

THE NEED OF ETHICAL HACKING INTEGRATION IN ALBANIA

A THESIS SUBMITTED TO
THE FACULTY OF ARCHITECTURE AND ENGINEERING
OF
EPOKA UNIVERSITY

BY

GRIDI CAMI

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
ELECTRONICS AND DIGITAL COMMUNICATION

MARCH 2024

Approval sheet of the Thesis

This is to certify that we have read this thesis entitled “**The need of Ethical Hacking Integration in Albania**” and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Assoc. Prof. Dr. Arban Uka
Head of Department
Date: 01/03/2024

Examining Committee Members:

Assoc. Prof. Dr. Dimitrios A. Karras

Prof. Dr. Betim Çiço

Assoc. Prof. Dr. Arban Uka

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name Surname: Gridi Cami

Signature: _____

ABSTRACT

The Need of Ethical Hacking Integration in Albania

Cami, Gridi

M.Sc., Department of Computer Engineering

Supervisor: Assoc. Prof. Dr. Dimitrios A. Karras

Network security is a rapidly growing industry which is related to the rapid growth of the technology. This paper is going to cover aspects and the need of ethical hacking integration within the network security industry in Albania. Methodology will be presented in order to give details on the methods and tools used throughout this paper, such as: KaliLinux, OpenVAS scanner, Social Engineering Tools. Key aspects, related to the impact, integrity and benefits of ethical hacking will be discussed. Furthermore the paper will discuss the impact of cyberthreat in Albania. Key simulation of ethical hacking cyberattacks are going to be demonstrated, which will include a bruteforce and a phishing attack. Albanian institutions domains vulnerability scan are going to be compared to a well-established institution in the world. Lastly there will be a overview of the conclusions.

Keywords: *ethical hacking, tools, cyberattack, KaliLinux, network security*

ABSTRAKT

Nevoja per Integrimin e Hakerimit Etik ne Shqiperi

Cami, Gridi

Master Shkencor., Departamenti i Inchinierise Kompjuterike

Udhëheqësi: Assoc. Prof. Dr. Dimitrios A. Karras

Sigurimi i rrjetit është një industri në rritje të vazhdueshme, gjë e cila është gjithashtu e lidhur drejtpërdrejt me zhvillimin e dixhitalizimit të teknologjisë. Kjo tezë do të mbulojë aspektet kryesore dhe nevojën për integrimin e hackerimit etik në industrinë e sigurimit të rrjetit në Shqipëri. Metodologjia do të prezantojë metodat dhe paisjet e përdorura në këtë tezë, sic janë: Kali Linux, skaneri OpenVAS, Social Engineering Tools. Gjithashtu do të diskutohen aspektet kryesore të lidhura me impaktin, integritetin dhe përfitimet në lidhje me hackerimin etik. Do të parashtrohet situata në Shqipëri dhe impakti i kërcenimit kibernetikë në këtë shtet. Do të kryhen skanimeve vulnerabiliteti dhe simulime kyce të hackerimit etik, të cilat lidhen me metodat e sulmeve kibernetike të përdorura nga hakerat. Skanime të vulnerabiliteteve të institucioneve Shqipëtare do të krahasohen me një institucion të huaj. Në përfundim do të prezantohet një përmbledhje dhe konkluzionet.

Fjalët Kycë: hackerimi etik, paisje, kibernetik, KaliLinux, vulnerabilitet, skanim

Table of Contents

ABSTRACT.....	iii
ABSTRAKT.....	iv
LIST OF TABLES	vii
LIST OF FIGURES	viii
CHAPTER 1	1
INTRODUCTION	1
CHAPTER 2	3
LITERATURE REVIEW.....	3
2.1 Introduction	3
2.2 Ethical Hacking	4
2.3 Ethical Hacking Methodologies	5
CHAPTER 3	7
METHODOLOGY.....	7
CHAPTER 4	9
Exploring Attributes of Ethical Hacking.....	9
4.1 Impact of Ethical Hacking Education on Specialists	9
4.2 Benefits and Real-World Applications.....	12
4.3 Maintaining Integrity in Ethical Hacking.....	16
4.4 Legal Aspects	18
4.5 Analysis of Cyber Attack	20
Chapter 5	24

Network Security in Albania.....	24
5.1 Cybert-attacks on Albania	24
5.2 Albanian Hackers	26
Chapter 6	29
Simulation and Results.....	29
6.1 Vulnerability scan.....	29
6.2 Bruteforce Simulation	33
6.3 Phishing Attack Simulation.....	36
6.4 Vulnerability Comparisons.....	40
Chapter 7	46
Conclusion	46

LIST OF TABLES

Table 1. Theoretical knowledge and abilities of ethical hacking.....	9
Table 2. Ethical Hacking Areas of Learning.....	11
Table 3. Component of a ethical hacking report.....	18
Table 4. Legal Aspect Considerations	19
Table 5. Cyber attacks statistics	22
Table 6. Vulnerability scanners groups.....	29
Table 7 Vulnerability reports comparison	45

LIST OF FIGURES

Figure 1. Nslookup command on a public domain	30
Figure 2 Vulnerability report of a public domain	31
Figure 3 Summary of a high threat-vulnerability.....	31
Figure 4. Details of a high-threat vulnerability	32
Figure 5. Solution to a high-threat vulnerability	32
Figure 6. Metasploitable2 IP information	33
Figure 7. DVWA Vulnerable Web App.....	33
Figure 8. Test log-in page	34
Figure 9. Burpsuite interception.....	34
Figure 10. Targeting the password on Burpsuite	35
Figure 11. Payload settings list in Burpsuite.....	35
Figure 12. Log-in tab in Burpsuite.....	36
Figure 13. SET attack vectors	37
Figure 14. Web attack methods in SET	37
Figure 15. Website clone methods	38
Figure 16. IP address set	38
Figure 17. Templates for website cloning.....	38
Figure 18. Start of phishing attack	39

Figure 19. Cloned site for phishing attack 39

Figure 20. Results of phishing attack 40

Figure 21 Albanian institution vulnerability report 41

Figure 22 Albanian institution high severity vulnerability 41

Figure 23 Montenegro institution vulnerability report 42

Figure 24 Montenegro institution high severity vulnerability 42

Figure 25 Kosovo institution vulnerability report..... 43

Figure 26 North Macedonian institution vulnerability report 43

Figure 27 Romanian institution vulnerability report..... 43

Figure 28 Italian institution vulnerability report 44

Figure 29 Italian institution medium severity vulnerability 44

Figure 30 USA institution vulnerability report 45

CHAPTER 1

INTRODUCTION

As the world becomes more digitalized, there has been a growing need in network security sector. General population tend to store all their information, such as their credentials or even their credi cards information, in various platforms. Intruders make use of these situation and have developed tools and methods to gain unauthorized access to valuable information which can vary from a social media account or even gaining access to a bank account.

