



SPARTA

D9.4

Pilot of Cyber training & exercise Framework (Ct&eF)

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

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 / D9.4 / V1.0
Work package contributing to the deliverable	WP9
Due date	July 2021 – M30
Actual submission date	29 th July 2021

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

Abstract	The document contains the study of infrastructure for the technical realization of training activities at consortium partners. The cyber training & exercise framework includes tools presented by partners (KTU, BUT, CNIT, and UBO) and federated by the SPARTA JCCI integrator.
Keywords	Cyber training, cyber exercises, cyber range, platform



Editor

Algimantas Venčkauskas (KTU)

Contributors (ordered according to beneficiary numbers)

Tomas Lieskovan, Jan Hajny (BUT)

Arnold Sykosch (UBO)

Giorgio Bernardinetti, Giuseppe Bianchi (CNIT)

Šarūnas Grigaliūnas, Stasys Maciulevičius, Nerijus Morkevičius (KTU)

Reviewers (ordered according to beneficiary numbers)

Nelson Escravana (INOV)

Aleksandra Pawlicka (ITTI)

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

Organizations and individual users face an increased risk of cyberattacks. The attackers have become more organized, and tend to use 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 infrastructure for the technical realization of training activities at multiple consortium partners. 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 the 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 the SPARTA JCCI integrator. The training and exercise tools provided by the partners cover the areas of knowledge as shown in section 3.1.

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 and stakeholders, of the information gathered about cyber security threats and corresponding defence 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, the purpose and architecture of one of the first open-source cyber ranges on the European market are described, the installation requirements are shown, the full installation manual, as well as the deployment at BUT premises and demonstrate the sample training scenario, are provided. Furthermore, the team presents the description and results of the first pilot using the KYPO cyber range tools that took place at BUT premises with real students. The section is finished with the description of the following 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 the 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 Content

Chapter 1	Introduction.....	1
Chapter 2	Structure of Cyber training & exercise Framework	3
2.1	The target groups.....	3
2.2	Knowledge areas	4
2.3	Mapping of target groups to knowledge areas	8
2.4	Training & exercise activities.....	9
2.5	Cybersecurity Competitions	12
2.6	Mapping of training & exercise activities to knowledge areas	14
2.7	Cybersecurity Platforms and Training Environments	15
2.8	Cyber Range as training & exercise platform.....	17
2.8.1	Taxonomy of Cyber Ranges	18
2.8.2	Benefits of a Cyber Range.....	21
Chapter 3	Pilot of Cyber training & exercise Framework	23
3.1	Architecture of Cyber training & exercise Framework	23
Chapter 4	KTU Pilot of Cyber Security Training Platform	27
4.1	Description of KTU Cyber training & exercise Framework	27
4.2	Pilot of KTU Cyber training & exercise Framework	29
4.2.1	Description of KTU Cyber training & exercise Platform.....	30
4.2.2	Installation of KTU Cyber training & exercise Platform.....	30
4.2.3	Pilot of Red Team / Blue Team exercise on KTU Platform.....	30
4.2.4	How to play storyline?.....	34
4.2.5	The benefits of using the Cyber training & exercise Framework	36
Chapter 5	CNIT – own platform with a storyline	38
5.1	The Nautilus Platform.....	38
5.1.1	Core Design and Principles	38
5.2	The Pilot: CTF platform for cyber competition	41
5.2.1	How to run the exercise	43
5.2.2	CTF challenges	43
5.2.3	Benefits of using the Nautilus Cyber Range.....	44
Chapter 6	BUT Pilot of KYPO Cyber Range Platform.....	45
6.1	Deploying KYPO CRP.....	45
6.1.1	Requirements	45
6.1.2	Recommendations.....	47



6.1.3	Deployment at BUT	48
6.2	Using KYPO	49
6.2.1	Example Scenario	50
6.2.2	Creating New Scenarios	51
6.3	Piloting Cyber training Exercise	52
6.3.1	Laboratory Settings	52
6.3.2	Training Scenario	53
Chapter 7	UBO – a framework to measure IT-Security Awareness within working staff	57
7.1	Description	57
7.1.1	Artifact-based Assessment of IT security Awareness	57
7.1.2	itsape: IT-Security Awareness Penetration Testing Environment	59
7.2	Use Case	59
7.2.1	Preparation	60
7.2.2	Pre-test	61
7.2.3	Intervention	62
7.2.4	Post-test	63
7.3	Test Pilot	63
Chapter 8	Summary and Conclusion	65
Chapter 9	List of Abbreviations	66
Chapter 10	Bibliography	69
Annexes	71	
Annex No. 1	- The installation of a virtual machine image	71
Annex No. 2	- The infrastructure of an attack model of a typical organization and its functions	75
Annex No. 3	- An attack model in an IT infrastructure of typical organization with attack scenarios and an attack map	77
Annex No. 4	- Storyline A1 – bruteforce attack	80
Annex No. 5	- The infrastructure of an attack model of a typical organization and its functions	85
Annex No. 6	- Storyline A3 – exploiting WP vulnerability	90
Annex No. 7	- Storyline B1 – distant workplace attack	93
Annex No. 8	- Trainers Manual. Description of the Attacks	96
Annex No. 9	- Installation and Troubleshooting of KYPO	99
Annex No. 10	- Installation of the toolkit to measure IT-Security Awareness	107

List of Figures

Figure 1: Mapping of target groups to knowledge areas.....	8
Figure 2: Learning pyramid	9
Figure 3: Covering of Knowledge Areas by Exercises, Training and Competitions.....	15
Figure 4: Cyber Range taxonomy [16].....	19
Figure 5: Federated infrastructure of Cyber training & exercise Framework	23
Figure 6: Acquisition of knowledge and practical skills using KTU Cyber training & exercise platform	24
Figure 7: The typical topology of institution	27
Figure 8: Infrastructure of KTU Pilot of Cyber training & exercise Framework	30
Figure 9: Attacks vectors based on storyline scenarios	34
Figure 10: Creating a new Scenario	39
Figure 11: Creating a Scenario with 3 VMs	39
Figure 12: Adding a CVE to a Virtual Machine	40
Figure 13: Nautilus Console	41
Figure 14: Scenario Report	41
Figure 15: CTF Architecture	42
Figure 16: Services in PROD and DEV environment.....	42
Figure 17: Automatic deploy pipeline	43
Figure 18: KYPO CRP User Interface	45
Figure 19: Network Infrastructure needed for KYPO	46
Figure 20: BUT KYPO CRP Rack	49
Figure 21: KYPO Portal.....	50
Figure 22: BUT Laboratory with running KYPO	53
Figure 23: First task	54
Figure 24: Second task	54
Figure 25: Third task	55
Figure 26: Fourth task.....	55
Figure 27: Scoring board.....	56
Figure 28: Situation model of terminal work	57
Figure 29: Classes of possible artifacts.....	58
Figure 30: Combinations of user reaction classes	58
Figure 31: Preparation phase within the artifactomat	60
Figure 32: Test execution within the artifactomat	62



List of Tables

Table 1: Brief description of CyBOK Knowledge Areas [6]	5
Table 2: Correspondence of ACM CSEC 2017 and CyBOK Knowledge Areas	7
Table 3: Use of different cyber security exercises in different Knowledge Areas	14
Table 4: Covering of different Knowledge Areas by partners' platforms	26
Table 5: Methodology of choosing practical and organizational measures	32
Table 6: Additional information to be provided by the relevant staff.....	35
Table 7: Information exchange between Cyber training & exercise Framework and the JCCI platform	36
Table 8: Minimal hardware requirements for 10 players	46
Table 9: Recommended hardware requirements for 10 players	46
Table 10: Recommended Operation Systems.....	47
Table 11: BUT Deployment Specification.....	48
Table 12: Decomposition of the IT security awareness components	64
Table 13: Application Credentials details	99
Table 14: Flavors and images to run KYPO CPR.....	105
Table 15: System requirements of the server.....	107
Table 16: System requirements of the clients.....	107

Chapter 1 Introduction

Living in the age of global communication and the Internet also means that the possibilities of violating the computer networks and computers are increasing, while all devices connected to the Internet. In the everyday life, there is a risk of being attacked by various threat actors, even by state-sponsored attackers from other countries. They have become more organized and started using more powerful and computerized processes and procedures.

Computers and online repositories contain large amounts of information. Theft or disclosure of it may do great harm to the owners of the information or even the society in general.

The purpose of these cyber-attacks can be different:

- A cyber-attack can cause major damage to a business. It can have an impact on a company's reputation and consumer trust. A security breach can have financial, reputational, and legal ramifications.
- 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 illegally acquire 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 almost 90% of data breaches¹. Every organization faces the risk of a cyber-attack. One mistake by a single employee could compromise an entire network. Therefore, in order to keep the organization secure, every employee should understand taken actions.

Information theft is the most costly and fastest-growing segment of cybercrime². 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 abroad.
- The spread of the Internet of mobile devices and things.
- The spread of social networking and e-commerce.

According to one research, 60 percent of small firms go under within six months a successful cyberattack¹. A successful cyber-attack takes an average of more than 7 months to detect and recover from, and the normal disruption to corporate operations costs around \$1 million USD.

According to ENISA (The European Union Agency for Cybersecurity) Threat Landscape Report 2020, the main trends in the 2020's cyber threat landscape were [1]:

- *“During and after the COVID-19 pandemic users are more dependent on secure and reliable cyberspace.*
- *The number of fake online shopping websites and fraudulent online merchants reportedly has increased during the COVID-19 pandemic.*

¹ <https://www.infosecurity-magazine.com/news/90-data-breaches-human-error/>

² <https://www.upguard.com/blog/cybersecurity-important>

- *The number of cyberbullying and sextortion incidents also increased with the COVID-19 pandemic.*
- *COVID-19-themed attacks include messages carrying malicious file attachments and messages containing malicious links that redirect users to phishing sites or malware downloads.*
- *Business Email Compromise (BEC) and COVID-19-themed attacks are being used in cyber-scams resulting in the loss of millions of euros for EU citizens and corporations.*
- *Financial reward is still the main motivation behind most cyber attacks.*
- *Some attacks on high-value data, such as intellectual property and state secrets, are being planned and executed often by state-sponsored actors.*
- *Ransomware remains widespread with costly consequences to many EU organisations.*
- *Many cybersecurity incidents still go unnoticed or take a long time to be detected.*
- *Skill and capability building are the focus of defenders. Public organizations struggle with staff retention due to strong competition with the 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.*
- *The number of potential vulnerabilities in a virtual or physical environment continues to expand.”*

Preventing such attacks requires an increased cyber security awareness of the general 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 the development of modern training programs that use cyber security labs for training and exercises.

ENISA also recommends – to meet the current market needs in cyber threat intelligence training, more training offerings must be developed.

Detection of these attacks and building effective protection against them is very important, so it is necessary to increase the knowledge of cybersecurity. Corresponding education and practice are critical also for the security professionals who should improve their strategies, tactics, and technology for defence. 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 to be able to prevent, react and protect their citizens against cyber threats.

Chapter 2 Structure of Cyber training & exercise

Framework

Many people face or are likely to face information security issues, ranging from security professionals to ordinary computer users. This chapter discusses the knowledge that users at different levels should acquire.

It is important to use a variety of training and exercise environments for performing practical tasks in order to acquire the basics of security knowledge and gaining practical skills. Special laboratories, particularly cyber ranges, are ideal for this, as they allow staff and consumers to be trained on the latest threats and practice handling specific real-world scenarios.

2.1 The target groups

In relation to cyber security, the following four groups of the society can be distinguished:

- Academics;
- Professionals;
- Employees;
- Public.

Academics

To protect the organization from cybercrimes in modern-day society, trained cyber security professionals need. Such professionals can be educated and trained at universities and colleges. Students learn how to safeguard computer operating systems, networks, and data from cyber-attacks in cyber security programs. Universities are developing degree programs from inside their existing departments of computer science, business, and engineering. Academics are developing new cybersecurity courses in response to real-world needs in both the public and private sectors. Courses in cybersecurity cover a wide range of topics in 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 cybersecurity training should emphasize real-world applications and be taught by experts who can relate to current and actual challenges. Practical sessions are generally included in this form of training (case studies for organizational topics and human sciences, hands-on courses for technical topics).

The knowledge acquired by professionals is often confirmed by cyber security certifications. Certifications are specialized credentials that professionals obtain in a certain field to demonstrate their knowledge and skill set, and they typically require passing an exam. Companies, professional associations, and government bodies frequently provide these services.

Certificates are a form of abbreviated degree or diploma program that students can achieve to first enter the certain sector. Certificate programs in cyber security can be found at most colleges or universities.



Employees

Today employees are often the greatest source of vulnerability³. Employees leaving laptops and mobile devices unattended in susceptible settings like public transportation, autos, and restaurants, according to some experts, is still the number one threat to cyber security.

Because organizations and businesses cannot fulfill their cyber security goals just through the employment of hardware and information technology specialists, all employees who utilize computers and computer networks must be trained in cyber security knowledge, skills, and policies. 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 dangers of social engineering and how to avoid classic social engineering scams such as phishing emails.

Public

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

In the time of information and technology, when a lot of time is spent using computers or other smart devices, it is necessary to have a good understanding not only of how to use them in a general sense but also how to use them safely. A single mistake or careless click on the email attachment and the personal information becomes available for malicious use.

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

2.2 Knowledge areas

All disciplines including technology, people, and processes to enable assured operation in the face of dangers and adversaries are referred to as **cyber sciences**. It includes all activities related to the development, operation, analysis, and testing of secure computer systems, as well as risk-taking and risk reduction [3, 4, 5].

According to Cybersecurity Curricula 2017 Curriculum Guidelines, within and across different computing-based disciplines, the **knowledge area** (KA) represents significant knowledge with broad importance. Knowledge areas represent the entire body of knowledge in the topic of cybersecurity when taken together [4]:

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 the design, implementation issues, static and dynamic testing, configuring and patching, ethics, especially in development, testing and vulnerability disclosure.
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.

³ <https://blog.symquest.com/why-human-error-biggest-cyber-security-vulnerability>

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 the use of the 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 cyber security. The essential concepts covered by this KA and its learning goals are Identity management, social engineering, awareness and understanding, social-behavioural 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.”

The Cyber Security Body of Knowledge (CyBOK) defines 19 Knowledge Areas [5, 6], a brief description of which is given in Table 1.

Table 1: Brief description of CyBOK Knowledge Areas [6]

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.



<i>Security Operations & Incident Management</i>	<i>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.</i>
<i>Forensics</i>	<i>The collection, analysis, & reporting of digital evidence in support of incidents or criminal events.</i>
Systems Security	
<i>Cryptography</i>	<i>Core primitives of cryptography as presently practised & emerging algorithms, techniques for analysis of these, and the protocols that use them.</i>
<i>Operating Systems & Virtualisation Security</i>	<i>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.</i>
<i>Distributed Systems Security</i>	<i>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.</i>
<i>Authentication, Authorisation, & Accountability</i>	<i>All aspects of identity management and authentication technologies, and architectures and tools to support authorisation and accountability in both isolated and distributed systems.</i>
Software and Platform Security	
<i>Software Security</i>	<i>Known categories of programming errors resulting in security bugs, & techniques for avoiding these errors, both through coding practice and improved language design, as well as tools, techniques, and methods for detection of such errors in existing systems.</i>
<i>Web & Mobile Security</i>	<i>Issues related to web applications and services distributed across devices and frameworks, including the diverse programming paradigms and protection models.</i>
<i>Secure Software Lifecycle</i>	<i>The application of security software engineering techniques in the whole systems development lifecycle resulting in software that is secure by default.</i>

Infrastructure Security	
<i>Network Security</i>	<i>Security aspects of networking & telecommunication protocols, including the security of routing, network security elements, and specific cryptographic protocols used for network security.</i>
<i>Hardware Security</i>	<i>Security in the design, implementation, & deployment of general-purpose and specialist hardware, including trusted computing technologies and sources of randomness.</i>
<i>Cyber-Physical Systems Security</i>	<i>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.</i>
<i>Physical Layer & Telecommunications Security</i>	<i>Security concerns and limitations of the physical layer including aspects of radiofrequency encodings and transmission techniques, unintended radiation, and interference.</i>

Analysis of ACM Cybersecurity Curricula (CSEC) 2017 and CyBOK Knowledge Areas allows such correspondence to be observed (see Table 2).

Table 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], the ACM CSEC 2017 [4] knowledge areas will be used.

2.3 Mapping of target groups to knowledge areas

The relationship of target groups to knowledge areas is depicted in this picture (Figure 1):

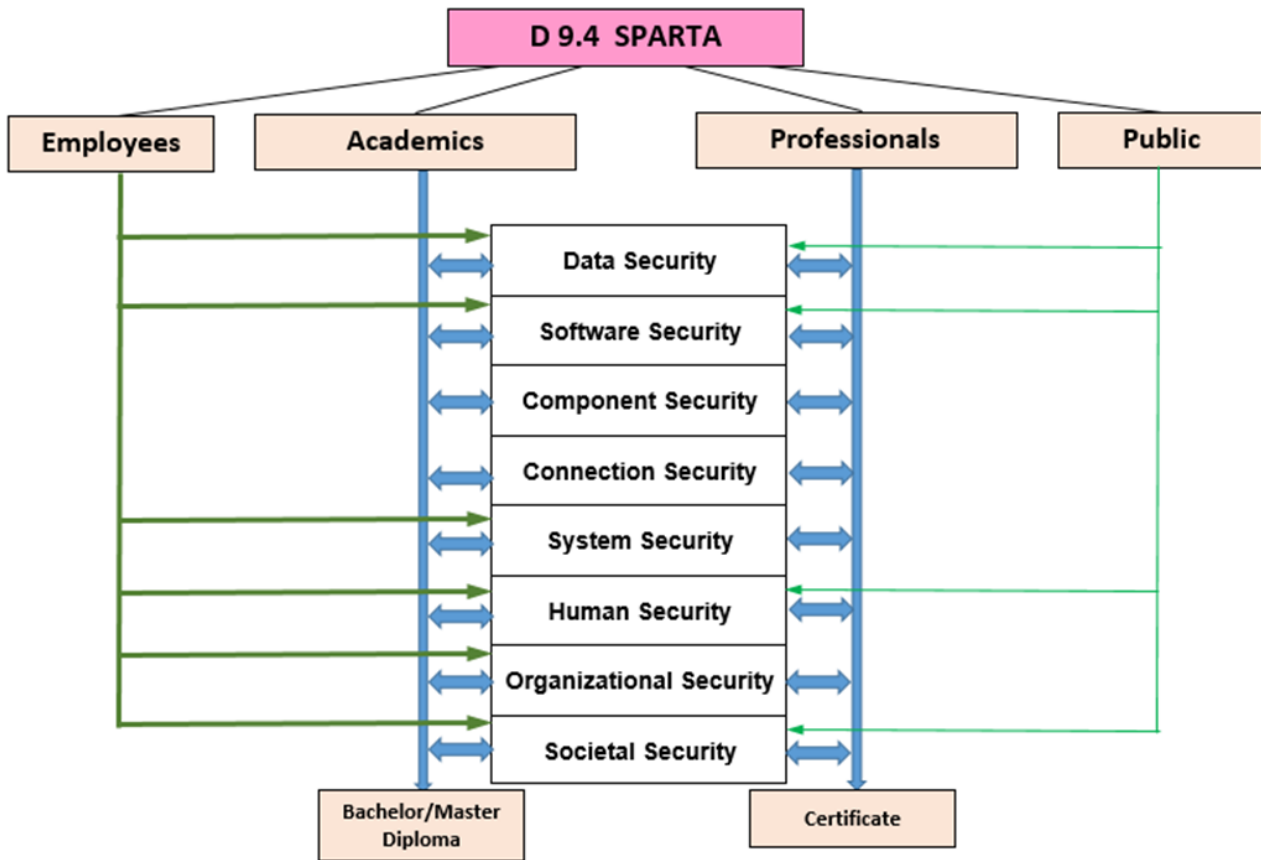


Figure 1: Mapping of target groups to knowledge areas

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 the same level) to all knowledge areas as it depends on study program curricula. For instance, some topics in the study program are voluntary, so students have the opportunity to choose for themselves some topics of cyber security. An exhaustive analysis of university bachelor and master study programs is presented in the SPARTA-D9.2 report [3].

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

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

The general public should have a good understanding of how to use computers and information technologies safely. A sufficient understanding should include data security, software security, human security (social engineering, social behavioural privacy and security, personal data privacy and security) and societal security (cyber threats, privacy).

2.4 Training & exercise activities

Military and security personnel have been using exercises as training techniques for millennia. Validating policies, plans, and procedures, as well as training, enhancing current tools or rolling out new equipment, testing information and communications technology (ICT), and detecting resource shortfalls can all benefit from conducting exercises [7].

Training is critical for both developing tomorrow's cybersecurity workforce and keeping current cybersecurity employees up to date on new skills and threats.

