze 3104 CPU, 32 GB DDR4 RAM, 1TB RAID 1 SSD)* |
| Compute Server | Dell ProLiant DL385 gen10 (2x AMD EPYC 7552 48-Core, 512 GB RAM, 1TB SSD RAID1 + 24 TB HDD RAID5) |
| KYPO Portal | HP ProLiant DL380 Gen9 Server (VMware vSphere 6.7 – Intel Xeon CPU E5-2630 v4, 128GB RAM) |
| Backup Server | Synology RS820RP+ (24TB RAID5 Storage) |
| Networking | Switch Mikrotik (CRS326-24S+2Q+RM, 24 SFP+ 10 Gbps ports, 2 QSQP 40Gbps ports)  Switch Mikrotik (only for management purposes – CRS-226-24G-2S+) |
| UPS | APC Smart-UPS C 1500 |



Figure 6.3: BUT KYPO CRP Rack

### Installation

KYPO CRP is built on the OpenStack platform. If you do not have OpenStack deployed, please see Appendix 6.A for installation instructions.

Before the actual installation of KYPO, it is necessary to obtain two important data:

* application Credentials from Open Stack,
* KYPO Proxy Private Key.

To obtain Application Credentials, you must log in to Horizon OpenStack service. After logging in, there is an *Identity -> Application Credentials* field in the left menu. Once opened, there is a Create Application Credentials button in the upper right corner. For Application Credentials fill in credentials from Table 6.5.

Once created, Application Credentials are displayed. Save this information (id and secret) for later use.

Table 6.5: Application Credentials details

|  |  |
| --- | --- |
| **Name** | kypo-unrestricted |
| **Description** | As you like |
| **Secret** | Leave blank (it will generate one for you) |
| **Expiration Date** | Intended expiration date (the longer the better) |
| **Expiration Time** | Intended expiration time |
| **Roles** | admin |
| **Access Rules** | none |
| **Unrestricted** | tick |

To obtain a KYPO Private Key, you first need to create this virtual machine. Before creating a virtual machine, you need to create a flavor for that virtual machine:

root@controller#~: source keystonerc\_admin  
root@controller#~: openstack flavor create --ram 2048 --disk 20 --vcpus 1 --public standard.small

After creating the flavor, you still need to upload the necessary image. We will check the available images:

root@controller#~: openstack image list

If there is no image named „ubuntu-focal-x86\_64“, we need to create it with:

root@controller#~: wget https://cloud-images.ubuntu.com/focal/current/focal-server-cloudimg-amd64.img -P /tmp/

root@controller#~: openstack image create --disk-format qcow2 --container-format bare --public --property

os\_type=linux --file /tmp/focal-server-cloudimg-amd64.img ubuntu-focal-x86\_64

After downloading and creating image, we create the machine:

Horizon -> Project -> Instances -> Create New Instance. Only few things are needed:

|  |  |
| --- | --- |
| Name | kypo-proxy-jump |
| Source | ubuntu-focal-x86\_64 |
| Flavor | standard.small |
| Networks | kypo-base-net |

After clicking “Launch Instance” the instance will be created. After creation it is possible to access Console via Horizon. In OpenStack, Instances are created using SSH with private and public key. To get to the instance:

root@controller#~: ssh ubuntu@(IP address of the Instance)

It will automatically connect you to this Instance. To get the KYPO Proxy Jump Private Key:

ubuntu@kypo-proxy-jump#~: sudo -i

root@kypo-proxy-jump#~: cat .ssh/id\_rsa | base64

This key needs to be stored in base64 format for KYPO CRP purposes. Also save the public part of the key (/root/.ssh/id\_rsa.pub).

Now it is time to Install KYPO CRP. It can be installed on virtual machine or physical machine. In both cases, it is recommended to use a graphical interface. Assuming the installation of a minimum configuration, it is necessary after installation run:

root@KYPO #~: apt update && apt upgrade

This command updates all packages to the latest version.

Before installation any other packages, it is needed to download and install via graphical interface:

|  |  |  |
| --- | --- | --- |
| Technology | UTL to Download | Version |
| VirtualBox | https://www.virtualbox.org/wiki/Downloads | 5.2.34+ |
| Vagrant | https://www.vagrantup.com/downloads.html | 2.0.2+ |
| Vagrant Disk Plugin | https://github.com/sprotheroe/vagrant-disksize | 0.1.3+ |

After downloading and installing this software, run:

root@kypo #~: apt install ansible python3-passlib git

root@kypo #~: pip3 install bcrypt

After installing it is necessary, to download repository of KYPO:

root@kypo #~: git clone git@gitlab.ics.muni.cz:muni-kypo-crp/prototypes-and-examples/kypo-crp-demo.git

After downloading the repository, open file “local-demo-extra-vars.yml”

root@kypo #~: nano local-demo-extra-vars.yml

And fill:

|  |  |
| --- | --- |
| Parameter | Value |
| kypo\_crp\_os\_auth\_url: | http://(IP address of management interface of controller) |
| kypo\_crp\_os\_application\_credential\_id: | Application Credential ID |
| kypo\_crp\_os\_application\_credential\_secret: | Application Credential secret |
| kypo\_crp\_proxy\_host: | IP of kypo-proxy-jump instance |
| kypo\_crp\_proxy\_user: | ubuntu |

Edit file /root/local-demo-secrets.yml:

root@kypo #~: nano local-demo-secrets.yml

And fill the base64 encoded private key after parameter *kypo\_crp\_proxy\_key: |-* (secret stars after dash).

Insert the content of the public part of the key to ~/.ssh/authorized\_keys file of the user, specified in the previous step on the VM (i.e. kypo-proxy-jump).

After configuration, we can use vagrant to build the create virtual machine with KYPO:

root@kypo #~: vagrant box update

root@kypo #~: EXTRA\_VARS=./local-demo-extra-vars.yml,./local-demo-secrets.yml vagrant up

### Troubleshooting

In this chapter are described the most common mistakes when deploying KYPO. Each version of OpenStack and KYPO CRP may have different installation problems, only those we encountered are described here.

**Problem: Ansible gets stuck on Restart nova-spicehtml5proxy container]**

Ansible cannot deploy OpenStack, gets stuck on “HTTPError: 404 Client Error: Not Found for url” when trying to download “spicehtml5proxy” package.

**Solution:**

Check configuraton file “/etc/kolla/globals.yml” for “nova\_console” parameter (expected “spice”). Then go to “ansible/roles/nova-cell/defaults/main.yml” and check line 34, if there is url for downloading the package, instead of:

image: "{{ nova\_spicehtml5proxy\_image\_full }}"

replace with:

image: "registry.gitlab.ics.muni.cz:443/cloud/kolla/centos-binary-nova-spicehtml5proxy:10.2.0-centos-8-w07"

After editing this file run “vagrant provision” once more.

**Problem: After successful change from NoVNC to SPICE cannot connect to any console**

When changing NoVNC to SPICE, there is an error connecting to console.

**Solution:**

SPICE console is configured when instance is created. There is need to delete all instances and deploy all instances again. That should fix the problem.

**Problem:**

When changing NoVNC to SPICE console, there is an error connecting to console.

**Solution:**

SPICE console is configured when instance is created. There is need to delete all instances and deploy all instances again. That should fix the problem.

**Problem:**

When changing NoVNC to SPICE console, there is an error connecting to console.

**Solution:**

SPICE console is configured when instance is created. There is need to delete all instances and deploy all instances

## Using KYPO

KYPO CRP is by default accessible on IP address 172.19.0.22 (or whatever address that is in the config file). KYPO CRP is web-based service, for accessing it, type in the browser url: https://172.19.0.22/. You should be redirected to the Authentication Service OpenID. By default, the credentials are as follows:

* **Admin user:** kypo-admin
* **Regular user:** kypo-user, john.doe, jane.doe
* **Password for all of them:** password

After logging in, the portal should be available, which looks like on Figure 6.4:

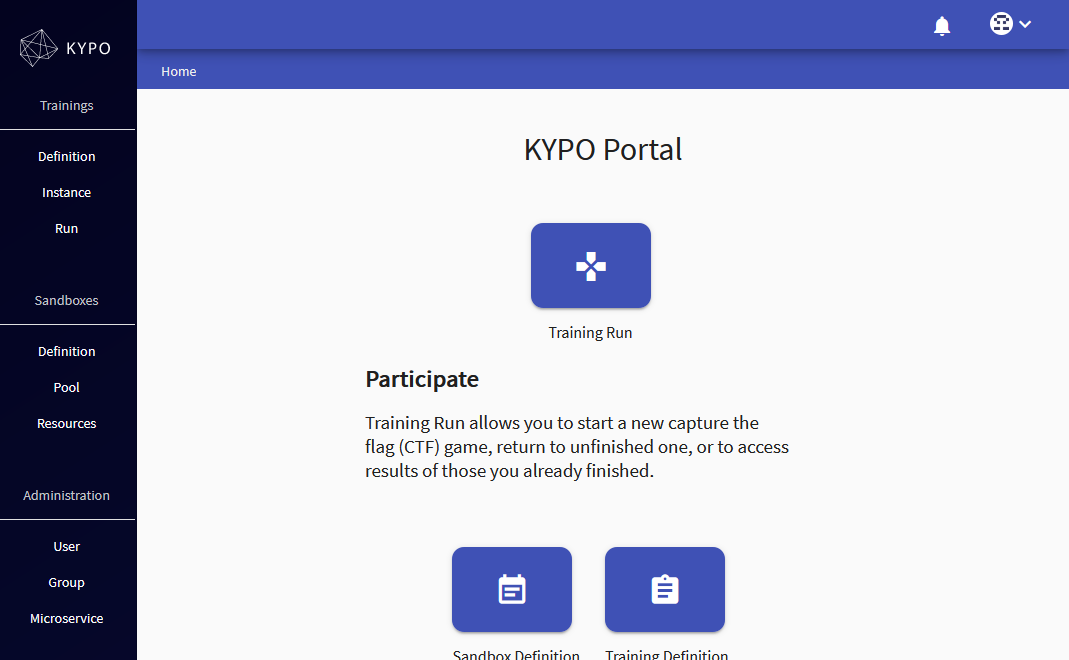


Figure 6.4: KYPO Portal

On the left side is navigation panel.

New users can be created in OpenID portal, that is accessible on:

<https://172.19.0.22:8443/csirtmu-dummy-issuer-server/usersList>

If you would like to add a new user, use this link:

<https://172.19.0.22:8443/csirtmu-dummy-issuer-server/usersNew>

KYPO Portal uses external authentication, that means, it does not know about newly created users in OpenID Portal. For using these users, it is necessary to log in to KYPO Portal.

After logging in these new users has to be added to “Training Trainees” Group, to get access to trainings.

On the left side there is a navigation panel in the graphical user interface. Trainings are defined in Training section. This means the graphical interface and the story of the individual trainings, including the determination of flags and points. This is followed by the Sandboxes section, which is in charge of the technical side of the training. Sandbox defines environments for running training, such as networks, IP addresses, routers, switches, computers, servers, settings, program installation, etc. The last group is Administration, where users, groups and microservices can be managed.

### Example Scenario

By default, KYPO CRP has a demo scenario included. This example scenario is intended to demonstrate the possibilities and capabilities of this platform.

First task is to scan open ports on a machine to find open telnet port (see Figure 6.1). To comply, the user must be familiar with the tools for scanning ports and their use. After a successful scan, the number of the found port is flag.

Second task is to do a dictionary attack on the telnet service. The student's task is to get acquainted with the tools for attacking services and dictionaries with the most common passwords. After a successful attack, the flag in the user's root folder is a text file.

Third and the last task is to escalate privileges. The student has access to a standard user account. The task is to escalate permissions so that it can execute commands as root. The principle of the task is to find the processes that are run as root and take advantage of this fact.

This Example scenario can be run as follows. The training definition must be loaded first. Download Training Definition from:

https://gitlab.ics.muni.cz/muni-kypo-trainings/demos/muni-kypo-trainings-demo-training

the Training Definition is in the training.json file. This file must be uploaded to: KYPO Portal -> Trainings -> Definition -> Upload and choose previously downloaded training.json file.

Subsequently, the sandbox definition must be selected and then the sandbox definition must be selected. For this training, a sandbox definition is prepared on the internal git at:

git@git-internal-ssh:/repos/prototypes-and-examples/sandbox-definitions/muni-kypo-trainings-demo-training

Paste this path into: KYPO Portal -> Sandbox -> Definition -> Create. As revision type “master”.

After successfully creating a training and sandbox definition, you need to create a Pool. The pool can be created in KYPO Portal -> Sandboxes -> Pool -> Create. Select number of sandboxes (1 for example) and press create. After creation you can press the Allocate Sandboxes icon to start allocation of the pool.

The final step is to create Training Instance in KYPO Portal -> Training -> Instance -> Create. In this particular case, choose:

* Title – name as you like
* Start Time - now
* End Time – select end time
* Access Toke Prefix – prefix for token, for example “demo”
* Training Definition – select previously created Training Definition “Uploaded KYPO Cyber Range Training Platform – Demo Training”

And Click at Create and Continue Editing. After that, in Pool section select previously defined pool and click Create. After creating Training Definition, access token should be visible in the Training Instance table. This token then can be used in KYPO Portal -> Training -> Run. Type this token and start playing.

### Creating New Scenarios

To create new scenarios can be used the Cyber Sandbox Creator tool. This tool can be downloaded from:

https://gitlab.ics.muni.cz/muni-kypo-csc/cyber-sandbox-creator

or

root@kypo-sandbox-creator #~: git clone git@gitlab.ics.muni.cz:muni-kypo-csc/cyber-sandbox-creator.git

In order to be able to use Cyber Sandbox Creator fully, certain things must be fulfilled. Because the platform works with a virtualized environment it is necessary to enable virtualization in the BIOS. If this step is not met, the created environment will not work. We will then install third party programs that the Cyber Sandbox Creator runs is Ubuntu 20.04. The reason for using this operating system is that it contains the latest packages and dependencies.

First, we installed the python3 and python3-pip packages:

root@kypo-sandbox-creator #~: apt install python3 python3-pip

Python3 is required for the actual launch of the platform and python3-pip will allow us to install later libraries for the python3 programming language.

Cyber Sandbox Creator uses VirtualBox as virtualization software. VirtualBox can be installed:

root@kypo-sandbox-creator #~: apt install virtualbox

If we have virtualization software installed, we can install the virtual environment manager. The Vagrant program will play this role. Vagrant can be installed:

root@kypo-sandbox-creator #~: curl -O https://releases.hashicorp.com/vagrant/2.2.9/vagrant\_2.2.9\_x86\_64.deb

root@kypo-sandbox-creator #~: apt install ./vagrant\_2.2.9\_x86\_64.deb

The last program that needs to be installed is Ansible, which provides the management of virtual machines after their initial startup. Ansible can be downloaded from:

root@kypo-sandbox-creator #~: apt install ansible

After successful installation of all programs, it is necessary to install the necessary libraries for the *python3* programming language. The first installed library is named setuptools. Use this command to install:

root@kypo-sandbox-creator #~: pip3 install setuptools

For the next procedure, we must go to the sandbox-creator folder.

root@kypo-sandbox-creator #~: cd sandbox-creator

The folder contains the requirements.txt file, which contains the names of the required libraries and their versions. We installed them with the command:

root@kypo-sandbox-creator #~/sandbox-creator: pip3 install -r requirements.txt

## Piloting Cyber training Exercise

### Laboratory Settings

KYPO was configured as a local service, so proxy server settings on all client web browsers were required for access. Furthermore, KYPO was configured to use a local authentication authority, which meant that each user had their own user account, their own sandbox, and also their own training.

The network was configured according to standard procedures, one management network and one provider network. Furthermore, it was necessary to arrange the connection of local computers, which were connected to the management network, from which it is possible to access the network provider. Remote users were connected to a VPN network with a different scope, but routing to both the management and the network provider was provided here.

Users were divided into local and remote, both groups had different prerequisites for connection to the infrastructure. In the case of local users, everything was set up in advance and tested locally on laboratory computers, so there were no complications and users did not have to configure anything further (see Figure 6.5). The situation was different for remote users who had to be connected via VPN, when these users first had to download and set up a VPN client, and only then could they start the training itself.

A simple guide was created for both groups of users, which guides the student through the entire process of connecting to the training. The manual also included a chapter on the most common errors, where the most common configuration errors were described and how to eliminate them.

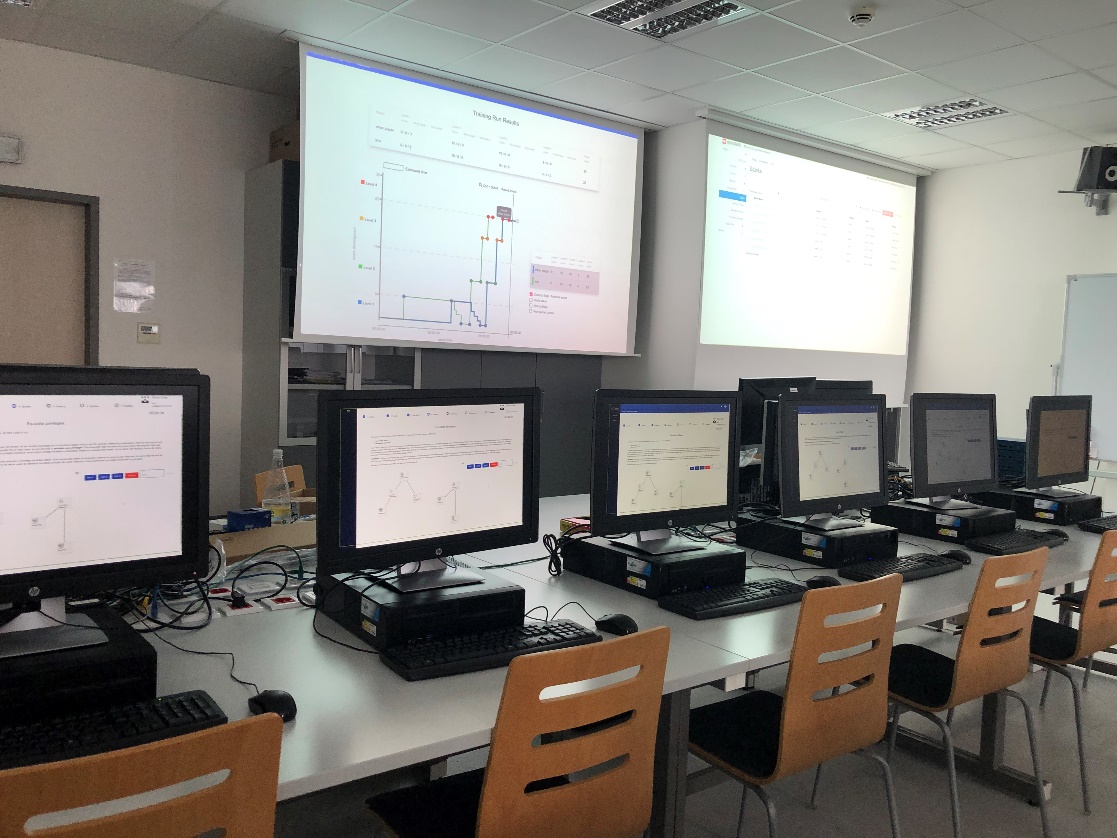


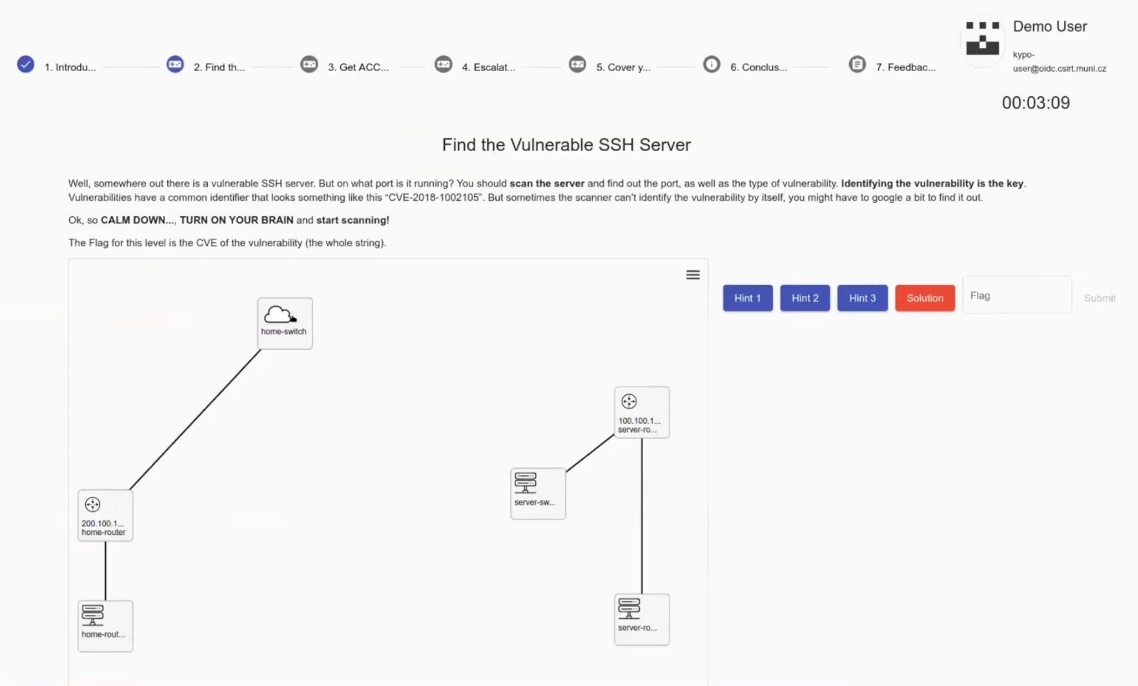
Figure 6.5: BUT Laboratory with running KYPO

### Training Scenario

The purpose of this scenario is to demonstrate the features of KYPO CRP while testing that all features are working properly. The virtual machines in this scenario can be accessed using a Web browser and SSH. In addition, the scenario includes tasks that require access to multiple devices and internal relatively complex networking settings. Last but not least, the scenario aimed to demonstrate the functionality of the BUT environment.