The information that is gained by the intruders can pose serious threats to the victim, therefore there has been developed a need for network security protection. Eventho there have been developed various systems with the intention to prevent cyber-attacks from happening, intruders have constantly found methods to crack the systems and break them. Therefore, it has been developed the need of training the specialists in ethical hacking, in order for them to get an overview on how the intruders act and think.

This thesis objective is to demonstrate the benefits of ethical hacking integration in network security. There will be introduced methods and tools that intruders use to gain access to their victim hardware or software. These methods will assist with gaining a broader knowledge on how the intruders act, which will assist to develop the skills needed to mitigate cyber threats in the future.

To demonstrate the practical skills of an ethical hacker three simulations are performed. These simulations are identical with the methods used by real hackers to gain unauthorized access to various system and data. The purpose of these simulation is to familiarize the specialist with penetration testing and vulnerability scans. A simulation was performed using an open-source tool on an IP, which was gained through command prompt nslookup command. This tool demonstrates how to gain information on the vulnerabilities of a web page, which can lead to harmful exposure. Making use of these tools, a specialist in the area of ethical hacking is able to detect

all the vulnerabilities that may be exploited by the intruders and therefore they can work on minimizing the exposure or the kind of threat.

Bruteforce and Phishing ethical attacks are going to demonstrate how these cyber-attacks are performed. In addition, these simulations help the user to gain a better knowledge on the methods used by intruders and therefore better security systems can be developed in order to mitigate these kind of threats.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Network security became a topic when people started to realize that the data stored held important values. As the information, which was stored, was rapidly growing and at the same time becoming more valuable, it brought the risk of sensitive information being stolen. The first type of the earliest cyber attacks was recorded in France in 1834, when attackers stole information related to financial market from French telegraph system. [1]. Later on, with the introduction and mass adoption of the internet as well as the digitalization of the data stored, cybercrime gain a significant increase. They made use of their early adaption of technology, to create and execute methods that would grant them unauthorized access to various systems thus enabling them to steal sensitive information.

One of the earliest modern cyber attacks which was documented, is said to be performed against MIT computer network in 1962. [2]. The attack managed to type up all tie-lines between Harvard and MIT. During the early 1970s, in order to store the data, companies used large mainframes that were accessed by either plugging directly into it or from one of the terminals within the building of the company. As time passed, the companies started noticing that the data they stored held important value and information of different aspects such as personal details, credit card data, demographic information etc. It was during this time that information started being treated as commodity.. In 1971, the first computer virus named Creeper was developed by Bob Thomas. [3]. This virus, which was detected on ARPANET was the beginning of future viruses created with the intent of inflicting harm to steal information from various systems. Cyber criminals managed to continuously develop their viruses. The first cyber worm dates on 1988, when a malicious program was spread through the internet from a MIT computer that was created from a 23-year-old Robert Morris. [4].

Due to its nature of featuring multiple vectors of attack, the Morris Worm managed to spread widely. This cyber worm was responsible of affecting 6,000 computers. Harvard, John Hopkins, NASA were some of the institutions affected from this attack. Eventho this attack did not compromise any file, it still managed to slow the functions of these institutions. The damages were estimated to be in millions.

During the 1990s, attackers began targeting different sectors of the industry. One of the most notable case is that of Vladimir Levin in 1995. Levin penetrated into Citibank network and transferred more than 10 million USD in different bank accounts across the world. [5]. As cyber attacks became more efficient and sophisticated, they started causing significant damage to various areas of economy. Due to the rising threat, cybersecurity became a main concern especially for governments which were constantly targeted and suffered immense financial losses. To prevent cyber threats and minimize their exposure, companies began hiring skilled specialists, who were able to secure the systems. Ethical hacking field emerged with the purpose of training specialists by using the same methods a hacker employes.

2.2 Ethical Hacking

Ethical hacking is considered one of the key skills in network security industry. It is the process of learning how to perform penetration tests and vulnerability scans while maintain ethical integrity. [6] The main reason on why this is considered as a key skill, is due to the fact that it's specialists are familiar with the methods that most hackers employ and thus are capable of intervening with malicious cyber attacks. To distinguish ethical hacking specialists, various certifications are awarded, such as EC-Council certifications [7]. In order to gain these certifications, the specialist needs to demonstrate the needed knowledge to evaluate a system's security by performing various vulnerability test, while maintaining the legal integrity aspect.

Depending on the specific testing objectives and environments of the specialist, ethical hacking can be divided into three different types. White-box, Black-box and Gray-box. Upon the information that the specialist poseses on the system, these types are respectively divided as below:

1. White-Box testing

White-Box testing is referred when the specialist has detailed information about the target system. [8]

2. Black-Box testing

Black-Box testing is referred when the specialist has no prior information about the target system. [9]

3. Gray-Box testing

Gray-Box testing is a combination of both white-box and black-box. [10]

2.3 Ethical Hacking Methodologies

Ethical hacking field has witness rapid deveolpment through the recent years when it comes to it's methodologies. In order to obtain and identify various vulnerabilites, penetration testing is performed by ethical attacks. Penetration testing are considered as the main element of ethical hacking. Their objective is to train the user with real-world attacks that are performed by the intruders, and their purpose is for the users to gain experience on the steps taken throughout these attacks in order to know how they are initiated, which prepares the user to come up with solutions on how to mitiage them.

Different open-source and paid software are used to create virtual machines, which are typically set as targets for testing as they imitate real computer systems. The specialist trains their vulnerability and penetration testing skills using various tools. Since the virtual machine simulate computer systems, it means that the testing

performed on these machines have the same effects on real computer systems. By performing these tests, the specialist is equipped with similar skills as real hackers and is able to identify vulnerabilities within various systems, which can assist with important information on how to upgrade a system in order to prevent future attacks from unwanted parties.

Virtual machines [11] are one of the key tools used by ethical hackers. These are virtualizations of a system that is based on computer architecture with the objective of acting similar to a computer. There are two types of virtual machines:

1. System Virtual Machines [12]
2. Process Virtual Machines [13]

When it comes to Linux, Kali Linux is a popular tool which is used commonly from both hackers and professionals of network security with the intention of performing penetration testing. It was developed by Offensive Security, which is a training company specialized in courses related to ethical hacking. This tool acts as a System Virtual Machine which is easily attainable by anyone. It is specially designed in order to perform penetration tests and thus is equipped with various tools and utilities that can be used for different testing techniques. [14] Apart from the 600 tools which are already installed in this machine, the user can also install other penetrating tools by manually downloading and setting them up through its terminal. Since it has a variety of tools and has demonstrated to achieve high results, Kali Linux is the main choice when it comes to learning ethical hacking.

Vulnerability Scanners such as Nessus [15] or OpenVAS [16], are capable of assessing for known weaknesses on various systems. These scanners are often used before initiating an attack in order to assess the weakest points of a system. They are among the key tools used in ethical hacking and in network security which assist to gather information. In addition, vulnerability scanners are known for their capability of producing real time solution for each weakness of the system.

Metasploitable was developed by Metasploit Project and is specifically designed vulnerable virtual machine which is usually used in order to perform penetration testing techniques. It is commonly used as a target machine from ethical hacker with the intention of practicing and further developing their skills.