Training and exercises are important for deeper mastering of teaching materials. This is confirmed by the learning pyramid [8]. This pyramid (Figure 2) shows the importance of practical activities in acquiring new knowledge or raising qualifications.

Although practical education, including hands-on experience, plays an essential role in the construction of curricula, only 30-40% of existing courses offer some sort of practical education, according to an analysis of the current curriculum [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 importance of the students' practical understanding of security issues.

The cyber security exercises (or cyber defence exercises – CDX) can be used also as testbed platforms to test and assess IT and OT systems [9] while they have been crucial in assessing governments' or organizations' technical cyber capabilities, cyber training, and boosting cyber awareness.

CDX can improve the ability to test and develop common and coordinated technical and strategic mobility in response to cyberattacks that may take place on a national and international scale, as well as strengthen cooperation and coordination between the public and private sectors in cyberspace and collect empirical data for cybersecurity research.

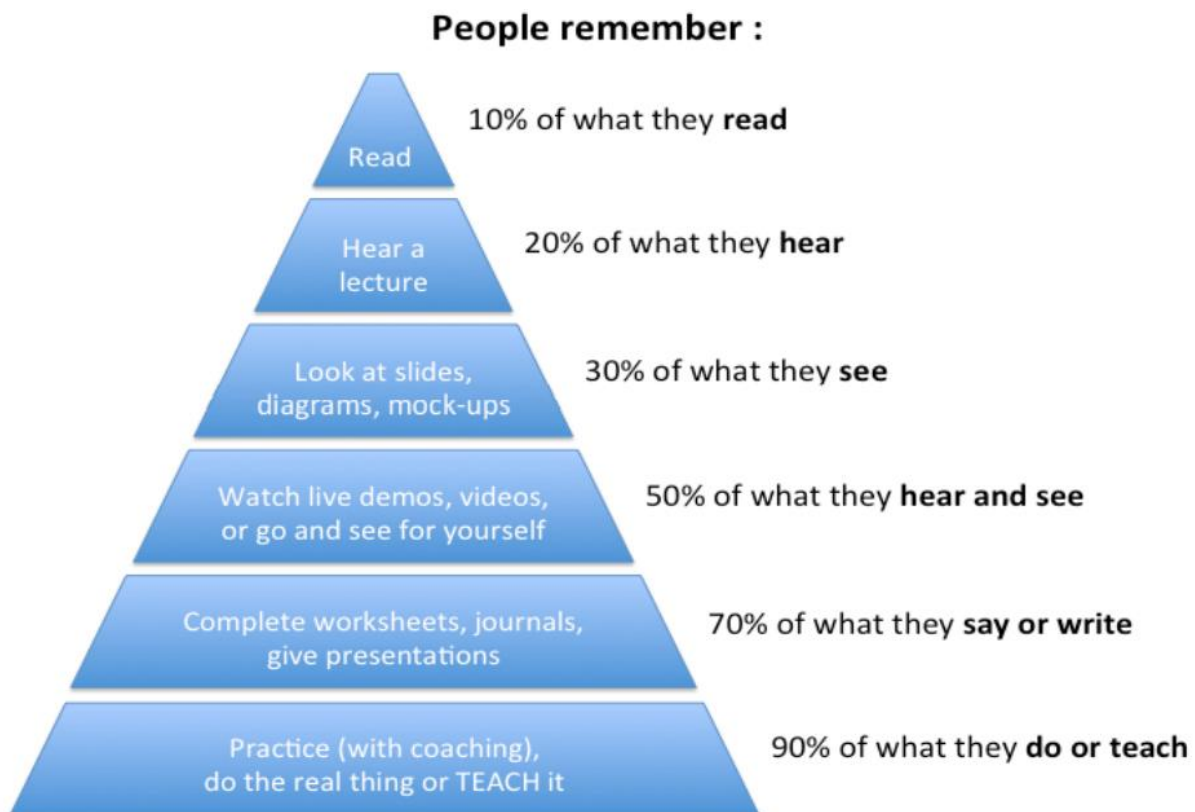


Figure 2: Learning pyramid



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 type of information security competition in which players are challenged to complete a number of objectives relating to cyber security⁴. 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 completing an individual challenge, the player is awarded a "flag," which they must submit to the CTF server in order to receive points. Players can take on the numerous challenges on their own or as part of a team to see who can get the most points.

CTF events are usually timed, and the points are tallied after the time limit has passed. The winning player/team will be the one that completes the most challenges and so earns the most points.

CTF is a type of wargaming in which players are divided into two teams, with one acting as the aggressor or hacker and the other as the defender. 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.

The skill level for CTFs varies between events, as it does for many other competitions. Some programs are aimed at high school and college students, while others are aimed at professionals who have operated on cyber security teams.

Discussion-based games

Game-based learning allows students to participate in an engaging activity while learning by actively learning and practising. Studies show that the brain is 68% more involved when engaged in entertaining activities⁵. Typically, the game begins slowly and progresses in difficulty until the student is able to effectively navigate more challenging stages. Many of these opportunities are provided by game-based learning, one of which is the ability to gradually enhance abilities by immersing people in real-life scenarios and rewarding them depending on their outcomes.

By combining cybersecurity with the concept of gaming, it is critical to provide a learning platform for the future generation of cyber security professionals to learn and be better equipped. Some of the games were created to provide some obstacles and to need a higher level of thought. This system delivers an immersive, learner-centered learning experience that is excellent for cybersecurity awareness training and practical skill acquisition for learners of all backgrounds.

Drills

⁴ <https://cybersecurity.att.com/blogs/security-essentials/capture-the-flag-ctf-what-is-it-for-a-newbie>

⁵ <https://www.livingsecurity.com/blog/10-best-games-cyber-security>



A drill is a controlled, coordinated activity used to evaluate a single, specific process or function within a single unit⁶. This term refers to the practice of many repetitions of a skill or tool in a systematic manner.

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

A cyber security assessment technique that involves simulated attacks is known as a red team/blue team exercise. In a low-risk environment, it performs simulated attacks to assess the organization's current security capabilities and recommend areas for improvement⁷. This exercise, modelled on military exercises, is a clash of two teams of high-level cyber security professionals.

red team is a group of people who are brought in to evaluate the performance of a security program. To make it as realistic as feasible, they should imitate the behaviors and approaches of likely attackers. The internal security squad tasked with thwarting these simulated attacks is known as the blue team.

The ultimate purpose of a test like this is to evaluate an organization's security maturity as well as its capacity to identify and respond to an attack. Depending on the simulation, the persons engaged, and the assaults being tested, such an exercise can take up to three or four weeks.

Seminars

A seminar is a form of academic instruction offered by a business or professional organization or a university. Its goal is to bring small groups together for recurring meetings, with each meeting focusing on a new topic and requiring all attendees to actively engage. An informal meeting in which participants debate new or revised plans, policies, or processes is known as a seminar.

Simulation-based exercises

A simulation-based exercise is a training activity in which participants are placed in a simulated environment and are required to perform in the capacity that would be expected of them in a real-life situation. Its goal is to improve readiness by putting policies and plans to the test, as well as standard operating procedures and personnel training.

The main benefits of simulation-based exercises include allowing people to practice their roles, get experience in their professional activity without really having to deal with an actual disaster.

Table-top exercises

This is a paper-driven exercise with scripts prepared by exercise planners and delivered using 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. Depending on the number of companies engaged, this type of exercise can be organized and done fast.

Table-top exercises got their name because, in most situations, the planners and participants sit at one table to carry out the exercise. The training audience for a table-top activity should be small, and the objectives should be well specified. This type of environment allows diverse parties to communicate with one another and aids in the establishment of business processes for planning, executing, and training throughout an exercise. The injections are fictitious, completely pre-planned, and scripted down.

⁶ <https://sfdem.org/drill>

⁷ <https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/>

Workshops

A workshop is similar to a seminar, except it is designed to create specific products, such as a draft plan (such as a Training and Exercise Plan) or policy.

High school students can explore computer and network security ideas and skills through on- and offline hands-on activities at university workshops. 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.

2.5 Cybersecurity Competitions

Contemporary 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 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.

Individuals or teams participate in cybersecurity activities such as methodologies, practices, strategy, policy, and ethics in cybersecurity competitions, which are interactive events or exercises.

Students can put their talents to the test and develop team-based management skills in a real-world business setting by participating in a cybersecurity competition. 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]:

- *“understanding of the importance of cybersecurity and threat intelligence;*
- *benchmarking in schools or colleges for young people;*
- *the early identification of young persons with an potential for information security;*
- *understanding of the various types of jobs available in cyber security;*
- *the development of mechanisms in the education sector to achieve IT security excellence;*
- *the attraction of information technology and information security to young people;*
- *building professional IT security competence in Europe through national and European networks of excellence.”*

At the municipal and national levels, there are numerous cybersecurity competitions. They're all trying to encourage professional growth and cybersecurity education outside of the 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 capturing the flag events, in which scoreboards often highlight the number of points held by all of the competing teams.

The most popular formats for CTF competitions are:



- **Jeopardy**⁸: 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-centred 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 defence**: 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 business with more than 50 employees, up to 12 servers, and shared Internet services including a web server, mail server, and e-commerce website. The ability of the team to detect and respond to external threats, maintain the availability of existing services, and respond to business needs (for example, by creating a new e-commerce site that combines best security practices with business needs, service availability, network protection against attacks) will be evaluated during the competition.

In the **Network security competition**, competitors seek to control shared resources and the most important services for those resources. When a competitor takes over a resource, it must be protected 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 a series of quiz questions. Some tasks focus on a potentially vulnerable web server, other quests include forensics, package capture analysis, and more.

In the **Digital Forensics competition**, a simulated scenario for participants is 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, analyze 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 Cyberlympics⁹ is an online cyber security competition in which teams from around the world compete in a variety of fields: digital forensics, web application exploitation, malware analysis, reverse engineering, cryptography. Initially, teams compete in a 12-hour online elimination round. Two top-scoring teams from each continent will then be invited to compete at the Global Cyberlympics World Finals event.
- The European Cyber Security Challenge¹⁰ (ECSC) is an ENISA initiative aimed at cybersecurity talent search and educating across Europe. The competition is promoted by the European Commission. In the ECSC participate the winners of the national contests representing their countries. In topics such as web security, mobile security, crypto puzzles, reverse engineering, and forensics, contestants must solve security-related problems.

⁸ Named after *Jeopardy!*, an American television game show created by Merv Griffin in 1964.

⁹ <https://www.cyberlympics.org/about-global-cyberlympics/>

¹⁰ <https://europeancybersecuritychallenge.eu/about>

- The National Cyber League¹¹ (NCL) arranges NCL Games for individual students and teams. Here students can validate their skills with challenges they will likely face in real-world cybersecurity practice. There are challenges in each category at three difficulty levels (easy, medium and hard) so players with different levels of cybersecurity expertise can assess their progress. Players can also receive feedback from the games that highlight their strengths within industry-relevant challenges. This feedback is a great resource for those entering the industry and helps competition participants stand out when seeking IT and cybersecurity jobs.
- CyberPatriot's National Youth Cyber Defense Competition¹² is the world's largest cyber security competition, in which teams of high school and middle school students must identify and remedy cybersecurity flaws in virtual operating systems. Throughout the academic year, competitions are held on weekends.
- Locked Shields, organized by NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Estonia bring together approximately 1,000 cyber specialists from 30 countries¹³. Locked Shields is a helpful and useful exercise that helps cyber defenders to learn, practice, and enhance critical skills like teamwork and adaptability, as well as get experience dealing with genuine cyber occurrences that mimic real-world attacks. This exercise emphasizes the necessity of NATO Allies working together and reminds that cybersecurity is a shared responsibility.

2.6 Mapping of training & exercise activities to knowledge areas

Different training & exercise activities can be used to further improve the mastery level of teaching materials in cyber security. Analysis of the description of knowledge areas (see Table 1) and the above description exercise's content allows establishing how different cyber security exercises can be used for acquiring relevant knowledge and developing skills in cyber security (see Table 3).

Table 3: Use of different cyber security exercises in different Knowledge Areas

<i>Exercises</i>	<i>Capture the flag</i>	<i>Discussion based game</i>	<i>Drill</i>	<i>Red team / blue team</i>	<i>Simulation</i>	<i>Table-top</i>	<i>Seminar</i>	<i>Workshop</i>
Data Security	X	X	X	X		X	X	X
Software Security			X				X	X
Component Security							X	X
Connection Security	X	X	X	X	X		X	X
System Security			X	X	X	X	X	X
Human Security	X	X				X	X	X
Organizational Security							X	X
Societal Security	X						X	X

¹¹ <https://nationalcyberleague.org/>

¹² <https://www.uscyberpatriot.org/competition/Competition-Overview/competition-overview>

¹³ <https://natoassociation.ca/a-glimpse-into-locked-shields-2019/>

Competitions are valuable activities that can be used to deepen various cybersecurity aspects, invigorating the training process and making it more attractive. This is shown in Figure 3.

The relationship between the topics and content of the competitions and the areas of knowledge is determined based on the short overview of the types of competitions shown above.

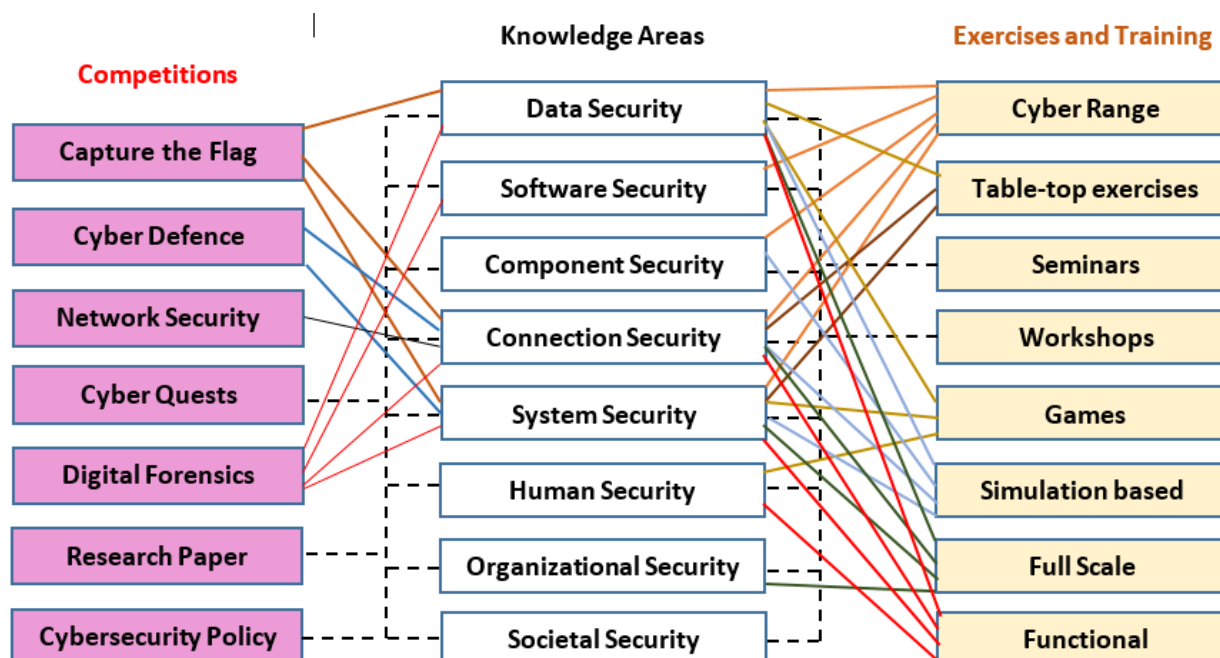


Figure 3: Covering of Knowledge Areas by Exercises, Training and Competitions

2.7 Cybersecurity Platforms and Training Environments

What does the term **cybersecurity platform** mean exactly? The term "platform" is used by vendors to denote an integrated consolidation of products that forms a common and compatible architecture.

What general requirements must be met by the cybersecurity platform? A short list of such requirements is provided below [11]:

1. **Coverage from endpoints to data centres 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 tool should provide the best possible 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 plan 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 threat intelligence analysis/sharing, static/dynamic file analysis, reputation list compilation/distribution, machine learning modelling, 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 purchase a whole set of components, customers may wish to purchase and install tools gradually, depending on their budget capabilities. Considering this, 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 main challenge that businesses and various organizations face today is to protect themselves from modern and complex security challenges. Dangers become more likely as digital transformation drives innovation, and the team must be prepared not only for present threats but also for future threats.

The cyber security training environment is a cyber-security training tool that allows practising and improving cyber security skills, as well as to develop and learn new knowledge and test both older and emerging cyber threat concepts in the field of information security.

Cyber security training develops cognition needs, integration, communication and cooperation 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, it can also serve as a dedicated location for student computer forensics exercises and other hands-on activities.

The lab also houses servers that are set up to provide students with a self-service private cloud. This private cloud allows students to get a hands-on experience with cloud computing and design their own test/practice laboratories. Students can also employ scalable compute resources and pre-configured virtual machines to complete a range of activities.

Cybersecurity Virtual labs

Virtual cyber security 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:

- The virtual lab is available from anywhere, enables encountering real-world scenarios and working through them, it is cheaper and ensures high-quality training.
- Because training is mostly conducted through an Internet browser on the learners' terminal, a virtual lab eliminates the need for travel fees or high-end technology on the client side. With nothing more than an Internet connection, the simulation may be accessed from anywhere at any time.
- Upgrading a lab to keep up with ever-changing technology and security trends is inexpensive and can be done quickly.
- Instructors and students receive immediate and accessible feedback. Instructors can provide assistance at any time, track user involvement, and conduct other pertinent analysis.

Virtual laboratories are more than just a way to learn about cybersecurity. They can also be built to deliver the most up-to-date certifications from well-known organizations such as Cisco or Microsoft.

Cybersecurity training platforms

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

Using simulations based on real-world attacks that the business has put into the curriculum, the cybersecurity training platform will make it easier to teach cybersecurity professionals how to maximize investments in cybersecurity solutions.

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

End-users can get cybersecurity training materials via online portals provided by security awareness training platforms. 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 now allow users to simulate phishing attempts to see if they can detect them.

End-users can get cybersecurity training materials via online portals provided by security awareness training platforms. Admins can develop training campaigns that include interactive quizzes and exams to check that users are learning and engaging with the information.

Another widely known type of security training platforms is the cyber range.

Cyber Ranges

European Cyber Security Organization (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 organization’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 realization and use of the simulation environment and additional components which are, in turn, desirable or required for achieving specific cyber range use cases*” [13].

The use of cyber ranges for practical training was a key factor in the development of good-practice curriculum. Virtualization technologies and gamified training methods such as CTF, Red Blue teaming, or table-top exercises should be regarded a considerable improvement over current training methods and might provide hands-on experience. [3].

2.8 Cyber Range as training & exercise platform

From ordinary computer users to cyber experts and executives preparing to respond to cyber incidents, every person can improve cyber defence skills at special training facilities. One kind of such facility is cyber range.

Government agencies first created cyber ranges to train their cyber operators on skills and techniques. Instead of using the agency's operational network infrastructure, which may be compromised during such training, cyber range providers created virtual representations of genuine networks, systems, and tools to assist cyber professionals safely train in virtual, secure environments.

Today, cyber ranges are used in the cybersecurity sector to effectively train IT professionals in all industries and help improve defences 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 to train for cyberwarfare and software development². Cyber ranges are virtual Internet-level representations of an organization's local network, system, tools, and applications. They provide a secure environment for product

development and security posture assessment, as well as a safe, legal environment for gaining hands-on cyber skills.

Actual hardware and software, as well as a mix of real and virtual components, make up a cyber range. The Internet level of the range environment includes not only simulated traffic, but also network services such as webpages, browsers, and email that the consumer requires.

A Cyber Range may be a training centre for cyber defence that allows organizations to increase the skills of their teams in the defence of their network infrastructures.

Companies can use these environments to educate staff and consumers about the latest dangers and practice managing specific real-world events.

Military and government institutions, private enterprises, and colleges that specialize on cybersecurity all use cyber ranges:

- professionals from information technology, cybersecurity, and others use cyber ranges to improve their knowledge and capabilities as individuals and teams;
- students can use cyber ranges to put their networking skills to use, develop cyber skills;
- cyber ranges can be used as a classroom for instructors;
- cyber ranges can be used by businesses to assess their capabilities to defend against cyber threats, train personnel on cyber defence 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.”*

2.8.1 Taxonomy of Cyber Ranges

An exhaustive study of Cyber Ranges is presented in the paper [10]. The authors proposed an initial taxonomy to classify cyber ranges (see Figure 4).