The student's first task was to find a vulnerable SSH server (see Figure 6.6). On this task, the student had to get acquainted with its virtual infrastructure and identify individual computers. After finding the target computer, it was necessary to select the correct tool for this attack and run it correctly. The flag of this task is the port number of the detected vulnerable SSH server.

The second task was to find a suitable tool to exploit a vulnerable SSH server and use this tool (see Figure 6.7). The flag was then in the home directory of the compromised user.

Figure 6.6: First task

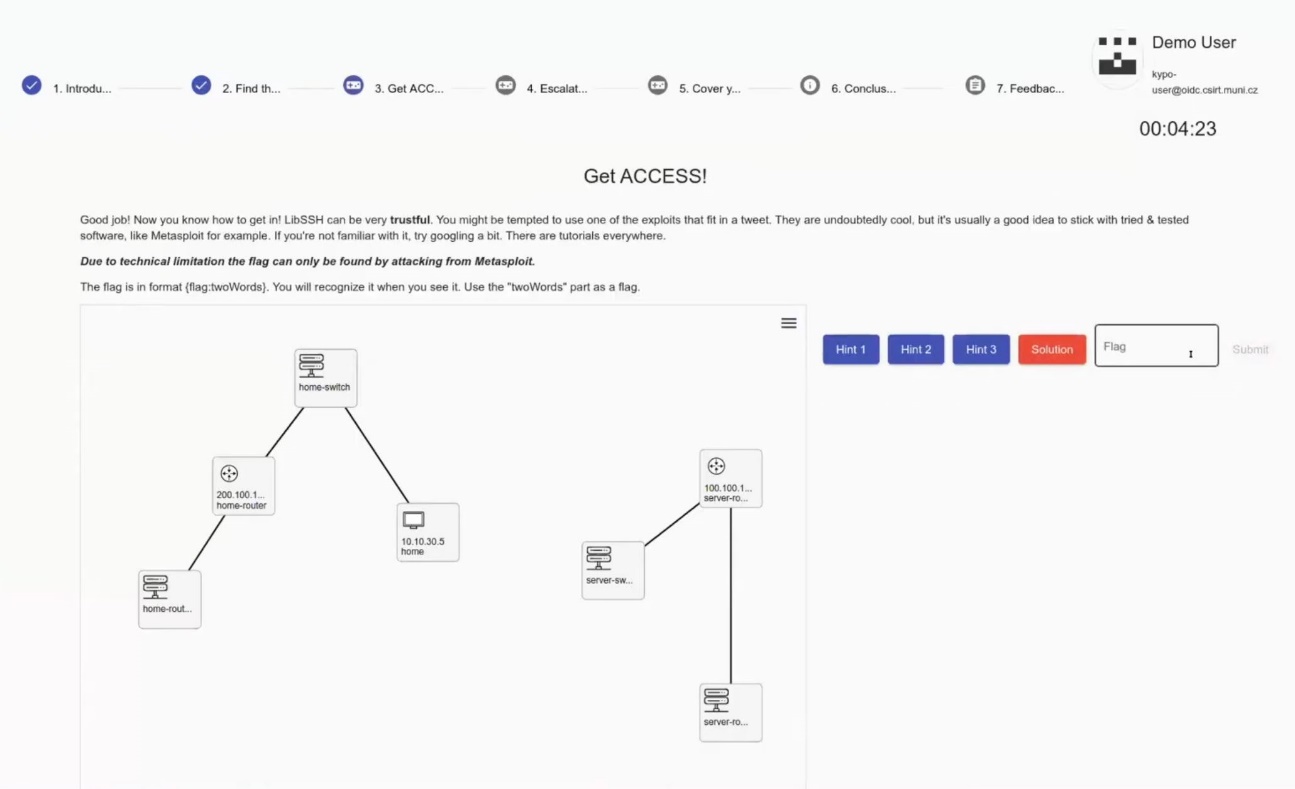


Figure 6.7: Second task

The third task is to increase permissions (see Figure 6.8). A broken user is a standard non-root user. The student's task is to find a way to increase this authorization. The flag for this task is located in the home directory of the root user.

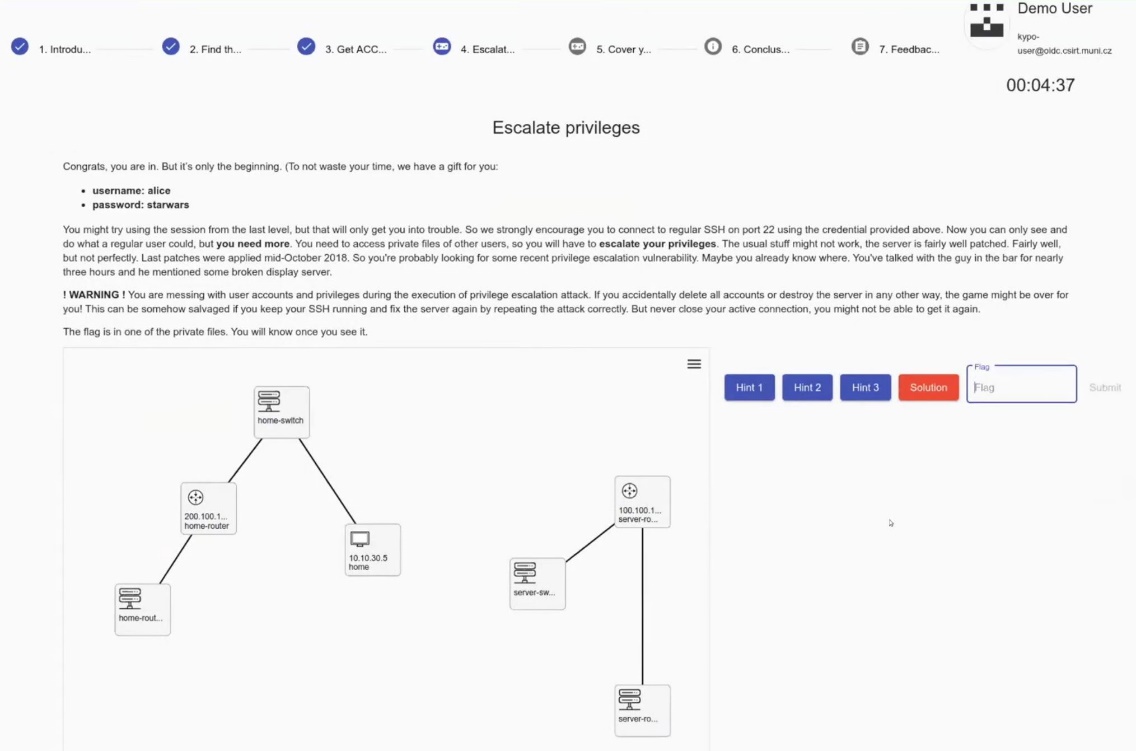


Figure 6.8: Third task

The last task is then to erase the tracks. In this step, the student will learn where the system stores logs or used commands (see Figure 6.9). There is a flag in one of these files.

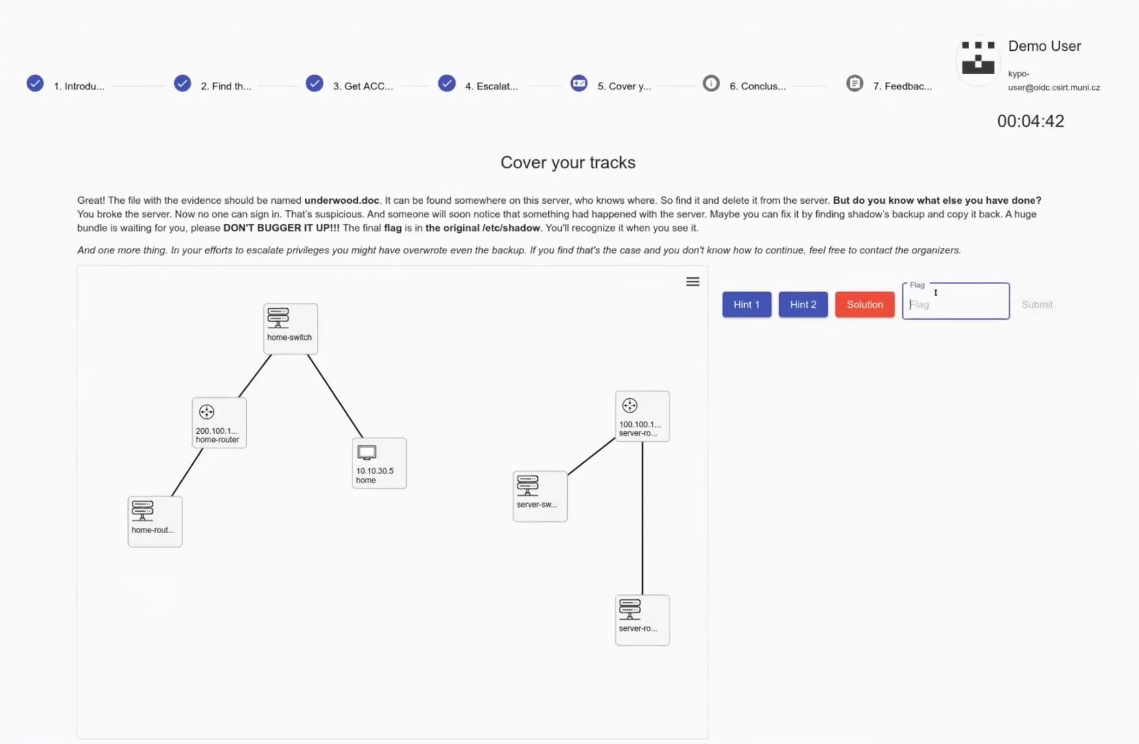


Figure 6.9: Fourth task

Scoring was set so that the student received 2 points for completing the task. In case of using the help, he received a penalty of 1 point. If the student viewed the solution of the task, he received a penalty of 2 points, so he did not get any points in the result (see Figure 6.10).



Figure 6.10: Scoring board

Now, after stress testing, we can say that most things were working, but there were 3 problems. The first problem was with the proxy server used, which behaved unstably under heavy load and the service restarted twice, causing the console sessions to restart.

The second problem we encountered was overloading the controller. In the initial design, the controller was not expected to be computationally exploited in this way, so performance was not given priority. Our controller had 6 computing cores without hyper trading and all cores were used to 100% load during the creation of instances, which slowed down the process of creating trainings.

The third problem was a poorly chosen network node service on OpenStack. This particular network node caused it to take longer to create more networks with a larger number of networks, which led to a situation where additional networks could not be created due to internal timeouts within OpenStack.

The time required to create these trainings was not large at the beginning, however, due to the limitations described above, with each subsequent training, the creation was longer. The first training took about 8 minutes, the last around 2 hours. These problems can be solved by increasing the performance of the controller and choosing a more powerful network node.

### Pilot Evaluation

We can now say that the pilot testing was successful. On all tested stations and computers, all users successfully completed the entire training without any major problems.

After completing the tasks, users were asked for feedback (see Figure 6.11). Most users stated that they did not have any serious problems with the use of KYPO CRP and were satisfied with the training.

Obsah obrázku text

Popis byl vytvořen automaticky

Figure 6.11: Feedback

In terms of performance, the compute node showed no signs of poor performance. At full load, it had a load of around 5-7 (linux format), which corresponds to approximately 3% load, as the computing server has 196 threads available. Around 50 GB of RAM was used and about 1.5 TB was used on the HDD. But the situation on the controller was different. The controller, especially when instantiating, was permanently around 12, which corresponds to approximately 200% load (a total of 6 threads). This caused slow training loads or line generation on the virtual machine console.

Another improvement will be in the elimination of problems that we have detected by stress testing, especially the increase in the computing power of the controller and the replacement of the network node service on OpenStack.

After eliminating these problems, it is planned to develop and test other scenarios and connect these scenarios to the real infrastructure, especially the industrial one (see Figure 6.12). One of the goals is to connect the Cyber Range laboratory with the Critical Infrastructure Equipment Laboratory, which contains electricity meters, control centers and concentrators used to measure electricity consumption (see Figure 6.13, 6.14). Here is possible to perform demonstrations of escapes to these devices and defenses against these attacks.

|  |  |
| --- | --- |
|  |  |
| Figure 6.12: Automation laboratory | Figure 6.13: Critical Infrastructure Equipment Laboratory |



Figure 6.14: Critical Infrastructure Equipment Laboratory

# UBO – a framework to measure IT-Security Awareness within working staff

Cyber security is not improved solely by the knowledge of the humans that are interacting with an IT infrastructure, but their behavior. Hence, training and exercise activities should be measured by the change in behavior they induce. To this end, the University of Bonn developed a framework to measure IT security awareness within working staff [44]. The framework consists of a method and a software toolkit implementing that method. This framework can capture employees behavior and analyze it for the expression of IT security awareness. Hence, it targets the group of employees (cf. Section 2.1) and their expression of Human Security (cf. Section 2.2). For the remainder of this document, employees that are to be tested for their IT security awareness are called participants. Within this chapter the framework is described, subsequently the installation procedure of the toolkit is described, and finally a possible use case is laid out.

## Description

The framework can be used to quantify the training effect of an awareness exercise. Hence, the framework facilitates the comparison of different exercises based on effectiveness. It may be tailored to identify gaps in employees’ security awareness within the targeted knowledge area. In the remainder of this section the method of artifact-based assessment of IT security awareness is described and the accompanying software toolkit itsape: IT Security Awareness Penetration Testing Environment is introduced.

### Artifact-based Assessment of IT security Awareness

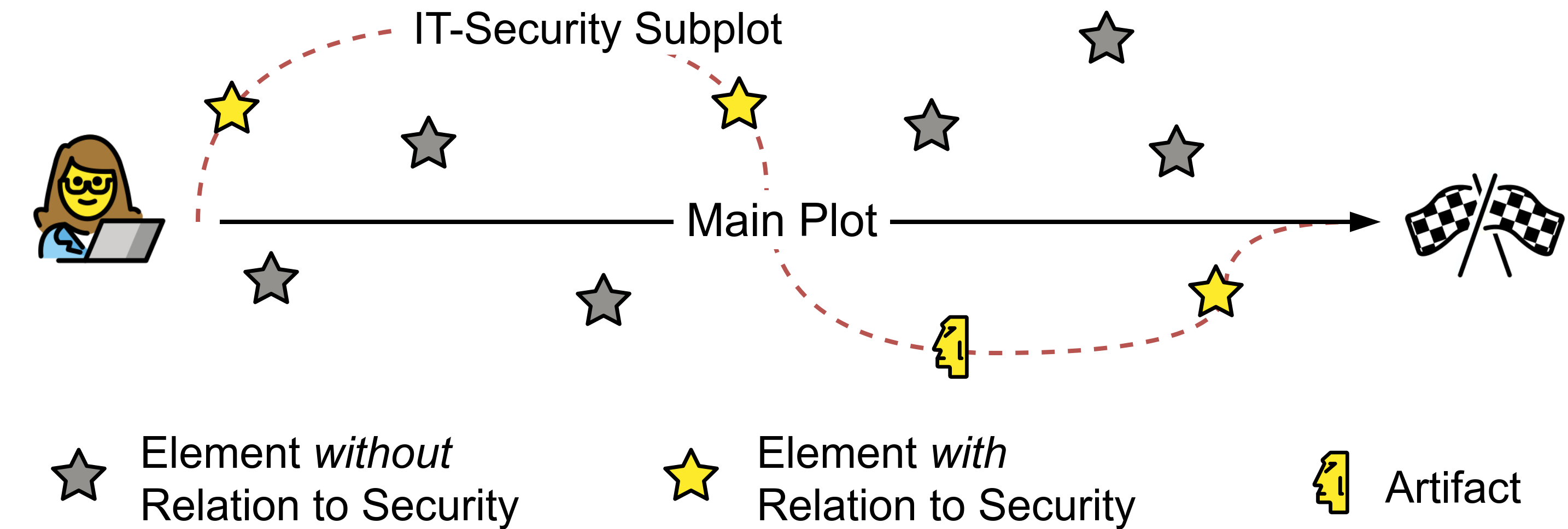
Testing is conducted during day to day operation of employees within a company. A user does not use the computer to *achieve* cyber security, but they pursue a goal nonetheless. During the usage of the computer, a user perceives and interacts with different elements in order to achieve her or his goal, whatever that may be. Some of these elements relate to IT security, some do not. An illustration of this model may be found in Figure 7.1.

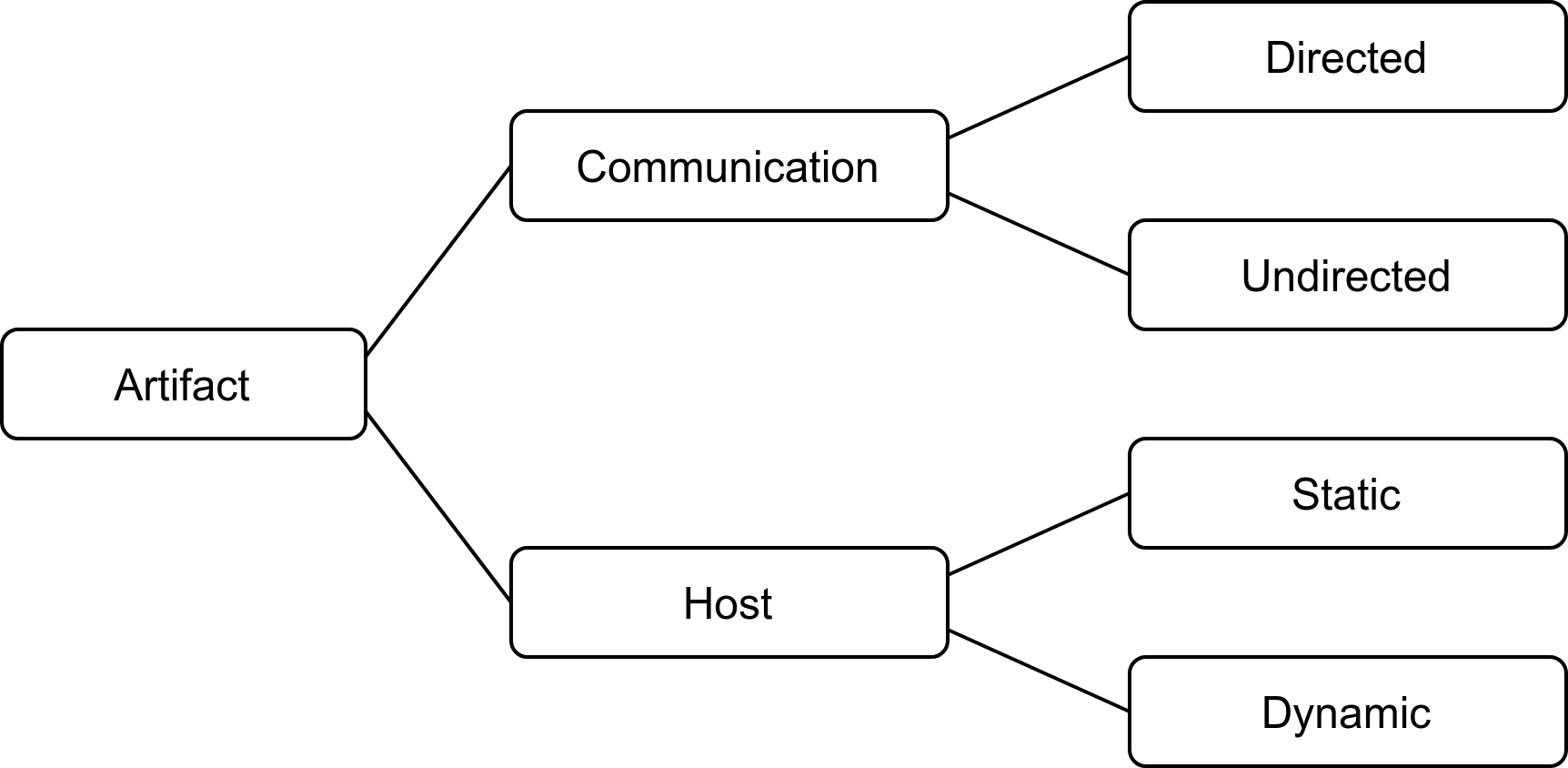
Figure 7.1: Situation model of terminal work

The way a user handles elements with relation to security is an expression of their IT security awareness. In response to these security-related elements, a user might take action. This action may influence the security of the IT infrastructure as a whole. This influence might potentially impact security negatively, e. g., clicking on a link of a phishing email, or positively, e. g., reporting the phishing email to the IT support so that the spam filter might be adjusted. Actions that do not affect security are out of scope.

The monitoring of all possible elements and actions a user takes is not feasible. Therefore, an *artifact* is inserted into the user’s sphere of activity and the user’s reaction to that artifact is captured and analyzed subsequently.

#### Artifacts

The most basic form of this method is known by the name of *phishing experiments*. However, phishing emails are only one possible realization of an artifact. Artifacts are the carrier of the stimuli for the user. We were able to identify 4 types of artifacts, which are pictured in Figure 7.2 with their interdependence. Artifacts may either be attributed to the host or communication. Phishing mails are the prime example of *directed* communication-based artifacts. As an example for *undirected* communication-based artifacts, the defacement of a website can be used. There might be code fragments or errors visible to the visitor of a website that is suffering from an ongoing injection attack. An example for *static* host-based artifacts are placed files, like the background of a virtual disk [45]. *Dynamic* host-based artifacts are process-related, e. g. the resource consumption of a cryptocurrency mining process [43]. We assume most users already had contact with phishing artifacts, they may even be familiar with them. The remaining types are expected to be more of an obscure nature to users.

Figure 7.2: Classes of possible artifacts

#### User Behavior Analysis

Within an enterprise environment, the amount of possible user actions that affect IT security is limited. Users are commonly only able to initiate a security increasing or restoring process by reporting to the user’s support. This event is denoted with in Figure 7.3. The user’s interaction with an artifact has to be considered potentially harmful to the security of the infrastructure. This interaction is shown in Figure 7.3 as .