CHAPTER 3

METHODOLOGY

The paper will firstly consist of a chapter discussing on the impact of ethical hacking integration within network security. It will discuss various points related to :

- Integration
- Impact
- Integrity importance
- Legal aspects

Current state of network security and cyber threats in Albania are going to be presented. The difficulties during the recent years as this country has been constantly targeted from various attacks leading to sensitive data being leaked online.

Lastly, a vulnerability assesment and two simulations of cyber attacks will be presented, which will be relavent to methods used to teach ethical hacking. The vulnerability scan is performed on an IP that is obtained from a nslookup command in command prompt. After gaining the IP, Greenbone Enterprise Trial software is used to perform a vulnerability scan. At the moment that the scan is finished, the user is going to be presented with a report that will contain all the vulnerabilities found. These vulnerabilites are listed and separated in different categories related to their threat. Vulnerability scanners are key tools used in network security in order to achieve information on the threats.

Two cyber attacks are going to be simulated within the Kali Linux machine. One of the attacks is going to be a bruteforce [17]. This will be completed with the assist of burpsuite and a virtual machine metasploitable2, which is going to be the targeted machine. The attack will consist of a list of usernames and passwords which is going to try all the possible combinations in order to succeed.

The second attack is going to be a phishing attack [18], which will be done by making use of a social engineering attack tool withing Kali Linux. A web log-in page

will be cloned that will be followed with a phishing email to the target. At the moment that the target enters their credentials in the cloned page, the intruder gets the data in their terminal and thus is able to gain access to the victim account.

These two attacks aim to demonstrate the methods used by the intruders and the steps that they take. By learning the attacks, a specialist will be able to learn how to distinguish and mitigate the threat.

CHAPTER 4

Exploring Attributes of Ethical Hacking

4.1 Impact of Ethical Hacking Education on Specialists

The core of ethical hacking education is theoretical knowledge and competence acquisition. This aspect of education provides professionals with a thorough understanding of cyber security principles, network designs, and potential vulnerabilities. Theoretical training not only imparts knowledge but also prepares professionals for real-world application. Theoretical knowledge and abilities which are considered essential for a professional of this field. They include a comprehensive understanding of various aspects such as the understanding of cyber security principles, network and system architecture knowledge, learning about vulnerabilities and exploits, legal aspects and developing a security centric mindset. Each of these aspects plays a crucial role in the education of a specialists.

Table 1. Theoretical knowledge and abilities of ethical hacking

Understanding Cyber security Principles	A good understanding of cyber security principles is critical to ethical hacking education. This includes learning about many cyber risks, attack vectors, and network and system security concepts.
Network and System Architecture Knowledge	Ethical hacking necessitates a thorough knowledge of network and system infrastructures. Professionals are educated on the complexities of network architecture, including protocols, ports, and services. This knowledge is essential for discovering vulnerabilities and securing network infrastructures.

<p>Learning About Vulnerabilities and Exploits</p>	<p>Understanding vulnerabilities and exploits takes up a substantial portion of ethical hacking education. This includes understanding typical flaws such as buffer overflows, SQL injection, and cross-site scripting. Training programs frequently contain databases such as the Common Vulnerabilities and Exposures (CVE) list to familiarise professionals with known vulnerabilities. In their Guidelines on Network Security Testing (2022), National Institute of Standards and Technology (NIST) emphasizes the relevance of this expertise.</p>
<p>Legal and Ethical Aspects of Hacking</p>	<p>Understanding the legal and ethical boundaries is critical to ethical hacking education. Cyber security laws like the US Computer Fraud and Abuse Act (CFAA) and ethical standards are taught to professionals.</p>
<p>Developing a Security-Centric Mind-set</p>	<p>Theoretical training in ethical hacking also includes the development of a security-focused attitude. This attitude is concerned with predicting potential security issues and taking a proactive approach.</p>

Similar to theoretical knowledge, the development of practical skills in ethical hacking is highly important. This practical training program provides cyber security experts with the knowledge and skills to authentically recognize, assess, and mitigate cyber hazards. Main skills which are taught to ethical hacking professionals include:

- Proficiency in penetration testing
- Vulnerability assessment
- Expertise in various cyber security tools and technologies
- Enhancement skills related to problem-solving, critical thinking and effective communication
- Real world simulations and security drills

Security experts, who are trained with these skill sets are able to perform various test in order to discover vulnerabilities within the system. Penetration testing

are used to simulate cyber-attacks on systems, which familiarizes the professional with the methods used by hackers. Vulnerability assessments are performed with various open-source tools to gather data upon possible vulnerabilities of a system. Additionally, professionals are familiarized with various tools and are trained to other skill sets related to incident response and management.

Ongoing education is essential for the development and maintenance of ethical hacking expertise. This entails maintaining current knowledge regarding emergent threats and hacking techniques.

Table 2. Ethical Hacking Areas of Learning

Area of Learning	Description	Importance
New Vulnerabilities and Threats	Keeping update on emerging threats and vulnerabilities	Enables ethical hackers to anticipate and counter new types of cyber-attacks.
Advanced Hacking Techniques	Learning sophisticated hacking techniques and tools	Enhances the ability to identify and exploit complex vulnerabilities.
Cyber security Legislation	Understanding changes in cyber security laws and regulations.	Ensures legal compliance in ethical hacking practices.
Soft Skills Development	Improving communication, problem-solving, and analytical skills.	Facilitates better collaboration and effective reporting of findings.

Obtaining proficiency in ethical hacking substantially augments the prospects for career progression and market appeal for individuals working in the field of cyber security. With the growing awareness among organizations regarding the critical nature of strong cyber security measures, there has been an extraordinary surge in the need for proficient ethical hackers.

Ethical hackers exhibit a distinct advantage in sectors such as finance, healthcare, and government, where data security is of the utmost importance due to

their expertise in locating and addressing vulnerabilities. Compared to their non-certified counterparts, certified ethical hackers frequently command higher salaries and enjoy a greater variety of career opportunities. The certification, which is evidence of their expertise and understanding, enhances their prominence in employment and frequently results in promotions to higher-level, more influential positions within organizations.

Moreover, the ongoing progression of cyber hazards guarantees a sustained demand for the expertise of ethical hackers. Organizations have a significant demand for experts capable of proactively identifying and preparing for forthcoming challenges and addressing present threats. Ethical hackers have opportunities for ongoing skill development, career advancement, and learning in this ever-changing environment.

4.2 Benefits and Real-World Applications

A critical practice in cyber security, ethical hacking provides organizations with numerous benefits by simulating cyber-attacks to identify vulnerabilities. Implementing a proactive approach is crucial in a dynamic cyber threat environment.