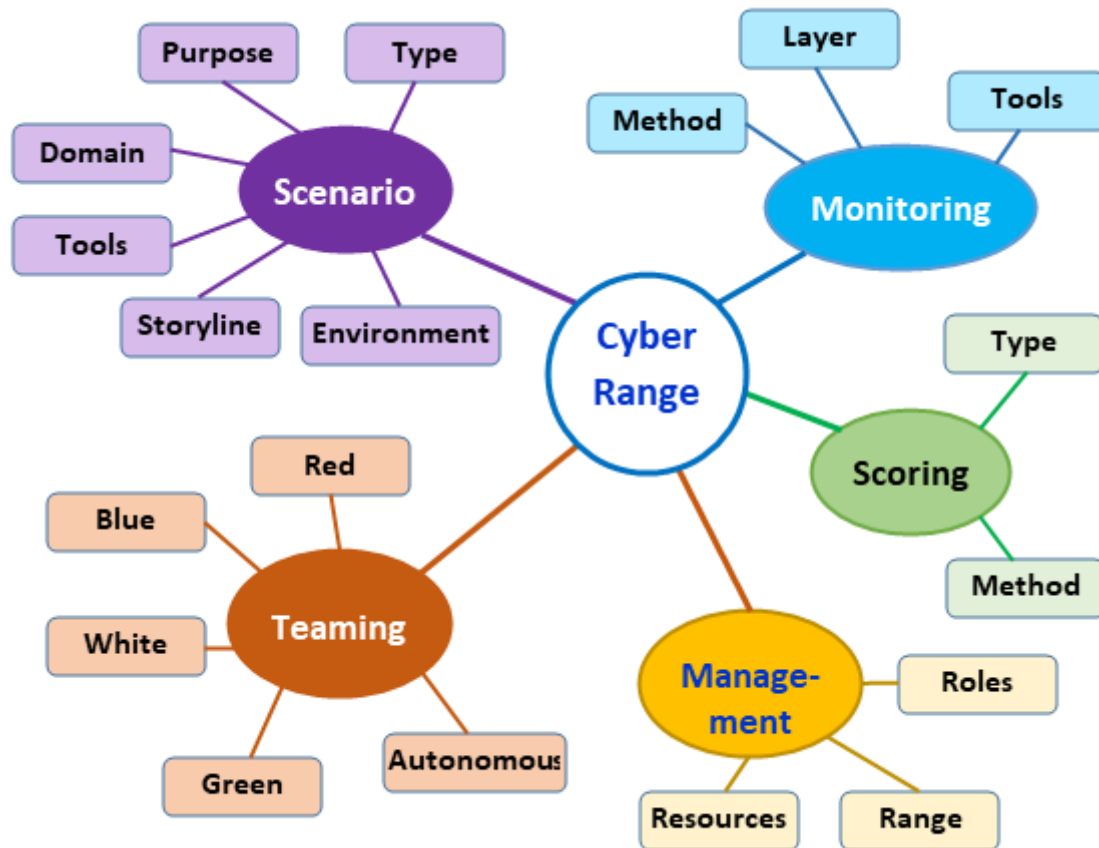


Figure 4: Cyber Range taxonomy [16]

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

- the scenario's **purpose** defines the scenario's goals (for example, the execution of a cyber-security training exercise or the validation of new cybersecurity tools and procedures);
- the scenario **type** indicates whether the scenario is static (in which case the environment is static and no changes are made during the execution of the exercise) or dynamic (in which case the scenario includes a dynamic component that will change during the scenario execution);
- the execution **environment** – the topology in which the scenario is carried out; in an operation-based exercise, the environment will be a technical infrastructure (computer-based, physical, virtualized, or hybrid); in a table-top or discussion-based exercise, the environment can be non-computer based;
- the **storyline** indicates how the exercise will be executed; this enables a scenario's general understanding and control, as well as the capacity to evaluate the exercise's (or test's) outcome;
- the scenario's application domain (e.g., Internet of Things, network, cloud etc.) is indicated by the **domain**;
- the **tools** denote the tools required to create the scenario's environment or the tools utilized to generate a storyline.

2. **Monitoring** refers to the methods, tools, and layers used to conduct real-time monitoring of cybersecurity exercises and testing:

- the **methods** used to monitor the cybersecurity exercise, or the test, can be categorised either automatically (using instruments that gather data for analysis) or manually (by human observers);
 - the **tools** categorize software and hardware tools that can be used to monitor cybersecurity exercises and testing; examples include security information and event management solutions, intrusion detection systems, and so on;
 - the **layers** classify the monitoring layer; depending on the type of exercise, monitoring can be performed at several TCP/IP layers (in case of an operation-based exercise) or at abstract social layer (in case of a table-top exercise).
3. **Teaming** is a group of individuals or an individual who design, develop, manage and participate in a cyber-security exercise or a test. Different colors are assigned to teams depending on their involvement in a cyber-security exercise:
- the **red team** is responsible for identifying and exploiting any potential vulnerabilities may exist in the exercise environment;
 - the **blue team** is responsible for identifying potential vulnerabilities that can be exploited by a red team;
 - the **white team** creates the scenario, objectives, regulations, and evaluation criteria for the exercise and experiment;
 - the **green team** is responsible for the development, monitoring and maintenance of the exercise infrastructure that was created by the white team;
 - **autonomous teams** are the teams the roles of which are being automated by different tools and techniques;

Additional teams, which are exercise-specific, are incorporated in some cybersecurity exercises:

- during the exercise, the **orange team** members delegate distinct technical tasks to the blue team members;
 - to maximize the success of the exercise, the **purple teams** perform communication and information sharing between multiple exercises teams;
 - members of the **yellow team** simulate the behaviour of ordinary users who use the infrastructure developed by the green team.
4. **Scoring** is a method of assigning performance-related semantics to low-level technical events observed during the monitoring of cybersecurity exercises and tests using data from monitoring systems. During an exercise or a test, the scoring method is also used to measure the teams' progress and test their progress. The scoring mechanism's methods and tools are as follows:
- the **methods** show whether the scoring is based on the achievement of a specified goal or on the analysis of logs created during cybersecurity exercises or tests;
 - the **tools** categorize the software and hardware tools used to score cyber security exercises or tests.
5. **Management** involves the assignment of roles and responsibilities to individuals and teams, as well as the allocation of computing and other resources needed to undertake a cyber-security exercise or a test, and the management in general:
- **Role management** categorizes the methods, tools and techniques used to manage the identities and roles of individuals and teams participating in a cyber-security exercise or test;
 - **Range management** categorizes the methods, tools and techniques used in portals and dashboards to give a holistic perspective of a cybersecurity exercise or test;

- **Resource management** categorizes the computational resources needed to complete a cybersecurity exercise or test, such as processing frequency, memory, and disk space.

2.8.2 Benefits of a Cyber Range

Cyber ranges provide a number of benefits that might assist a company in preparing for future cyber threats. These benefits include:

- Cyber ranges give employees and customers a virtual encounter with real-world threats. It is possible to test advanced cyberspace strategies, techniques, and procedures that need isolated environments of large networked systems.
- It enables testing that would otherwise be impossible on open operating networks due to the risk of catastrophic outcomes, such as the execution of extremely harmful attacks on realistic representations of systems and networks.
- It allows controlling these experiments, determining the parameters an individual will experience, as well as the speedy and realistic representation of operating environments at various levels of security and/or scale.
- It also enables the experiment to be repeated with precise control of the test environment, reconfiguration, and speedy return to a baseline checkpoint. This would allow for rapid changes in conditions, allowing hundreds of possibilities to be evaluated in a short amount of time.
- Cyber ranges allow employees and customers to learn how to recognize possible threats and respond appropriately.
- Cyber range apps can be used by software engineers to test new concepts, testing market viability, and more. Cyber ranges allow testing how applications will function in live environments, as well as how these products will interact with and behave within that domain.
- Cyber range can enable users in developing operational concepts, procedures, and training materials, as well as determining how resilient a system is against a cyberattack.
- Cyber range may make sure that products are compliant. Vendors can use the cyber range to check if their products meet security requirements (e.g. with NIST Risk Management Framework).
- Cyber ranges allow speeding up time to production. Using the cyber range gives the opportunity to address vulnerabilities during the design phase, to certify that the product complies with all operating specifications.
- Cyber ranges are simple to set up and cost minimal capital, so they allow saving the business time and money.
- A virtual cyber range is always up to date and available to assist in the testing of any threats.
- Training scenarios on the cyber range can be accessed from anywhere. Because of this, they're an excellent choice for keeping personnel and consumers trained, certified, and ready to cope with cybersecurity risks.
- Existing virtual environments can be upgraded whenever preferred and scaled up in the future. Only the resources must be paid for in a virtual environment.

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

The Cyber Ranges were reviewed and presented in [19]. The review contains the 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 that distinguish them from other Cyber Ranges

Short information about the organization where Cyber Range was developed

Chapter 3 Pilot of Cyber training & exercise Framework

3.1 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 the 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 5.

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

CNIT presents its own platform with a storyline

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 the working staff.

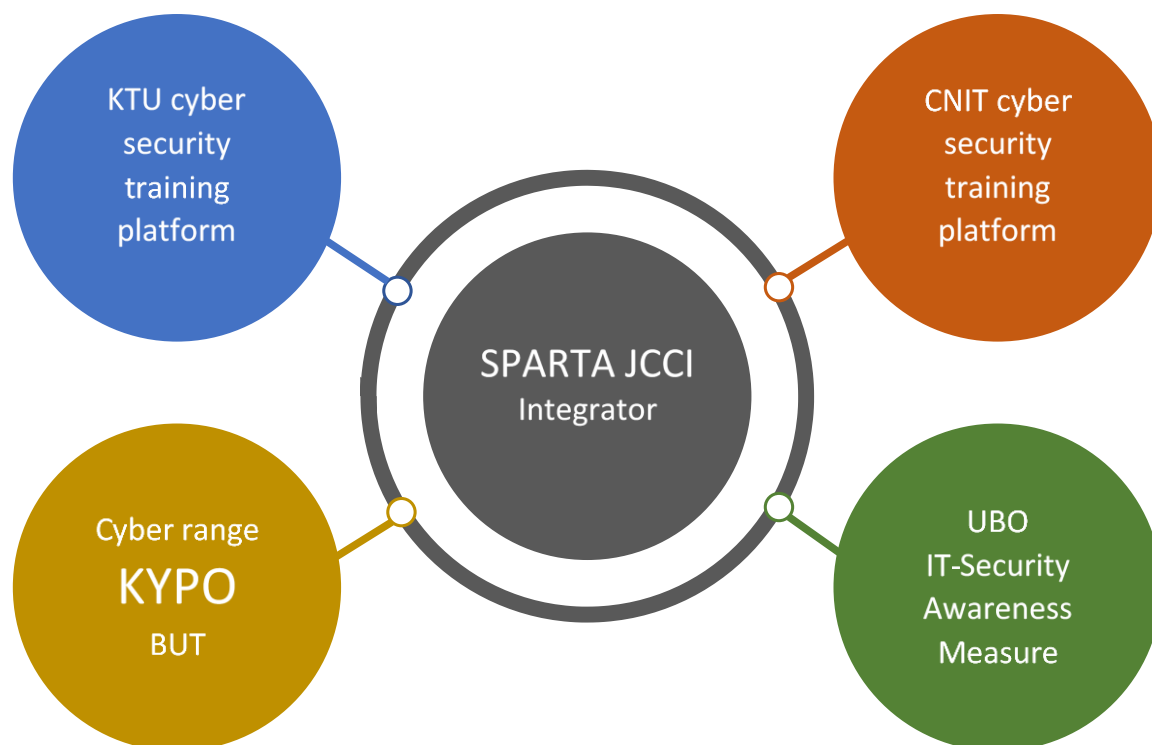


Figure 5: Federated infrastructure of Cyber training & exercise Framework

KTU. Developed information societies, such as the EU, are heavily reliant on data networks and computer systems as the world becomes more digital. This means that cyber attacks pose a threat to human well-being and possibly national security.

The interconnected environment of physical and electrical systems is commonly referred to as a cyber-domain in this complex world where the borders between digitalized infrastructure and the physical realm are blurred.

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-re The necessity for training against many forms of cyber-related risks is ever-growing in today's society, when the cyber domain is a vital part of people's lives. KTU has arranged a wide range of cyber training programs (Figure 6). Training to protect against threats should take place in a controlled environment, as realistic simulated attacks are required. If this were done on the open internet, mistakes could lead to breaches of the law or harm to outsiders. Furthermore, few businesses are prepared to risk compromising their production environment or continuity of company's business.

The cybersecurity exercises are conducted in closed cyber ranges that are disconnected from the internet but imitate the services and infrastructure of the real internet. Regardless of whether one is training in simulations or dealing with real-world cyber security problems in production systems, the necessity for correct situational awareness is always critical.

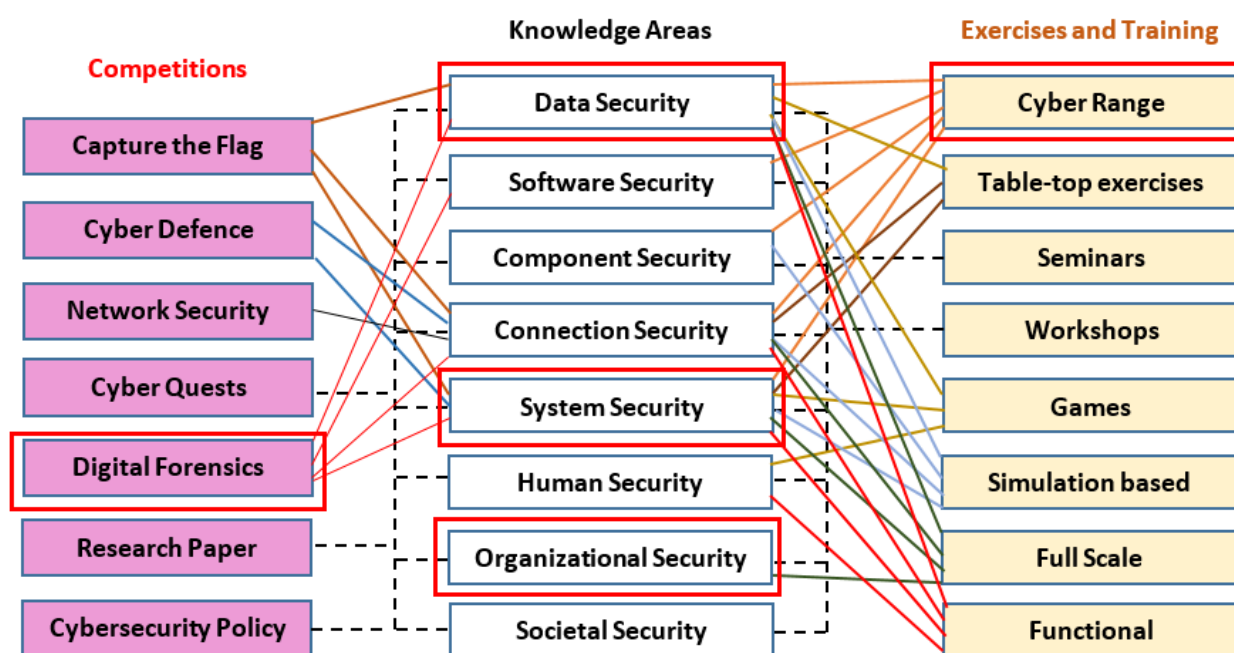


Figure 6: Acquisition of knowledge and practical skills using KTU Cyber training & exercise platform

CNIT. CNIT is piloting a Cyber Range infrastructure built internally, called Nautilus Cyber Range. The team believes 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 training 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 can be applied easily to new scenarios. The most valuable advantage of this knowledge sharing approach is the ease of 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 web app 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>. 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 practical training of students. It is built on the OpenStack cloud platform which is a set of freely available tools allowing 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 the 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 training can be available both locally and remotely via the HTTPS interface. For further details please follow KYPO CRP 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. A detailed description of the pilot design, deployment and results is provided in Chapter 6.

UBO. Common security guideline [25, 26] advise for awareness training for every user of an IT infrastructure. This kind of training should be repeated regularly and the effectiveness should be monitored. The motivation is a change in user behaviour that leads to a lower number of security incidents and a larger portion of user-reported security incidents. However, monitoring the effectiveness of such training and ultimately user behaviour is no trivial task. Phishing simulations became more and more popular the recent years to obtain a snapshot of the user phishing susceptibility. The “IT-Security Awareness Penetration Environment”, or “ITS.APE”, extends this concept to a full bandwidth behaviour analysis and supports it by a toolkit. The JCCI platform lists the link to the whole toolkit.

Different training & exercise activities can be used for deeper mastering of teaching materials in cybersecurity.

The analysis of the solutions presented by KTU and partners allows determining how their solutions cover the mentioned knowledge areas (Table 4).

Table 4: Covering of different Knowledge Areas by partners' platforms

Partner Knowledge Areas	Kaunas University of Technology (KTU)	National Consortium for Telecommunications (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				X
Organizational Security	X			
Societal Security	X			

Chapter 4 KTU Pilot of Cyber Security Training

Platform

KTU has a lot of experience in conducting cyber training exercises in the public and education sectors using the KTU Security Training and Awareness Platform. Over 300 people from over 40 Lithuanian government, cyber incident management and investigation, scientific, energy, communications operators, and other agencies took part in the cyber incident response exercises.

KTU Security Training and Awareness Platform as the basis of Cyber training & exercise Framework is presented in this chapter.

4.1 Description of KTU Cyber training & exercise Framework

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

- the experience in conducting cyber training exercises shows the importance of such training and exercises in the public and education sectors;
- the 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 presented in Figure 7.

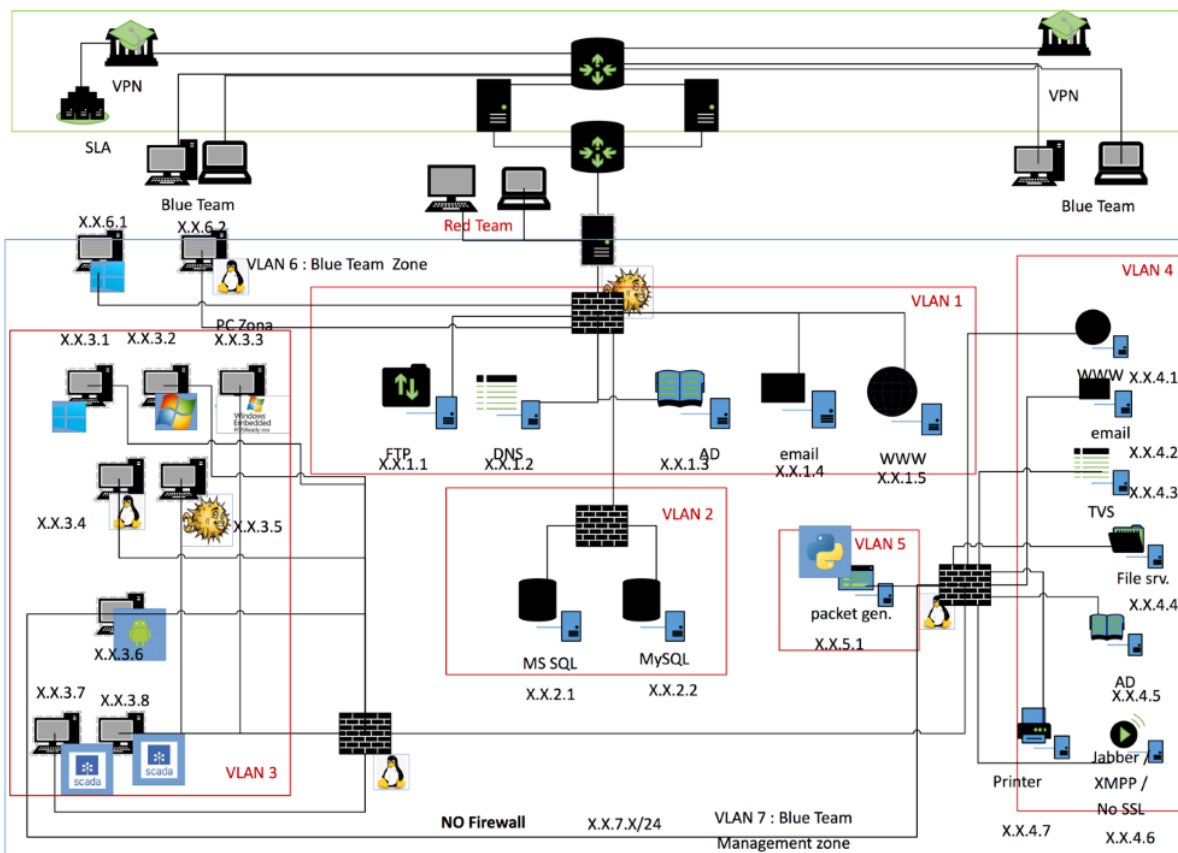


Figure 7: The typical topology of institution



Within the Cyber Range Platform, network segmentation with virtual local area networks (VLANs 1-6) produces a set of isolated networks. Every network has its own broadcast domain. VLAN segmentation, when properly implemented, significantly reduces access to system attack surfaces. It decreases the ability to sniff packets and increases the effort required by threat agents. Finally, authorized users can only see the servers and other devices they need to do their jobs. Protocol separation is another benefit of segmentation. Certain protocols can be restricted to specific Cyber Range segments by network design. In this scenario, it can be seen that the segmentation implemented makes gaining access to the internal network extremely difficult for an attacker. It also explains the network's flaws at the same time.