Figure 7.3: Combinations of user reaction classes

Figure 7.3 shows all possible combinations of events. If the participant does not interact with the artifact but reports it, i. e., , we assume the user has perceived the artifact but did not choose to interact with it and rather contacted the support. The worst possible outcome of an attack scenario occurs when participants interact with the artifact but do not choose to contact the support, . In this case, an attacker is able to pursue his or her objective undetected. It is the case where the participant demonstrated definitive unawareness regarding IT security. In all other cases, we assume the user to be aware. A measurement for IT security awareness of an individual based on these events may be given as the estimated probability of the complementary event of :

However, estimation of a group of individuals may be different. Assuming a organization of *n* individuals, an attacker might act as long are *one* individual interacted with the artifact and *no* individual reports the incident. Naturally, this poses a higher emphasis on the reporting of the incident. The IT security awareness of a group may be modeled by:

### itsape: IT-Security Awareness Penetration Testing Environment

The software toolkit that is able to support artifact-based IT security awareness measurement is called *“itsape: IT-Security Awareness Penetration Testing Environment”*. The main component is a server application that facilitates control and scheduling of individual test cases as well as the capture of the user reactions to the artifacts, called the *artifactomat*. Artifacts are constructed and optionally personalized to the recipient by *recipes* as a form of a construction plan. A recipe contains all configuration specific to the artifact itself:

1. Scripts to generate and deploy the artifact.
2. Scripts to generate supporting infrastructure elements, e. g. web server.
3. Scripts to monitor the artifact to detect problems during test execution.

The deployment of artifacts is supported by a client application that is used to present artifacts to the users and monitor the presence of the user to be tested. After test execution, captured user reactions can be exported from the server to be evaluated. Exported data is pseudonymized to protect the individual’s privacy. To evaluate a training or exercise action’s effect, measurement has to be taken before and after intervention. However, measurement is highly dependent on the artifacts used and therefore should be conducted as a post-only experiment with a control group.

The publication of the toolkit as an open source project is an ongoing effort of the University of Bonn within the SPARTA project.[[7]](#footnote-7)

## Installation Procedure

This section documents the general installation procedure. The toolkit is under active development. Hence, installation procedures are prone to change. This document will reference original documentation wherever possible in order to avoid inconsistencies. First the testing environments requirements are described. Following, the installation for each component is laid out.

### Requirements

Using the itsape toolkit requires a server component, the *artifactomat*. It has to be directly accessible by all clients within the company by TCP and UDP on IPv4 under a static IP address on all ports. Proxies and firewalls may render the usage of the toolkit impossible. IPv6 is currently not supported.

Table 7.1 depicts the artifactomat’s system requirements for ~300 participants and ~5 active artifacts at the same time. Values may need to be adjusted for larger deployments. A dedicated server is assumed.

Table 7.1: System requirements of the server

|  |  |
| --- | --- |
| Minimal | Recommended |
| 4 CPU cores with ≥ 2GHz frequency | 8 CPU cores with ≥ 4GHz frequency |
| 128 GB HDD | 512 GB SSD |
| 8 GB RAM | 32 GB RAM |
| 1 Gbps link speed | 10 Gbps link speed |

All clients need to run Windows 10 (64bit). Hardware specification is detailed in Table 7.2. Application of a software distribution solution is *strongly recommended,* because the client component needs to be installed to every participants computer. Participants need to use personalized accounts to log in to their working station. Generic or group accounts are not supported.

Table 7.2: System requirements of the clients

|  |  |
| --- | --- |
| Minimal | Recommended |
| 2 CPU cores with ≥ 2GHz frequency | 4 CPU cores with ≥ 4GHz frequency |
| 100 MB free disk space | - |
| 4 GB RAM | 8 GB RAM |

Requirements to use the toolkit within a working environment is not only technical by nature. Informed concent of every employee taking part in the measurement of the IT security awareness of the working force has to be given prior to testing. According to german law, this concent may be given by the proxy of a working council. However, national law applies.

### Clients

The client is provided as Windows Installer package (.msi)[[8]](#footnote-8). It needs to be installed on all workstations targeted. Installation by software distribution solution in strongly recommended.

### Server

1. The dedicated server is to be installed with Debian stable. At the time of writing 10.9, codename “buster”. Additional software according to the specific provisioning script[[9]](#footnote-9) is required:
2. Install additional software from the Debian software repository: ipset autoconf build-essential dpkg-dev libssl-dev libyaml-dev libreadline6-dev linux-headers-$(uname -r) zlib1g-dev libncurses5-dev libffi-dev libgdbm6 libgdbm-dev liblzma-dev libpq-dev libsqlite3-dev git bison libgdbm-dev ruby postgresql postgresql-client vim zsh screen dnsutils dkms netcat redis-server unzip psmisc gawk tcpdump python3 python3-pip python3-venv python3-setuptools python python-pip python-setuptools gnupg2 aptitude libsystemd-dev
   1. Ruby 2.6.3 has to be installed form source. The software relies on this specific version. However, this may change with an update.
   2. Install Docker from upstream
   3. Enable iptables and ip forwarding
   4. Install setuptools, wheel, and olefile by PyPI.
3. Setup the database by adding a user and increasing the allowed connection pool to 500 connections.
4. Since the software is open source (in the process of publishing at the time of writing), installing may be done by the respective package managers: To install the reporting module[[10]](#footnote-10) run:
5. sudo pip install awarenssometer
6. To install the artifactomat[[11]](#footnote-11), the core component of the toolkit, run:
7. sudo gem install artifactomat
8. Generate needed certificates according to the documentation in /etc/artifactomat/certs.

A test recipe, which does not generate a user visible effect, is placed at /etc/artifactomat/recipes. It may be used to test the installation and may serve as a template for recipe development. In order to profit form a baseline it is recommended to choose a fraction of well known artifacts (c.f. [44]). Building custom recipes tailored to the environment is a services offered by UBO.

## Use Case

Itsape supports the quantification of the effect of any kind of intervention to the IT security relevant behavior of employees. Possible interventions are changes to the infrastructure or organization, changes to the interface of the user, e. g., applications or operating system, as well as classical advertisement campaigns or classes. The only requirement is, that the tested employees may be separated into two groups, the employees exposed to the intervention and those not exposed for reference. This section describes the use of itsape in four phases: *Preparation, Pre-test, Intervention, Post-test*. Subsequently the results of a prototype study are summarized.

### Preparation

During Preparation Phase the following actions need to take place. Figure 7.4 illustrates the Preparation Phase with regard to support by the toolkit itself.

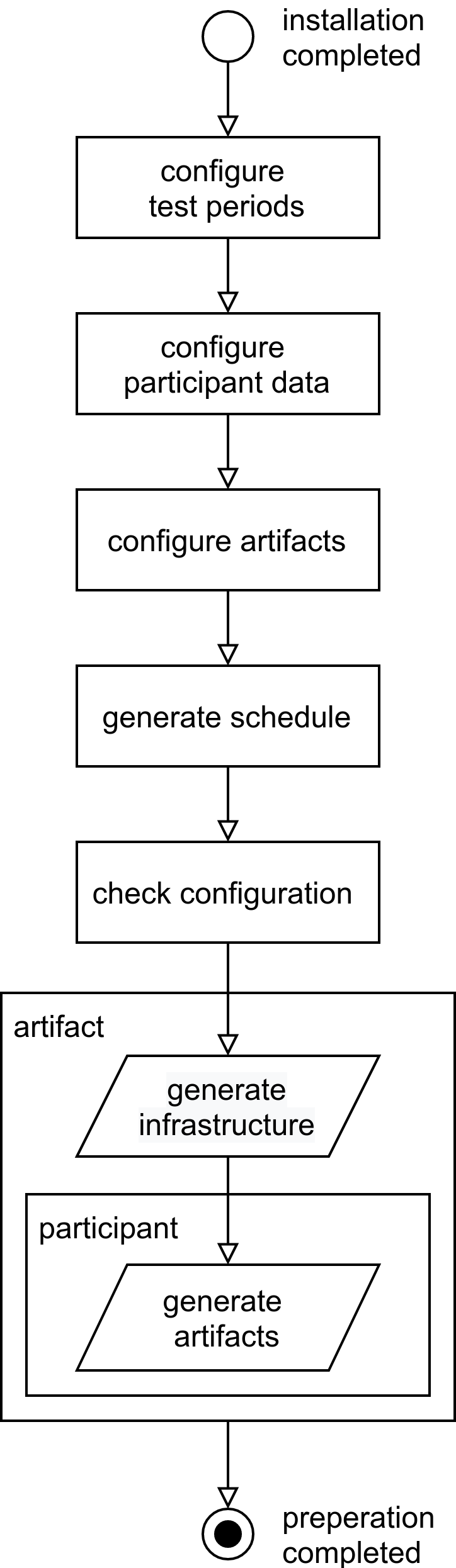
1. A test installation should be setup with the artifactomat and one client.
2. This test installation should be used to develop and test a battery of artifacts. Preliminary observations suggest a number of five artifacts per measurement [44].

Figure 7.4:Preparation phase within the artifactomat

1. Installation of the client to all workstations in question and verification of their operability by the included not user visible artifact.
2. All possible courses of action from the environment should be monitored, e. g. if a user may call a helpdesk or 1st-level support, calls of participant need to be captured and analyzed for a relation to the artifact. Hence, a technical interface has to be implemented to pass a list of participants that reported an artifact to the artifactomat. If local law forbids inference of the contents of the call, close timely proximity to the presentation of the artifact may be used to assume a relation to the artifact.
3. The measurement periods need to be set. This relates to the first step in Figure 7.4. 1st-level support needs to be informed about the test and the specific artifacts used. Testing might lead to an increased volume of support requests and the support employee needs to know which user reports reflect artifact sightings and which may indicate a real threat and should trigger security processes. The time period of the actual measurement should be large enough, so that the user does not suffer from increased cognitive load. However, if the period of time is chosen too long, the environments influence on the measurement increases. A period of one month per measurement period (five artifacts) is advised.
4. Participants may need to be selected and informed consent has to be sought form the employees to be tested. This may be achieved, either by proxy of a working council [44] or by opt-out enrollment with semi-informed consent [4]. Personal data has to passed to the artifactomat. Navigate to /etc/artifactomat/subjects and configure the targeted participants according to the readme.md within that folder.
5. Place the recipes in /etc/artifactomat/recipes and configure the artifacts that should be used in testing.
6. Generate a schedule. The artifactomat will roll out artifacts to participants at random, evenly distributed over the testing period, set in Step 5.
7. Check whether the configuration reflects the intended implementation. If not, go back to step which corresponds to the diverging configuration. If the configuration is as intended, proceed.
8. Start the preparation procedure. During this procedure infrastructure required by the artifact, e. g., webserver or man-in-the-middle proxies, will be generated from the recipe's configuration. Subsequently artifacts themselves are dynamically generated and fitted to configuration by participant. This concludes the Preperation Phase.

### Pre-test

During pre-test phase, all participants are scheduled to be tested by each artifact. The test execution from the perspective of the artifactomat is illustrated in Figure 7.5. The artifact supporting infrastructure is continuously monitored. If an error impairs infrastructure availability, a test is not started or ended immediately. Is the infrastructure available, the client will be activated and continuously monitor the participant activity by log-in events. If a participant is not at her/his desk when the test starts the test will be automatically deferred as long as the test schedules allows it. If it cannot be deferred further the tests is skipped. If the participant is logged in at the working station the artifact will be presented. After the artifact is presented, the subjects reactions are monitored until the test period expires. The client will be deactivated.

After the test is concluded and all reactions are collected, a debriefing should be send to all participants. Employees need to be made aware of the new purposes of data processing [47].

### 

Figure 7.5:Test execution within the artifactomat

### Intervention

Participants need to be split in two groups. One group receives the intervention, the other serves as control group. If the intervention is invite-based and the assignment to the treatment group may not be performed at random, motivational effects may influence the measurement, known as selection bias. In order to control selection bias it is advised to split the treatment group, participants that are willing to receive the treatment, into two groups. One group should receive the treatment before the post-test phase, the other group after. This may be achieved by limiting the group size and choosing the groups at random. This approach allows for controlling motivational aspects to the treatment.

### Post-test

Artifacts used in the post-test have to be different form the artifacts used in the pre-test. After the Post-test is concluded the clients may be removed from all workstations by the management method of the software distribution solution. Captured reaction data may be exported from the *artifactomat* and passed to the *artifactometer* for evaluation support.

The effect size can be measured by comparison of the average individual and organizational IT security awareness between the group that received the treatment and the group that did not. In case of an invite-based enrollment of participants to the treatment selection bias needs to be controlled. This is achieved by comparing the group of participants that received treatment with the group that did not have received treatment yet. To ensure that the effects did not exist prior to group selection, the displayed degree for IT security awareness may be compared within all groups on artifacts of the pre-phase.

To check for the effect of the selection bias by invitation, the group that responded positively to the invitation and hence, show themselves motivated, should be compared to the group that actually received the treatment.

## Test Pilot

This toolkit was deployed in the administration of one of Europe's larges health centers. The effect of an IT security awareness class was measured. During testing we were able to demonstrate that a common class aiming to increase IT security awareness may have a undesirable effect on user behavior [44]. The following sections describes the Pilot briefly.

In the Pre-test Phase 196 employees, working in departments outside of critical patient contact, were selected for participation in the study. Since participation is dynamic in an uncontrolled environment, not every participant participated in every test scenario. A scenario is passed by 51.25 participants on average. However, one participant passed 5.47artifacts on average.

52 participants voluntarily participated in the intervention. 50 expressed their interest either by email or phone, asking for more appointments, because they were unable to attend on proposed appointments. 94 participants did not respond to our invitation.

The interventions design goal is to resemble a commonly bought IT security awareness training, similar to the ones required to be held annually in order to receive security certification. The intervention is designed and held by a company having more than 15 years of experience in the field of penetration testing, security focused consulting, and IT security education. It was designed as a 60 minute, teacher-centered lesson. The lecturer presented slides and held a live presentation on artifacts and possible reactions. The goal was to deliver a commonly booked standard experience.

An introduction to the motivation of threat actors was given and the assumed role of the employees in an attack scenario was explained. Further content covers these five topics: Emails, Password, Browser, Physical Media, and Mobile Devices. After the lecture there were 15 minutes for open questions, followed by a 15-minute summary.

Additionally to the class, an e-learning platform was implemented, where five videos were hosted (average length 9:12 minutes). Each video recapitulated one of the topics and was accompanied by a short test of 10 questions regarding the content. After the test is completed, the result is shown. For each question the answer, given by the participant, is shown. If the given answer is not correct, the correct answer is also presented.

163 users were selected to participate in the second phase of the study. The same enrollment scheme is used in both phases. Hence, this number may only be explained by natural attrition within the workforce. 21 of the Phase 2 participants participated in the intervention beforehand. The set of participants in Phase 2 intersects with the set of participants of Phase 1 by 59 individuals.

The results are depicted in Figure 7.6. Group A, the intervention group, has an average individual IT security awareness of 0.86 on the artifacts of the Post-test Phase. Group B, the control group, has and average individual IT security awareness of 0.8. The intervention shows a positive effect on the individual IT security awareness.

However, a decomposition of the determining components of the IT security awareness computation shows a lower probability for a participant to report the sighting of an artifact after taking part of the class, described above. The values are displayed in Table 7.3. This does not only deminish the effect for the individual IT security awareness, it also results in decrease of organizational IT security awareness.

Table 7.3: Decomposition of the IT security awareness components

|  |  |  |  |
| --- | --- | --- | --- |
|  | ***P({ i*∧*¬r })*** | **P({ i })** | **P({ ¬r })** |
| **Intervention** | 0.143 | 0.167 | 0.956 |
| **No intervention** | 0.202 | 0.248 | 0.868 |

# Summary and Conclusion

The main objective of this report was to present framework for cybersecurity training & exercise. Such framework should enhance cybersecurity education and training for university students, cybersecurity professionals and IT staff to gain more knowledge and skills in tackling cyber threats and their consequences.

This report presents the overview of cybersecurity training target groups, knowledge areas, cybersecurity exercises and competitions. The analysis of these things made it possible to establish a relationship between them and mapping of training & exercise activities to knowledge areas.

The analysis of cybersecurity platforms and training environments, especially of cyber ranges, which are a popular environment for experiencing real-world threats in a virtual environment, learning how to identify potential threats and know how to deal with them show many benefits of cyber ranges in cybersecurity training & exercises.

The architecture of cyber training & exercise framework is presented. Partners (KTU, BUT, CNIT, and UBO) proposed its own tools and frameworks, which can be federated by SPARTA JCCI integrator. Presented by partners, training & exercise tools cover all knowledge areas within the field of cybersecurity.

# List of Abbreviations

|  |  |
| --- | --- |
| ***Abbreviation*** | ***Definition*** |
| ACM | Association for Computing Machinery |
| AD | Active Directory |
| AIT | Austrian Institute of Technology |
| API | Application Programming Interface |
| ASTRI | Applied Science and Technology Research Institute |
| BUT | Brno University of Technology |
| CC: | Carbon Copy |
| CCDCOE | Cooperative Cyber Defence Centre of Excellence |
| CDX | Cyber Defense Exercises |
| CyBOK | Cyber Security Body of Knowledge |
| CyRaaS | Cyber Range-as-a-Service |
| CJIS | Criminal Justice Information Services |
| CMD | Command (cmd.exe is the default command-line interpreter) |
| CMS | Content Management System |
| CNCI | Comprehensive National Cyber Security Initiative |
| CNIT | Inter-University Consortium for Telecommunications (Consorzio Nazionale Interuniversitario per le Telecomunicazioni) |
| CR | Cyber Range |
| CSA | Computer Security Act |
| CSE | Cyber Security Exercises |
| CSEC | Cybersecurity Curricula |
| CSR | Cyber Security Range |
| CTF | Capture the Flag |
| CVE | Common Vulnerabilities and Exposures |
| DB | Data Base |
| DC | District Columbia |
| DMZ | Demilitarized Zone |
| DNS | Domain Name System |
| DoD | Department of Defense |
| DST | Destination |
| ECSC | European Cyber Security Challenge |
| EDB | Exploit Database |
| EEST | Eastern European Summer Time |
| ENISA | European Union Agency for Cybersecurity |
| ESA | European Space Agency |
| ESEC | European Space Security and Education Centre |
| EU | European Union |
| FFIEC | Federal Financial Institutions Examination Council |
| FS | File Exchange Server |
| GB | Gigabyte |
| GHz | Gigahertz |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| IBM | International Business Machines Corporation |
| ICT | Information and Communications Technology |
| IOT | Internet of Things |
| IP | Internet Protocol |
| IR | Incident Response |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| JCCI | Joint Competence Centre Infrastructure |
| KBR | Kellogg, Brown and Root |
| KYPO | Cybernetic Polygon (Kybernetický polygon**)** |
| KTU | Kaunas University of Technology |
| LEOP | Launch and Early Orbit Phase |
| MSSP | Managed Security Service Provider |
| NATO | North Atlantic Treaty Organization |
| NCL | National Cyber League |
| NCR | National Cyber Range |
| NEC | Nippon Electric Company |
| NICE | National Initiative for Cybersecurity Education |
| NIST | National Institute of Standards and Technology |
| NKIVP | National Cyber Incident Management Plan (Nacionalinis kibernetinių incidentų valdymo planas) |
| NKSC | National Cyber Security Centre (Nacionalinis kibernetinio saugumo centras) |
| NSF | National Science Foundation |
| OCCP | Open Cyber Challenge Platform |
| OS | Operating System |
| OT | Operational Technology |
| PC | Personal computer |
| PCI | Payment Card Industry |
| RAM | Random-Access Memory |
| RDP | Remote Desktop Protocol |
| SCADA | Supervisory Control And Data Acquisition System |
| SIEM | Security Information and Event Management |
| SMB | Server Message Block |
| SMTP | Simple Mail Transfer Protocol |
| SOC | Security Operations Center |
| SQL | Structured Query Language |
| SSH | Secure Shell |
| STEM | Science, Technology, Engineering and Math |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TRMC | Test Resource Management Center |
| UBO | University of Western Brittany  (Université de Bretagne Occidentale) |
| US | United States |
| USD | United States Dollar |
| VDAI | State Data Protection Inspectorate (Valstybinė duomenų apsaugos inspekcija) |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |
| WDDM | Windows Display Driver Model |
| WP | WordPress |
| WS | Workstation |
| WWW, Web | World Wide Web |