- **Proactive Identification and Mitigation of Vulnerabilities:** Early detection of security vulnerabilities is one of the principal benefits associated with ethical hacking. Ethical hackers reveal potential entry points for cybercriminals through the simulation of assaults; this enables organizations to patch these vulnerabilities before their exploitation. According to a study published by the SANS Institute in 2020, businesses that consistently implement ethical hacking practices decrease their susceptibility to cyber-attacks by around 40%. [19]
- **Compliance and Avoidance of Penalties:** Adherence and Prevention of Penalties Data protection and privacy are subject to rigorous regulatory standards

across numerous industries. A business can comply with HIPAA in the US or GDPR in the EU with ethical hacking. Due to the severe penalties and legal consequences associated with noncompliance, ethical hacking is a crucial instrument for ensuring compliance. According to the Information Commissioner's Office (ICO) in 2021, instances of data intrusions that result in penalties are frequently attributable to the absence of proactive security measures, such as ethical hacking. [20]

- **Enhancing Cyber Defense Mechanisms: Strengthening Cyber Defense Systems Significantly,** ethical hacking contributes to improving an organization's cyber defense mechanisms. Organizations can optimize the resilience and flexibility of their security strategies by gaining insight into the operational methods of malicious actors. Kaspersky Lab (2019) [21] finds that organizations that consistently implement ethical hacking practices exhibit significantly enhanced resilience in the face of intricate cyber-attacks.

- **Building Consumer Trust and Brand Reputation: Establishing Brand Reputation and Consumer Trust** In a time when data intrusions can significantly harm an organization's reputation, ethical hacking is crucial to establishing consumer confidence. Customers frequently hold a more positive perception of businesses that are dedicated to cyber security via methods such as ethical hacking, and according to a report by Deloitte (2018) [22], organizations that placed a high value on cyber security measures, such as ethical hacking, observed improvements in consumer retention and brand reputation.

- **Cost Savings in the Long Run:** Ethical hacking requires an initial financial investment; however, it can yield significant long-term cost savings by preventing costly intrusions. A significant data intrusion can incur substantial expenses, such as legal fees, compensation, and business downtime, significantly surpass the cost of preventative measures like ethical hacking.

- **Enhanced Knowledge and Skill Development:** Development of Enhanced Knowledge and Skills Additionally, ethical hacking benefits the professional growth of IT personnel. It gives individuals the necessary understanding and abilities to anticipate, identify, and react proficiently to cyber

threats. In the contemporary workplace, this skill set is for cyber security specialists and all IT professionals.

The numerous advantages of ethical hacking include compliance and vulnerability assessment, as well as the improvement of cyber defence and the establishment of consumer confidence. It is impossible to overstate the significance of this procedure in preserving robust cyber security, as it remains a vital component in the fight against cybercrime. Ethical hackers assist organizations in identifying and fixing weaknesses by mimicking cyber-attacks and strengthening their defense against actual threats. Some of the sectors where ethical hackers are hired to perform such evaluations are:

1. **Financial Sector:** Due to the amount of financial data being available, the financial sector continues to be a top target for hackers. In order to store and protect their data, companies in this sector such as bank or insurance companies, hire ethical hackers in order to protect their database. They conduct vulnerability analyses and penetration testing to guard against financial fraud, identity theft, and data breaches. According to a report made by J.P Morgan Chase, ethical hacking has been a key factor in reducing the incidents related to cyber security in banking industry by 25%.

2. **Healthcare Industry:** Healthcare industry has always been a primary target because their database contains sensitive patient data. In this industry, ethical hacking main objective is safeguarding patient data and ensuring law protocols such as HIPAA are followed. By implementing an ethical hacking program, In 2020, The Mayo Clinic performed an ethical hacking program. The clinic managed to discover significant vulnerabilities within their system, an information which lead to them strengthening the security of patient data.

3. **Retail and E-Commerce:** As e-commerce establishes and becomes more popular, it also becomes a target of various attacks. Ethical hackers examine e-commerce systems for weaknesses such as cross-site scripting, SQL injection, and other potential attack points. Research done by Amazon and published in 2022, stated that ethical hacking was used to find flaws within the system which helped to fix and safeguard consumer information, as well as transaction security [23].

4. Government and Public Sector: Governmental organizations are sought-after targets for cyber terrorism and espionage because they hold vast amounts of sensitive data. Ethical hackers strive to safeguard vital infrastructure, citizen data, and national security in the public sector. Ethical hackers were hired by the US Department of Homeland Security to find weaknesses in their systems, greatly strengthening their security posture. [24]

5. Telecommunications: To prevent interruptions and system breaches, telecommunications companies hire ethical hackers since they oversee vital infrastructure for data transit and communication. In its 2020 Data Breach Investigations Report, Verizon emphasized how successful ethical hacking is in thwarting extensive DDoS assaults.

6. Cloud Computing and Data Centers: Modern businesses tend to adopt cloud based solutions. Due to this fact, cloud computing security have grown critical. Ethical hackers perform evaluation of various data encryption techniques, access limits, and cloud security setups. To guarantee the security and integrity of its cloud services, Google Cloud's security team (2018) periodically carries out ethical hacking exercises.

7. Education Sector: Research data, student information, and intellectual property are increasingly targeted at educational institutions. The Family Educational Rights and Privacy Act [25] and other privacy requirements are complied with by educational institutions with the aid of ethical hackers.

8. Automotive Industry: Because they depend increasingly on digital technology, modern cars could be targets for hackers. Infotainment systems, autonomous driving features, and car communication systems are the main targets of ethical hacking in the automotive industry. According to a Tesla report from 2023 [26], ethical hacking improved passenger safety by assisting in the discovery and repair of software vulnerabilities in automobiles.

The wide range of real-world online cyber threats illustrates how important it is to safeguard various industries with the assist of ethical hacking skill set.

4.3 Maintaining Integrity in Ethical Hacking

The ethical framework governing ethical hacking is founded upon the fundamental principle of "not harm" when performing penetration tests and security assessments. The International Council of E-Commerce Consultants (EC-Council) underscores this principle in its Certified Ethical Hacker (CEH) program. According to this program, ethical hackers must solely utilize their expertise for lawful and beneficial intentions. This dedication entails the observance of privacy principles, safeguarding of data, and prevention of detrimental testing techniques. To maintain integrity, a specialist needs to respect the following fields:

- **Permission and Authorization** - Obtaining explicit permission and authorization before testing is a fundamental aspect of the ethical framework. Ethical hackers must obtain explicit and documented authorization from the organization before system penetration. This characteristic is essential for distinguishing ethical hackers from malevolent actors. A fundamental tenet of ethical hacking authorization acquisition is emphasized by the Information Systems Audit and Control Association. [27]
- **Transparency and Accountability** - Accountability for decisions and transparency in conduct are essential elements of the ethical framework. It is the norm for ethical hackers to record their activities in detailed logs conscientiously and promptly notify the appropriate authorities within the organization of any discoveries. Transparency and thorough reporting are critical elements in preserving the confidence of the ethical hacker and the client, according to the SANS Institute's ethical hacking guideline. [28]
- **Confidentiality and Integrity** - An additional essential component of the ethical framework is preserving information integrity and confidentiality. Sensitive data and information are encountered by ethical hackers, who are obligated to safeguard this information against unauthorized access and misuse. Strict

adherence to confidentiality is mandated by the IEEE's ethical hacking standards to preserve the profession's integrity. [29]

- Respect for Laws and Regulations - Compliance and respect for laws and regulations are important ethical principles. Ethical hackers must comprehend cyber security regulations like the GDPR and the Computer Fraud and Abuse Act.