Red teams are tasked with penetrating various systems and determining their security levels. They're there to find, prevent, and eliminate security flaws.

A red team mimics real-world attacks that could affect a company or organization, and they go through all of the procedures that an attacker would go through. They show organizations what could be backdoors or exploitable flaws that pose a threat to their cybersecurity by taking the position of an attacker.

A typical approach is to hire someone from outside the organization for red teaming, someone who is knowledgeable about exploiting security flaws but is unaware of the organization's defenses.

A red team's tactics range from normal phishing and social engineering attempts aimed at employees to impersonating employees with the purpose of gaining admin access. Red teams must understand all of the tactics, techniques, and processes that an attacker would employ in order to be completely effective.

Red teams provide important advantages, such as a better understanding of potential data exploitation and the avoidance of future breaches. Companies ensure their security is up to date with the necessary defenses in place by simulating cyber assaults and network security risks.

A blue team is similar to a red team in that it examines network security and looks for any potential flaws. In most cases, the Blue Team and its supporters must defend against genuine attacks. They can be established and monitored with the assistance of an IT personnel over a quite long period of time or in a typical operating setting (e.g., as part of an operational exercise).

The task of blue team is to identify ways to defend, adapt, and re-group defense mechanisms to make the incident response much stronger once a red team imitates an attacker and attacks with distinct tactics and procedures. And attacks aren't the only thing that the blue team does. They are constantly working to improve the digital security infrastructure as a whole, using:

- Security audits, such as a DNS audit
- Log and memory analysis
- pcap
- Risk intelligence data analysis
- Digital footprint analysis
- Reverse engineering
- DDoS testing
- Developing risk scenarios

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:

- (i) Selection and training of the national teams towards their participation in the European Cyber Security Challenge.
- (ii) Summer school on cyber-security awareness and training.
- (iii) Common development of educational material and tutorial lectures and integration into the currently offered curricula.
- (iv) “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:
 - a) cyber-security training of digital natives,
 - b) security awareness of key stakeholders such as educators and parents,
 - c) 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 to 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).

4.2 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. A framework that will be based on the storyline is provided (scenario templates).
4. Partners can provide their own knowledge-based framework, which will cover the organizational and technical means.

Given the ever-increasing magnitude of cyberattacks today, hands-on cybersecurity education and training activities are vital. Only via such hands-on exercises will trainees gain the practical skills they need to cope with security issues in real-life settings. Current programs, on the other hand, rely

mainly on manual setup and configuration of learning and/or training settings, which is a time-consuming, inefficient, and ineffective approach.

4.2.1 Description of KTU Cyber training & exercise Platform

In Figure 8, an integrated cybersecurity training framework is presented. The implemented framework allows participants to choose the history of attacks, their descriptions and the collected evidence. The team can be divided into several groups: some deal with technical tasks (digital evidence, type of attack, timestamps, vulnerability), others deal with procedural issues (IT policy, tools applied, architecture).

The results show that the Cyber training & exercise Framework is well-suited for today’s training activities in terms of features, usability and execution performance.

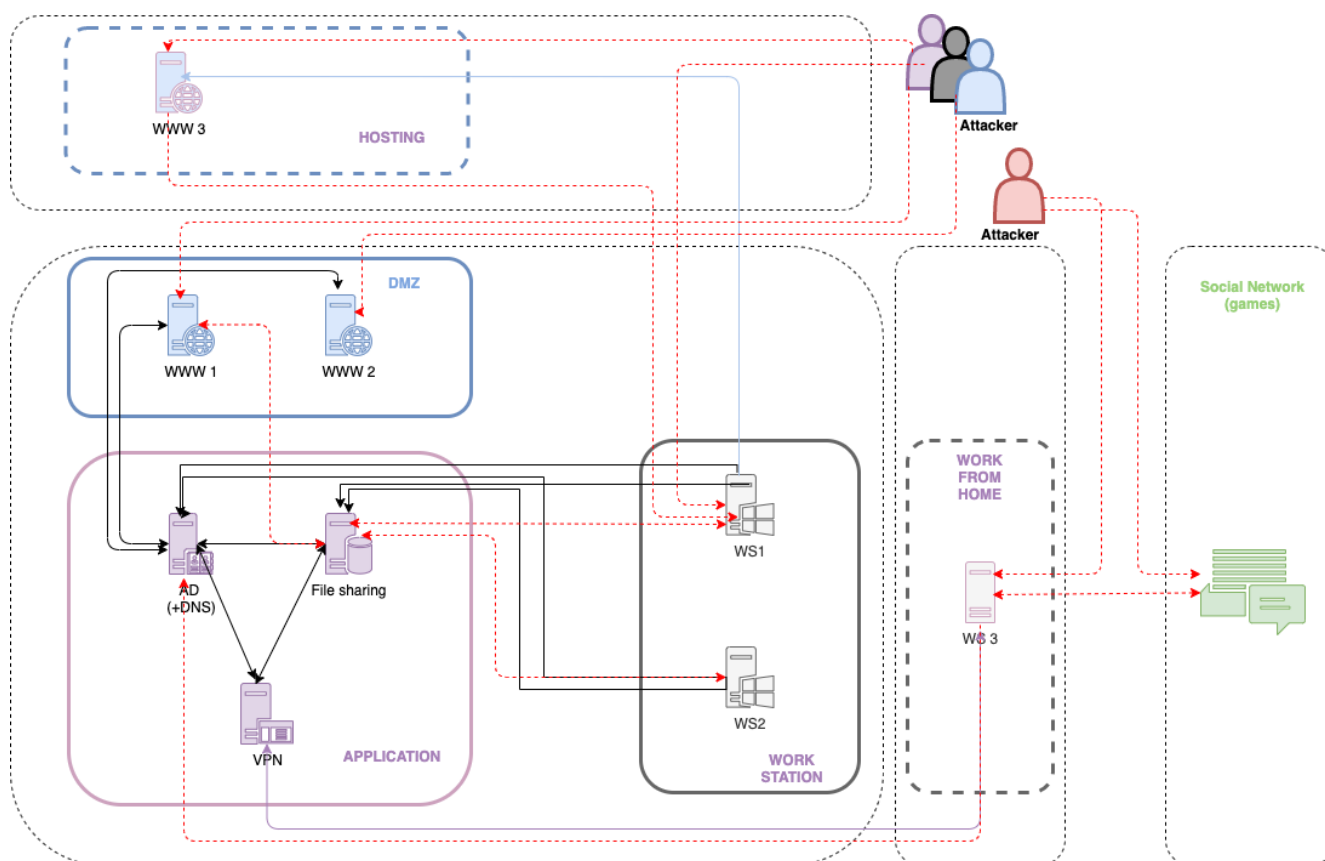


Figure 8: Infrastructure of KTU Pilot of Cyber training & exercise Framework

4.2.2 Installation of KTU Cyber training & exercise Platform

For the virtualisation of the KTU Cyber training and exercise platform, it is recommended to use a free, open-source VirtualBox solution. VirtualBox can install and run a disk image on OS X or Windows for free. Running Windows is basically the same as running any other application because it puts Windows into a virtual machine atop current operating system software, which makes it considerably easier than establishing Apple Boot Camp for a genuine Windows experience.

For more information regarding the installation see Annex No.1.

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

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

The main goal of the Red Team/Blue Team exercise is to develop practical cybersecurity skills of the participants, including technical staff and responsible for the organizational measure, to improve cooperation between cyber incident management and/or investigation centres, University technical staff and responsible for the 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 5:

- 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 the social network.

The first three columns in Table 5 represent incidents steps. Column **Incident** contain a brief description of the steps of the incident. The two next columns show, what measures (organizational and practical) are involved in incident handling. The last column indicates what systems (servers, websites, workstations, etc.) are affected by the incident.

Now the details for each storyline will be provided.

Storyline A1 (for additional information see in Annex No.4)

- 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. Then, proceeds to log in with the access profile (username/password) and view 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).

Table 5: Methodology of choosing practical and organizational measures

<i>Incident No.</i>			<i>Incident</i>	<i>In organizatio</i>		<i>The organizational system affected</i>
				<i>Organizational part</i>	<i>Technical part</i>	
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 viewing 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

Storyline A2 (for additional information see in Annex No.5)

- 1) Using the SQL injection method, the 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 downloads the file and opens it. Encryption of this workstation starts.
- 4) The disk image can be fully encrypted, the 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 (for additional information see in Annex No.6)

- 1) In this case, the Attacker exploits WordPress vulnerability in WWW2. Using the brute-force attack, Attacker gets access to CMS to obtain the 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. The said 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, the Attacker connects to the organization's AD server.
- 7) Since 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 a keylogger (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 (for additional information see in Annex No.5)

- 1) Attacker interacts with the child of a WS 3 user (who is the organization's IT administrator) in a 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 a child's computer.
- 3) Attacker sends to the 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 a user with administrator rights and enables keylogger.
- 4) Using VPN certificates stored in WS3, Attacker connects to the organization's Active Directory System (AD) server.

- 5) Since 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.

4.2.4 How to play storyline?

One of these possible storyline-based scenarios (Figure 9) is described below. It can be seen 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.

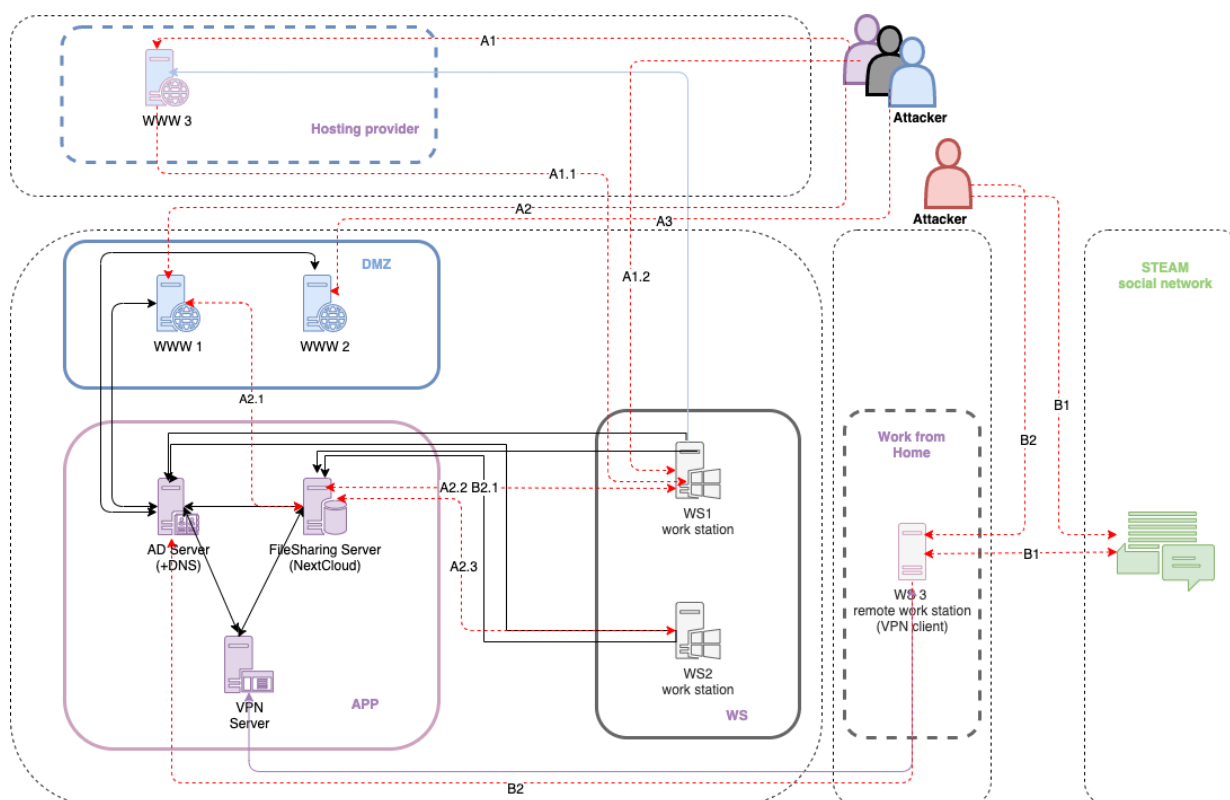


Figure 9: Attacks vectors based on storyline scenarios

Attack scenarios (storylines) are presented in Annex No. 1.

Below, one of the incidents is explained in detail – Incident A1.

Information of scenarios presented in Table 5 should be interpreted in such way.

Incident A1 starts with a cyber-attack using the password brute-force method. Attacker A hacks into the WWW3 website and places a malicious file there to prepare for a 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 their 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 written 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 the 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 the 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 6):

Table 6: 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

To make the exercises more effective and have a basis for realism, they can be started from an alleged incident report. The essence of the alert is that there is a message in the IT professional community forum about the leaked information. The leaked information is in a file (attachment No.1.xlsx) that can be found while examining the evidence. In this way, all participants will be interested in finding leaks, preparing reports of leaked information and investigating the incident.

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. 8.

Table 7 shows the integration and information exchange between the KTU-proposed Cyber training & exercise Framework and the SPARTA JCCI platform.

The Cyber Range platform developed by KTU can be used as a high-level requirement specification for a cybersecurity situational awareness system for defenders in cybersecurity exercises. A demonstration system that visualizes and aids in comprehending the present overall cybersecurity status and incident handling situation for a defense team should be possible to create and develop.

Table 7: Information exchange between Cyber training & exercise Framework and the JCCI platform

<i>Incident No. in KTU Cyber training & exercise Framework</i>			<i>SPARTA Joint Competence Centre Infrastructure (JCCI)</i>				
			<i>Data</i>	<i>Description</i>	<i>Interaction</i>	<i>Services</i>	<i>Tools</i>
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

4.2.5 The benefits of using the Cyber training & exercise Framework

The experience in conducting cyber training exercises allows drawing 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 the 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 the attacker ability to gain access to the internal network.
- Framework provides a possibility to expand using tools including those that may appear in the near future.
- Cyber training & exercise Framework can be used both for the training of the national cyber-security team and educating undergraduate and graduate students at universities.
- Cyber training & exercise Framework can be used for future research activities in contemporary topics related to cyber-security.



- The bulk of cybersecurity education programs use lectures or presentations to explain the issues to students and employees. Learning methods based on this approach are frequently constructed from the standpoint of the presenter, with a focus on presenting knowledge in a short amount of time rather than on effective transfer of information.
- The goal of using games is to raise cybersecurity awareness and training. This framework is built on existing frameworks that address the cyber domain's complexity, participants' unique characteristics, and the pedagogic potential of the planned games.
- It was demonstrated how combining these frameworks can improve the effectiveness, engagement, and ability to reflect in game practice.
- In order to fully grasp the potential of this framework and provide appropriate guidelines for the implementation of serious games, infrastructure must be installed on-site and play must begin.

KTU Cyber training & exercise framework explores how cybersecurity stakeholders should establish a robust and sustainable set of capabilities by quantifying the skill and motivation of the cybersecurity workforce. Learning by doing gives technicians, IT managers, and board members with sufficient training to close training gaps at all levels of enterprises and governments.

Chapter 5 CNIT – own platform with a storyline

5.1 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 and stakeholders, of the gathered information on cyber security threats and corresponding defence strategies. In that sense, it is proposed to use 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 cybersecurity 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 the cyber range community.

5.1.1 Core Design and Principles

The Cyber Range was designed with the following core principles:

- Easy configuration of dynamic scenarios and cyber threats
- Marketplace 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 storing 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 Figure 10 and Figure 11.

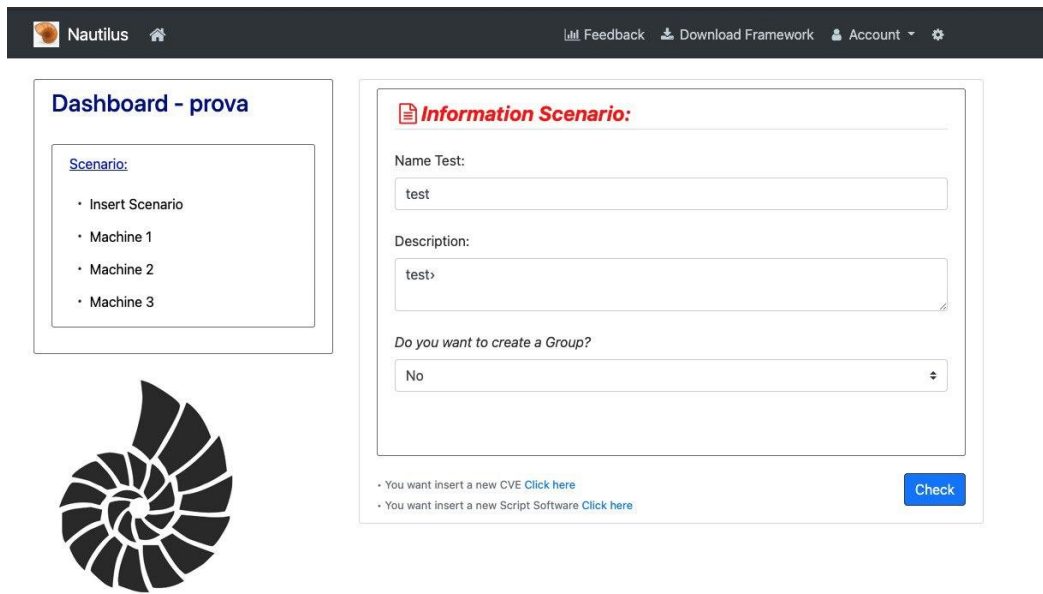


Figure 10: Creating a new Scenario

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 [27], each describing a core component of the scenario; when a scenario is built using the web interface, it is then stored inside the Nautilus database as a set of yaml files, thus providing a one-to-one mapping between these two methods.

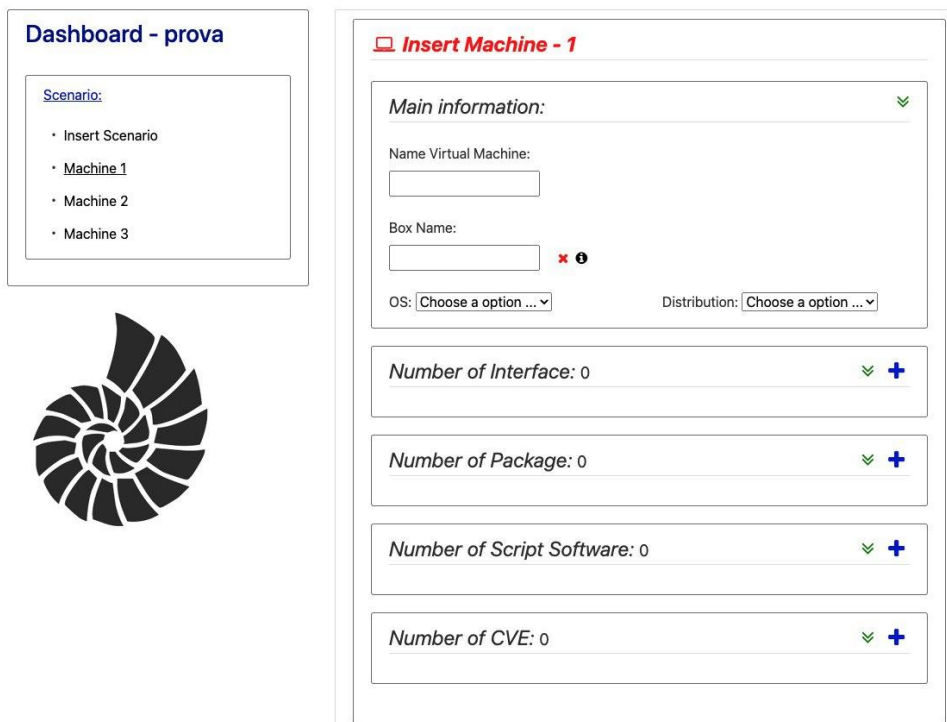


Figure 11: Creating a Scenario with 3 VMs

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 [28] 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 that is shared among scenarios made by different trainers. This example is shown in Figure 12.



Number of CVE: 1

Name CVE:

Choose a CVE ...

Search ...

Remove

Cve ShellShock User: steno - ID: CVE-2014-6271 - OS: Linux

CVE_fake User: tester - ID: CVE-2014-6271 - OS: Linux

Check

• You want insert a new CVE [Click here](#)

• You want insert a new Script Software [Click here](#)

Figure 12: Adding a CVE to a Virtual Machine

In other words, once the scenario is 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 13). Deploying to a remote server allows for decoupling the scenario creation step from the deployment step. Figure 14 shows the report of the execution of an example scenario deployed on a remote server.