# Bibliography

1. ENISA Threat Landscape Report 2018, January 2019. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018> [Accessed 19/6/20].
2. ECSC 2019 Analysis Report, December 2019. <https://www.enisa.europa.eu/publications/ecsc-2019-analysis-report> [Accessed 19/6/20].
3. SPARTA. Strategic programs for advanced research and technology in Europe. D9.2. Curricula descriptions. Ed. Jan Hajny, July 2020. <https://www.sparta.eu/assets/deliverables/SPARTA-D9.2-Curricula-descriptions-PU-M18.pdf>
4. ACM. Cybersecurity Curricula 2017. Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. <https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf>.
5. D9.1. Cybersecurity skills framework. <https://www.sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf>
6. CyBOK. The Cyber Security Body of Knowledge. Ed. A.Rashid et al. October 2018. <https://www.cybok.org/media/downloads/cybok_version_1.0.pdf>
7. Robert S. Dewar. Cybersecurity and Cyberdefense Exercises. Zürich, September 2018. <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf>
8. ENISA. Good Practice Guide on Training Methodologies. November 2014, 54 p. [https:/www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies](https://www.google.lt/url?sa=i&url=https%3A%2F%2Fwww.enisa.europa.eu%2Fpublications%2Fgood-practice-guide-on-training-methodologies%2Fat_download%2FfullReport&psig=AOvVaw31LRXoyW0Ez-ra_wTSZDja&ust=1605764400366000&source=images&cd=vfe&ved=2ahUKEwiaxtfWsIvtAhUEwSoKHci5Ar4Qr4kDegQIARA7).
9. Ensar Seker. Cyber Defense Exercises (CDXs) as a Testbed for Cyber Security. June 2020. <https://www.researchgate.net/publication/342040488_Cyber_Defense_Exercises_CDXs_as_a_Testbed_for_Cyber_Security_Assessments>
10. ENISA. The 2015 Report on National and International Cyber Security Exercises. Survey, Analysis and Recommendations. <https://www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises>. December 2015.
11. Jon Oltsik. What is a cybersecurity technology platform anyway? April 2018. [What is a cybersecurity technology platform anyway? | CSO Online](https://www.csoonline.com/article/3269398/what-is-a-cybersecurity-technology-platform-anyway.html)
12. The Top 10 Security Awareness Training Solutions for Business. Expert Insights. July 2020. <https://www.expertinsights.com/insights/the-top-security-awareness-training-platforms-for-businesses/>
13. ECSO. Understanding Cyber Ranges: From Hype to Reality. March 2020, from <https://ecs-org.eu/press-releases/understanding-cyber-ranges-from-hype-to-reality>
14. ENISA. Cyber security competitions — the status in Europe. October 2014. <https://www.enisa.europa.eu/publications/cybersecurity-competitions-2014-the-status-in-europe/at_download/fullReport>
15. C. Pérez. Cyber Range – The future of Cyber Security training. SANS Institute, 2020, 30 p. <https://www.sans.org/reading-room/whitepapers/training/cyber-range-future-cyber-security-training-39550> [Accessed 19/6/20].
16. M.M. Yamin, B. Katt, V. Gkioulos. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, Vol. 88, January 2020. <https://www.sciencedirect.com/science/article/pii/S0167404819301804> [Accessed 18/6/20].
17. NIST. Cybersecurity games: building tomorrow's workforce. Katzcy Consulting 2016. <https://www.Nist.Gov/System/Files/Documents/2017/04/24/Cyber_Games-_Building_Future_Workforce_Final_1031a_Lr.pdf>
18. O. Darwish et al. Survey of Educational Cyber Ranges. In: Barolli L., Amato F., Moscato F., Enokido T., Takizawa M. (eds) Web, Artificial Intelligence and Network Applications. WAINA 2020. Advances in Intelligent Systems and Computing, vol 1150, pp 1037-1045. Springer, Cham, 2020.
19. J. Vykopal et al. KYPO Cyber Range: Design and Use Cases. In Proceedings of the 12th International Conference on Software Technologies - Volume 1: ICSOFT. INSTICC, SciTePress, Madrid, Spain, 2017. pp. 310–321. <https://doi.org/10.5220/0006428203100321> [Accessed 11/7/2019].
20. N. Gaudreau and J. Combs, DoD Cyber Range. Open and Ready for Customers, CHIPS, July-September 2012. <https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=4035> [Accessed 11/7/2019].
21. B. Ferguson, A. Tall and D. Olsen, National Cyber Range Overview, *2014 IEEE Military Communications Conference*, Baltimore, MD, 2014, pp. 123-128, doi: 10.1109/MILCOM.2014.27. <https://ieeexplore.ieee.org/document/6956748> [Accessed 11/7/2019].
22. D. Raymond, Using Cyber Ranges for Cybersecurity Education. <https://csrc.nist.gov/CSRC/media/Events/Federal-Information-Systems-Security-Educators-As/documents/24.pdf> [Accessed 12/7/2019].
23. Cyberbit Range: Training at Your Convenience. <https://www.cyberbit.com/resource/cyberbit-range-training-at-your-convenience/> [Accessed 12/5/2020].
24. Raytheon Cyber Range Capability. <https://www.raytheon.com/sites/default/files/cyber/rtnwcm/groups/cyber/documents/content/rtn_256609.pdf> [Accessed 12/5/2020].
25. Cisco, Cisco Cyber Range (2017). <https://www.cisco.com/c/dam/global/en_au/solutions/security/pdfs/cyber_range_aag_v2.pdf> [Accessed 10/1/19]
26. S. Zatti, The ESA Cyber Range in Redu: Why it is important for ESA, EDA and all of us (2018). <https://eisc-europa.eu/images/stories/2018/Workshop/Final_upload/EISC_Presentations/The_ESA_Cyber_range_in_Redu_-_Stefano_Zatti.pdf> [Accessed 10/5/19]
27. CybExer. Simulation platform for cybersecurity training. <https://tracxn.com/d/companies/cybexer.com> [Accessed 10/5/20]
28. IBM. You’re under attack. Now live the response. <https://www.ibm.com/downloads/cas/01ZOGZQ6> [Accessed 10/5/20]
29. Palo Alto Networks. Cyber Range. [*https://www.paloaltonetworks.com/resources/techbriefs/cyber-range*](https://www.paloaltonetworks.com/resources/techbriefs/cyber-range) *[Accessed 16/5/19].*
30. Silensec. Cyber Range User Guide. <https://cyberstars.pro/docs/Cyber_Range_UserGuidev1.0.pdf> [Accessed 10/5/20
31. CyberStars. Cyber Range. <https://cyberstars.pro/cyber-range/> [Accessed 10/5/20].
32. AIT. Cyber Range & Training. <https://www.ait.ac.at/en/research-topics/cyber-security/cyber-range-training/> [Accessed 16/5/19].
33. IXIA Cyber Range Training Services. <http://ixia.cabanday.com/products/_content/br-cyber-range-training-services.pdf> [Accessed 16/5/19].
34. NEC Cyber Security Solutions. <https://jpn.nec.com/cybersecurity/pdf/NEC_CyberSecuritySolutions_en.pdf> [Accessed 16/5/19]
35. Georgia Cyber Center. <https://cyber.augusta.edu/georgia> [Accessed 4/1/19].
36. KBR. 7 Benefits of KBR’s New Cyber Range. <https://www.kbr.com/en/insights-events/stories/7-benefits-kbrs-new-cyber-range> [Accessed 16/5/19].
37. Cyber Test Systems. Cyber Range V2 bk – Cyber Intelligence. <https://cyberintelligence.my/cyber-range-v2-2/> [Accessed 16/6/19].
38. Merit. The Michigan Cyber Range. <https://www.merit.edu/cyberrange/> [Accessed 16/6/20].
39. Indra. The Minsait Cyber Range platform, the first capable of 'learning' from the student to offer completely customized training in cybersecurity. <https://www.indracompany.com/en/noticia/minsait-cyber-range-platform-first-capable-learning-student-offer-completely-customized> [Accessed 16/6/20].
40. J. Fonseca et al. The Open Cyber Challenge Platform. <https://www.nist.gov/system/files/documents/2017/01/19/d1_trk2_faywolfe_open_cyber_challenge_platform.pdf> [Accessed 16/6/20].
41. CyRaaS. Cyber Range-as-a-Service. <https://www.circadence.com/products/cyraas/> [Accessed 16/6/20].
42. ASTRI. Cyber Range. <https://www.astri.org/technologies/joint-research-laboratories/rd-centres/cyber-range/> [Accessed 16/6/20].
43. Pierluigi Paganini. 2018. In the past weeks, many Mac users have been infected with a new strain of Monero miner, the infections confirm the rise of this kind of malware.
44. Arnold Sykosch, Christian Doll, Matthias Wübbeling, and Michael Meier. 2020. Generalizing the phishing principle: Analyzing User Behavior in Response to Controlled Stimuli for IT Security Awareness Assessment. In *Proceedings of the 15th international conference on Availability, Reliability and Security*.
45. C. Xiao. 2014. *WIRELURKER: A new era in iOS and OS x malware*. PALO ALTO NETWORKS: unit42.
46. David B. Resnik and Peter R. Finn. 2018. Ethics and Phishing Experiments. In: *Science and Engineering Ethics*.
47. European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Annex No. 1. Summary information about Cyber Ranges

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Cyber Range** | **Mission** | **Capabilities** | **Advantages** | **About Organization, Project** |
| **KYPO CR** [19] | Realistic environment for cyber-training and support for cyber-testing, research, and training for students and researchers. | Hosted in the cloud, web access, role-based access, User-specific content, dynamically creation and destruction of the virtual environments, large target networks can be replicate for multiple and simultaneous usage | Complete training stack, training scenarios, advanced customization tools, malware forensics, network security, penetration testing, certification, Capture-the-flag environment | The KYPO project was funded by the Ministry of Interior of the Czech Republic as part of the Security Research Program of the Czech Republic |
| **DoD Cyber Security Range**  [20] | Environment to support exercises, training, testing, evaluation, and education for the military. | Traffic generator, configurable user emulation, malware, spyware, and botnets emulation | Cyber-security and computer network | The Department of Defense (DoD) Cyber Security Range (CSR) is funded by the 2009 Comprehensive National Cyber Security Initiative (CNCI) |
| **US National CR** [21] | Realistic environment for cyber-training and support for cyber-testing complex governmental systems. | Secure facility, role-based access, focus on cyber-security and computer network defense | Malware analysis, forensic analysis, architecture analysis, training events, research, Capture-the-flag environment, testing and product evaluation | The National Cyber Range (NCR), operated by the Test Resource Management Center (TRMC), provides the ability to produce realistic cyber-security testing, evaluation and training.  The architecture is the same as the KYPO cyber range |
| **Virginia CR**  [22] | Provide an environment to increase the number, and the preparedness, of students entering the cybersecurity workforce in operations. | Hosted in the cloud, web access, role-based access, User-specific content, dynamically creation and destruction of the virtual environments, large target networks; can be replicated for multiple and simultaneous usage | Cyber-security and computer network defense, training exercises for SCADA (Supervisory Control And Data Acquisition System) and Industrial Control Systems, cyber-law and policy topics, CTF (capture-the-flag) competitions | The Virginia Cyber Range’s scope is to enhance cyber-security education for students in Virginia's high schools and colleges |
| **Cyberbit CR**  [23] | To provide hyper-realistic simulated training environments to enterprises, governments, academic institutions and managed security service providers (MSSPs). | Virtual Network Replica, Attack Generator, local and remote seats for trainees, Pre-Build Networks, User Generated Networks, Pre-Build Scenarios, User generated Scenarios, inject real-life attack scenarios to the network, Realistic Traffic Generator, Knowledge base, real time monitoring, score and evaluation, Virtual and physical SCADA training, cross-functional executive training and new attack scenarios such as ransomware variants. | Complete training stack, trainer console, training scenarios, advanced customization tools, malware forensics, network security, penetration testing and IR (Incident Response), certification courses, Capture-the-flag environment. | Cyberbit is a provider of cyber range environments which aims to provide hyper-realistic simulated training environments to enterprises, governments, academic institutions and MSSPs around the globe |
| **Raytheon CR**  [24] | To provide an environment to support training and education for companies. | Network environment emulation for air traffic control, power grids, water supplies, SOCs (Security Operations Centers) capabilities, scalable and agile architecture, automation, interconnection with external hardware. | Reverse engineering, firmware code analysis, Radio frequency and wireless vulnerability and radiated emissions testing, cyber professional training, penetration testing, Mitigation planning and consulting, capture-the-flag environment. | Raytheon is an international aerospace and defence company specialized in various sectors, such as defense, civil government and cyber-security solutions. Raytheon Cyber develops and distributes cyber-security products and solutions to its clients |
| **Cisco CR**  [25] | To provide an environment to support training and education for the participants of an organization to combat modern cyber-threats. | Implemented with variety of application which provide visibility, intelligence, threat detection, firewalling and thread detection e.g. Cisco Stealthwatch, Cisco Splunk, Control. Includes traffic generator, configurable user emulation, malware, spyware, and botnets emulation, individual and team training, end-to-end real-time solution for machine data delivery. | Focus in cyber-security and computer network defense, threat detection, identification of various application, network traffic pattern, secure network and applications, Cisco Stealthwatch, Cisco Splunk, Cisco TrustSec. | The Cisco Cyber Range is offered as a service. It is a training course that aims to train the participants to combat modern cyber-threats |
| **European Space Agency (ESA) CR**  [26] | To provide a training and simulation platform facility to provide training and testing and develop knowledge in awareness, detection, investigation, response and forensics to counter cyber-attacks specific to the space sector | Provide specialized space cyber-emulation environment to securing space assets | Instantiation of a full mission environment, mission control systems, Pre-Launch, Launch, LEOP (Launch and Early Orbit Phase), IOT, ground and satellite simulators, space segment, data segments, operations and development networks | ESA has established a cyber training range at the European Space Security and Education Centre (ESEC), Redu, Belgium |
| **CybExer CR**  [27] | Environment to support training and education for | Exercise management, red teaming capability, exercise Management Toolkit, automation, customized scenarios, | Complete training stack, trainer console, training scenarios, | CybExer Technologies OÜ is a joint company established by two Estonian cyber-security and cyber-solutions companies: BHC Laboratory OÜ and Bytelife Solutions OÜ.  CybExer Range Platform can be deployed on-premise in an organization or it can be accessed through CyberExer infrastructure |
| **IBM CR**  [28] | Provide an environment to offer an experience in a cyber-incident | Exercise rapid-response thinking in a pressured environment, understand how security solutions work together, experience how your teams work together. | Discover gaps in enterprise’s response plan, technical cyber response and leadership best practices, attacking tools, cybercrime topics, risk analysis | IBM Cyber Range aims to offer the experience of a cyber-attack at IBM X-Force Command Center. It aims to train all the departments of an enterprise, from security operations center (SOC) to human resources (HR) and Legal |
| **Palo Alto CR**  [29] | To train the participants of an organization to combat modern cyber-threats and enhance their prevention, detection and response skills through hyper-realistic network simulation exercises | Provides an isolated and realistic environment with network traffic-generator capabilities, application traffic-generator, multiple courses. | Identify advanced attacks, mitigate advanced attacks, collaboration between teams, Industrial Control Systems attack scenarios, various training scenarios, Capture-the-flag environment | Palo Alto Networks Cyber Range is headquartered in Amsterdam with hubs is Washington DC, Santa Clara and Sydney. Palo Alto Networks CR is offered as a service to organizations, but it can also be implemented on-premise in an organization data center |
| **Silensec CR**  [30, 31] | To provide a training environment for individuals and enterprises to practice cyber-security skills in a fun and challenging way through advanced gamification modules. | Advanced monitoring, Security Information and Event Management (SIEM), cloud based, available as a service, support interconnection with IoT and ICS environments, competence-based scoring and assessment, virtualization automation. | Protection, detection, reaction, certifications, various training scenarios, indent response and investigations, Capture-the-flag environment and cyber-security | Silensec is an Information Security Management Consulting and Training company. Silensec Cyber Range provides an environment for individuals and organizations to practise cyber-security skills in a fun and challenging way |
| **Austrian Institute of Technology (AIT) CR**  [32] | An environment for sharing the knowledge in cybersecurity domain for critical infrastructure providers, industry, research and public sector. | Advanced training exercises and competition on different levels, visualization, industrial control systems, digital networks and critical infrastructures, focus in cyber security research and development. | Various training scenarios, offers risk assessment and evaluation modules, certifications, testing of contingency plans, incident response processes. | AIT CR aims to share the knowledge in cyber-security with various actors, such as critical infrastructure providers, industry, research and public sector, providing an isolated and realistic environment for testing and analysing various scalable scenarios in the cyber-security domain |
| **IXIA CR**  [33] | Provide an environment to train the participants of an organization to combat modern cyber-threats using a variety of IXIA’s products | Offered as a service, flexible, scalable, application and threat intelligence, visualizations modules, SIEM, traffic generator | Complete training stack, trainer console, training scenarios, advanced customization tools, various training scenarios, Capture-the-flag environment and cyber-security competitions. | IXIA is a security assessment company focusing on the security and monitoring of networks. IXIA offers a variety of its products as a Cyber Range solution. IXIA CR offered as a service can replicate corporate networks and the created scenarios can be inserted with real malicious traffic like distributed denial-of-service (DDoS) attacks with the application and threat intelligence (ATI) service |
| **NEC CR**  [34] | To provide an environment to customers a virtualized framework for cyber-security training, modelling and simulation | Self-paced security challenges in various topic areas, classroom-based training for different levels of expertise, team-based exercises, interconnects with physical systems. | Complete training stack through classroom module, training scenarios, network security, penetration testing, certification, Capture-the-flag environment. | The NEC Cyber Range is offered as a service and aims to provide their customers with a virtualized framework for cyber-security training, modelling and simulation |
| **Augusta University CR**  **(Georgia Cyber Institute)**  [35] | Environment to support exercises and training for education and research | Certified courses with University training methodology | Complete training stack through courses | Georgia Cyber Range is available to students, industry and government professionals and aims to strengthen cyber-security preparedness through certified courses. Georgia CR uses the University’s training methodology |
| **KBR’s New Cyber Range]**  [36] | To create IT and Operational Technology virtual environments that mimic an organization’s networks, systems, tools and applications | Advanced network environment simulations to customers that need to perform real-world cyber testing without impact to mission-critical systems. To provide the next wave of hardware and software security solutions for government and private agencies, helping them secure information and systems from destructive cyber threats | Customers can remotely access the cyber range and use it to strengthen their IT assets while evaluating the efficiency of applications in a live environment.  Customers can also use the cyber range to transmit information to their own networks through SecDevOps, ensure compliance with National Institute of Standards and Technology guidelines and cut time alloted for vulnerability assessments during the design phase of new technologies | KBR, Inc. (formerly Kellogg, Brown and Root) is an American engineering, procurement, and construction company, formerly a subsidiary of Halliburton. Located in Houston, its cyber lab in North Charleston, South Carolina |
| **Cyber Test System’s Cyber Range**  [37] | Training facility for cyber defense exercises that allows organizations to increase and test the cyber response skills of individual and teams defending their network infrastructures | To replicate a realistic environment – Civilian, Military and Critical Infrastructure networks; to perform Product Evaluation – validate your network infrastructure, validate your solution, validate your website security; to perform  Product Certification – Performance Tests, QA Tests, meet Qualification criteria in contracts, regulations, or specification | This training facility provides a hyper-realistic simulation of an actual cyber attack with legitimate and malicious traffic generated from a Network Traffic Generator developed by Cyber Test Systems, France, allowing participants to practice the entire chain of cyber defense. The Cyber Range provides tools that help strengthen the stability, security and performance of cyberinfrastructures and IT systems used by government, military agencies and civilian organizations | Cyber Intelligence Sdn. Bhd or “CI” is a Cyber Security company established in 2010. CI was the first to setup the Cyber Range facilities in Malaysia, in collaboration with CyberSecurity Malaysia and International Islamic University Malaysia in 2016 |
| **Michigan Cyber Range**  [38] | The Michigan Cyber Range aims to strengthen Michigan’s cyber defenses by mitigating the growing number of cyber threats and providing a more secure environment that promotes economic development | To provide access to lab-based experiential learning and certification for all compliance requirements and frameworks, including the (National Institute of Standards and Technology) NIST 800 Standards, NICE (National Initiative for Cybersecurity Education) Framework, National Security Agency, DoD 8570, HiTrust, FFIEC (Federal Financial Institutions Examination Council), PCI (Payment Card Industry), CJIS (Criminal Justice Information Services) and CSA (Computer Security Act). To engage, support and attract surrounding industries and entrepreneurs to provide cost effective and scalable access to software, systems and penetration testing. | Custom training programs can be tailored to each customer’s needs.  Michigan Cyber Range exercises are wholly contained within the secure Michigan Cyber Range and are extremely affordable for organizations of all sizes and can be customized to meet your scheduling and organizational needs | Powered by Merit Network, the US longest-running research and education network, the Michigan Cyber Range is the nation’s largest unclassified, network accessible cybersecurity training platform |
| **Minsait Cyber Range platform**  [39] | It is one of the most advanced cyber-entertainment solutions on the market. It has been designed by Indra to support intensive individual and group training in techniques and tactics related to cyber-defense, cyber attacks and forensic analysis | In the military field, the Indra unit offers all the security guarantees to protect classified content and has a private cloud equipped with all the technical security measures | Minsait offers its clients training as a service, so that they are not forced to incur costs related to purchasing equipment. It provides them with the maximum ease of use, scalability and flexibility according to the needs that they have at all times | Minsait, Indra's digital transformation business unit, works with the Carlos III University of Madrid in an innovative project to equip its Minsait Cyber Range training platform |
| **Open Cyber Challenge Platform**  [40] | Cyber challenges, where groups of students defend/attack/investigate a network and/or data center with realistic attacks, have proven to be both wonderful recruiting tools in high school and college competition events, and effective teaching tools in academic and training courses that use them | Provide controlled scenarios that teach, demonstrate, and evaluate skills in cyber security areas including Network Defense, Penetration Testing, Incident Response, Malware Analysis, Digital Forensics, and Secure Programming | Free, configurable, open-source virtualization platform for cyber security educators and challenge event coordinators. Reasonable in terms of cost of required hardware, and in terms of required technical installation and maintenance expertise, for a wide variety of organizations, including high schools, colleges, companies, and government agencies to use in courses and/or conduct challenge events.  Easily extensible to allow the community to post new challenges and scenarios that can be performed using the base OCCP (Open Cyber Challenge Platform) | The University of Rhode Island has a current grant from the National Science Foundation (NSF) to seed the open cyber challenge platform development |
| **Cloud and On-Prem Cyber Range Solution–CyRaaS™**  [41] | Circadence is redefining the modern cyber range with fully elastic, cloud-based ons built from 25+ years of expertise, continued research and development, and 30+ patents across the fields of massively multiplayer online (MMO) gaming, latency and optimization | Cyber Range-as-a-Service (CyRaaS) platform allows academic institutions the opportunity to train in realistic environments that mirror their actual company networks  ` | The potential of CyRaaS is limitless, with the ability to support collective Nation State exercises as well as modeling for entire cities to develop living physical and fifth domain environments. Combined with Circadence’s Project Ares, Orion Mission Builder™, and StrikeSet™, organizations can learn and grow without impacting your operations | Circadence offers cyber range solutions and cybersecurity learning platforms that leverage artificial intelligence and custom content to address critical security challenges for enterprise, government, and academic institutions  Headquarters – Circadence® Corporation Boulder, CO  Advanced Research & Development Facility Tupelo, MS  Center For Cyber Autonomy & Data Science San Diego, CA |
| **Cyber Range – ASTRI**  [42] | To provide cybersecurity training services to professionals from law enforcement agencies as well as the financial services industry | The facility uses an ‘attack and defence’ simulation model to equip its trainees with adequate skills   * Server farm supports up to 240 Virtual Machines (VMs) simultaneously * Training of cyber forensic techniques * ‘Blue-team-red-team’ model of attack/defence training * Exercise VM preparation and rapid deployment to trainees * Adaptive assessment of trainees * Visualisation of VMs under attack | The courses are delivered by security professionals with solid security audit and assessments experiences.  These are practical, exercise courses, which show you how the attackers would attack in the real world, i.e. the entire kill-chain, and how to defend against them. | The first Cyber Range facility in Hong Kong was established at ASTRI (Applied Science and Technology Research Institute) in collaboration with the Hong Kong Police Force in 2016 |

Annex No. 2. The installation of a virtual machine image

**Installation Requirements**

* Processor: 1 gigahertz (GHz) or faster
* RAM: 2 GB (64-bit)
* Free hard disk space: 32 GB (Virtual Size: 40.00 GB; Actual Size: 13.00 GB)
* Graphics card: Microsoft DirectX 9 graphics device with WDDM driver
* Windows 10 Installation Requirements for VirtualBox
* Download VirtualBox from this link: https://www.virtualbox.org/wiki/Downloads

**Installing process**

1. Download VirtualBox disk image (ImageName.vdi) (Workstation image is available to download).
2. Open ORACLE VM VirtualBox 6.x and select the window to create a new virtual machine. The virtual machine name and type must be specified.