- Professional Competence - The ethical framework surrounding ethical hacking places utmost importance on professional competence. This involves remaining informed about the most recent cyber security threats, techniques, and best practices. Ethical hackers are anticipated to engage in ongoing education and skill refinement to deliver service of the utmost quality.

- Non-Maleficence - The ethical framework predicates non-maleficence, meaning "not causing harm." Ethical hackers must guarantee that their actions do not damage the systems they examine or the wider digital ecosystem. This principle is explicitly stated in the Code of Ethics (2022) of the Association for Computing Machinery (ACM), which underscores the obligation of cyber security experts to avert injury to the greatest extent feasible proactively. [30]

- Promoting Ethical Conduct - Ethical hackers contribute to the advancement of ethical behavior among members of the cyber security community. They establish a precedent and foster a climate of honesty and accountability within the discipline by strictly adhering to elevated ethical principles. To bolster the standing and credibility of the cyber security field, the Cyber security and Infrastructure Security Agency (CISA, 2022) advocates for promoting ethical behaviour. [31]

To maintain integrity, ethical and effective hacking reporting requires a comprehensive and precise exposition of the conclusions drawn from security assessments. The process entails the documentation of identified vulnerabilities, testing methodologies employed, and suggestions for minimizing the risks identified. Comprehensive reporting is essential for clients to comprehend their security posture and take informed actions, according to the SANS Institute.

Table 3. Component of a ethical hacking report

Component	Description	Significance
Vulnerability Details	Detailed information about identified vulnerabilities.	Helps in understanding the nature and severity of the risks.
Testing Methodologies	Methods and tools used during the assessment.	Ensures transparency and reliability of the results.
Impact Assessment	Analysis of the potential impact of the vulnerabilities.	Assists in prioritizing the mitigation efforts.
Remediation Recommendations	Suggested measures to address the vulnerabilities.	Provides a clear action plan for improving security.

4.4 Legal Aspects

Ethical hacking, while a vital component in strengthening cyber security defenses, operates within a complex legal landscape which is considered to be the foundation of a responsible cyber security practice. The legality of hacking activities hinges on adherence to laws and regulations designed to distinguish between malicious intent and legitimate security work. The International Council of E-Commerce Consultants (EC-Council) defines the legal scope of ethical hacking as actions performed with explicit permission and for the purpose of improving security, distinguishing it from illegal hacking activities.

Table 4. Legal Aspect Considerations

Aspect	Description
Permission & Authorization	Ethical hackers must obtain explicit permission for security assessments to avoid legal issues.
National & International Laws	Knowledge of laws like CFAA (US) and GDPR (EU) is crucial for compliance in different jurisdictions. [32]
Legal Agreements & Contracts	Contracts and MoUs define the scope and legal boundaries of ethical hacking projects. [33]
Privacy Laws Compliance	Ethical hackers must adhere to privacy laws when handling personal data during assessments.
Intellectual Property	Awareness and respect for intellectual property laws and software licenses are necessary. This includes respecting software licenses and avoiding the unauthorized use of proprietary tools and techniques. [34]
Incident Reporting	Legal obligations often require reporting certain types of data breaches to authorities and affected individuals. [35]
Vulnerability Disclosure	Responsible disclosure of vulnerabilities is a complex process that must balance informing organizations with legal risks.
Legal Challenges	Ethical hackers can face legal challenges due to ambiguous laws or misinterpretation of their actions. Case studies highlight these issues.
Global Legal Trends	Ethical hackers must stay informed about global legal trends and new regulations in cybersecurity, affecting international practices.

The legal aspects of ethical hacking are multifaceted and critical to the legitimacy and effectiveness of ethical hacking practices. For these reasons, specialists

undergo rigorous training to operate by moral and legal standards, guaranteeing that their actions remain within the bounds of the law and ethical principles. Navigating these legal waters requires knowledge, careful planning, and a proactive approach to compliance.

As cyber security continues to grow in importance, the integration of legal expertise and ethical sensibility is fundamental for upholding confidence and standing in the realm of cyber security. Because organizations entrust ethical hackers with sensitive data and critical infrastructure, strict adherence to legal and ethical principles becomes imperative. The legal framework surrounding ethical hacking will likely evolve, necessitating ongoing vigilance and adaptation from professionals in the field.

4.5 Analysis of Cyber Attack

Cyber-attacks can be described as an attempt to maliciously access or make use of a resource. It is critical to comprehend these attacks' diverse forms and methods to formulate efficacious cyber security strategies. Cyber attack consists of great variety. The most known are phishing, malware, DoS assaults, ransomware etc [36]. Each attack is categorized by their specific attributes.

- Phishing attacks

Phishing is an electronic assault that employs spoofed electronic mail as a vector. The objective is to deceive the email recipient into downloading an attachment or clicking a link by presenting the message as if it were something they desire or require, such as a note from their employer or a request from their bank. This is achieved by capitalizing on psychological vulnerabilities by frequently exploiting victims' sense of urgency, fear, or authority to coerce hasty action [37].

Many phishing attack vectors, such as spear phishing, email phishing, whaling, and smashing (SMS phishing), can be identified. Traditional phishing methods employ

a broad scope, whereas spear-phishing and whaling techniques employ personalized messages to target individuals or organizations. These attacks can affect individual victims, organizations, and, in certain instances, entire sectors. Reputational harm, financial losses, data intrusions, and identity theft are all potential outcomes of successful attacks.

- Malware attack

Adversarial software, such as spyware, viruses, worms, and trojans, is developed and distributed as part of malware attacks. The characteristics and methods of operation of each variant of malware are unique. Malware is predicated on the intention to inflict harm upon a computer, server, client, or computer network. [38] Exploitation of software vulnerabilities, compromised websites, email attachments, and unsecured networks are all potential vectors for malware propagation. Common uses for malware include unauthorized system access, data theft, and operation disruption.

- Ransomware

Ransomware is a form of malicious software in which the target files are encrypted, and the perpetrator demands a ransom in exchange for the ability to decrypt the data [39]. Per the cyber security and Infrastructure Security Agency, ransomware attacks have exhibited a notable escalation in complexity, frequently focusing on critical infrastructure and businesses.

Multiple methods exist by which ransomware can infiltrate systems, including fraudulent emails, exploiting network vulnerabilities, and malware-laden websites. Social engineering is a prevalent method attackers use to deceive users into downloading ransomware. The consequences of ransomware assaults transcend the monetary damages incurred as a direct result of the ransom demand. These encompass potential harm to operations, loss of data, injury to reputation, and occasionally even critical safety hazards. Recovering from a ransomware attack can be expensive and time-consuming, frequently surpassing the ransom amount.