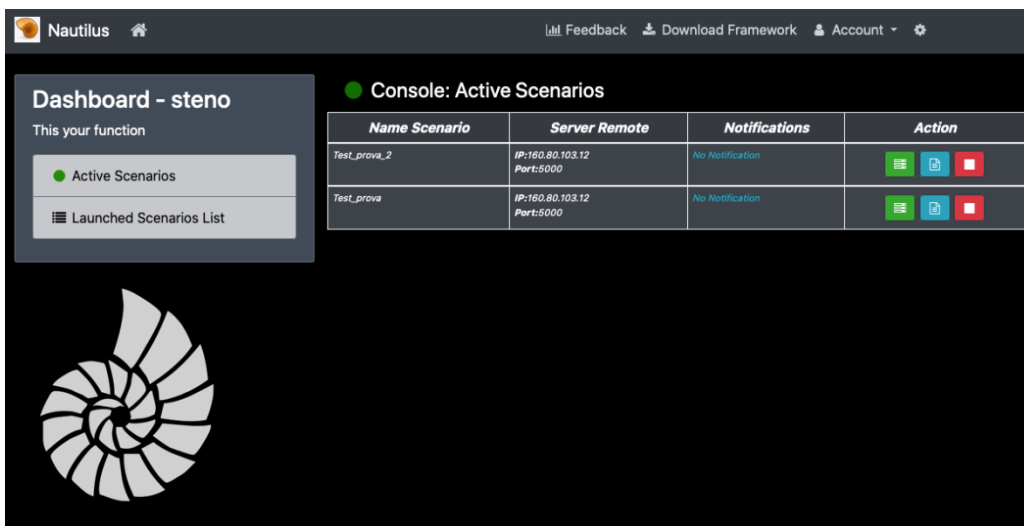


Figure 13: Nautilus Console

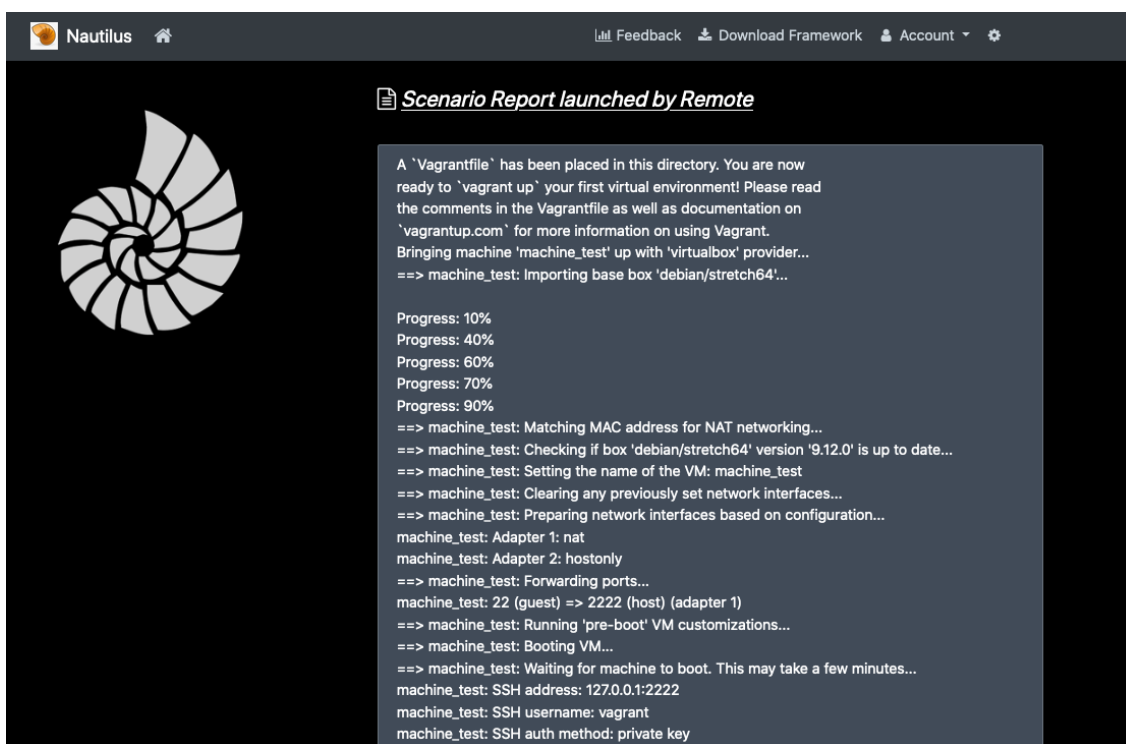


Figure 14: Scenario Report

5.2 The Pilot: CTF platform for cyber competition

The presented storyline 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 15). The PROD environment contains the deployed challenges; in other words, this is the environment that is attacked by the other teams. The DEV environment contains the source code of the deployed challenges in form of a git repository (Figure 16). 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 17). Fixing a Service means that other teams will not be able to exploit it.

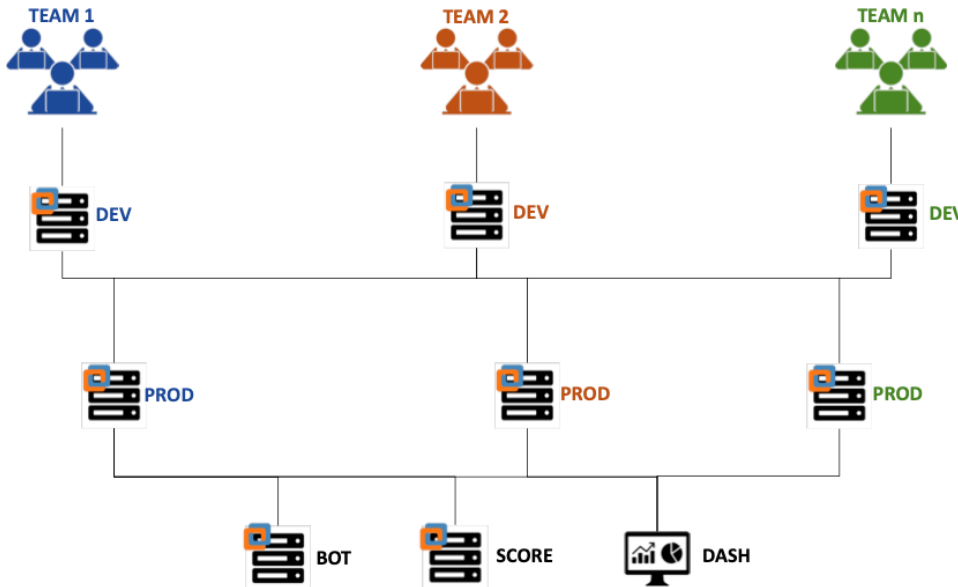


Figure 15: CTF Architecture

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 for controlling all the environments and making sure each team is behaving legitimately.

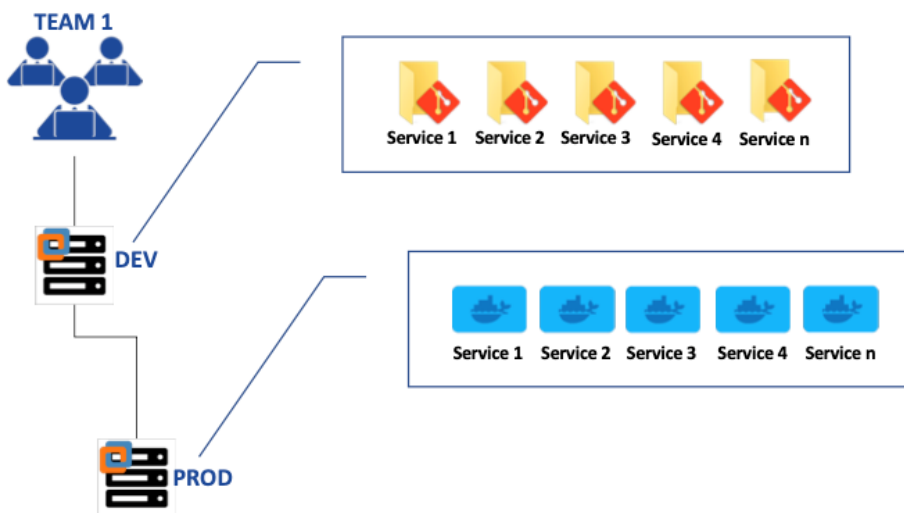


Figure 16: Services in PROD and DEV environment

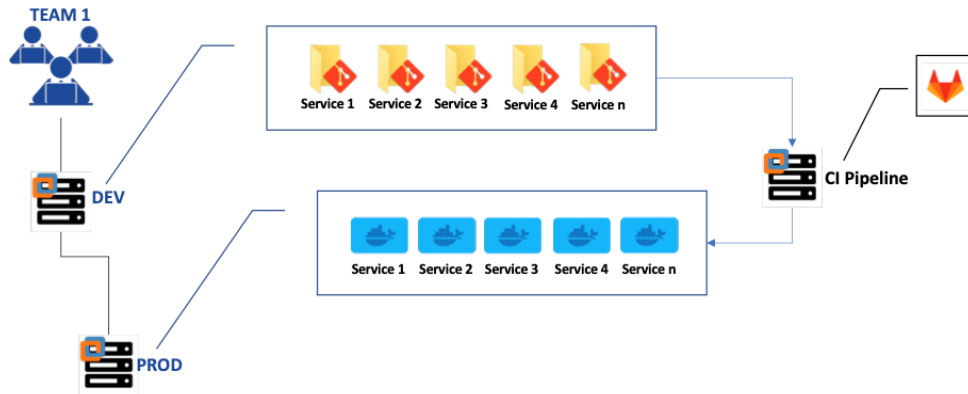


Figure 17: Automatic deploy pipeline

5.2.1 How to run the exercise

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

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

5.2.2 CTF challenges

Each PROD environment is composed of 5 containerized services for which 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 file system, thus reading the flag.
3. Patents managing application, which allows submitting 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 file system, 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 in the decryption process of documents to be printed. 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.

5.2.3 Benefits of using the Nautilus Cyber Range

CNIT tested the usability of Nautilus among different users, namely both instructors and trainees of an Ethical Hacking course at the University of Rome “Tor Vergata”. To summarize, the benefits of using the proposed Cyber Range, gathered from the aforementioned analysis, are as follows:

- Marketplace of CVEs, vulnerable software, ...
- 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

Chapter 6 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 18) through which the entire training is available. These pieces of training can be available both locally and remotely. For further details please follow KYPO CPR documentation (available at <https://docs.crp.kypo.muni.cz/>).

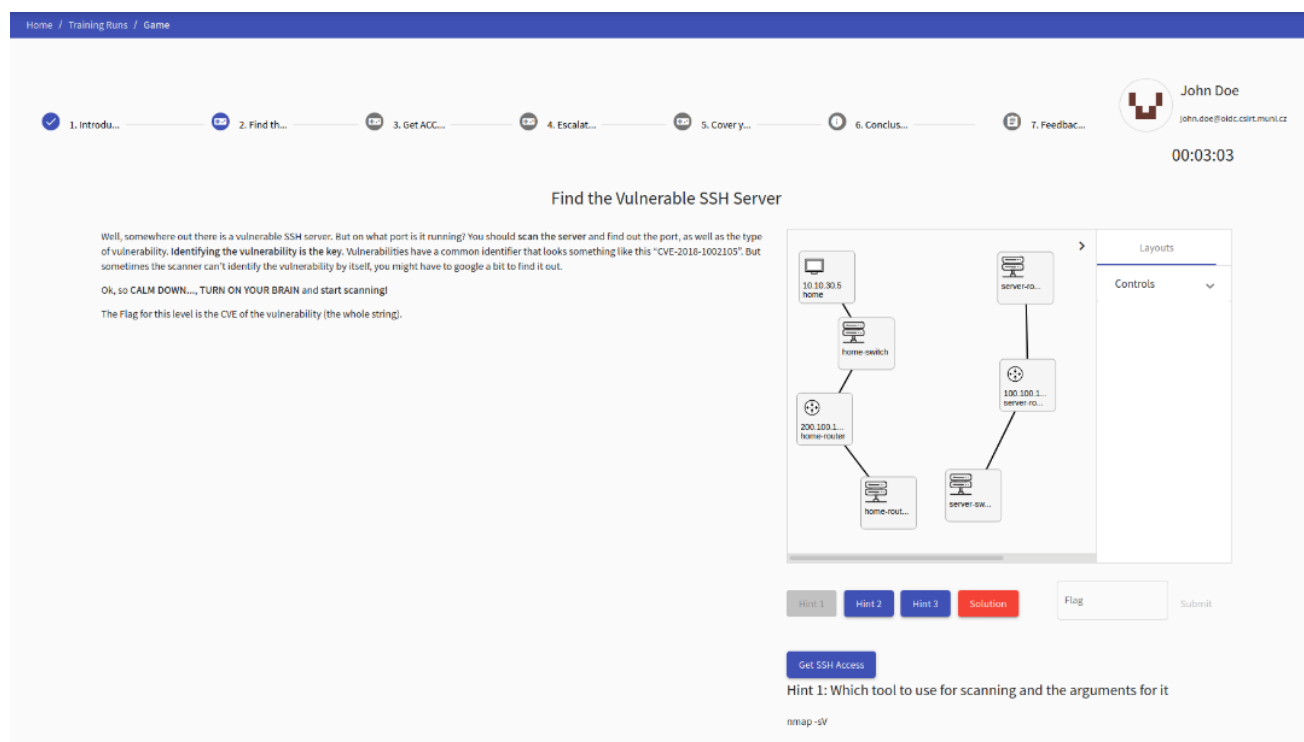


Figure 18: KYPO CRP User Interface

6.1 Deploying KYPO CRP

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

6.1.1 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).

Hardware recommendations are different for every server, Table 8 shows minimal requirements for running 10 average trainings.

Table 8: 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
Computer	20	128	1500	2

These requirements are sufficient, but not recommended. Recommended hardware requirements for 10 average trainings are shown in Table 9:

Table 9: 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
Computer	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 19). One network is dedicated to management. Second network is dedicated as a provider network for virtual appliances.

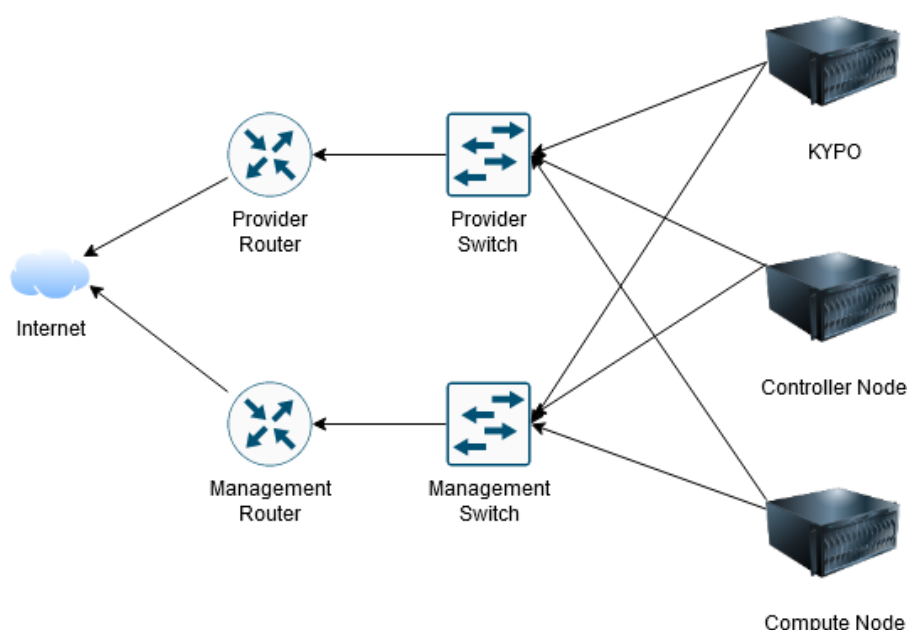


Figure 19: Network Infrastructure needed for KYPO

KYPO CRP Portal can be installed on a 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 process (see Annex No.9).

6.1.2 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:

- Operating System (see Table 10);
- Disk controller;
- RAID;
- Network Infrastructure.

Table 10: 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

As for the storage controller, it 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 to ensure that this infrastructure does not 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.

6.1.3 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).

To meet the requirement for long-term operation, it was necessary to purchase hardware that will meet the performance requirements. 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 a bottleneck due to the speed of 10Gbps, all servers have twice as many interfaces as 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 installed, 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 20):

Table 11: BUT Deployment Specification

Purpose	Device + Technical Specification
Controller Server	SuperMicro Server (<i>X11SPi-TF Motherboard, Intel Xeon Bronze 3104 CPU, 32 GB DDR4 RAM, 1TB RAID 1 SSD</i>)
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)

Purpose	Device + Technical Specification
Networking	Switch Mikrotik (CRS326-24S+2Q+RM, 24 SFP+ 10 Gbps ports, 2 QSFP 40Gbps ports) Switch Mikrotik (only for management purposes – CRS-226-24G-2S+)
UPS	APC Smart-UPS C 1500

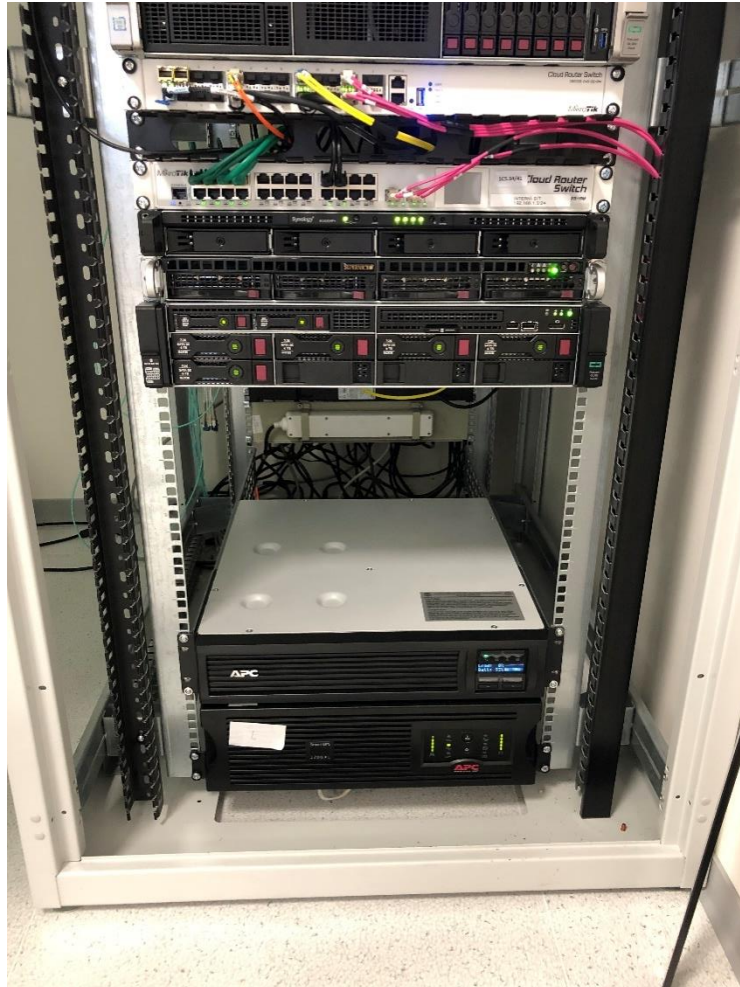


Figure 20: BUT KYPO CRP Rack

Installation procedure and troubleshooting see in Annex 9.