Graphical user interface, text, application

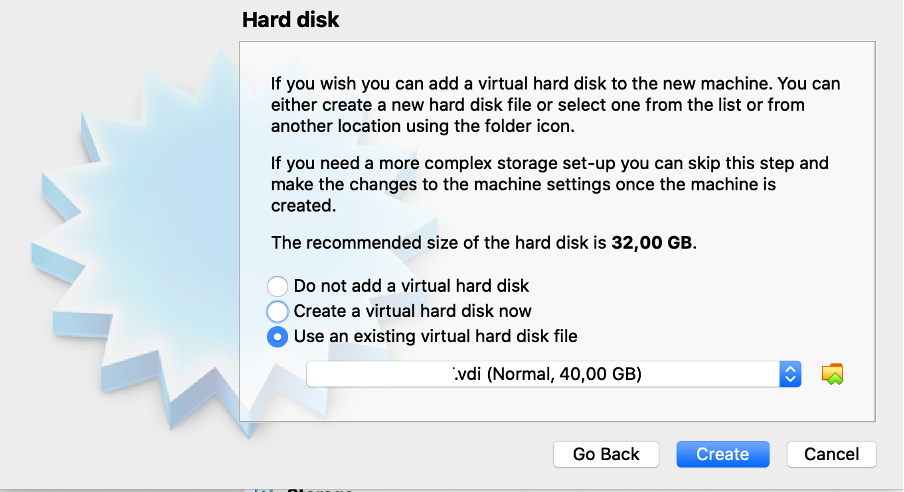
Description automatically generated

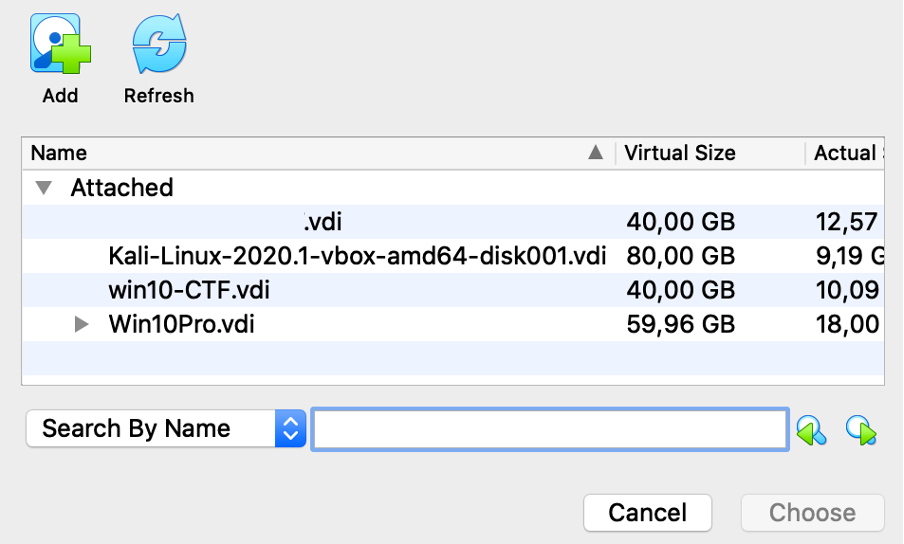
1. Press “Continue”.
2. Select the amount of RAM (random access memory) and click " Continue".

A screenshot of a cell phone

Description automatically generated

1. Select "Do not add a virtual hard drive" and click "Create" and "Continue" again. Click, select an existing disk and specify the path to the saved disk image (file : NAME.vdi).





We also want to recommend other useful settings you can choose from Settings Menu. For security reasons, it is recommended that you uncheck the network settings and prevent the virtual machine from accessing the Internet:

A screenshot of a cell phone

Description automatically generated

or set possibility that the virtual machine is only available to you (Host-only Adapter):

A screenshot of a cell phone

Description automatically generated

1. Once you have done all the settings, you can press the S**tart button**.

Annex No. 3. The infrastructure of an attack model of a typical organization and its functions

Files and their malware:

* Win32.exe – Ransomware WannaCry
* 8.1.2\_AdbeRdr812\_lt\_LT.exe – remote reverse shell – for establishing session
* update\_new.exe – Ports scanning software (installation file).

IP addresses:

* www3\_wp 10.10.15.243, 83.171.40.178
* www2 10.10.15.151, 83.171.40.243
* www1 10.10.15.137, 83.171.40.214
* www3\_idam 10.10.15.118, 83.171.42.50
* www3\_win 10.10.15.89, 83.171.40.206
* ws1 W10 10.10.15.5, 83.171.40.129, 2001:778:1:17::1f
* ws2 W7 10.10.15.8, 83.171.40.115, 2001:778:1:17::11
* ws3 W10 83.171.40.102, 2001:778:1:1::77
* dc WS-2008-R2 10.10.15.10, 83.171.40.185, 2001:778:1:17::5
* Attacker\_B 180.95.128.43, 83.171.41.220
* Attacker\_A 42.83.90.245, 83.171.42.241

|  |  |  |  |
| --- | --- | --- | --- |
| *Zone* | *Object* | *Name* | *Destination* |
| DMZ | WWW 1 | Website owned by the organization | A site dedicated to publicizing an organization’s activities, hosted on the organization’s server in the DMZ zone, is administered by the organization’s internal network. |
|  | WWW 2 | Website owned by the organization | A site dedicated to publicizing an organization’s activities, hosted on the organization’s server in the DMZ zone, is administered by the organization’s internal network. |
| Hosting | WWW 3 | Website owned by the organization | A site dedicated to publicizing an organization’s activities, hosted on the hosting server, administered over a public network.. |
| Services | AD (Active Directory) | Organization‘s Directory Service | Organization‘s users management, name server, management of user rights and policy. |
|  | FS (File Sharing) | Organization‘s file sharing server | A system for synchronizing files on a directory service server and workstations. Predefined directories on workstations WS1, WS2, WS3 are constantly synchronized with the File Exchange Server. |
|  | VPN | Virtual Private Network Access Server | An organization's virtual private network for administration and remote work. |
| Employees | WS 1 (Workstation 1) | Organization‘s workstation | An organization-owned Microsoft Windows 10 workstation on an organization's network, has automatic file sharing with the FS client installed. |
|  | WS 2 | Organization‘s workstation | An organization-owned Microsoft Windows 7 workstation, ready for operation on organization's network, has automatic file sharing with the FS client installed. |
|  | WS 3 | Organization‘s workstation for remote work | An organization-owned Microsoft Windows 10 workstation for remote work on an organization's network, has automatic file sharing with the FS client installed (Nexcloud). Has ready access using a VPN client connection (OpenVPN) to the VPN server. Employee - information systems administrator. |
| Public internet | STEAM  (Game platform) | Social communication | An online gaming and chat site. The most popular gaming portal will be used for STEAM communication. |

Annex No. 4. An attack model in an IT infrastructure of typical organization with attack scenarios and an attack map

|  |  |  |
| --- | --- | --- |
| *Incident No.* | *Incident* | *Short description* |
| A1 | Obtaining WWW 3 CMS „Idamas“ and Wordpress site administration rights using password hacking (*brute force*) | Your organization has an informational, publicly accessible website, www3.spart-ktu-cyberrange.com. The website is hosted on a hosting server over which you have no direct control, only a service agreement exists. This morning, your organization receives a call from another "friendly" organization you are supposed to be collaborating with (in fact, the call is fake). You are informed that the results of the project you are running are not exactly what needs to be made public. The project “service provider” posted the results of the project on your website, and you did not check what specific information was uploaded and whether it was uploaded by the provider or whether it was a cyber attack. |
| A1.1 | Review of a malicious file (\*.priedasNr1.xlsm arba \*.pdf) | The employee responsible for the content of the publicly accessible website (WS 1) logs in with his access profile (username / password) and reviews the information uploaded by the “service provider”. The employee has found out about this newly uploaded information through two channels: by phone from the "provider" (by fraudulent phone) and by e-mail (which the scammer has informed by phone that e-mail will be sent). The organization bought a service (all contracts are public, so criminals used public information, found out who did the work, when and where, formed a compelling story based on it), the result of which must be posted on the organization’s website (WWW 3). |
| A1.1.1 | received a phone call | Telephone call or e-mail to interested parties informing them of updates to the organisation's website and templates available for review.  The fact that the employee who reviewed the information (WS1) was infected with malware is established (*phishing* / *malware* attack). |
| A1.1.2 | received an e-mail | Organization‘s user (WS 1) received an e-mail to his organization's mailbox with information about the work performed. All information about the work is posted on the website of the organization (WWW 3). The e-mail asks you to review the prepared documents in order to sign the transfer and acceptance certificate (order?). |
| A1.2 | Access to the CMD via a reverse shell | An employee who downloads and opens a document from the content management system of the organization's website (WWW 3) infects his workstation (WS 1), thus giving Attacker A access control to the organization's workstation (WS 1). |
| A1.2.1 | Malware synchronization | An Attacker A moves a malicious file to a directory whose files are synchronized continuously, and the file is distributed throughout the organization's workstations (WS 1, WS 2, WS 3). Malicious software (8.1.2\_AdbeRdr812\_lt\_LT.exe, Win32.exe, update\_new.exe) is loaded. A new system user mr1kry with Administrator rights is created. |
| A1.2.2 | Internal network scanning, SMB vulnerability | Spread of malicious activity in the internal network of the organization. An Attacker A attacks an AD server. (An internal network scan is in progress). |
| A2 | SQL request („injection“) | Using SQL injection, an Attacker A obtains usernames and passwords. Using one of them, he connects to the WWW 1 (CMS) and places a file with ransomware. This file is placed in the CMS directory, which is automatically synchronized by the File Exchange Server (FS). WWW 1 is then used for information leakage. |
| A2.1 | Malware synchronization | File Exchange Server synchronizes the infected file with the organization's users workstations WS 1, WS 2, WS 3. |
| A2.2 | Malware activation | The malware enters the organization's workstation WS 2. The user receives an automatic message about the file being shared with him and opens it. This workstation is encrypted. (Investigators are provided with an image with malicious code, which is running but stopped for full encryption, for analysis. Another image is provided fully encrypted.) |
| A3 | CMS (Wordpress) plugin that will allow you to view the full content tree. | The organization has a TRUST box (WWW 2) to report cases of corruption in the organization. Attacker A gains access to the CMS and the contents of the box in it where the information about project participants, administrator (AD) and staff access is presented. Data leakage occurs. |
| A3.1 | Database hijacking is in progress | Sql dump is being downloaded by Attacker A. |
| A3.2 | Malware („reverse shell“) | An Attacker A downloads malware (Document - Remote Work Procedures) through the organization's Web site WWW 2, which is automatically synchronized. This information is accessed by the remote employee (WS 3). Computerized WS 3 workstation is taken over. An attacker user Insider will be created, it will be used later to leak information. |
| A3.2.1 | Remote connection with saved settings. | The user of the computer WS 3 is the network administrator and his access is linked to all internal information systems. VPN (OpenVPN client1 certificates) and RDP (via mr1kry created by the Attacker) remote connection settings are stored on the employee's (WS 3) computer. |
| A3.2.2 | WWW 2 and data leakage to the outside. | Information is transmitted from the AD, and it is forwarded to WWW 2, which is taken by Attacker A. Information is leaked from the organization through the user Insider. |
| B1 | Social network (Web game communication channel "chat") | The Attacker B communicates in a public space using a employee's WS 3 computer with a child, who is left on the official computer so that he does not interfere with daily activities.  The child (via chat) is advised on how to help the father / mother speed up the computer (social engineering). (Child: alarvelis; Attacker: mr1kry) |
| B1.1 | Reverse shell access to CMD | The child fulfills the recommendations: opens access to the CMD through the reverse shell.  The user of the computer WS 3 is the network administrator and his access is linked to all internal information systems. (instrukcija.pdf) |
| B1.2 | DC attack, combination with administrator access | The consequence of an attack (DC exploits the capture of keyboard clicks on the WS 3 in the Attacker's system) is access to all AD policies (via RDP), which is executed through a VPN (OpenVPN certificates client1) from a trusted WS3 user. |
| B1.3 | Data transfer from AD to WWW1 | The information from the AD is transmitted to WWW 1, from where it is retrieved by Attacker B. (AD user list with passwords is exported and loaded to www 1. Later downloaded by Attacker B). |
| B1.3.1 | WWW1 and data leakage to the outside. Data theft. | Attacker B brings data (user-list) outside the perimeter of the organization (data theft) |
| B1.4 | Access from AD to FS and later to WS2. | The malicious code is forwarded to the AD; then it is forwarded to the organization’s file exchange information system, then to the employee workstation (WS 2) and is activated by Attacker B. Malicious code is a ransomware (win32.exe file) that requires a ransom. |

Annex No. 5. Storyline A1 – bruteforce attack

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Date** | **Time** | **SL** | **Type** | **Action line varia-tion** | **Who is respon-sible** | **From** | **To** | **Description** | **External file** | **Comment** |
| 10/19/2020 | 14:50 | A1 | Info |  |  |  |  | Using the password caution method, Attacker A hacks into the WWW3 website and places a malicious file there. |  | **Comment** |
| 10/19/2020 | 15:03 | A1 | Info |  |  |  |  | The employee responsible for the content of the public website (WS1) receives an e-mail informing about the uploaded information, logs in with its access profile (username / password) and views the file uploaded by the "service provider" (attachment No.1 .xlsm) thus giving the Attacker A access control to the organization's workstation (WS 1) (initiated by reverse-shell) | email0.0-AtakA-WS1darbuotojas.txt |  |
| 10/19/2020 | 15:20 | A1 | Info |  |  |  |  | Attacker A moves malicious files (8.1.2\_AdbeRdr812\_en\_US.exe, Win32.exe) to a directory whose file synchronization (FS) is performed continuously, and the file is also distributed throughout the organization's workstations (WS 2, WS 3, WS n). WS 1 creates a new system user with Administrator rights: mr1kry. The internal network scan starts. |  |  |
| 10/20/2020 | 8:10 | A1 | Plugin |  | State Infra- structure | WS1 User | IT (security) depart-ment | The user WS1 calls the provider to discuss the contents of the uploaded file and learns that the provider did not actually upload the information. The user suspects that the site was hacked yesterday and became a victim of social engineering. He informs his IT (security) department about the received e-mail. | email1.0-WS1darbuotojas-Itsauga.txt |  |
| 10/20/2020 | 9:20 | A1 | Response |  |  | IT (security) department | IT administra-tor | Procedure to get and deliver a WS1 image |  |  |
| 10/20/2020 | 9:30 | A1 | Response |  |  | IT (security) department | Hosting provider | Request data (logs, disk image, etc.) |  |  |
| 10/20/2020 | 9:40 | A1 | Response |  |  | IT (security) department | Security Represen-tative | Information on the situation and planned actions |  |  |
| 10/20/2020 | 9:41 | A1 | Response |  |  | Security Represen-tative |  | Evaluation: risk, damage |  |  |
| 10/20/2020 | 11:00 | A1 | Response |  |  | IT administra-tor | IT (security) depart-ment | The IT administrator provides the image of WS1 |  | State Infrastructure provides the image of WS1 |
| 10/20/2020 | **11:10** | A1 | Response |  |  | IT (security) department |  | **Starts a WS1 forensics** |  |  |
| 10/20/2020 | 13:00 | A1 | Plugin | Option 2.0.1 | State Infra- structure | Hosting provider | IT | Provides requested WWW3 files without discussion | email2.0.1-hosting-provider--it--(hostingas-duoda-failus).txt | State Infrastructure provides files |
| 10/20/2020 | 13:00 | A1 | Plugin | Option 2.0.2 | State Infra- structure | Hosting provider | IT | Provides requested WWW3 files but not in accordance with the term specified in the contract | email2.0.2-hosting-provider--it--(hostingas-duos-kazkada.txt | State Infrastructure does not provide files |
| 10/20/2020 | 13:00 | A1 | Plugin | Option 2.0.3 | State Infra- structure | Hosting provider | IT | No data provided. There are no opportunities. | email2.0.3-hosting-provider--it--(hosting-apsvarste-neduos).txt | State Infrastructure does not provide files |
| 10/20/2020 | **13:10** | A1 | Response |  |  | IT (security) department |  | **Starts a WWW3 forensics** |  |  |
| 10/20/2020 | 13:30 | A1 | Additio-nal plugin | Option 3.1 | State Infra- structure | NKSC | IT (security) department or Security Representative | If the IT (security) department does not respond, the NKSC forwards information about the detected malicious file on the WWW3 website. | email3.1-NKSC-administracija.txt |  |
| 10/20/2020 | 15:00 | A1 | Response |  |  | Security Representative | IT (security) department | Ask for more information on the progress and results of the WS1 and possibly WWW3 forensics |  |  |
| 10/20/2020 | 15:05 | A1 | Response |  |  | Security Representative | Management | Information on the situation |  |  |
| 10/20/2020 | 15:10 | A1 | Response |  |  | Security Representative | All User | Information on the situation, prohibition to run automatically files 8.1.2\_AdbeRdr812\_en\_LT.exe, Win32.exe distributed through workstations. |  |  |
| 10/20/2020 | 15:50 | A1 | Response | Option 3.1 |  | Security Representative | Institutions | Inform on the inicident |  | Notifications to NKSC, VDAI, Police, etc. |
| 10/20/2020 | 15:50 | A1 | Response | Option 3.2 |  | Security Representative | Institutions | Do not inform on the incident. Does not meet the requirements |  |  |
| 10/20/2020 |  | A1 | Response |  |  | IT (security) department, Security Representative, Public relations | Manage-ment | Periodic information on the situation |  |  |
| 10/21/2020 | 9:00 | A1 | Response |  |  | IT (security) department | Security Representa-tive | Final forensics results, report. Gap identified / |  |  |
|  |  |  | Response |  |  |  |  | hacking vector detected (weak password), user list audited, etc. |  |  |
| 10/21/2020 | 9:30 | A1 | Response |  |  | IT (security) department | Manage-ment, Security Representa-tive, Employees | Information on the inicident forensics. |  | It is unclear how much more WS are infected in the organization |
| 10/20/2020 | 9:50 | A1 | Response | Option 4.1 |  | Security Representative | NKSC, VDAI, Police | Information about incident elimination information in accordance with internal procedures and NKIVP |  | If it is decided that notifica-tion is necessary, the relevant authorities shall be informed of the decision |
| 10/20/2020 | 9:50 | A1 | Response | Option 4.2 |  | Security Representative | NKSC, VDAI, Police | Do not inform on the incident. Does not meet the requirements |  |  |
| 10/20/2020 | 10:00 | A1 | Response | Option 5.1 |  | Security Representative | Media | Press release about the incident and possible damage to all who downloaded file attachment No.1 .xlsx |  | The organization voluntarily informs the public about the uploading of the malicious file to the organization's website. |
| 10/20/2020 | 10:00 | A1 | Response | Option 5.2 |  | Security Representative | Local instructor | Do not make the incident public. |  |  |
| 10/20/2020 | 11:00 | A1 | Additio-nal plugin | Option 6.0 | State Infra- structure | Journalist | Public relations or Security Represent-ative or Director | Information has appeared in the public domain (IT security community forums) that an infected \* .xlsx file could be downloaded from your site yesterday. A screenshot of the site is attached and request for a comment is added. | email4.0-zurnalistas--viesieji-rysiai.txt | Information is needed quickly, an article is prepared to be published in two hours. If no information is received after an hour re-inject: Do we have preliminary investigatory  information? |
| 10/20/2020 | 11:10 | A1 | Response |  |  | Public relations | Security Represen-tative, Director | A comment is required |  |  |
| 10/20/2020 | 13:00 | A1 | Response |  |  | Public relations | Journalist | Answer / Press release. |  |  |