- DoS and DDoS attacks

DDoS attacks are a cyber-assault that seeks to inaccessibly inundate a system, server, or network with traffic, preventing authorized users from accessing it. DDoS attacks are comparable; however, they are carried out via a distributed network of compromised computers or devices, commonly known as a botnet [40], this renders them more arduous to counteract. These assaults take advantage of the vulnerabilities present in network resources, leading to disruptions in service and deterioration. Volume-based, Protocol and Application Layer attacks are the main mechanisms and tactics of DoS and DDoS attack.

It is worth noting an exponential rise in each cyber threat method. These attacks have resulted in various data breaches but also money frauds and extortion. The following table showcases various statistics related to some attacks.

Table 5. Cyber attacks statistics

Attack Method	Statistics
Phishing	<ul style="list-style-type: none"> • 300,497 phishing victims in USA for 2022 • 173% increase in Q3 2023 compared to Q2 [41]
Malware	<ul style="list-style-type: none"> • McAfee estimated a global loss in billions of dollars as for 2022 • 110% increase in Q3 2023 compared to Q2 2023 [41]
Ransomware	<ul style="list-style-type: none"> • In 2023, 72% of businesses were affected [42] • Average cost of recovery from ransomware sits at 1.85 million USD
Dos and DDoS	<ul style="list-style-type: none"> • Average attack in 2023 sustained campaigns for more than 20 minutes [43] • 50% more attacks longer than 1 hour during 2023 compared to previous year

Ethical hackers are specialized to come up with methods needed to prevent and mitigate these kinds of attacks. Widely accepted methods include:

- Layered Defense Strategy
- Regular Software and System Updates
- Advanced Threat Detection Systems
- Employee Education and Awareness Training
- Robust Network Security Measures
- Incident Response Planning
- Data Encryption and Backup

Chapter 5

Network Security in Albania

Albania is considered to be on its earliest stages when it comes to network security industry and thus this is perceived as a great investment opportunity from entrepreneurs, as well as established tech firms that operate in this sector.

During the last decade it is noticed an increase of interest by students, who's intentions are to pursue their studies in network security programs. This is outlined in a report by INSTAT, where Technology and Digital Communication programs are noted to have an increase of 10% since last year, which is the second highest in any program. [44]. A considerable amount of higher education institutes have expanded their program sections in order to provide more diverse variety when it comes to network security education. It is worth mentioning a substantial increase in the number of certification programs, which objective is to provide valuable skill sets and certifications. In addition, the government is also actively endeavoring to stimulate this growing interest in the field. They are offering training lectures to public employees as well as scholarships to excellent students in order to assist them with their objective of pursuing a career in network security.

5.1 Cyber-attacks on Albania

Despite the growing interest and the efforts to develop this sector, during the past few years Albania has witnessed various leaks made public. This came due to the fact of this country constantly being targeted by malicious cyber attacks which have targeted the main data base of high-ranking government organisations, as well as high ranking political profiles.

Homeland Justice is a hacker group that has constantly targeted high-profile organizations and politicians in Albania during the recent years. There have been various data leaks made public, which contain highly sensitive information such as general population credentials, telephone numbers, car license plates associated with the name of the owner, bank accounts details, tax history, salaries etc.

CISA released a report containing information related to this cyber-attack, detailing methods used by the hackers. [45]. Initially access was gained by exploiting a Internet-facing Microsoft SharePoint vulnerability, CVE 2019-0604. Afterwards the hackers employed several .aspx webshells in order to carry on persistence. One to six months after the initial compromise, searches were run on various mailboxes by using a compromised Microsoft Exchange account. The hackers were capable of creating a new Exchange account and connect this new account to the Organization Management role group. Afterward the intruders created thousands of HTTP POST requests to Exchange servers. A year after the initial compromise, connections were made to IP addresses, which belonged to the organization VPN device. Two compromised accounts and a Advanced Port Scanner were used for this task. Afterward the intruders ran Mellona.exe which would spread GoXml.exe encryptor to internal machines. This process managed to encrypt all files on the affected system and left a ransom note in each folder. At the same time by using Disk Wiper tool, they wiped raw disk drivers. During eight hours, various RDP connections were logged from a infected server to other hosts on the network.

The main data leaks and sensitive information included:

- Emails of various high ranking political figures, that included the prime minister, ministers, Director-General of Police. Their emails were made public, which raised the concern of sensitive information being leaked through these emails to the general public, that could be later used in order to affect various cases.
- Personal credentials database of the general population was considered the most notable case. It included various information such as name, surname, gender, profession, ID number, birth date, birth place etc. This leak posed a great threat as someone with this kind of information can

easily commit identity theft. With the leak being available to anyone through the internet, it still raises a lot of concern for the public.

- Salaries, bank accounts details and the taxes of different people or companies were made public. The hackers managed to steal databases that were stored which included the salaries that are declared for each company employee but also the database which showed the amount of tax that each individual or company had paid. In addition, they also published a file which contained information about some bank account details for various people in a second level bank. This raised very serious concerns as it directly affected a lot of people and businesses, by having their personal finances be made public to everyone.

Their latest successful attacks were achieved on December. It managed to hack one of the two main telecommunication companies and delete all its backup files and it also managed to shut down the parliament official website. The group claims that they have gained access to the data of the parliament and the login to the server. In addition, they also claim to have hacked the flying airline “Air Albania” which would raise concern as the data poses a great threat to the privacy of all its customers.

On the other hand, this group has also managed to showcase a real problem which was related to the border police in Albania. They have released real footage on the corruption in the borders which resulted in one of the biggest scandals in recent years. The footage showcased various occasions of bribe being committed in the borders. Homeland Justice raised the question as why there had not been filed any reports on this matter even though cameras had captured these moments.

5.2 Albanian Hackers

Apart from the great interest of students to become professionals in network security, there have been two notable cases when it comes to hackers from Albania.

One of them is a 25-year-old named Aldo Ymeraj who was arrested in Tirana and the other is Arion Kurtaj, who has managed to penetrate highly secure companies such as Nvidia, Rockstar gaming and BT/EE.

At the moment when Aldo was arrested, he was an unknown name for the media and police. He had the nickname “kubanezi” in the virtual life and was part of a infamous group named “In fraud we trust”. This organization was believed to have operated from 2010 up until 2018, and was involved in stealing sensitive information. [46]. It was started by Svyatoslav Bondarenko and it is assumed that it is responsible for the theft of 530 million USD. Aldo was one of the 10,000 people registered in this group and is believed to have played the role of a vendor that sold credit card dumps. The Albanian was only 25 years old when he was arrested by Albanian authorities in the region of Tirana. [47]. His neighbours in his hometown portrayed Aldo as a quiet kid who did not show any wealth and never got into trouble. This organization used open forums in the internet in order to purchase and sell stolen information about credit cards or bank statements. They had formed a structured group in which everyone had their specific roles. Aldo’s role was that of a vendor. They were in charge of selling illegal products and services to the general members of the group which were interested on these kinds of information, by using his own website. They would even allow the members to put their own reviews for these kinds of products, in order to ensure the quality of the product. Depending on the reviews, the organization would decide if they would keep a certain vendor or not. Aldo used a website named “niii.in” in order to sell his products. After being arrested in Tirana, Aldo was extradited to USA in order to receive his sentence, for which the FBI believes that through the years of 2016-2017 he had been using “Skimmer” to clone cards and then sell them on the website named “niii.in” . He is also believed to be responsible for the cloning of more than 1000 cards, bank accounts and other on-line transactions.