6.2 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 a web-based service, for accessing it, type in the browser url: <https://172.19.0.22/>. User 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 as shown in Figure 21:

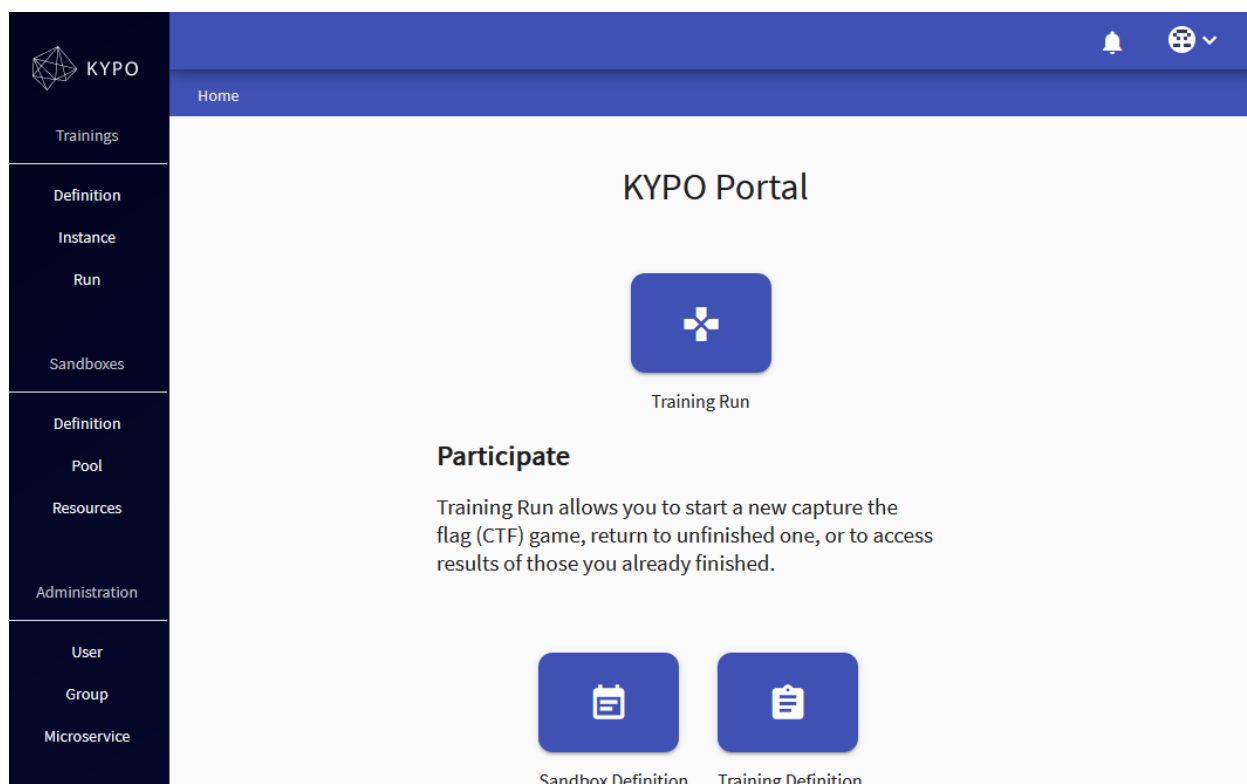


Figure 21: KYPO Portal

On the left side is the navigation panel.

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

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

In order to add a new user, use this link:

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

KYPO Portal uses external authentication, meaning that 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 the “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 the 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 micro services can be managed.

6.2.1 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 an open telnet port (see Figure 22). 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 a 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. Training Definition can be downloaded 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, a Pool has to be created. The pool can be created in KYPO Portal -> Sandboxes -> Pool -> Create. Select the number of sandboxes (1 for example) and press create. After creation, the Allocate Sandboxes icon can be clicked 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 preferred
- Start Time - now
- End Time – select end time
- Access Toke Prefix – prefix for a 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 the Pool section select the previously defined pool and click Create. After creating the Training Definition, the 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.