Annex No. 6. Storyline A2 – sql injection attack

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Date** | **Time** | **SL** | **Type** | **Action line variation** | **Who is responsible** | **From** | **To** | **Description** | **External file** | **Comment** |
| 10/21/2020 | 15:50 | A2 | Info |  |  |  |  | Using the SQL injection method, Attacker A attacks WWW1, obtains usernames and passwords to access the WWW1 CMS. AD users / passwords are synchronized with the CMS authentication DB. A ransomware file is placed in a directory that is automatically synchronized by the File Exchange Server (FS). |  |  |
| 10/21/2020 | 16:10 | A2 | Info |  |  |  |  | The ransomware file is distributed to organization's workstations, including WS2. Its user received a message about file sharing. User downloads the file and plays it. Encryption for this workstation begins. |  |  |
| 10/21/2020 | 16:30 | A2 | Info | Option 1.0 |  | WS2 user | IT administrator | The employee, noticing that several of his colleagues' computers were encrypted, clicked **Suspend** and informed the IT administrator. | email1.1.1-WS2user --it-administratorius | An image with malicious code running is presented to Investigators but stopped for full encryption. It is possible to find the keys that can be used to decrypt the data. |
| 10/22/2020 | 8:00 | A2 | Response | Option 1.1 |  | WS2 user | IT administra-tor | When an employee comes to workplace, turns the WS on and understands from the image on the screen that the WS is encrypted. He informs the IT administrator. The continuity of the company 's activities depends on this employee (for instance, hospital reception, document management in the municipality, registration of disturbances in the energy supply system, etc.) | email1.1.2-WS2user --it-administratorius | Full encryption. Opportunity / goal to test the actions of IT administrators in this case. Also estimate how long it would take to prepare a full workstation from backup so that the user can work again. |
| 10/22/2020 | 9:00 | A2 | Response |  |  | IT administrator | IT (security) department | Information about encryption of WS. |  |  |
| 10/22/2020 | 9:30 | A2 | Response |  |  | IT (security) department | IT administrator | Procedure to get and deliver a WS2 image |  | Local Trainer submits the files |
| 10/22/2020 | 10:00 | A2 | Response |  |  | IT (security) department | Security Representative | Information on the situation and planned actions |  |  |
| 10/22/2020 | 10:20 | A2 | Response |  |  | Security Representa-tive |  | Evaluation: risk, damage |  |  |
| 10/22/2020 | 11:00 | A2 | Response |  |  | IT (security) department |  | **Starts a WS2 forensics** |  |  |
| 10/22/2020 | 11:00 | A2 | Response |  |  | WS2 user | IT administra-tor | Request to create conditions for work as soon as possible due to customer dissatisfaction. | email2.0-WS2user -ITadmin |  |
| 10/22/2020 | 11:10 | A2 | Info |  |  | The IT administrator is looking for opportunities to restore the workplace |  |  |  |  |
| 10/22/2020 | 11:30 | A2 |  | Option 1.1 |  | Director | Security Representative | Colleagues mentioned about the problems, what happened? What computers, what information were on them? |  |  |
| 10/22/2020 | 11:40 | A2 |  |  |  | Security Representa-tive | IT (security) department | Request for preliminary information on forensics. Were the services restored? |  |  |
| 10/22/2020 | 11:50 | A2 |  |  |  | IT (security) department | Security Representative | Initial assessment |  |  |
| 10/22/2020 | 12:00 | A2 |  |  |  | Security Representa-tive | Director | Initial assessment |  |  |
| 10/22/2020 | 13:00 | A2 |  | Option 1.2 |  | Media | Manager / Public relations professional | The company’s customers can’t get services, turning en masse to the media. The media asks for a comment from the manager / public relations professional. |  |  |
| 10/22/2020 | 13:10 | A2 |  | Option 1.1.1 |  | Security Representa-tive | IT (security) department | Request for preliminary information on forensics. Were the services restored? |  |  |
| 10/22/2020 | 13:10 | A2 |  | Option 1.2.1 |  | Public relations specialist | Security Representative; CC Director | What about here? Prepare an answer within 1 hour. |  |  |
| 10/22/2020 | 13:40 | A2 |  |  |  | Security Representa-tive; | Public relations specialist | Submission of information |  |  |
| 10/22/2020 | 14:00 | A2 |  |  |  | Public relations professional | Media | Press release |  |  |
| 10/22/2020 | 16:00 | A2 |  |  |  | Security Representative | All employees | Preliminary results of the forensics, recommendations. |  |  |
| 10/22/2020 | 16:30 | A2 |  | Option 2.1 |  | Security Representa-tive | Institutions | Reporting about the incident. |  |  |
| 10/22/2020 | 16:30 | A2 |  | Option 2.2 |  | Security Representa-tive | Institutions | Do not inform on the incident. Does not meet the requirements. |  |  |
| 10/22/2020 |  | A2 |  | Option 3.1. |  | IT (security) department, Security Representa-tive, Public relations | Management | Periodic information on the situation. |  |  |
| 10/23/2020 | 8:00 | A2 |  | Option 3.2. |  | IT (security) department | Security Representative | Final forensics results, report. Gap identified / |  |  |
|  |  |  |  |  |  |  |  | hacking vector detected (weak password), user list audited, etc. |  |  |
| 10/23/2020 | 8:00 | A2 |  |  |  | IT (security) department | Manage-ment, Security Representa-tive, Employees | Information on the forensics of incident. |  |  |
| 10/23/2020 | 9:00 | A2 |  | Option 4.1. |  | Security Representa-tive | NKSC, VDAI, Police | Information about incident elimination information in accordance with internal procedures and NKIVP |  |  |
| 10/23/2020 | 9:00 | A2 |  | Option 4.2. |  | Security Representa-tive | NKSC, VDAI, Police | Do not inform on the incident. Does not meet the requirements. |  |  |
| 10/23/2020 | 10:00 | A2 |  |  |  | Security Representa-tive | Media | Press release about the incident and possible damage to all who downloaded file attachment No.1 .xlsx |  |  |
| 10/23/2020 | 10:00 | A2 |  |  |  | Security Representa-tive | Local instructor | Do not make the incident public. |  |  |
| 10/23/2020 | 11:00 | A2 |  |  |  | Journalist | Public relations or Security Representa-tive or Director | Information has appeared in the public domain (IT security community forums) that an infected \* .xlsx file could be downloaded from your site yesterday. A screenshot of the site is attached and request for a comment is added. |  |  |
| 10/23/2020 | 11:00 | A2 |  |  |  | Public relations | Security Representa-tive, Director | A comment is required |  |  |
| 10/23/2020 | 13:00 | A2 |  |  |  | Public relations | Journalist | Answer / Press release. |  |  |

Annex No. 7. Storyline A3 – exploiting WP vulnerability

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Date** | **Time** | **SL** | **Type** | **Action line variation** | **Who is respon-sible** | **From** | **To** | **Description** | **External file** | **Comment** |
| 10/21/2020 | 15:50 | A3 | Info |  |  |  |  | WP Vulnerability of WWW2 is exploited . The WP CMS administrator password and access to the DB are obtained. Connection to the site CMS is established. A CMS user **Insider** is created (it will be used later for data leakage). |  |  |
| 10/21/2020 | 16:10 | A3 | Info |  |  |  |  | The malicious file "remote work order.pdf" is placed in the CMS. The document is uploaded to an automatically synced directory. File is distributed to WS2 and WS3. The "remote work order" file opens in both WS2 and WS3. |  |  |
| 10/21/2020 | 16:30 | A3 | Info |  |  |  |  | With DB access, the DB (sql\_dump) is exported and downloaded. |  |  |
| 10/21/2020 | 16:40 | A3 | Info |  |  |  |  | Attacker A connects to WS3, runs Meterpreter (reverse shell), runs Keystrokes (keylogger) |  |  |
| 10/21/2020 | 16:50 | A3 | Info |  |  |  |  | Attacker A takes over stored in WS3 login data (VPN certificates, RDP settings). Waits until the network administrator connects to the organization's network (receives a username / password). |  |  |
| 10/21/2020 | 17:10 | A3 | Info | Option 1.1 |  |  |  | Using VPN certificates stored in WS3, Attacker B connects to the organization's AD server. |  |  |
| 10/21/2020 | 18:00 | A3 | Info | Option 1.2 |  |  |  | Because access to the organization's network requires not only certificates but also passwords, Attacker B waits until the administrator connects to the organization's network by entering the login name / password, which is read by keeloger. |  |  |
| 10/21/2020 | 19:00 | A4 | Info |  |  |  |  | The attacker enters the organization's network. Connects to DC, exports user data to user-list.txt file. This file is uploaded to WWW2 and retrieved from there. |  |  |
| 10/22/2020 | 9:00 |  | Response |  | State Infra- structure | Website administrator | Security Representa-tive | Question about a new CMS user **Insider** found. | email1.0-web-admin--saugos-igaliotinis |  |
| 10/22/2020 | 9:20 |  | Response |  |  | Security Representa-tive | IT (security) department | Conduct forensics of WWW2. |  |  |
| 10/22/2020 | 9:30 |  | Response |  |  | IT (security) department | Website administra-tor / IT Administra-tion Dept. | Request to provide WWW2 image, logs, network traffic images. |  |  |
| 10/22/2020 | 10:00 |  | Response |  |  | Website administrator /IT Administra-tion Dept. | IT (security) department | The requested data is provided |  | State Infrastructure submits |
| 10/22/2020 | 10:10 |  | Response |  |  | IT (security) department |  | Starts forensics of WWW2. |  |  |
| 10/22/2020 | 12:30 |  | Response |  |  | Security Representa-tive | IT (security) department | What are the preliminary results of the forensics? |  |  |
| 10/22/2020 | 13:00 |  | Response |  |  | Security Representa-tive | NKSC | Information about Cyber Incident |  |  |
| 10/22/2020 | 14:00 |  | Info |  |  |  |  | The head of the organization receives an e-mail from a malicious person who stole data. | email1.0-piktavalis--Director |  |
| 10/22/2020 | 14:10 |  | Response |  | State Infra- structure | Director | TD, Security Representa-tive | E-mail with the text "I received a message blackmailing that they have our data, a screenshot is attached. Really? Do I have to inform the VDAI, NKSC, Police?" | email2.0-Director--saugos-igaliotinis |  |
|  |  |  |  |  |  |  |  |  | sarasas.txt |  |
| 10/22/2020 | 14:30 |  | Response |  |  | Website administrator / IT Administration Dept. | IT (security) department | The requested data is provided |  | State Infrastructure submits |
| 10/22/2020 | 14:40 |  | Response |  |  | IT (security) department |  | Starts forensics of WWW2. |  |  |
| 10/22/2020 | 15:00 |  | Response |  |  | Security Representa-tive | IT (security) department | What are the preliminary results of the forensics? |  |  |
| 10/22/2020 | 16:00 |  | Response |  |  | Security Representa-tive | NKSC, VDAI | Reporting about a cyber incident and leakage of personal data. |  |  |

Annex No. 8. Storyline B1 – distant workplace attack

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Date** | **Time** | **SL** | **Type** | **Action line variation** | **Who is respon-sible** | **From** | **To** | **Description** | **External file** | **Comment** |
| 10/20/2020 | 10:00 | B1 | Info |  |  |  |  | Attacker B communicates in the chat room of the game platform STEAM with the child of a WS 3 user (who is the organization’s IT administrator). |  |  |
| 10/20/2020 | 13:00 | B1 | Info |  |  |  |  | The child complains that the computer is too weak for games. He gets advice to google about this problem. |  |  |
| 10/20/2020 | 17:00 | B1 | Info |  |  |  |  | Attacker B sends a link to the document "instruction.pdf". The child opens the document. The document is empty. WS3 is preowned (reverse-shell (Meterpreter) is established). User mr1cry with administrator rights will be created. The keylogger is activated. |  |  |
| 10/20/2020 | 17:10 | B1 | Info | Option 1.1 |  |  |  | Using VPN certificates stored in WS3, Attacker B connects to the organization's AD server. |  |  |
| 10/20/2020 | 18:00 | B1 | Info | Option 1.2 |  |  |  | Because access to the organization's network requires not only certificates but also passwords, Attacker B waits until the administrator connects to the organization's network by entering the login name / password, which is read by keeloger. |  |  |
| 10/20/2020 | 18:10 | B1 | Info |  |  |  |  | The list of users with password hashes is exported to the file, the file is uploaded to WWW2 and downloaded from Attacker B. The file is uploaded for public viewing on the Internet. |  |  |
| 10/20/2020 | 18:20 | B1 | Info |  |  |  |  | A file (system-update.exe) with ransomware is uploaded to the synchronized directory. |  |  |
| 10/21/2020 | 1:00 | B1 | Info |  |  |  |  | The head of the organization receives an e-mail from a malicious person who stole data. | email1.0-piktavalis--Director |  |
| 10/21/2020 | 9:00 | B1 | Response |  | VI | Director | TD, Security Representa-tive | E-mail with the text "I received a message blackmailing that they have our data, a screenshot is attached. Really? Do I have to inform the VDAI, NKSC, Police?" | email2.0-Director--saugos-igaliotinis |  |
|  |  |  |  |  |  |  |  |  | sarasas.txt |  |
| 10/21/2020 | 9:10 | B1 | Response |  |  | Security Representative | IT (security) department | Procedure to conduct a forensics. |  |  |
| 10/21/2020 | 9:20 | B1 | Response |  |  | IT (security) department | IT Administra-tion Dept | Request for AD image, network traffic image. |  |  |
| 10/21/2020 | 9:30 | B1 | Response |  |  | IT Administra-tion Dept. | IT (security) department | IT administrators provide the requested data. |  |  |
| 10/21/2020 | 10:00 | B1 | Response |  | VI | IT (security) department |  | A forensics is launched |  |  |
| 10/21/2020 | 12:00 | B1 | Response |  |  | Security Representative | NKSC, VDAI | Information on the cyber inicident forensics and leakage of personal data. |  |  |
| 10/21/2020 | 13:00 | B1 | Response |  |  | Director | Security Representa-tive | What are the preliminary results of the forensics? |  |  |
| 10/21/2020 | 15:00 | B1 | Response |  | VI | Media | Public relations or Security Representa-tive or Director | Information has appeared in the public domain (IT security community forums) that user data for your organization is public. A screenshot of the site is attached and request for a comment is added | email3.1-zurnalistas--Director.txt sarasas\_pastebin.png |  |
| 10/21/2020 | 16:00 | B1 | Response |  |  | Public relations | Security Representa-tive | Need help for preparing the answer to media |  |  |
| 10/21/2020 | 16:30 | B1 | Response |  |  | Public relations | Director | Public announcement, position, response media |  |  |

Annex No. 9. Trainers Manual. Description of the Attacks

**WWW1 (Windows)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Question** | **Answer** | **Hints** | **How answer should be found** |
| How was the site taken over?  When was this done?  Which CMS plugin was vulnerable? | An SQL injection-type attack was performed to exploit a vulnerability in the WordPress (WP) plugin.  2020-10-19 12:21  An outdated version of the WP plugin has been used Wp-FileManager 1.2, WordPress <= 1.5.1.1. | 1. Run WWW1 VM in virtual environment, view WWW1 Apache / CMS log entries, view WP plugin versions. 2. View the separate WWW1 Apache log file Access.log. 3. View a copy of the network traffic (pcap) with Wireshark. | C:\xampp\htdocs\wp\wp-content\plugins\wp-filemanager.php  C:\xampp\htdocs\wp\wp-includes\version.php  Export Apache.log: error.log, access.log.  C:\xampp\apache\logs\access.log  42.83.90.245 - [19/Oct/2020:12:21:13 +0300] "GET /wp/index.php?c at=999%20UNION%20SELECT%20null,CONCAT(CHAR(58),user\_pass,CHAR(58),user\_login, CHAR(58)), null,null,null%20FROM%20wp\_users HTTP/1.1" 200 3077 "-" " LWP::Simple/6.36 libwww-perl/6.36"  42.83.90.245 - [19/Oct/2020:12:57:51 +0300] "GET /wp/index.php? cat=999%20UNION%20SELECT%20null,CONCAT(CHAR(58),user\_pass,CHAR(58),user\_login, CHAR(58)),null,null,null%20FROM%20wp\_users HTTP/1.1" 200 3077 "-" "LWP::Simple/6.36 libwww-perl/6.36" |
| What malicious request was sent?  When was it sent?  From what IP address was this done?  What was its purpose? | /wp/index.php?cat=999%20UNION%20SELECT%20null,CONCAT(CHAR(58), user\_pass,CHAR(58),user\_login,CHAR(58)),null,null,null%20FROM%20wp\_users  2020-10-19 12:58  42.83.90.245  To extract the username (itadmin) and password from the wp-admin.php file. | 1. Run the WWW1 VM in a virtual environment, view WWW1 Apache / CMS log entries. 2. View the separately provided WWW1 Apache log entry file Access.log, search for the GET method. 3. View network traffic copy (pcap), HTTP. | C:\xampp\apache\logs\access.log  42.83.90.245 - [19/Oct/2020:12:58:25 +0300] "POST /wp/wp-admin/fm.php?&output=upload&upload=true HTTP/1.1" 200 9455 "-" "python-requests/2.21.0"  42.83.90.245 - [19/Oct/2020:12:58:30 +0300] "GET /wp/files/win32.exe HTTP/1.1" 200 3514368 "-" "python-requests/2.21.0" |
| What CVE has been exploited? | EDB-ID:1033 CVE: 2008-0222 | After determinating the version of the plugin, search the CVE and EDB vulnerability databases | <https://www.exploit-db.com/exploits/1033> <https://www.exploit-db.com/exploits/4844> |
| What actions was taken by the villain who connected to the CMS  When were these actions performed? | Uploaded the win32.exe file to the directory C:\xampp\htdocs\wp\files\  2020-10-19 12.58 | * + - 1. Run the WWW1 VM in a virtual environment, view WWW1 Apache / CMS log entries.       2. View the separate WWW1 Apache log entry file Access.log with a text editor.       3. View network traffic copy (pcap), HTTP. | C:\xampp\apache\logs\access.log  42.83.90.245 - [19/Oct/2020:12:58:25 +0300] "POST /wp/wp-admin/fm.php?&output=upload&upload=true HTTP/1.1" 200 9455 "-" "python-requests/2.21.0"  42.83.90.245 - [19/Oct/2020:12:58:30 +0300] "GET /wp/files/win32.exe HTTP/1.1" 200 3514368 "-" "python-requests/2.21.0" |
| How did the file spread after the organization's workstations? | Directory C:\xampp\htdocs\wp\files\  Is synchronized by the file server with the workstations. Users receive notifications about a file shared with them. |  | Where to find FS communications with WS?  Pcap, search command → ip.addr == 83.171.43.82  Or on the fileshare(fs) machine go to the directory /var/www/html/nextcloud/data  image name: fs\_organizacija\_ks2020\_lt |
| What IP addresses possibly have downloaded malicious code from your website WWW1? | 20 external IP addresses?  42.83.90.245  125.83.12.245  42.12.12.21  43.85.91.245  42.83.15.32  42.83.15.19  42.83.14.35  42.83.36.95  42.83.45.65  42.83.78.154  42.83.56.214  42.83.10.26  42.83.11.125  42.83.11.48  42.83.67.15  42.83.78.45  42.83.62.22  42.83.15.15  42.83.54.51  42.83.22.44 | * + - 1. Run the WWW1 VM in a virtual environment, view WWW1 Apache / CMS log entries.       2. View the separate WWW1 Apache log file Access.log.       3. View the HTTP GET method in journal entries. | Make a "http" filter and look for information related to "GET" in the win32.exe file.  3.C:\xampp\apache\logs\access.log  42.83.62.22 - [19/Oct/2020:12:59:38 +0300] "GET /wp/files/win32.exe HTTP/1.1" 200 3514368 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko" |