In December 2023, Arion Kurtaj got sentenced to life in hospital prison in Great Britain [48] after he had managed to hack Rockstar Inc. and leaked data footage of it’s unreleased games. Kurtaj was considered as a threat due to his continuous desire to engage in cybercrime. He was part of the infamous hacker group “Lapsus\$”, a group responsible for various data breaches all over the world [49]. Arion was considered of having autism and being unfit to stand trial. He went through a mental health

evaluation, where he displayed intent to continue performing cybercrimes therefore, he was placed in a hospital prison after taking his mental condition in consideration. Prior to his sentence, Kurtaj had been out on bail after he had previously successfully managed to hack Nvidia and BT/EE, two highly secure firms in the fields of cyber security. What is interesting about this case is that Kurtaj was reported to have managed performing his attack on Rockstar Games while staying in a hotel by using tv remote controller, a new smart phone and a set of keyboard and mouse. Rockstar has announced that it has spent more than 5 million dollars in order to recover from these cyber attacks.

Chapter 6

Simulation and Results

6.1 Vulnerability scan

In order to gain access to the victim's software or hardware, intruders make use of different vulnerability scanners in order to find the most vulnerable point of the systems. These scanners are computer programs which are specifically built and designed with the purpose of gathering data by assessing all kind of systems for known weaknesses. This is achieved by making use of different flaws that are created from flawed programming or that are created from misconfiguration. Some examples of these kind of flaws can be found within:

- Firewall
- Web server
- Router

Vulnerability scanners can be divided in two groups:

Table 6. Vulnerability scanners groups

Authenticated	Unauthenticated
<ul style="list-style-type: none">• Makes use of remote administrative protocol (SSH , RDP) ,in order to directly access assets of interes.• Authentication is performed by operating system credentials which are provided• Manages to gain access to low-level data• Produces detailed information related to the system and software	<ul style="list-style-type: none">• Can not produce detailed information related to software or operating system• It often provides high number of inaccurate results• Main purpose is to evaluate the security of external assets

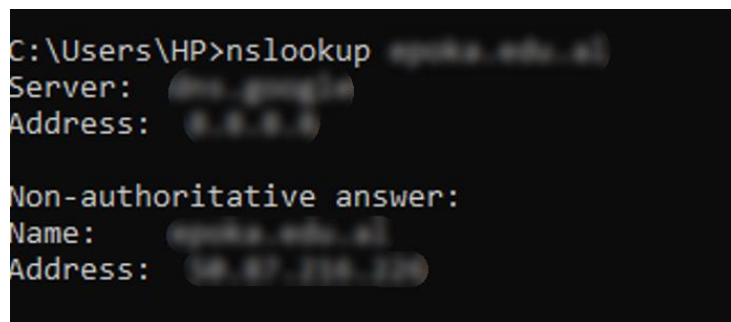
One of the main open-source scanners was created by Greenbone. This company began its development for OpenVAS since 2006. OpenVAS is a vulnerability scanner which is capable of performing both authenticated and unauthenticated tests. Greenbone Enterprise Trial is an open-source community edition developed by Greenbone which is available and able to perform tests. It can be used of virtual environments such as:

- Oracle Virtual Box
- Vmware Workstation Pro

The company has also provided the necessary steps, that are needed in order to complete the set up.

After finishing the set up and running the software in a virtual environment, the user can access this scanner by simply entering his IP on a web browser and log in with the credentials which they created while setting up the software.

After the set up is performed and the user has gained access to the scanner, it is needed to gain the IP address of the target. This step can easily be completed with a simple nslookup command through linux terminal or command prompt.



```
C:\Users\HP>nslookup
Server: [redacted]
Address: [redacted]

Non-authoritative answer:
Name: [redacted]
Address: [redacted]
```

Figure 1. Nslookup command on a public domain

Greenbone scanner is capable of performing a variety of scans. The one that is commonly used is their custom which is capable of performing a full and fast scan of the target IP. Results of the vulnerabilities are shown as below:

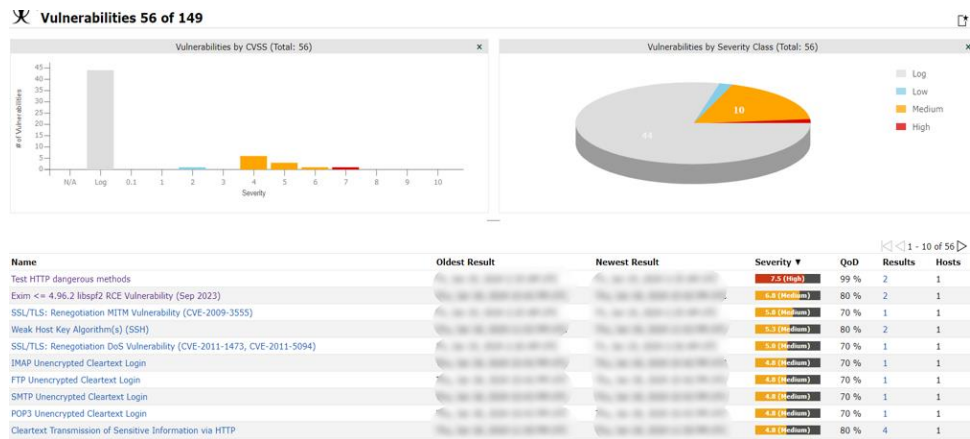


Figure 2 Vulnerability report of a public domain

The vulnerabilities that were found are divided in 4 main categories depending on their severity such as:

- Log
- Low
- Medium
- High

Each of the vulnerability is also associated with specifications related to its nature, impact and solution.

In the results which were presented above it is found one vulnerability with high severity impact.

Summary

Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE.

Scoring

CVSS Base **7.5 (High)**
 CVSS Base Vector AV:N/AC:L/Au:N/C:P/I:P/A:P
 CVSS Origin N/A
 CVSS Date Thu, Nov 3, 2005 1:08 PM UTC

Figure 3 Summary of a high threat-vulnerability

The nature of this vulnerability is described as above. In this case it is a high severity vulnerability related to HTTP methods such as PUT and DELETE.

Detection Method

Checks if dangerous HTTP methods such as PUT and DELETE are enabled and can be misused to upload or delete files.
Quality of Detection: remote_vul (99%)

Affected Software/OS

Web servers with enabled PUT and/or DELETE methods.