6.2.2 Creating New Scenarios

For creating new scenarios the Cyber Sandbox Creator tool can be used. 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
```

Because the Cyber Sandbox Creator 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. It will be followed by the installation of third-party programs that the Cyber Sandbox Creator runs in Ubuntu 20.04. The reason for using this operating system is that it contains the latest packages and dependencies.

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



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

Python3 is required for the actual launch of the platform and python3-pip will allow installing libraries later 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 the virtualization software is installed, then the virtual environment manager can be installed. 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, 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. They can be installed using this command:

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

6.3 Piloting Cyber training Exercise

6.3.1 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 22). 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 guide also included a chapter on the most common errors, where the most common configuration errors were described and how to eliminate them.

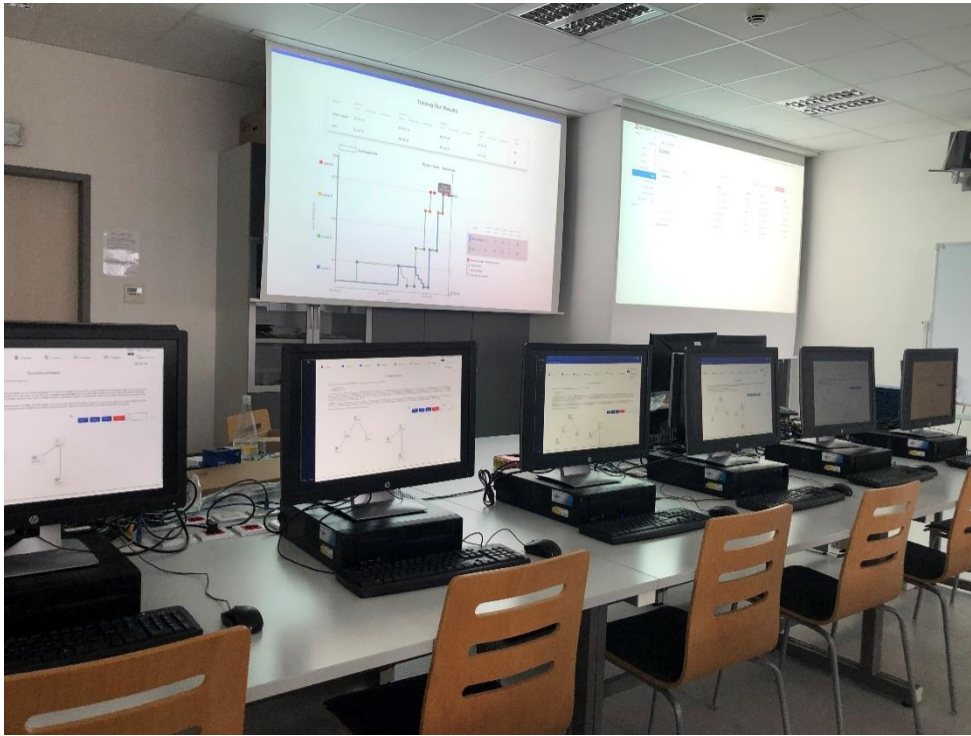


Figure 22: BUT Laboratory with running KYPO

6.3.2 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 aims to demonstrate the functionality of the BUT environment.

The student's first task was to find a vulnerable SSH server (see Figure 23). 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 is to find a suitable tool to exploit a vulnerable SSH server and use this tool (see Figure 24). The flag was then in the home directory of the compromised user.

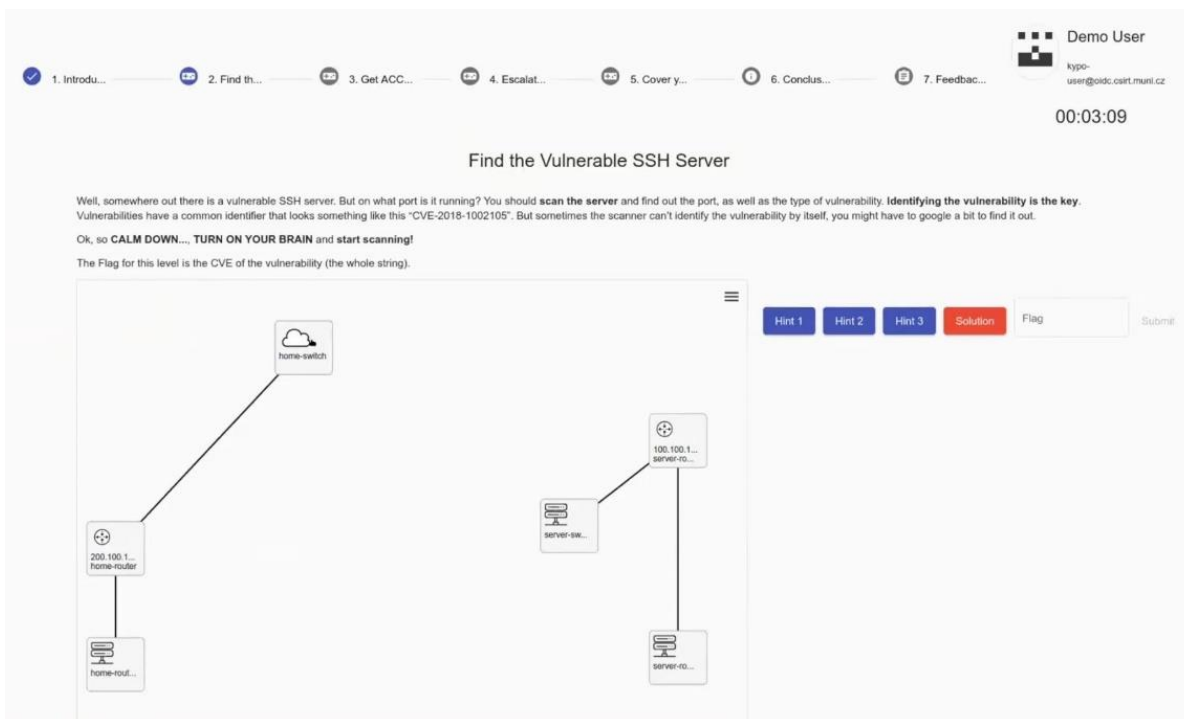


Figure 23: First task

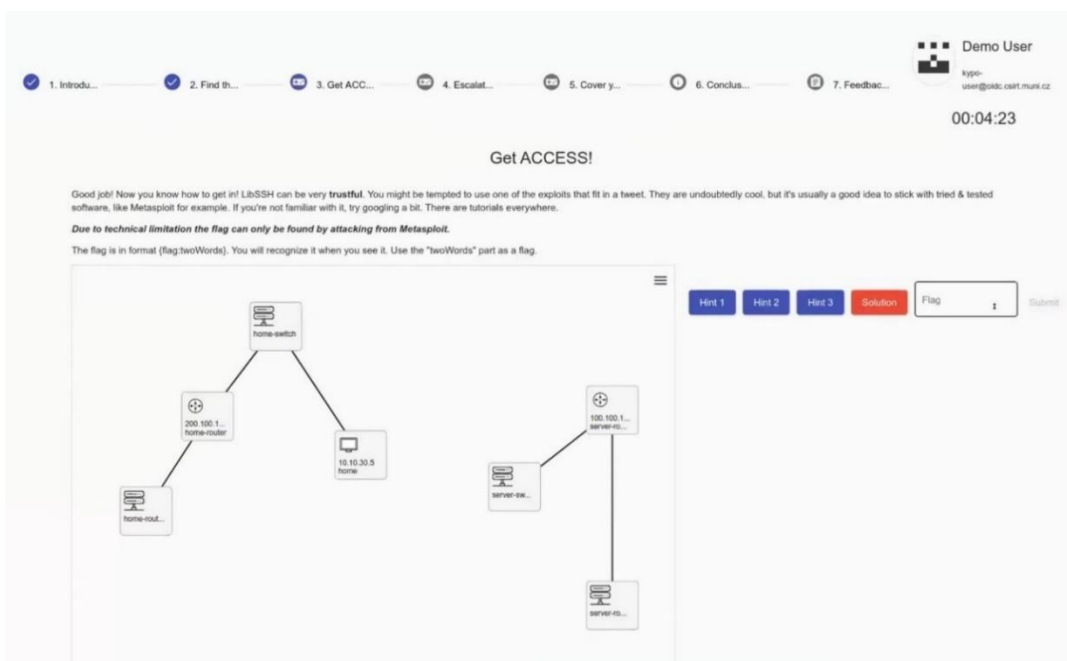


Figure 24: Second task

The third task is to increase permissions (see Figure 25). The compromised 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.

1. Introdu... 2. Find th... 3. Get ACC... 4. Escalat... 5. Cover y... 6. Conclus... 7. Feedbac...

Demo User
kypc-user@oidc.cisrt.muni.cz
00:04:37

Escalate privileges

Congrats, you are in. But it's only the beginning. (To not waste your time, we have a gift for you:

- username: alice
- password: starwars

You might try using the session from the last level, but that will only get you into trouble. So we strongly encourage you to connect to regular SSH on port 22 using the credential provided above. Now you can only see and do what a regular user could, but you need more. You need to access private files of other users, so you will have to **escalate your privileges**. The usual stuff might not work, the server is fairly well patched. Fairly well, but not perfectly. Last patches were applied mid-October 2016. So you're probably looking for some recent privilege escalation vulnerability. Maybe you already know where. You've talked with the guy in the bar for nearly three hours and he mentioned some broken display server.

I WARNING! You are messing with user accounts and privileges during the execution of privilege escalation attack. If you accidentally delete all accounts or destroy the server in any other way, the game might be over for you! This can be somehow salvaged if you keep your SSH running and fix the server again by repeating the attack correctly. But never close your active connection, you might not be able to get it again.

The flag is in one of the private files. You will know once you see it.

home-switch
200.100.1.1 home-router
home-rout...
home 10.10.30.5
100.100.1.1 server-sw
server-co...

Hint 1 Hint 2 Hint 3 Solution Flag Submit

Figure 25: 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 26). There is a flag in one of these files.

1. Introdu... 2. Find th... 3. Get ACC... 4. Escalat... 5. Cover y... 6. Conclus... 7. Feedbac...

Demo User
kypc-user@oidc.cisrt.muni.cz
00:04:42

Cover your tracks

Great! The file with the evidence should be named `underwood.doc`. It can be found somewhere on this server, who knows where. So find it and delete it from the server. But do you know what else you have done? You broke the server. Now no one can sign in. That's suspicious. And someone will soon notice that something had happened with the server. Maybe you can fix it by finding shadow's backup and copy it back. A huge bundle is waiting for you, please **DONT BUGGER IT UP!!!** The final flag is in the original `lets/shadow`. You'll recognize it when you see it.

And one more thing. In your efforts to escalate privileges you might have overwrote even the backup. If you find that's the case and you don't know how to continue, feel free to contact the organizers.

home-switch
200.100.1.1 home-router
home-rout...
home 10.10.30.5
100.100.1.1 server-sw
server-co...

Hint 1 Hint 2 Solution Flag 1 Submit

Figure 26: Fourth task

Scoring is set so that the student receives 2 points for completing the task. In the case of using the help, a penalty of 1 point is received. If the student views the solution of the task, receives a penalty of 2 points, therefore not getting any points in the result (see Figure 27).

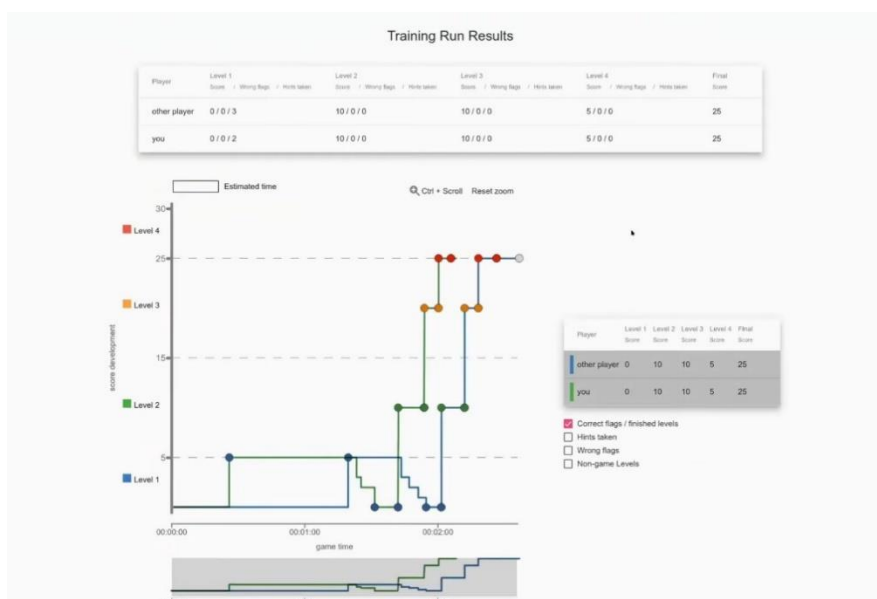


Figure 27: Scoring board

Now, after stress testing, it can be stated that most things are working properly, although there are 3 issues. The first problem is with the proxy server used, which behaved unstably under heavy load and the service tends to restart.

The second encountered problem 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. The controller had 6 computing cores without hyper threading 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.

The pilot verification will be performed under D.5.

Chapter 7 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 behaviour. Hence, training and exercise activities should be measured by the change in behaviour they induce. To this end, the University of Bonn developed a framework to measure IT security awareness within working staff [21]. The framework consists of a method and a software toolkit implementing that method. This framework facilitates the capture and analysis of the behaviour of employees as an expression of their 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.

7.1 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 the IT security awareness of employees 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.

7.1.1 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* cybersecurity, but they pursue a goal nonetheless. During the usage of the computer, a user perceives and interacts with different elements in order to achieve the set goal, whatever it may be. Some of these elements relate to IT security, some do not. An illustration of this model may be found in Figure 28.

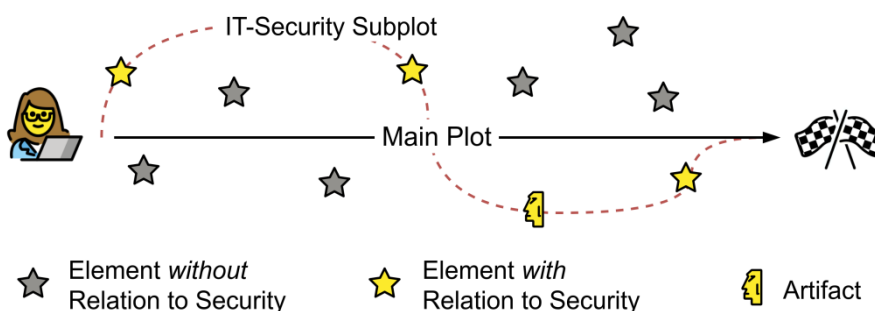


Figure 28: Situation model of terminal work

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.

1.1.1.1 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. For the user, artifacts are the carriers of stimulus. Figure 29 shows the four categories of artifacts that were detected, along with their interdependencies. Artifacts can be ascribed to either the host or the communication.. Phishing emails are a good example of artifacts that are based on directed communication.. The desecration of a website may be used as an example of undirected communication-based artifacts.. A user to a website that is under a continuous injection attack may see source code or errors.. Inserted files, such as the backdrop of a virtual disk, are an example of static host-based artifacts. [22]. *Operation-related dynamic host-based artifacts include, for example, the resource usage of a bitcoin mining process.* [20]. Most people are likely to have come across phishing artifacts and would therefore be aware with them. The other types are supposed to be more enigmatic character to users.

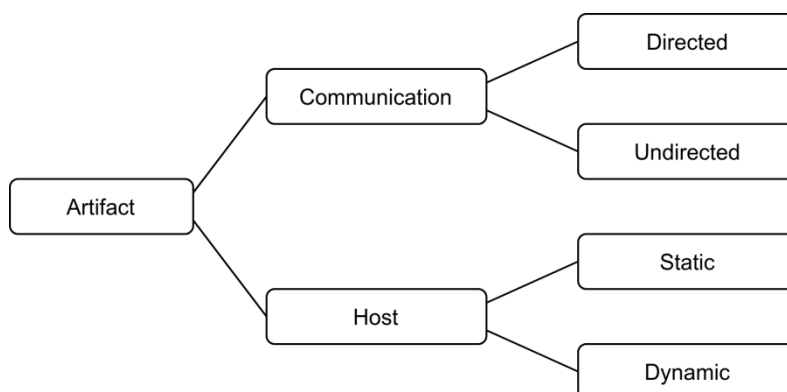


Figure 29: Classes of possible artifacts

1.1.1.2 User Behavior Analysis

Within an enterprise environment, the number of possible user actions that affect IT security is limited. Users are commonly only able to initiate security increasing or restoring process by reporting to the user’s support. This event is denoted with r in Figure 30. The interaction of the user with an artifact has to be considered potentially harmful to the security of the infrastructure. This interaction is shown in Figure 30 as i .

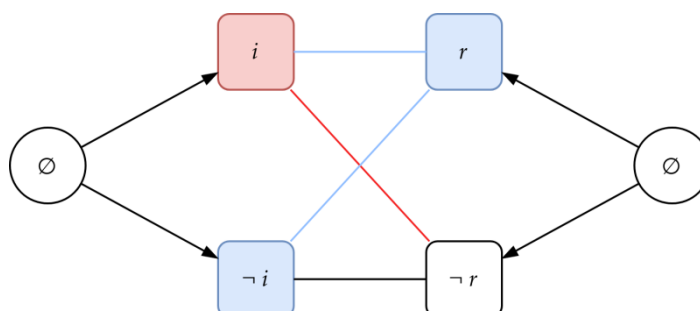


Figure 30: Combinations of user reaction classes

Figure 30 shows all possible combinations of events. If an user does not communicate with the artifact but reports it, i. e., $\{ \neg i \wedge r \}$, It's presumed that the user saw the artifact but decided not to interact with it, instead contacting assistance.. When people engage with the artifact but do not opt to call help, the worst potential consequence of an assault scenario happens., $\{ i \wedge \neg r \}$. In this situation, an attacker can pursue the goal without being discovered. It is a situation in which the participant exhibited a complete lack of understanding about IT security. In all other situations, the user is considered 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 $\{i \wedge \neg r\}$:

$$1 - P(\{i \wedge \neg r\})$$

However, the estimation of a group of individuals may be different. Assuming an organization of n individuals, an attacker might act as long as *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 modelled by:

$$1 - \frac{1}{n-1} \cdot \sum_{x=1}^n P(\{i \wedge \neg r\}) \cdot P(\{\neg r\})^{x-1}$$

7.1.2 *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 privacy of the individual. To evaluate a training or exercise effect of the action, measurement has to be taken before and after the 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.¹⁴

General installation procedure of the toolkit is presented in Annex 10.

7.2 Use Case

Itsape supports the quantification of the effect of any kind of intervention on the IT security-relevant behaviour 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.

¹⁴ <https://gitlab.com/itsape>

7.2.1 Preparation

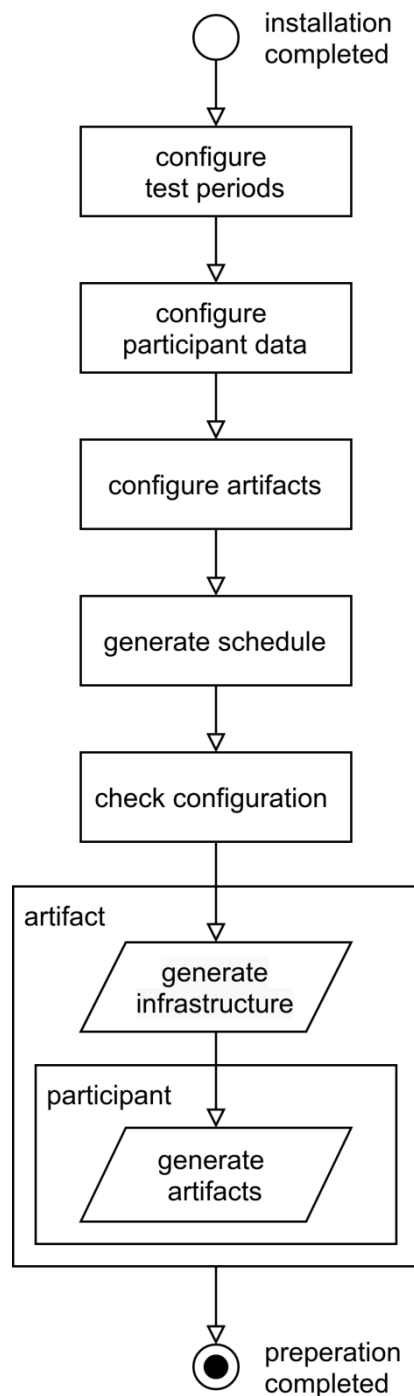


Figure 31: Preparation phase within the artifactomat

During Preparation Phase, the following actions need to take place. Figure 31 illustrates the Preparation Phase with regard to support by the toolkit itself.

1. A test installation should be set up 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 [21].
3. Installation of the client to all workstations in question and verification of their operability by the included not a user-visible artifact.

4. 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.
5. The measurement periods need to be set. This relates to the first step in Figure 31. 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 the increased cognitive load. However, if the period of time is chosen too long, the environment's influence on the measurement increases. A period of one month per measurement period (five artifacts) is advised.
6. Participants may need to be selected and informed consent has to be sought from the employees to be tested. This may be achieved, either by proxy of a working council [21] or by opt-out enrollment with semi-informed consent [4]. Personal data has to pass to the artifactomat. Navigate to `/etc/artifactomat/subjects` and configure the targeted participants according to the `readme.md` within that folder.
7. Place the recipes in `/etc/artifactomat/recipes` and configure the artifacts that should be used in testing.
8. Generate a schedule. The artifactomat will roll out artifacts to participants at random, evenly distributed over the testing period, set in Step 5.
9. Check whether the configuration reflects the intended implementation. If not, go back to the step which corresponds to the diverging configuration. If the configuration is as intended, proceed.
10. 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 configuration of the recipe. Subsequently, artifacts themselves are dynamically generated and fitted to configuration by the participant. This concludes the Preparation Phase.

7.2.2 Pre-test

During the 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 32. The artifact supporting infrastructure is continuously monitored. If an error impairs infrastructure availability, a test is not started or ended immediately. If the infrastructure available, the client will be activated and continuously monitor the participant activity by log-in events. If a participant is not at a desk when the test starts the test will be automatically deferred as long as the test schedules allow 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 reactions of the subjects 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 sent to all participants. Employees need to be made aware of the new purposes of data processing [24].

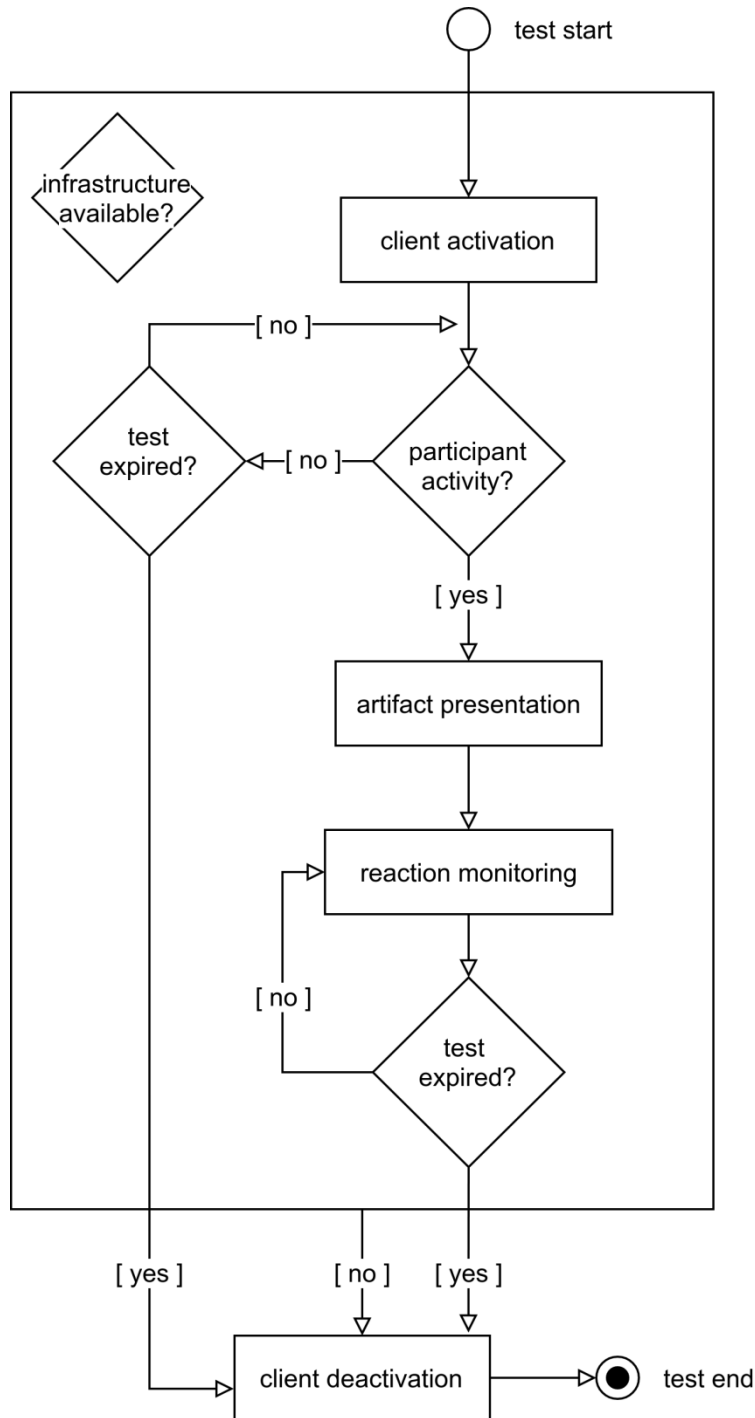


Figure 32: Test execution within the artifactomat

7.2.3 Intervention

Participants need to be split into two groups. One group receives the intervention, the other serves as a 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 afterwards. This may be achieved by limiting the group size and choosing the groups at random. This approach allows for controlling the motivational aspects of the treatment.

7.2.4 Post-test

Artifacts used in the post-test have to be different from 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.

7.3 Test Pilot

This toolkit was deployed in the administration of one of Europe's largest health centres. The effect of an IT security awareness class was measured. During testing, it was possible to demonstrate that a common class aiming to increase IT security awareness may have an undesirable effect on user behaviour [21]. The following sections describe the Pilot briefly.

196 individuals from departments not involved in crucial patient contact were chosen for the research during the pre-test phase. Because participation is unpredictable in an unregulated situations, not everyone take part in each test scenario. A scenario is passed by 51.25 participants on average. However, one participant passed 5.47 artifacts on average.

The intervention included 52 individuals who volunteered to take part. 50 people indicated interest via email or phone, requesting more appointments since they were unable to attend the previously scheduled ones. The invitation was not accepted by 94 people. The intervention's objective is to seem like a commercially available IT security awareness training, comparable to the ones that are necessary to be done periodically in order to acquire security certification. The intervention is planned and carried out by a firm with over 15 years of proficiency in penetration testing, cyber security consulting, and training. It was intended to be a 60-minute teacher-led class. The instructor demonstrated artifacts and probable reactions using slides and a realistic demonstration. The objective was to provide a typical experience that was often ordered. An overview of threat actors' motivations was provided, as well as the expected function of workers in an attacking scenario. Emails, Passwords, Browsers, Physical Media, and Mobile Devices are other covered themes. There was 15 minutes for open questions after the lesson, then a 15-minute overview. In addition to the lesson, an e-learning site was set up, with five videos uploaded on it (average length 9:12 minutes). Each video summarize one of the themes and was complemented by a 10-question exam on the material. The result is displayed when the test has been finished. The participant's response to each question is displayed. If the supplied response is wrong, the right response is also displayed.

A total of 163 people were chosen to take part in the study's second phase. In both phases, the same enrolling technique is utilized. As a result, natural change within the staff is the sole explanation for this statistic. Twenty-one of the Phase 2 individuals had already taken part in the intervention. By 59 people, the Phase 2 participant group overlaps with the Phase 1 participant group.

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 in the class, described above. The values are displayed in Table 12. This does not only diminish the effect

for the individual IT security awareness, but it also results in a decrease in organizational IT security awareness.

Table 12: Decomposition of the IT security awareness components

	$P(\{i \wedge \neg r\})$	$P(\{i\})$	$P(\{\neg r\})$
Intervention	0.143	0.167	0.956
No intervention	0.202	0.248	0.868

Chapter 8 Summary and Conclusion

The main objective of this report was to present a 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 aspects 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 the cyber training & exercise framework is presented. Partners (KTU, BUT, CNIT, and UBO) proposed their own tools and frameworks, which can be federated by the SPARTA JCCI integrator. Presented by partners, training & exercise tools cover all knowledge areas within the field of cybersecurity.

Chapter 9 List of Abbreviations

Abbreviation	Translation
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
BEC	Business Email Compromise
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
HDD	Hard Disk Drive
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
KA	Knowledge area
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
SSD	Solid State Drive
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

Chapter 10 Bibliography

- [1] ENISA Threat Landscape Report 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected, October 2020. <https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020> [Accessed 19/5/21].
- [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>.
- [9] Ensar Seker. Cyber Defense Exercises (CDXs) as a Testbed for Cyber Security. June 2020. https://www.researchgate.net/publication/342040488_Cyber_Defense_Exercises_CD_Xs_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](#)
- [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] Evangelos C. Chaskos. Cyber-security training: A comparative analysis of cyberranges and emerging trends. 2019, Athens. <https://pergamos.lib.uoa.gr/uoa/dl/frontend/file/lib/default/data/2864976/theFile>
- [20] 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.
- [21] 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*.
- [22] C. Xiao. 2014. *WIRELURKER: A new era in iOS and OS x malware*. PALO ALTO NETWORKS: unit42.
- [23] David B. Resnik and Peter R. Finn. 2018. Ethics and Phishing Experiments. In: *Science and Engineering Ethics*.
- [24] 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).
- [25] Wilson, Mark & Hash, Joan: Building an Information Technology Security Awareness and Training Program. NISP Special Publication NIST SP 800-50. National Institute of Standards and Technology, 2003. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf>
- [26] International Organization for Standardization: ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.
- [27] YAML version 1.2. <https://yaml.org/spec/1.2/spec.html>.
- [28] CVE. The MITRE Corporation. <https://cve.mitre.org/>.

Annexes

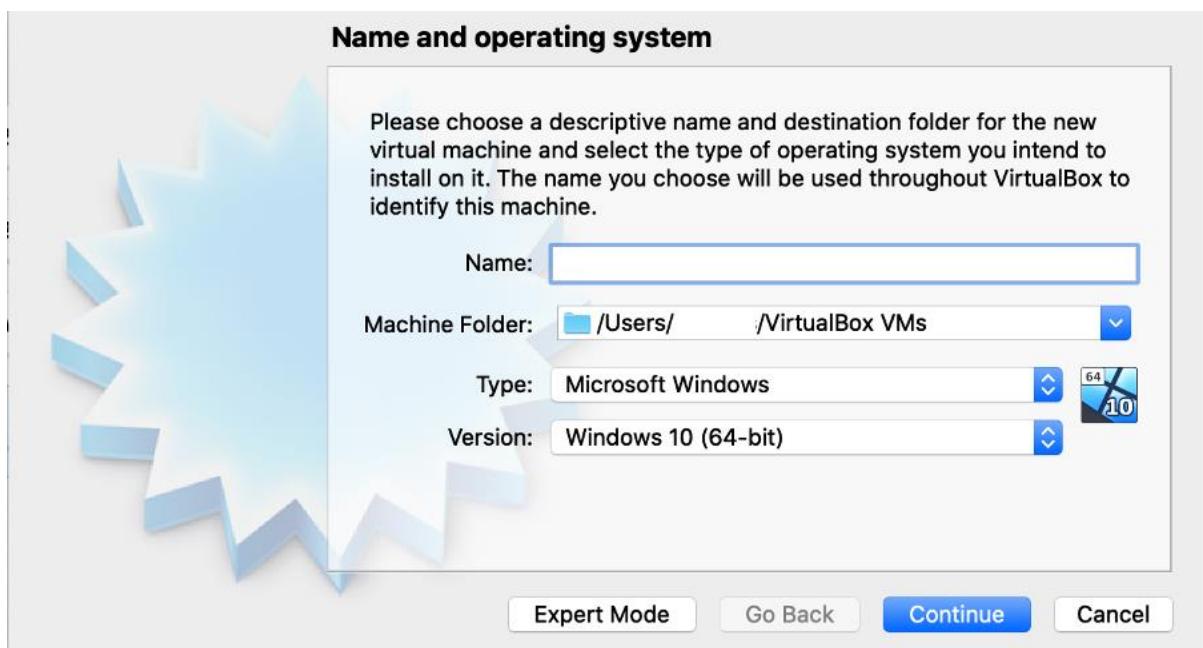
Annex No. 1 - The installation of a virtual machine image

Installation Requirements

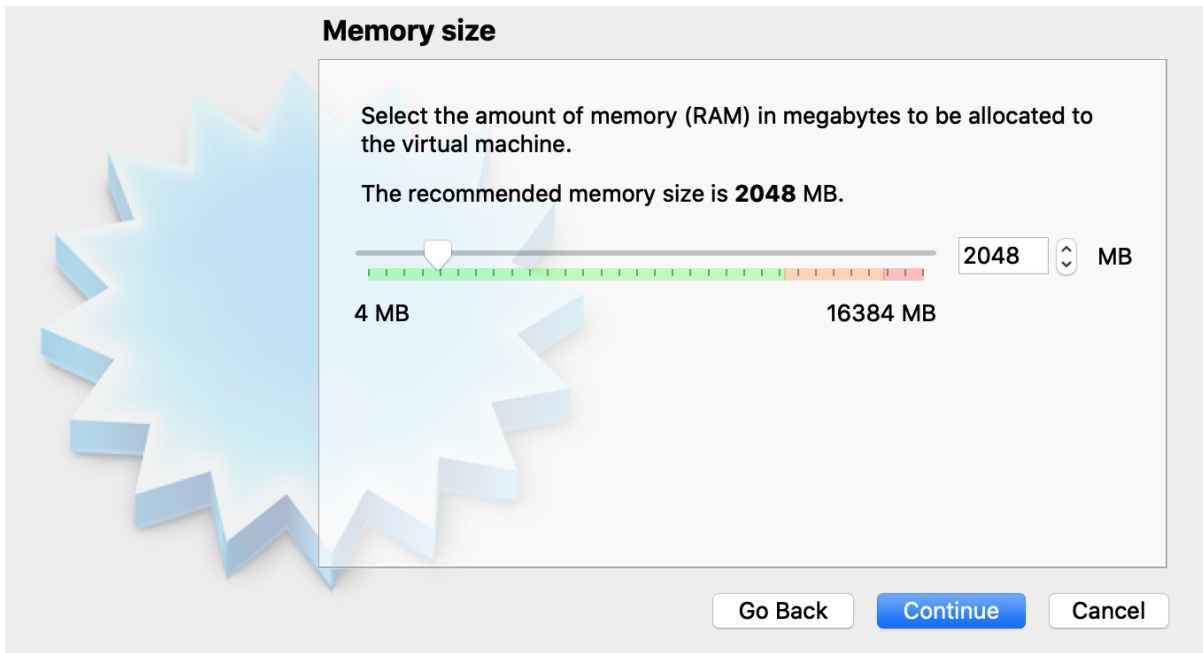
- Processor: 1 gigahertz (GHz) or faster
- RAM: 2 GB (64-bit)
- Free hard disk space: 32 GB (Virtual Size: 40.00 GB; Actual Size: 13.00 GB)
- Graphics card: Microsoft DirectX 9 graphics device with WDDM driver
- Windows 10 Installation Requirements for VirtualBox
- Download VirtualBox from this link: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

Installing process

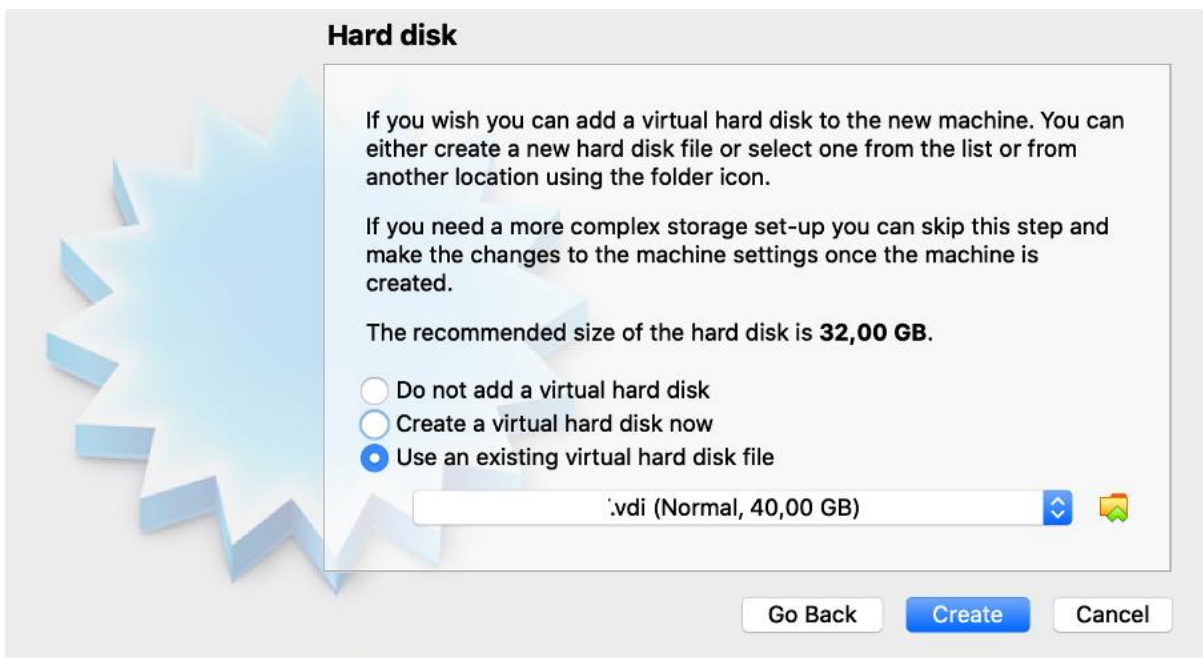
1. Download VirtualBox disk image (ImageName.vdi) (Workstation image is available to download).
2. Open ORACLE VM VirtualBox 6.x and select the window to create a new virtual machine. The virtual machine name and type must be specified.

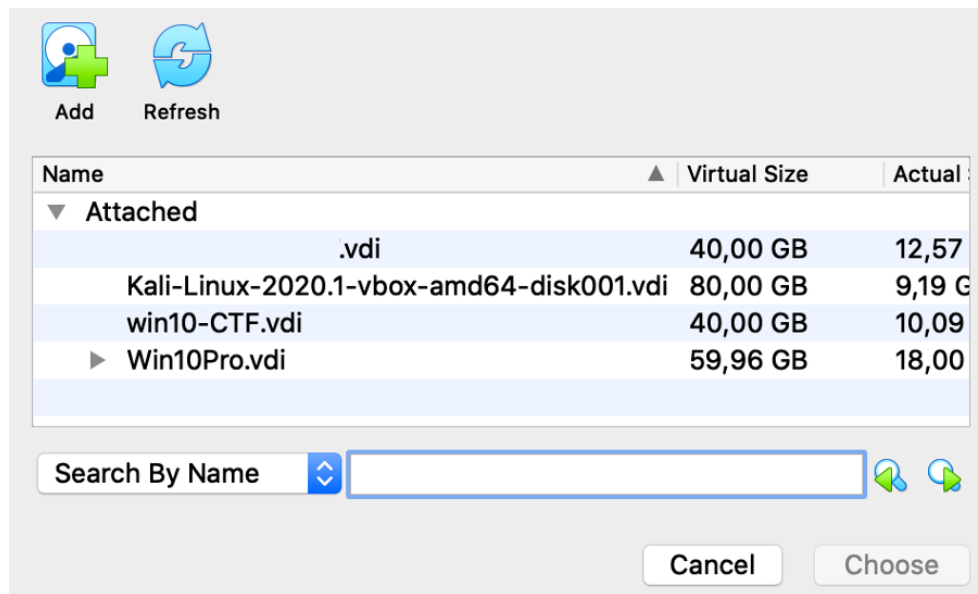


3. Press "Continue".
4. Select the amount of RAM (random access memory) and click "Continue".

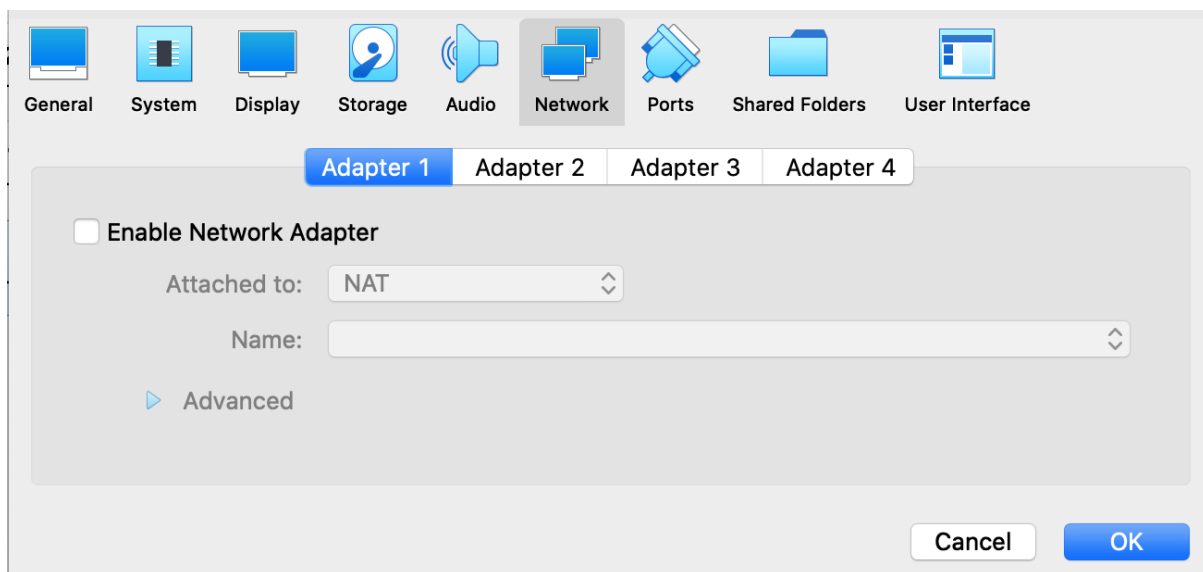


5. Select "Do not add a virtual hard drive" and click "Create" and "Continue" again. Click, select an existing disk and specify the path to the saved disk image (file: NAME.vdi).

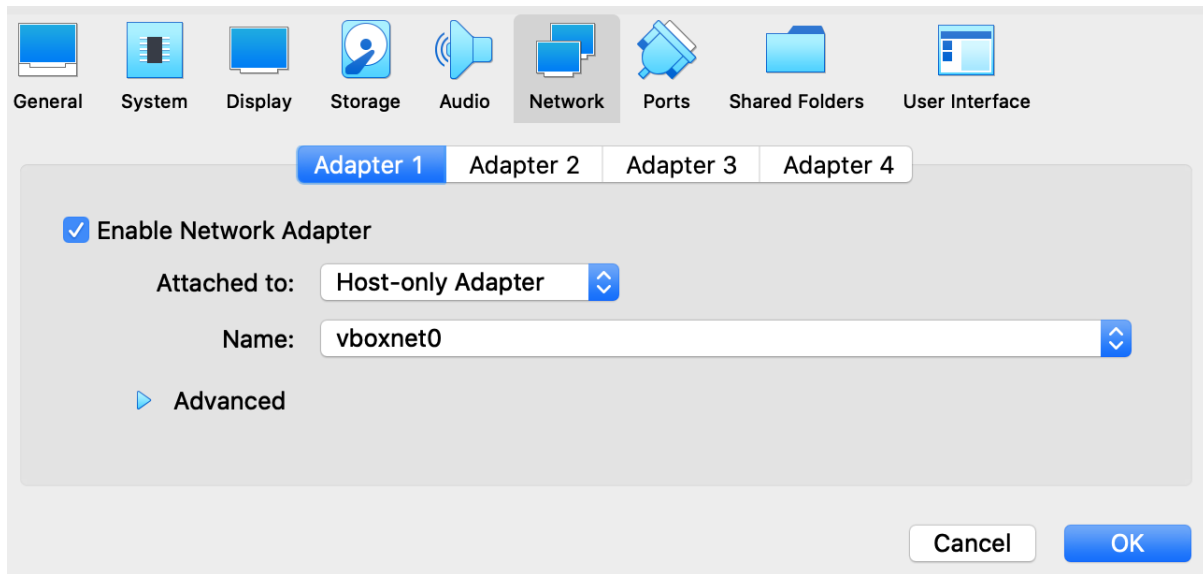




Additional recommendations include other useful settings that can be selected from the Settings Menu. For security reasons, it is recommended to uncheck the network settings and prevent the virtual machine from accessing the Internet:



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



After selecting all the settings, press the **Start** button.

Annex No. 2 - 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 a 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 user 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



Zone	Object	Name	Destination
			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 the 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. 3 - 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 and WordPress site administration rights using password hacking (<i>brute force</i>)	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)	<p>The employee responsible for the content of the publicly accessible website (WS 1) logs in with personal 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).</p> <p>To start the exercise, you can take advantage of the offered scenario: The organization has purchased programming work for the websites. Hackers took advantage of this information and sent an email about the completion of the work, which is a phishing attack, with a malicious file. And they are waiting for someone from the organization to click on the link. (WWW3).</p>
A1.1.1	received a phone call	<p>A phone call or e-mail to interested parties informing them of updates to the organisation's website and templates available for review.</p> <p>The employee who reviewed programming work that the organization purchased from the workstation (WS1) was infected with malware by clicking the link (It's a phishing/malware attack).</p>
A1.1.2	received an e-mail	Organization's user (WS 1) received an e-mail to the organization's mailbox with information about the work performed. All information about the work is posted on the website of the organization (WWW 3). Email is used to infect an employee of an organization with malware. It is necessary to own the workstation and gain access to the organization's network.
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



Incident No.	Incident	Short description
		(WWW 3) infects the 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_It_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, Attacker A obtains usernames and passwords. By using one of them, 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 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 viewing 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	An 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 the 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.



Incident No.	Incident	Short description
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")	Attacker B communicates in a public space using an employee's WS 3 computer with a child, who is left on the official computer so that the child 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 fulfils the recommendations: opens access to the CMD through the reverse shell. The user of the computer WS 3 is the network administrator and personal 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 ransomware (win32.exe file) that requires a ransom.

Annex No. 4 - Storyline A1 – bruteforce attack

Date	Time	SL	Type	Action line variation	Who is responsible	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.		
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 their access profile (username/password) and views the file uploaded by the "service provider" (attachment No.1 .xslm) 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 the file synchronization (FS) of which 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.		



Date	Time	SL	Type	Action line variation	Who is responsible	From	To	Description	External file	Comment
10/20/2020	8:10	A1	Plugin		State Infrastructure	WS1 User	IT (security) department	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. The user informs the IT (security) department about the received e-mail.	email1.0-WS1darbuotojas-ltsauga.txt	
10/20/2020	9:20	A1	Response			IT (security) department	IT administrator	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 Representative	Information on the situation and planned actions		
10/20/2020	9:41	A1	Response			Security Representative		Evaluation: risk, damage		
10/20/2020	11:00	A1	Response			IT administrator	IT (security) department	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		



Date	Time	SL	Type	Action line variation	Who is responsible	From	To	Description	External file	Comment
10/20/2020	13:00	A1	Plugin	Option 2.0.1	State Infrastructure	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 Infrastructure	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 Infrastructure	Hosting provider	IT	No data provided. There are no opportunities.	email2.0.3-hosting-provider--it--(hosting-apsvarsteneduos).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	Additional plugin	Option 3.1	State Infrastructure	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,		



Date	Time	SL	Type	Action line variation	Who is responsible	From	To	Description	External file	Comment
								Win32.exe distributed through workstations.		
10/20/2020	15:50	A1	Response	Option 3.1		Security Representative	Institutions	Inform on the incident		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	Management	Periodic information on the situation		
10/21/2020	9:00	A1	Response			IT (security) department	Security Representative	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	Management, Security Representative, Employees	Information on the incident 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 notification is necessary, the relevant authorities shall be informed of the decision



Date	Time	SL	Type	Action line variation	Who is responsible	From	To	Description	External file	Comment
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	Additional plugin	Option 6.0	State Infrastructure	Journalist	Public relations or Security Representative 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 a request for comment is added.	email4.0-zurnalistas--viesieji-rysiat.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 Representative, Director	A comment is required		
10/20/2020	13:00	A1	Response			Public relations	Journalist	Answer / Press release.		

Annex No. 5 - The infrastructure of an attack model of a typical organization and its functions

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 the 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 the 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.



Date	Time	SL	Type	Action line variation	Who is responsible	From	To	Description	External file	Comment
10/22/2020	8:00	A2	Response	Option 1.1		WS2 user	IT administrator	When an employee comes to the workplace, turns the WS on and understands from the image on the screen that the WS is encrypted. Employee 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 Representative		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 administrator	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				



Date	Time	SL	Type	Action line variation	Who is responsible	From	To	Description	External file	Comment
						to restore the workplace				
10/22/2020	11:30	A2		Option 1.1		Director	Security Representative	Colleagues mentioned the problems, what happened? What computers, what information was on them?		
10/22/2020	11:40	A2				Security Representative	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 Representative	Director	Initial assessment		
10/22/2020	13:00	A2		Option 1.2		Media	Manager / Public relations professional	The company's customers cannot 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 Representative	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 Representative;	Public relations specialist	Submission of information		



Date	Time	SL	Type	Action line variation	Who is responsible	From	To	Description	External file	Comment
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 Representative	Institutions	Reporting about the incident.		
10/22/2020	16:30	A2		Option 2.2		Security Representative	Institutions	Do not inform on the incident. Does not meet the requirements.		
10/22/2020		A2		Option 3.1.		IT (security) department, Security Representative, 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	Management, Security Representative, Employees	Information on the forensics of incident.		



Date	Time	SL	Type	Action line variation	Who is responsible	From	To	Description	External file	Comment
10/23/2020	9:00	A2		Option 4.1.		Security Representative	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 Representative	NKSC, VDAI, Police	Do not inform on the incident. Does not meet the requirements.		
10/23/2020	10:00	A2				Security Representative	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 Representative	Local instructor	Do not make the incident public.		
10/23/2020	11:00	A2				Journalist	Public relations or Security Representative 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 a request for comment is added.		
10/23/2020	11:00	A2				Public relations	Security Representative, Director	A comment is required		
10/23/2020	13:00	A2				Public relations	Journalist	Answer / Press release.		

Annex No. 6 - Storyline A3 – exploiting WP vulnerability

Date	Time	SL	Type	Action line variation	Who is responsible	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. The 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.		



D9.4 – Pilot of Cyber training & exercise Framework (Ct&eF)

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 a keylogger.		
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 Infrastructure	Website administrator	Security Representative	Question about a new CMS user Insider found.	email1.0-web-admin--saugos-galiotinis	
10/22/2020	9:20		Response			Security Representative	IT (security) department	Conduct forensics of WWW2.		
10/22/2020	9:30		Response			IT (security) department	Website administrator / IT Administration Dept.	Request to provide WWW2 image, logs, network traffic images.		
10/22/2020	10:00		Response			Website administrator / IT Administration 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 Representative	IT (security) department	What are the preliminary results of forensics?		



D9.4 – Pilot of Cyber training & exercise Framework (Ct&eF)

10/22/2020	13:00		Response			Security Representative	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 Infrastructure	Director	TD, Security Representative	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 Representative	IT (security) department	What are the preliminary results of forensics?		
10/22/2020	16:00		Response			Security Representative	NKSC, VDAI	Reporting about a cyber incident and leakage of personal data.		

Annex No. 7 - Storyline B1 – distant workplace attack

Date	Time	SL	Type	Action line variation	Who is responsible	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 not powerful enough for games. The child then gets advice to look for information regarding 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 a keylogger.		
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		



Date	Time	SL	Type	Action line variation	Who is responsible	From	To	Description	External file	Comment
								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 Representative	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-igalioinis	
									sarasas.txt	
10/21/2020	9:10	B1	Response			Security Representative	IT (security) department	Procedure to conduct forensics.		
10/21/2020	9:20	B1	Response			IT (security) department	IT Administration Dept	Request for AD image, network traffic image.		
10/21/2020	9:30	B1	Response			IT Administration Dept.	IT (security) department	IT administrators provide the requested data.		
10/21/2020	10:00	B1	Response		VI	IT (security) department		Forensics is launched		
10/21/2020	12:00	B1	Response			Security Representative	NKSC, VDAI	Information on the cyber incident forensics and leakage of personal data.		



Date	Time	SL	Type	Action line variation	Who is responsible	From	To	Description	External file	Comment
10/21/2020	13:00	B1	Response			Director	Security Representative	What are the preliminary results of forensics?		
10/21/2020	15:00	B1	Response		VI	Media	Public relations or Security Representative 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 a request for comment is added	email3.1-zurnalistas--Director.txt sarasas_pastebin.png	
10/21/2020	16:00	B1	Response			Public relations	Security Representative	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. 8 - Trainers Manual. Description of the Attacks

WWW1 (Windows)

Question	Answer	Hints	How answer should be found
<p>How was the site taken over?</p> <p>When was this done?</p> <p>Which CMS plugin was vulnerable?</p>	<p>An SQL injection-type attack was performed to exploit a vulnerability in the WordPress (WP) plugin.</p> <p>2020-10-19 12:21</p> <p>An outdated version of the WP plugin has been used Wp-FileManager 1.2, WordPress <= 1.5.1.1.</p>	<ol style="list-style-type: none"> 1. Run WWW1 VM in a 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. 	<p>C:\xampp\htdocs\wp\wp-content\plugins\wp-filemanager.php</p> <p>C:\xampp\htdocs\wp\wp-includes\version.php</p> <p>Export Apache.log: error.log, access.log.</p> <p>C:\xampp\apache\logs\access.log</p> <p>42.83.90.245 - [19/Oct/2020:12:21:13 +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"</p> <p>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"</p>
<p>What malicious request was sent?</p>	<p>/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</p> <p>2020-10-19 12:58</p>	<ol style="list-style-type: none"> 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. 	<p>C:\xampp\apache\logs\access.log</p> <p>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"</p> <p>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"</p>



Question	Answer	Hints	How answer should be found
<p>When was it sent?</p> <p>From what IP address was this done?</p> <p>What was its purpose?</p>	<p>42.83.90.245</p> <p>To extract the username (itadmin) and password from the wp-admin.php file.</p>	<p>3. View network traffic copy (pcap), HTTP.</p>	
<p>What CVE has been exploited?</p>	<p>EDB-ID:1033 CVE: 2008-0222</p>	<p>After determining the version of the plugin, search the CVE and EDB vulnerability databases</p>	<p>https://www.exploit-db.com/exploits/1033 https://www.exploit-db.com/exploits/4844</p>
<p>What actions were taken by the villain who connected to the CMS</p> <p>When were these actions performed?</p>	<p>Uploaded the win32.exe file to the directory C:\xampp\htdocs\wp\files\ 2020-10-19 12.58</p>	<p>1. Run the WWW1 VM in a virtual environment, view WWW1 Apache / CMS log entries.</p> <p>2. View the separate WWW1 Apache log entry file Access.log with a text editor.</p> <p>3. View network traffic copy (pcap), HTTP.</p>	<p>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"</p>
<p>How did the file spread after the organization's workstations?</p>	<p>Directory C:\xampp\htdocs\wp\files\ Is synchronized by the file server with the workstations. Users receive notifications about a file shared with them.</p>		<p>Where to find FS communications with WS? Pcap, search command → ip.addr == 83.171.43.82</p> <p>Or on the fileshare(fs) machine go to the directory /var/www/html/nextcloud/data</p>



Question	Answer	Hints	How answer should be found
			image name: fs_organizacija_ks2020_It
What IP addresses possibly have downloaded malicious code from the website WWW1?	20 external IP addresses (these are fake IP's)? 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 an "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"

Annex No. 9 - Installation and Troubleshooting of KYPO

KYPO CRP is built on the OpenStack platform. If there is no OpenStack deployed, please see **9.3. OpenStack installation guide for KYPO** below.

9.1. Installation

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, a login to the Horizon OpenStack service is required. 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 13.

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

Table 13: 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, one first needs to create this virtual machine. Before creating a virtual machine, the user needs to create a flavour for that virtual machine:

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

After creating the flavor, it is still needed to upload the necessary image. One can check the available images with the command:

```
root@controller#~: openstack image list
```

If there is no image named „ubuntu-focal-x86_64“, it needs to be created 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, machine can be created:



Horizon -> Project -> Instances -> Create New Instance. Only a 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 the private and public key. To get to the instance:

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

It will automatically connect 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 a 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 the 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, vagrant can be used to build the create a virtual machine with KYPO:

```
root@kypo #~: vagrant box update
```

```
root@kypo #~: EXTRA_VARS=./local-demo-extra-vars.yml,./local-demo-secrets.yml vagrant up
```

9.2. 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 that were 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 configuration 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 the successful change from NoVNC to SPICE cannot connect to any console

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

Solution:



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

9.3. OpenStack installation guide 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 set up it manually afterwards.
- 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 the partition home directory and assign the free space to the root partition (/)

After fresh install it is recommended to do:

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

Now it is necessary 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 the controller, python and pip have to be installed:

```
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 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 inventory 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 have to be defined. Check the network interfaces with the 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 it is 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 configured in the 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

For OpenStack customization, 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
```

The 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 the row with parameter:

```
physical_interface_mappings
```

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

```
[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 an external network configuration:

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

Now first network in OpenStack can be created:

```
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 (Table 14). 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
```

Table 14: Flavors and images to run KYPO CPR

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



Flavor	vCPU	RAM (GB)	Disk size (GB)
csirtmu.large8x16	8	16	80
csirtmu.large8x32	8	32	80
csirtmu.jumbo16x32	16	32	100
csirtmu.jumbo16x64	16	64	100

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

```
root@controller #~: openstack flavor list
```

If there are two or more flavors with the same name, one of them has to be deleted. If two or more flavors of the same name are left, OpenStack may not know which flavor to choose and creating an instance may fail.

For deleting instance use the 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
```

Annex No. 10 - Installation of the toolkit to measure IT-Security Awareness

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.

10.1. 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 15 depicts the artifactomat's system requirements of the artifactomat 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 15: System requirements of the server

Minimal	Recommended
4 CPU cores with \geq 2GHz frequency	8 CPU cores with \geq 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 16. Application of a software distribution solution is *strongly recommended* because the client component needs to be installed on every participant's computer. Participants need to use personalized accounts to log in to their working station. Generic or group accounts are not supported.

Table 16: System requirements of the clients

Minimal	Recommended
2 CPU cores with \geq 2GHz frequency	4 CPU cores with \geq 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 consent 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 consent may be given by the proxy of a working council. However, national law applies.

Clients

The client is provided as a Windows Installer package (.msi)¹⁵. It needs to be installed on all workstations targeted. Installation by software distribution solution is 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 script¹⁶ 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-`

¹⁵ <https://gitlab.com/itsape/windows-client>

¹⁶ <https://gitlab.com/itsape/platform/-/blob/a237d513/vm-provisioning-main.sh>



```
$(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 from the 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 module¹⁷ run:
 5. `sudo pip install awarenssometer`
6. To install the `artifactomat`¹⁸, 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 from a baseline, it is recommended to choose a fraction of well-known artifacts (c.f. [21]). Building custom recipes tailored to the environment is a service offered by UBO.

¹⁷ <https://gitlab.com/itsape/awarenessometer>

¹⁸ <https://gitlab.com/itsape/artifactomat>