**WWW2 (Windows)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Question** | **Answer** | **Hints** | **How answer should be found** |
| How the site was taken over.  When was this done?  Which CMS plugins were vulnerable? | Exploiting a vulnerability in the WP plugin (Wordpress Site Import 1.0.1).  2020-10-19 13:00  wp-FileManager-1.3.0  Site Import 1.0.1 **–** the attack was executed due to this plugin | 1. Run WWW2 VM in virtual environment, view WWW2 Apache / CMS log entries, view WP plugin versions. 2. View the separate WWW2 Apache log file Access.log. 3. With Wireshark view a copy of network traffic (pcap) | After logging in to the content management system as an administrator and clicking on “Plugins”.  C:\xampp\htdocs\wp\wp-content\plugins\ wp-filemanager\wp-filemanager.php  C:\xampp\htdocs\wp\wp-content\plugins\ site-import\site-import.php |
| What malicious request was sent?  When was it sent?  From what IP address was this done?  What was (could have been) the purpose of the request? | http://10.10.15.151/wp/wp-content/plugins/ site-import/admin/page.php?url= ..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\xampp\htdocs\wp\wp-config.php  2020-10-19 13:00  83.171.42.241  The goal is to get the CMS administrator name / password and DB username / password logins / passwords from the WP-config.php file. | 1. Run WWW2 VM in virtual environment, view WWW2 Apache / CMS log entries, view WP plugin versions. 2. View the separate WWW2 Apache log file Access.log. 3. With Wireshark view a copy of network traffic (pcap) | C:\xampp\apache\logs\access.log  83.171.42.241 - [19/Oct/2020:13:00:34 +0300] "GET /wp/wp-content/plugins/site-import/admin/page.php?url=. .%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5 Cxampp%5Chtdocs%5Cwp%5Cwp-config.php HTTP/1.1" 200 3137 "-" "Wget/1.20.1 (linux-gnu)"  Open pcap with Wirreshark and look for a GET query with the wp-config.php file. |
| What CVE has been exploited? | EDB-ID:25440 EDB-ID:39558 | Once the plugin version has been determined, search the CVE and EDB vulnerability databases | https://www.exploit-db.com/exploits/25440  [https://www.exploit-db.com/exploits/39558](https://www.exploit-db.com/exploits/39558%20) |
| Which user account was used by a malicious person to sign in to CMS and when? | An user Insider account has been used to sign in to CMS.  2020-10-19 13:09 | 1. Run WWW2 VM in virtual environment, view WWW2 Apache / CMS log entries. 2. View the separate WWW2 Apache log file Access.log. 3. With Wireshark view a copy of network traffic (pcap) | C:\xampp\apache\logs\access.log  77.111.247.11 - [19/Oct/2020:13:09:12 +0300] "POST /wp/wp-login.php HTTP/1.1" 302 - "http://83.171.40.243/wp/wp-login.php?redirect\_to=http%3A%2F%2 F83.171.40.243 %2Fwp%2Fwp-admin%2F&reauth=1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36 OPR/68.0.3618.173" |
| What further action did the malicious person take and when?  From what IP address were the actions taken?  When were the actions taken? | Created by CMS user Insider to connect to a content management system and upload a malicious file  remote\_work order.pdf  2020-10-19 13:15  Connecting to WS3 at 2020-10-19 13:25  User mr1kry vas created at 2020-10-19 13:29  Attacker A connects via RDP from IP 196.240.54.44 at 2020-10-19 14:01  Access to AD (DC)  (directory - C:\xampp\htdocs\wp). After running this file initiates a connection to the malicious workstation (via a reverse shell).  Using password for DB found in wp-config.php, logged in to the DB and performed the DB export (file ks2020\_www2.sql)  Download time: 19/10/2020 13:05  Insider creation time: 2020-10-19 13:02  IPv6: 2001:67c:2660:425:4::10a  IPv4: 77.111.247.40 | 1. Run WWW2 VM in virtual environment, view WWW2 Apache/TVS/mySQL log entries. 2. View the separate WWW2 Apache log file Access.log. 3. With Wireshark view a copy of network traffic (pcap) | In pcap use filter „mysql“  and look for what commands have been executed  Attacker A: 77.111.247.11  OpenVPN key was uploaded to WWW2 (client.zip file): 2020-10-19 14:04 and downloaded by Attacker A at 2020-10-19 14:05  C:\xampp\apache\logs\access.log  83.171.42.241 - [19/Oct/2020:14:05:30 +0300] "GET /wp/client.zip HTTP/1.1" 200 5312 "-" "Wget/1.20.1 (linux-gnu)"  user-list.txt (C:\Windows\) 14:12  file uploaded to WWW2 (user Insider) at 14:17. Attacker A downloads user-list.txt at 14:17  C:\xampp\apache\logs\access.log  83.171.40.185 - [19/Oct/2020:14:17:29 +0300] "POST /wp/wp-admin/admin.php?page= wp-filemanager%2Ffm.php&output=upload&upload=true HTTP/1.1" 200 66051 "http://83.171.40.243/wp/wp-admin/admin.php?page=wp-filemanager%2Ffm.php &path&action=upload" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0" |
| How was the database leaked to the outside?  From what IP address was it downloaded?  When was it downloaded? | The exported DB (file - ks2020\_www2.sql) is placed in the WWW2 directory C:\xampp\htdocs\wp\wp-admin\ and downloaded.  IP: 83.171.42.241  2020-10-19 13:05 | * + - 1. Run the WWW2 VM in a virtual environment, view WWW2 Apache / CMS log entries.       2. View the separate WWW2 Apache log entry file Access.log, search for GET queries.       3. View a copy of the network traffic (pcap) with Wireshark. | Look for GET suspicious queries in C:\xampp\apache\logs\access.log.  83.171.42.241 - [19/Oct/2020:13:04:57 +0300] "GET /wp/wp-admin/ks2020\_www2.sql HTTP/1.1" 200 71228 "-" "Wget/1.20.1 (linux-gnu)" |
| How was the AD data leaked outwards?  From what IP address was it downloaded?  When was it downloaded? | Exported AD data (file user-list.txt) placed in WWW2 directory C: \ xampp \ htdocs \ wp \ wp-admin \ and downloaded.  83.171.42.241  2020-10-19 14:17 | * + - 1. Run the WWW2 VM in a virtual environment, view WWW2 Apache / CMS log entries.       2. View the separate WWW2 Apache log entry file Access.log, search for GET queries.       3. View a copy of the network traffic (pcap) with Wireshark. | 83.171.42.241 - [19/Oct/2020:14:17:51 +0300] " GET /wp/user-list.txt HTTP/1.1" 200 3177 "-" "Wget/1.20.1 (linux-gnu)" |

**WWW 3 (IDAMAS – Linux)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Question** | **Answer** | **Hints** | **How answer should be found** |
| Which user uploaded the file priedasNr1.xlsm?  From what IP address was the file uploaded?  When was the file uploaded? | Itadmin,  *42.83.90.245*  2020-10-19 10:56 (Brute force attack begins)  2020-10-19 11:59 | 1. Run WWW3 VM in virtual environment, view WWW3 Apache / MySQL log entries. 2. View the separate WWW3 Apache log entry file Access.log. 3. With Wireshark view a copy of network traffic (pcap) | *Email naudotojas@organizacija.ks2020.lt opened:* 2020-10-19 12:03*. (files uploaded at 12:10)*  42.83.90.245 - [19/Oct/2020:11:59:19 +0000] " POST /action.php?ru=XYJ1P13WCt HTTP/1.1" 302 604 "-" "python-requests/2.21.0" |
| How was connected to the site (what type of attack)?  From what IP address was connected?  When was logged in? | Bruteforce attack trying connect using 20,000 of the most popular passwords.  user: itadmin,  password: Ks2020-7  IP: 42.83.90.245  2020-10-19 11:47 | 1. Run the WWW3 VM in a virtual environment, view the WWW3 Apache / MySQL log entries.  2. Log in to the database and look up a large number of log attempts in the log table.  3. View the separate WWW3 Apache log entry file error.log. With Wireshark view a copy of network traffic (pcap). Search for attempts to connect. Watch after which POST to wp-login.php started the session and cookies were set. | */var/*www/html/system/config.php  Let's see what the login to data base details are.  Let's run the command: mysql -u itadmin -p  Enter the password "ks2020-7-mysql"  Commands after connection were established:  “show databases;”  “use ks2020\_www3;  “show tables;”  “select \* from logs;” |
| Search for attempts connect to site.  */var/log/apache/access.log*  42.83.90.245 - [19/Oct/2020:11:47:00 +0000] " POST /action.php?ru=cy6B3F86KH HTTP/1.1" 302 1347 "-" "python-requests/2.21.0"  42.83.90.245 - [19/Oct/2020:11:47:00 +0000] "GET /l.php?tmpl\_into[0]=index&tmpl\_name[0]=m\_site\_index2&tmpl\_into[ 1]=middle&tmpl\_name[1]=m\_admin\_administration&no\_cache= 1 HTTP/1.1" 302 445 "-" "python-requests/2.21.0" |
| What actions was taken by the villain who connected to the CMS. | File upload. | 1. Run WWW3 VM in virtual environment, view / analyze WWW3 CMS events. 2. View the separately provided WWW3 Apache log entry file access.log, search for the POST method. 3. With Wireshark, view a copy of the network traffic (pcap), collect the objects transferred in the network traffic. | Search for information in both Apache log entries and pcap with Wireshark using the query “POST /action.php?ru=XYJ1P13WCt”  and in pcap you will see what file and with what name was uploaded |
| What files were uploaded online and when?  Which directory was used for uploading? | priedasNr1.xlsm  2020-10-19 11:59  update1.ps1  2020-10-19 12:02  Directory: /var/www/html/tinklarastis/m/m\_files/wfiles/ | * + - 1. Run WWW3 VM in virtual environment, analyze events in WWW3 CMS.   Note: Idam CMS renames the file after uploading  (file \* number \*.xlsm)  (file \* number \*.ps1)   1. View WWW3 Apache log access.log, search for POST method. 2. With Wireshark, view a copy of the network traffic (pcap), collect objects. | Search for information in both Apache log entries and pcap with Wireshark using the query “POST /action.php?ru=XYJ1P13WCt”  and in pcap you will see what file and with what name was uploaded |
| Who (which workstation) from our organization (from what IP address) downloaded the file?  From what IP address download was performed?  When files were downloaded? | WS1  IP 10.10.15.5  2020-10-19 12:10 | 1. View WWW3 Apache log access.log with a text editor, look for the GET method. 2. With Wireshark view a copy of the network traffic (pcap), filter by IP DST address (WS1). | 10.10.15.5 - [19/Oct/2020:12:10:33 +0000] "GET /tinklarastis/m/m\_files/wfiles/file7.xlsm HTTP/1.1" 200 13967 "http://10.10.15.118/tinklarastis/m/m\_files/wfiles/" " Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 OPR/71.0.3770.228"  10.10.15.5 - [19/Oct/2020:12:10:35 +0000] " GET /tinklarastis/m/m\_files/wfiles/file8.ps1 HTTP/1.1" 200 2043 "http://10.10.15.118/tinklarastis/m/m\_files/wfiles/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 OPR/71.0.3770.228" |

**WWW 3 (WordPress Windows)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Question** | **Answer** | **Hints** | **How answer should be found** |
| Which user uploaded the file priedasNr.1.xlsm?  From what IP address was the file uploaded?  When was the file uploaded? | Itadmin,  42.83.90.245  2020-10-19 10:56 (Brute force attac)  2020-10-19 11:59 | 1. Run WWW3 VM in virtual environment, view WWW3 Apache / MySQL log entries. 2. View the separate WWW3 Apache log entry file Access.log. 3. With Wireshark view a copy of network traffic (pcap) | *Email naudotojas@organizacija.ks2020.lt opened:* 2020-10-19 12:03 *(files uploaded at 12:10)*  42.83.90.245 - [19/Oct/2020:11:59:38 +0300] "POST /wp/wp-content/plugins/page-flip-image-gallery/upload.php HTTP/1.1" 200 23 "-" "python-requests/2.21.0" |
| How was connected to the site (what type of attack was performed)?  From what IP address was connected?  When was logged in? | Bruteforce attack trying connect using 20,000 of the most popular passwords  user: itadmin,  password: Ks2020-7  42.83.90.245  2020-10-19 11:45 | * + - 1. Run the WWW3 VM in a virtual environment, view the WWW3 Apache / MySQL log entries. Log in to the database and look for a large number of log attempts in the log table.       2. View the separate WWW3 Apache log entry file error.log.  1. View a copy of the network traffic (pcap) with Wireshark. Search for attempts to connect. View after which POST to wp-login.php started a session and cookies were set. | C:\xampp\apache\logs  42.83.90.245 - [19/Oct/2020:11:45:07 +0300] "POST /wp/wp-login.php HTTP/1.1" 200 5384 "-" "python-requests/2.21.0"  42.83.90.245 - [19/Oct/2020:11:45:07 +0300] "GET /wp/wp-admin/index.php HTTP/1.1" 200 50013 "-" "python-requests/2.21.0"  Pcap“ wireshark:  Apply the filter "http" and look for a successful login to the site. |
| What actions was taken by the villain who connected to the CMS. | File upload. | * + - 1. Run WWW3 VM in virtual environment, view / analyze WWW3 CMS events.       2. View the separately provided WWW3 Apache log entry file access.log, search for the POST method.       3. With Wireshark, view a copy of the network traffic (pcap), collect objects. | Pcap“ wireshark:  Apply the filter "http" and look for „POST /wp/wp-content/plugins/page-flip-image-gallery/upload.php“ |
| What files were uploaded online and when?  Which directory was used for uploading? | priedasNr1.xlsm  2020-10-19 11:59  update1.ps1  2020-10-19 12:02  C:\xampp\htdocs\wp\wp-content\pageflip\upload | * + - 1. Run WWW3 VM in virtual environment, analyze events in WWW3 CMS.       2. View WWW3 Apache logos access.log, search for POST method.       3. With Wireshark, view a copy of the network traffic (pcap), collect objects. | 42.83.90.245 - [19/Oct/2020:11:59:38 +0300] "POST /wp/wp-content/plugins/page-flip-image-gallery/upload.php HTTP/1.1" 200 23 "-" "python-requests/2.21.0"  42.83.90.245 - [19/Oct/2020:12:02:35 +0300] "POST /wp/wp-content/plugins/page-flip-image-gallery/upload.php HTTP/1.1" 200 - "-" "python-requests/2.21.0" |
| Who (which workstation) from our organization (from what IP address) downloaded the file?  From what IP address download was performed?  When files were downloaded? | WS1,  10.10.15.5  2020-10-19 12:09:01  2020-10-19 12:09:26 | * + - 1. Run WWW3 VM in virtual environment, analyze events in WWW3 CMS.       2. View WWW3 Apache logos access.log, search for GET method.       3. With Wireshark, view a copy of the network traffic (pcap), collect objects. | 10.10.15.5 - [19/Oct/2020:12:09:01 +0300] "GET /wp/wp-content/pageflip/upload/update1.ps1 HTTP/1.1" 200 1783 "http://10.10.15.89/wp/wp-content/pageflip/upload/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 OPR/71.0.3770.228"  10.10.15.5 - [19/Oct/2020:12:09:26 +0300] "GET /wp/wp-content/pageflip/upload/priedasNr1.xlsm HTTP/1.1" 200 13642 "http://10.10.15.89/wp/wp-content/pageflip/upload/" " Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 OPR/71.0.3770.228" |

**WWW 3 (WordPress Linux)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Question** | **Answer** | **Hints** | **How answer should be found** |
| Which user uploaded the file priedasNr.1.xlsm?  From what IP address was the file uploaded?  When was the file uploaded? | Itadmin,  42.83.90.245  2020-10-19 11:50 (Brute force attac)  2020-10-19 11:58 | 1. Run WWW3 VM in virtual environment, view WWW3 Apache / MySQL log entries. 2. View the separate WWW3 Apache log entry file Access.log. 3. With Wireshark view a copy of network traffic (pcap) | *Email naudotojas@organizacija.ks2020.lt* opened*:* 2020-10-19 12:03 *(files uploaded at 12:07)*  42.83.90.245 - [19/Oct/2020:11:58:56 +0000] "POST /wp-content/plugins/page-flip-image-gallery/upload.php HTTP/1.1" 200 202 "-" "python-requests/2.21.0" |
| How was connected to the site (what type of attack was performed)?  From what IP address was connected?  When was logged in? | Brute force attack trying connect using 20,000 of the most popular passwords  user: itadmin,  password: Ks2020-7  42.83.90.245  2020-10-19 11:56 | * + - 1. Run the WWW3 VM in a virtual environment, view the WWW3 Apache / MySQL log entries. Log in to the database and look for a large number of log attempts in the log table.  1. View the separate WWW3 Apache log entry file error.log. 2. View a copy of the network traffic (pcap) with Wireshark. Search for attempts to connect. View after which POST to wp-login.php started a session and cookies were set. | */var/*log/apache2/access.log  42.83.90.245 - [19/Oct/2020:11:56:07 +0000] "POST /wp-login.php HTTP/1.1" 200 3129 "-" "python-requests/2.21.0"  42.83.90.245 - [19/Oct/2020:11:56:07 +0000] "GET /wp-admin/index.php HTTP/1.1" 200 13251 "-" "python-requests/2.21.0"  Apply the filter "http" and look for a successful login to the site. |
| What action was taken by the villain who connected to the CMS? | File upload. | * + - 1. Run WWW3 VM in virtual environment, view / analyze WWW3 CMS events.       2. View the separately provided WWW3 Apache log entry file access.log, search for the POST method.       3. With Wireshark, view a copy of the network traffic (pcap), collect objects. | Search for information in both Apache log entries and pcap with Wireshark using the query „*POST /wp-content/plugins/page-flip-image-gallery/upload.php“*” |
| What files were uploaded online and when?  Which directory was used for uploading? | priedasNr1.xlsm  2020-10-19 11:58  update1.ps1  2020-10-19 12:02  /var/www/html/wp-content/pageflip/upload/ |  | Search for information in both Apache log entries and pcap with Wireshark using the query „*POST /wp-content/plugins/page-flip-image-gallery/upload.php*  42.83.90.245 - [19/Oct/2020:11:58:56 +0000] "POST /wp-content/plugins/page-flip-image-gallery/upload.php HTTP/1.1" 200 202 "-" "python-requests/2.21.0"  42.83.90.245 - [19/Oct/2020:12:02:40 +0000] "POST /wp-content/plugins/page-flip-image-gallery/upload.php HTTP/1.1" 200 202 "-" "python-requests/2.21.0" |
| Who downloaded the file? | ws1 | Windows user WS1 | Tik apache loguose tiek „pcap“ matosi  It is seen in both Apache logs and pcap |
| Who (which workstation) from our organization downloaded the file?  From what IP address download was performed?  When files were downloaded? | WS1,  10.10.15.5  2020-10-19 12:07:50  2020-10-19 12:07:52 | * + - 1. Run WWW3 VM in virtual environment, view / analyze WWW3 CMS events.       2. View the separately provided WWW3 Apache log entry file access.log, search for the GET method.       3. With Wireshark, view a copy of the network traffic (pcap), collect objects. | 10.10.15.5 - [19/Oct/2020:12:07:50 +0000] "GET /wp-content/pageflip/upload/priedasNr1.xlsm HTTP/1.1" 200 13967 "http://10.10.15.243/wp-content/pageflip/upload/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 OPR/71.0.3770.228"  10.10.15.5 - [19/Oct/2020:12:07:52 +0000] "GET /wp-content/pageflip/upload/update1.ps1 HTTP/1.1" 200 2043 "http://10.10.15.243/wp-content/pageflip/upload/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 OPR/71.0.3770.228" |

**AD (domain controler)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Question** | **Answer** | **Hints** | **How answer should be found** |
| What new user was created on the DC server?  When was the new user created?  From what IP address? | New user mr2kry was created:  2020-10-19 14:58  IP address: 83.171.40.102 | 1. Run AD and WS3 images in a virtual environment. Use Event viewer on both machines, compare log entries (Security)r creation entry, Administrator login information (RDP). 2. View a copy of network traffic, use HTTP filter (pcap), collect objects. 3. View a copy of the network traffic, use the HTTP filter (pcap) on the AD server (connection to WWW2, user Insider). | View the AD Security.evtx file. Lines 374352 - 374397 show that a new user mr2kry has been created. The creation time is shown on the line 374359 – 2020-10-19 14:58  View the file Microsoft-Windows-TerminalServices-RemoteConnectionManager% 4Operational.evtx.  Lines 104-125 show the searched event.  EventID - 1149.  Line 119 shows the user who was logged in via the Remote Desktop App - Administrator.  Line 121 shows the IP address from which the connection was made - 83.171.40.102.  View the file www2\_isore.pcap. Applying the http.request.method == POST filter to this file and viewing line 56661 after expanding „HTML Form URL Encoded“, the login name and password of the user who sent the files extracted from the DC server are visible. |
| What information was taken from the DC server?  Ar netrūksta čia klausimų? | User list Sarasas.txt (storyline B1) has been extracted.  Sarasas.txt was uploaded to FS for retrieval via WWW1 (after synchronization) at 2020-10-19 15:01  Sarasas.txt was uploaded to ???????  Attacker B:  IP: 83.171.41.220  2020-10-19 15:03  Extracted file user-list.txt.  user-list.txt placed in directory www2.  User-list.txt was uploaded to ???????  Attacker A:  IP: 83.171.42.241  2020-10-19 14:17 | View the C:\Windows directory | Sarasas.txt is in directory C:\Windows\  View the file nextcloud.log, which is located on the file sharing station (fs), in the / var / www / html / nextcloud / date directory. After executing the command more nextcloud.log | grep Sarasas.txt | grep 83.171.40.185, a line is returned showing that Sarasas.txt was placed in the Documents (2) directory of the nextcloud DC user account. Because this station has an EEST time zone, you need to add 3 hours to the upload time to get the actual time when the file was uploaded (2020-10-19 15:01).  View the file at www1.pcap. Apply the http.request.method == GET filter to this file, and the line number 61008 shows that the file Sarasas.txt was downloaded from the IP address 83.171.41.220 that belongs to Attacker B. After expanding the „Frame“ column, in the „Arrival Time“ line can be seen that the Attacker downloaded the file on 19/10/2020 15:03  Extracted file user-list.txt is in directory C:\Windows  View the file at www2\_isore.pcap. Apply the http.request.method == GET filter to this file, and the line number 57004 shows that the file user-list.txt was downloaded from the IP address 83.171.42.241 that belongs to Attacker A. After expanding the „Frame“ column, in the „Arrival Time“ line can be seen that the Attacker downloaded the file on 19/10/2020 14:17 |

**WS1**

|  |  |  |  |
| --- | --- | --- | --- |
| **Question** | **Answer** | **Hints** | **How answer should be found** |
| What type of attack was performed against the WS1 user?  When was it fulfilled?  Which e-mail was used? | Phishing attack  2020-10-19 12:03  f[oralllists@gmail.com](mailto:ForAllLists@gmail.com) | 1. Open a WS1 image in a virtual environment, analyze the message header (mail client, etc.) 2. Analyze the subject of the message (will be presented as a separate artifact). Export email message. | Open ThunderBird Mail Reader. Found the message, which was received at 12:03 p.m., and open it. The "from" line appears in the window that opens. The email on this line the mail is from the attacker. |
| What malicious files have been downloaded to WS1?  When was the malicious files downloaded? | In directory Downloads:  File7.xlsm ir File8.ps1 (when WWW3 is Idamas CMS).  2020-10-19 12:10  PriedasNr1.xlsm and update1.ps1 (when WWW3 is WordPress)  2020-10-19 12:07 | 1. Run WS1 image in virtual environment, view downloaded files (by date). 2. View a copy of network traffic, use HTTP filter (pcap), collect objects. | View the ws1.pcap file. After applying the filter „http.request.method == GET“ and reviewing lines 26521 and 26542, it can be seen that the file file7.xlsm and the file file8.ps1 have been downloaded. When you expand the column „Frame“, the „Arrival Time“ row shows the download time – 2020-10-19 12:10  View the ws1.pcap file. After applying the filter „http.request.method == GET“ and reviewing lines 24797 and 24813, it can be seen that the file priedasNr1.xlsm and the file update1.ps1 have been downloaded. When you expand the column „Frame“, the „Arrival Time“ row shows the download time – 2020-10-19 12:07. |
| What commands and when did the xlsm malicious files execute? | An xlsm file with macros commands downloaded a .ps1 attachment from WWW3 and launched it.  Running .ps1 establishes a reverse shell over TCP/IP port 8080.  2020-10-19 12:15 | 1. Run WS1 in a virtual environment. Use Event viewer to search Windows PowerShell to find records by the date, when the malicious file was downloaded. 2. View a copy of network traffic, use HTTP filter (pcap), collect objects. | When you open the PowerShell.evtx file, lines 284-529 show that the update1.ps1 file was run, which was downloaded and saved to C:\update1.ps1. When you open this file with a text editor, the first line shows that the TCP 8080 port has been used.  (TIME IN LOGS IS 3 HOURS BACK)  Using the ws1.pcap file, apply the filter „http.request.method == GET“, and the line number 32106 shows that the file file8.ps1 was downloaded, which was renamed to update1.ps1 during the download. The rename can be found by opening the file file7.xlsm in Excel and reviewing the macros. The download was completed on 19/10/2020 12:15.  Applying the filter „tcp.port == 8080“ to the ws1.pcap file shows that a session was established on port 8080 with an IP address of 83.171.42.241. |
| What were the next steps in the malicious actions fter establishing the connection?  When were these steps performed? | From the outside to the Nextcloud sync directory files were loaded:   * 8.1.2\_AdbeRdr812\_lt\_LT.exe (scanner with reverse shell)   2020-10-19 12:27   * Win32.exe   2020-10-19 12:27  Note: Win32.exe - Ransomware with symmetric key, decryption is possible.   * update\_new.exe   2020-10-19 12:27  User mr1kry was created on workstation WS1 on  2020-10-19 at 12:17  An internal network scan is initiated (TCP/IP ports 135, 137, 139, 445) pn  2020-10-19 at 12:55 |  | View the file nextcloud.log, which is located on the file sharing station (fs), in the / var / www / html / nextcloud / date directory. After executing the command more nextcloud.log | grep ws1 | grep PUT is seen that files 8.1.2\_AdbeRdr812\_en\_US.exe, Win32.exe and update\_new.exe have been shared from the ws1 nextcloud account.  2020-10-19 12:27  Lines 9400 -9446 in the Security.evtx file show that a new user (mr1kry) has been created.  Executed command:  net user mr1kry One12345 @ / add  2020-10-19 09:17 (3 HOURS)  The user is assigned to the Administrators group:  net localgroup Administrators mr1kry /add  2020-10-19 12:18  The user is assigned to the Remote Desktop group:  net localgroup "Remote Desktop Users" mr1kry /add  2020-10-19 12:18  C2 IP address  Use ws1 Application.evtx. Lines 421 - 641 show that the Advanced Port Scanner program that initiated the port scan was used. |

**WS2**

|  |  |  |  |
| --- | --- | --- | --- |
| **Question** | **Answer** | **Hints** | **How answer should be found** |
| How did the malicious file get to the WS2 workstation?  When did this file appear on workstation WS2? | The win32.exe file was loaded through a file synchronization server  From the outside to the Nextcloud sync directory files were loaded:   * 8.1.2\_AdbeRdr812\_lt\_LT.exe (skanner with reverse shell)   2020-10-19 12:47   * Win32.exe   2020-10-19 12:47  Note: Win32.exe - Ransomware with symmetric key, decryption is possible.   * update\_new.exe   2020-10-19 12:47 | 1. Run the WS2 image in a virtual environment. View the Windows Event Log (Application), Nextcloud client logs, and search for files that occurred during the incident. 2. View a copy of network traffic, use HTTP filter (pcap), collect objects. 3. Look for file synchronization information in the logs of the file server (nextcloud.log) | View the file nextcloud.log, which is located on the file sharing station (fs), in the / var / www / html / nextcloud / date directory.  After executing the command more nextcloud.log | grep ws2 | grep GET, the results show that via the ws2 nextcloud user were downloaded files 8.1.2\_AdbeRdr812\_lt\_LT.exe, Win32.exe, update\_new.exe 2020-10-19 09:47 |
| Who launched the malicious file and when? | ws2 user (name – Administrator)  Win32.exe (ransomware) was launched on  2020-10-19 at15:07 | Run a WS2 image in a virtual environment. | View the ws2 Application.evtx file. Lines 84-122 show that an ambiguous process was executed that clipped encrypted the workstation. Užkriptavo ???? |

**WS3 (Story Line A3)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Question** | **Answer** | **Hints** | **How answer should be found** |
| What malicious file was downloaded to WS3?  In which directory it was saved?  When was the malicious file downloaded? | Storyline A3:  nuotolinio\_darbo\_tvarka.pdf  (C:\Users\itadmin\NextCloud\)  2020-10-19 13:15 | * + - 1. Run the WS3 image in a virtual environment. See C: \ Windows \ Prefetch.       2. Look for file synchronization information in the log files of the file server (nextcloud.log) | View the file nextcloud.log, which is located on the file sharing station (fs), in the / var / www / html / nextcloud / date directory.  After executing the command more nextcloud.log | grep ws3 | grep GET among the results obtained it is seen that there is a file remote\_work\_order.pdf. This file has been saved in the nextcloud Documents directory 2020-10-19 13:15. |
| What commands were executed by the malicious file Nuotolinio\_darbo\_tvarka.pdf  Which TCP / IP address / port was communicated with?  When was the communication established? | Reverse-shell communication with the outside were established.  IP address 83.171.40.220  TCP/IP port:3301  2020-10-19 13:23 | * + - 1. Run the WS3 image in a virtual environment. See C: \ Windows \ Prefetch.       2. View a copy of network traffic, use HTTP filter (pcap), collect objects. | View the ws3.pcap file. Using the filter „tcp.port == 3301“ shows records that indicate that communication has been established with the 83.171.40.220 Ip address through port 3301. When you expand the „Frame“ column in the first record, the „Arrival Time“ row shows the start time 2020-10-19 13:23 |
| What were the further acts of malice when the connection was made, when were they made? | User „mr1kry“ has been created, this user was added to Administrators and RDP groups, Keylogger was enabled.  2020-10-19 13:28 | * + - 1. Run the WS3 image in a virtual environment. See C: \ Windows \ Prefetch.       2. View Windows Log (Security) log entries.       3. View Windows processes, look for an unusual process with port 3301. | View the ws3 Security.evtx file. Search for an event with ID number 4720. This ID means that a new user has been created. The event on lines 5082-5127 indicates that the user „mr1kry“ was created. An event with ID number 4672 means that special privileges have been granted to the user. Lines 5742 - 5772 show that the user „mr1kry“ has been added to the Administrators group. Lines 5773-5803 show that the user “mr1kry“ has been added to the Remote Desktop group. |
| What files were downloaded / sent to / from ws3 and to / from which IP address? | From the outside to the Nextcloud sync directory files were loaded:  • 8.1.2\_AdbeRdr812\_lt\_LT.exe (skanner with reverse shell)  2020-10-19 12:47  • Win32.exe  2020-10-19 12:47  Note: Win32.exe - Ransomware with symmetric key, decryption is possible.  • update\_new.exe  2020-10-19 12:25 | Search for newly created files during the incident (Win32.exe  8.1.2\_AdbeRdr812\_lt\_LT.exe, client1.ovpn).  View a copy of the network traffic, use an HTTP filter (pcap), collect objects (Win32.exe only).  Search for Windows Event RDP session, search for logins to AD. | View the file nextcloud.log, which is located on the file sharing station (fs), in the / var / www / html / nextcloud / date directory.  After executing the command more nextcloud.log | grep ws3 | grep GET, the results show that the files 8.1.2\_AdbeRdr812\_en\_LT.exe, Win32.exe, update\_new.exe were downloaded via the ws2 nextcloud user 2020-10-19 12: 24-27 |

**WS3 (Storyline B1)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Question** | **Answer** | **Hints** | **How answer should be found** |
| What malicious file was downloaded to WS3?  When was the malicious file downloaded? | instrukcija.pdf  (C:\Users\admin\Downloads\)  2020-10-19 14:35 | * + - 1. Run the WS3 image in a virtual environment. See C: \ Windows \ Prefetch.       2. View a copy of network traffic, use HTTP filter (pcap), collect objects.       3. Look for file synchronization information in the logs of the file server (nextcloud.log) | View the ws3.pcap file. After applying the filter „http.request.method == GET“ and reviewing the line number 2865951, it can be seen that the file instruction.pdf has been downloaded. When the „Frame“ column is expanded, the „Arrival Time“ row shows the download time - 2020-10-19 14:35 |
| What commands were executed by the malicious file **instrukcija.pdf**.  Which TCP / IP address / port was communicated with?  When was the communication established? | Užmezgė reverse-shell komunikaciją su išore.  IP address 83.171.40.220,  TCP/IP port: 3302  2020-10-19 14:44 | * + - 1. Run the WS3 image in a virtual environment. See C: \ Windows \ Prefetch.       2. View a copy of network traffic, use HTTP filter (pcap), collect objects. | View the ws3.pcap file. Using the filter „tcp.port == 3301“ filters out records that indicate that communication has been established with the IP address 83.171.40.220 through port 3301. When you expand the „Frame“ column in the first record, the „Arrival Time“ row shows the start time 2020-10-19 14:44 |
| What were the further acts of malice when the connection was made, when were they made. | All download client.zip (VPN files) were uploaded to FS (Nexcloud) and become available via WWW1  2020-10-19 14:46  Attacker B downloaded the client.zip file from WWW12020-10-19 14:50  OpenVPN has been started  2020-10-19 14:55 and connection with the AD was established  User „mr2kry“ was created in AD  2020-10-19 14:58 | * + - 1. Run the WS3 image in a virtual environment. See C: \ Windows \ Prefetch.       2. View Windows Log (Application) log entries.       3. View Windows processes, look for an unusual process with port 3302.       4. Search for Windows Event RDP session, search for logins to AD. | View the file nextcloud.log, which is located on the file sharing station (fs), in the / var / www / html / nextcloud / date directory.  After executing the command more nextcloud.log | grep ws3 results show that client.zip file was shared via ws3 nextcloud user 2020-10-19 14:46  View the file at www1.pcap. After applying the filter „http.request.method == GET“ and reviewing the string number 59277, it can be seen that Attacker B downloaded the client.zip file from the IP address 83.171.41.220. When you expand the „Frame“ column, the „Arrival Time“ row shows the download time – 14:50  View the file Microsoft-Windows-TerminalServices-RemoteConnectionManager% 4Operational.evtx. Lines 126 - 208 show RDP connections from ws3 to DC.  View the AD Security.evtx file. Lines 374352 - 374397 show that a new user, mr2kry, has been created. The creation time is shown on the line 374359 – 2020-10-19 14:58 |
| What files were downloaded / sent to / from ws3 and to / from which IP address? | Win32.exe was downloaded  2020-10-19 12:39  8.1.2\_AdbeRdr812\_lt\_LT.exe was downloaded  2020-10-19 12:39  update\_new was downloaded  2020-10-19 12:39 | Search for newly created files during the incident (Win32.exe  8.1.2\_AdbeRdr812\_lt\_LT.exe)  View a copy of the network traffic, use an HTTP filter (pcap), collect objects (Win32.exe only). | View the file nextcloud.log, which is located on the file sharing station (fs), in the / var / www / html / nextcloud / date directory.  After executing the command more nextcloud.log | grep ws3 shows all files that were triggered through the nextcloud account |
| What was the attacker's nickname on the social network STEAM? | MR2KRY | Search for WS3 game platforms client (software). | Open the Steam application, press “FRIENDS & CHAT”. There you can see that one friend has been added – "MR2KRY" |

Annex No. 10. OpenStack installation manual for KYPO

This annex is not intended to perform operating system installations, however, here are recommendations for custom installation:

* The Recommended OS is CentOS 8 or Ubuntu 20.04.1 (commands for this operating system need to be changed e.g., apt -> yum)
* Use minimal server installation
* Setting IP address while installing operation system – there will be no need to setup it manually afterward.
* Using LVM and xfs on single drive volume is not recommended, it causes problems with resizing drives and brings no benefits.
* In Partition Manager deleting partition home directory and a assign the free space to root partition (/)

After fresh install it is recommended to do:

root@controller #~: yum -y update  
root@compute1 #~: yum -y update

Now it is necesairy to assign domain names to the host file in /etc/hosts

root@compute1 #~: nano /etc/hosts

192.168.100.50 controller

192.168.100.60 compute1

For controller, we need to install phyton and pip:

root@controller #~: yum -y install python3-pip

root@controller #~: pip3 install -U pip

Install dependencies:

root@controller #~: yum -y install python3-devel libffi-devel gcc openssl-devel libselinux-python3

root@controller #~: pip install ansible

Now we can install git, kola and kola-ansible:

root@controller #~: yum -y install git

root@controller #~: cd /root/

root@controller #~: git clone -b stable/ussuri https://github.com/openstack/kolla.git

root@controller #~: git clone -b stable/ussuri https://github.com/openstack/kolla-ansible.git

Install requirements for kola and kola-ansible:

root@controller #~: pip install -r kolla/requirements.txt

root@controller #~: pip install -r kolla-ansible/requirements.txt

root@controller #~: pip install ./kolla

root@controller #~: pip install ./kolla-ansible

Copy configuration files:

root@controller #~: mkdir -p /etc/kola

root@controller #~: cp -r kolla-ansible/etc/kolla/\* /etc/kola

Copy invertory files to /root directory:

root@controller #~: cp kolla-ansible/ansible/inventory/\* /root/

Now is the Configuration part. If the intended system will run on one physical machine, the *all-in-one* file needs to be modified. If the system will be installed on multiple physical machines, the *multinode* file needs to be modified. In this file, network interfaces has to be defined. Check your network interfaces with command:

root@controller #~: ifconfig

root@compute1 #~: ifconfig

The *network\_interface* parameter means management interface and *neutron\_external\_interface* defines provider network. Fill this file with appropriate network interfaces.

Now it is time for creating ssh keys:

root@controller #~: ssh-keygen -t rsa -b 4096

root@controller #~: ssh-copy-id controller

root@controller #~: ssh-copy-id compute

Check connectivity with all hosts with:

root@controller #~: ansible -i /root/multinode all -m ping

To generate passwords use this script:

root@controller #~: cd kolla-ansible/tools

root@controller #~/kolla-ansible/tools: ./generate\_passwords.py

Check /etc/kola/passwords.yml for passwords

root@controller #~: cat /etc/kola/passwords.yml

Now its time to configure openstack. The configuration file is located in /etc/kola/globals.yml. KYPO CRP uses services Keystone, Neutron, Glance, Nova and Placement, which are in configured in configuration file by default. By default KYPO CRP uses NoVNC Console, which is not supported at the moment. KYPO CRP only supports spice console, to enable spice console it is necessary to do some modifications:

root@controller #~: nano /etc/kola/globals.yml

and change:

nova\_console: "novnc"

to

nova\_console: "spice"

To install spice, the easiest way to do it is to use external package:

root@controller #~: nano /root/kolla-ansible/ansible/roles/nova-cell/defaults/main.yml

and change

image: "{{ nova\_spicehtml5proxy\_image\_full }}"

to

image: "registry.gitlab.ics.muni.cz:443/cloud/kolla/centos-binary-nova-spicehtml5proxy:10.2.0-centos-8-w07"

To make OpenStack run better, it is a good idea to reserve hardware resources for key services.

root@controller #~: mkdir -p /etc/kolla/config/nova/

root@controller #~: mkdir -p /etc/kolla/config/zun/

and put this content:

[compute]

reserved\_host\_memory\_mb = 4096

reserved\_host\_cpus = 4

in:

root@controller #~: nano /etc/kolla/config/nova/nova-compute.conf

root@controller #~: nano /etc/kolla/config/zun/zun-compute.conf

**Preparing servers**

root@controller #~: cd kolla-ansible/tools

root@controller #~/kolla-ansible/tools: ./kolla-ansible -i /root/multinode bootstrap-servers

The return of this command should not contain any failed checks.

On the compute node it is necessary to initialize physical volume. To display discs type:

root@compute #~: lsblk

chose not used disk (for example /dev/sdc)

root@compute #~: pvcreate /dev/sdc

Create new “cinder-volume”:

root@compute #~: vgcreate cinder-volumes /dev/sdb

**Last checks**

Before deploying OpenStack, use playbook prechecks to check settings and configuration files:

root@controller #~: ./kolla-ansible -i /root/multinode prechecks

This command should not return any failed checks.

**Deployment**

Run playbook to deploy openstack:

root@controller #~: ./kolla-ansible -i /root/multinode deploy

this command should not return any failed commands.

**Customization of OpenStack for KYPO**

To OpenStack customatization, the OpenStack Client is needed:

root@controller #~: pip install python-openstackclient

To use OpenStack CLI Client, the OpenStack credentials file is needed. The file can be generated by:

root@controller #~: cd kolla-ansible/tools

root@controller #~/kolla-ansible/tools:./kolla-ansible post-deploy

root@controller #~: cp /etc/kolla/admin-openrc.sh /root/keystonerc\_admin

Before every use of OpenStack client this keystonerc\_admin file has to be sourced:

root@controller #~: source /root/keystonerc\_admin

Next step is to configure networking. As a networking service is used neutron-linuxbridge-agent. Edit configuration file:

root@controller #~: nano /etc/kolla/neutron-linuxbridge-agent/linuxbridge\_agent.ini

Find row with parameter:

physical\_interface\_mappings

and check, if your provider interface is selected. The whole row should look like:

[linux\_bridge]

physical\_interface\_mappings = physnet1:eth0

For applying changes linuxbriger agent needs to be restarted:

root@controller #~: docker restart neutron\_linuxbridge\_agent

And now let’s create external network configuration:

root@controller #~: openstack network create --provider-network-type=flat --share --provider-physical-network physnet1 --external public

And now you can create your first network in OpenStack:

root@controller #~: openstack subnet create --subnet-range 192.168.200.0/24 --allocation-pool start=192.168.200.100,end=192.168.200.200 --gateway 192.168.200.1 --network public public-subnet

**Adding Flavors for KYPO**

KYPO CRP needs custom flavors and images to run.

|  |  |  |  |
| --- | --- | --- | --- |
| **Flavor** | **vCPU** | **RAM (GB)** | **Disk size (GB)** |
| csirtmu.tiny1x2 | 1 | 2 | 20 |
| csirtmu.tiny1x4 | 1 | 4 | 20 |
| csirtmu.tiny2x4 | 2 | 4 | 40 |
| csirtmu.small2x8 | 2 | 8 | 40 |
| csirtmu.medium4x8 | 4 | 8 | 40 |
| csirtmu.medium4x16 | 4 | 16 | 40 |
| csirtmu.large8x16 | 8 | 16 | 80 |
| csirtmu.large8x32 | 8 | 32 | 80 |
| csirtmu.jumbo16x32 | 16 | 32 | 100 |
| csirtmu.jumbo16x64 | 16 | 64 | 100 |

All these flavors can be added with:

root@controller #~: openstack flavor create –vcpus 1 –ram 2048 –disk 20 csirtmu.tiny1x2

root@controller #~: openstack flavor create –vcpus 1 –ram 4096 –disk 20 csirtmu.tiny1x4

root@controller #~: openstack flavor create –vcpus 2 –ram 4096 –disk 40 csirtmu.tiny2x4

root@controller #~: openstack flavor create –vcpus 2 –ram 8192 –disk 40 csirtmu.tiny2x8

root@controller #~: openstack flavor create –vcpus 4 –ram 8192 –disk 40 csirtmu.tiny4x8

root@controller #~: openstack flavor create –vcpus 4 –ram 16384 –disk 40 csirtmu.tiny4x16

root@controller #~: openstack flavor create –vcpus 8 –ram 16384 –disk 80 csirtmu.tiny8x16

root@controller #~: openstack flavor create –vcpus 8 –ram 32768 –disk 80 csirtmu.tiny8x32

root@controller #~: openstack flavor create –vcpus 16 –ram 32768 –disk 100 csirtmu.tiny16x32

root@controller #~: openstack flavor create –vcpus 16 –ram 65536 –disk 100 csirtmu.tiny16x64

After setting all flavours is needed to check current flavours in system and check for duplicates:

root@controller #~: openstack flavor list

If there are two or more flavors with the same name, you must delete one of them. If you leave two or more flavors of the same name, OpenStack may not know which flavor to choose and creating instance may fail.

For deleting instance use command:

root@controller #~: openstack flavor delete (flavor id)

**Adding Images for KYPO**

There are three base images that are needed KYPO CRP to run:

|  |  |
| --- | --- |
| **Image name** | **Operation System** |
| **ubuntu-bionic-x86\_64** | Ubuntu 18.04 LTS |
| **ubuntu-focal-x86\_64** | Ubuntu 20.04.1 LTS |
| **debian-9-x86\_64** | Linux Debian 9 |

These images can be installed by:

root@controller #~: wget https://cloud-images.ubuntu.com/bionic/current/bionic-server-cloudimg-amd64.img -P /tmp/

root@controller #~: openstack image create --disk-format qcow2 --container-format bare --public --property

os\_type=linux --file /tmp/bionic-server-cloudimg-amd64.img ubuntu-bionic-x86\_64

root@controller #~: wget https://cloud-images.ubuntu.com/focal/current/focal-server-cloudimg-amd64.img -P /tmp/

root@controller #~: openstack image create --disk-format qcow2 --container-format bare --public --property

os\_type=linux --file /tmp/focal-server-cloudimg-amd64.img ubuntu-focal-x86\_64

root@controller #~: wget http://cdimage.debian.org/cdimage/openstack/current-9/debian-9-openstack-amd64.qcow2 -P /tmp/

root@controller #~: openstack image create --disk-format qcow2 --container-format bare --public --property os\_type=linux --file /tmp/debian-9-openstack-amd64.qcow2 debian-9-x86\_64

1. Named after ***Jeopardy!****,* an American television game show created by Merv Griffin in 1964. [↑](#footnote-ref-1)
2. <https://www.cyberlympics.org/about-global-cyberlympics/> [↑](#footnote-ref-2)
3. https://europeancybersecuritychallenge.eu/about [↑](#footnote-ref-3)
4. <https://nationalcyberleague.org/> [↑](#footnote-ref-4)
5. <https://www.uscyberpatriot.org/competition/Competition-Overview/competition-overview> [↑](#footnote-ref-5)
6. <https://natoassociation.ca/a-glimpse-into-locked-shields-2019/> [↑](#footnote-ref-6)
7. https://gitlab.com/itsape [↑](#footnote-ref-7)
8. https://gitlab.com/itsape/windows-client [↑](#footnote-ref-8)
9. https://gitlab.com/itsape/platform/-/blob/a237d513/vm-provisioning-main.sh [↑](#footnote-ref-9)
10. https://gitlab.com/itsape/awarenssometer [↑](#footnote-ref-10)
11. https://gitlab.com/itsape/artifactomat [↑](#footnote-ref-11)