Impact

- Enabled PUT method: This might allow an attacker to upload and run arbitrary code on this web server.
- Enabled DELETE method: This might allow an attacker to delete additional files on this web server.

Figure 4. Details of a high-threat vulnerability

The scanner also provides with detection method, affected software and Impact. These categories present possible threats which an intruder can make use in order to achieve his goal.

Solution

Solution Type: ↩ Mitigation

Use access restrictions to these dangerous HTTP methods or disable them completely.

Figure 5. Solution to a high-threat vulnerability

Each vulnerability is associated with an solution proposed to fix it. As for this example, it is proposed use access restrictions to these HTTP methods or disable them.

This tool can be very helpful for both intruders and network security professionals. Intruders can easily gain access to all the vulnerabilities which they can exploit, which are also associated with detailed descriptions. On the other hand the professionals, who deal with security matters, make use of this tools in order check all the vulnerabilities and gain information for each of them, that is needed to improve the security.

6.2 Bruteforce Simulation

In the 1st step the user needs to run the attacker machine (Kali Linux) on VMware and at the same time also run target machine metasploitable2 in a new window. The IP address of the metasploitable 2 machine is obtained after performing an ifconfig command in the terminal. After obtaining the IP from the machine, this IP can be used on Kali Linux browser in order to get to the test log-in page.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c1:28:6d
          inet addr:10.10.10.10      Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr::::        Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:103 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7909 (7.7 KB)  TX bytes:6324 (6.1 KB)
          Interrupt:17 Base address:0x2000
```

Figure 6. Metasploitable2 IP information

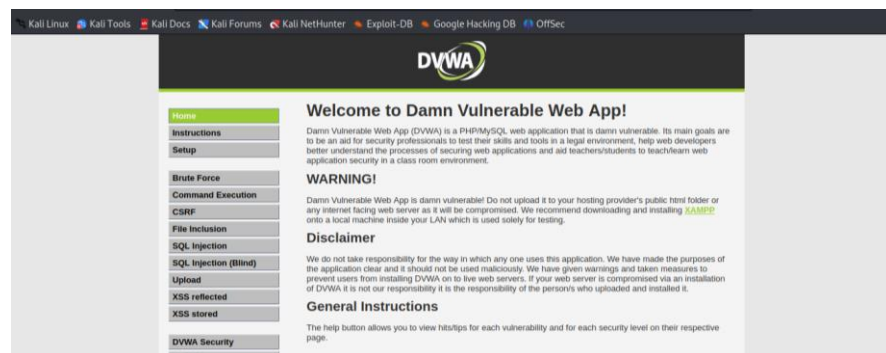


Figure 7. DVWA Vulnerable Web App

This test log-in page is going to act as the target for the user to perform the brute force attack with the assistance of Burpsuite. After running Burpsuite the user needs to head to interception tab and deactivate interception. After interception is activated, the web page that contains the IP of the metasploitable machine is refreshed thus opening the log in test page.

Username

Password

You have logged out

Figure 8. Test log-in page

The user proceeds with adding random guesses on username and password and try to log in. Afterwards interception is turned on, on burp suite. After clicking on Brute Force tab in DVWA home page it will redirect to login page where brute force attack was performed.

Random username and password are entered and then the login attempt is tried. Burpsuite proxy tab is where a request intercept by burpsuite which contain username and password that was entered in login page. Afterwards the request is sent to intruder.

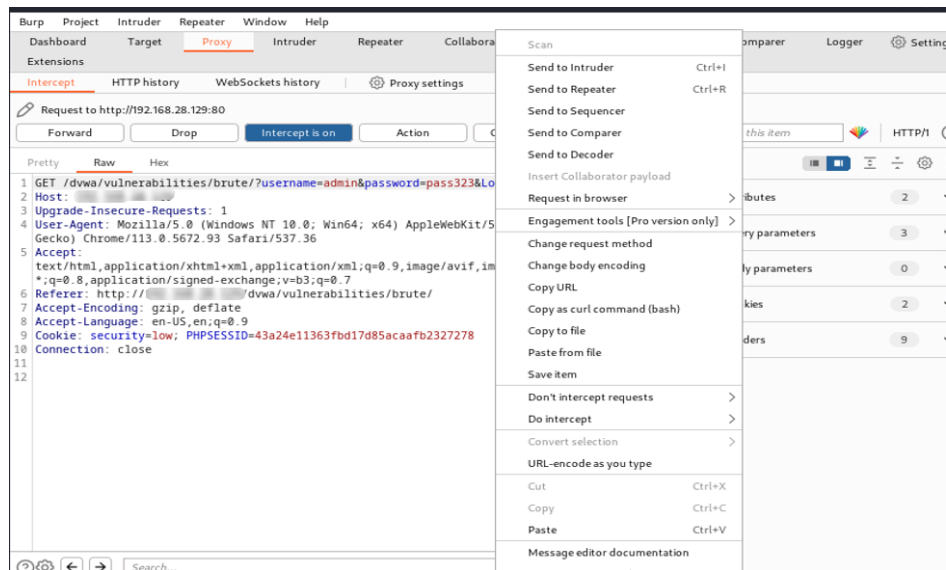


Figure 9. Burpsuite interception

The attack type is set to Sniper. On the Intruder page the user can select the password that was tested in login attempt and click on Add. In different cases when the intruder does not know the username, he can select both username and passwords to try different combination of usernames and passwords.

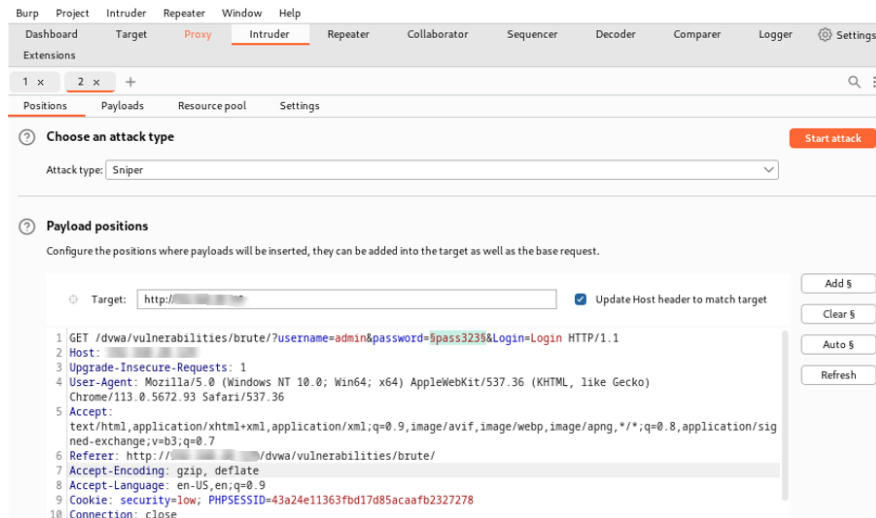


Figure 10. Targeting the password on Burpsuite

Afterwards the user is able to enter passwords manually or in different cases use provided lists from an open source. After the intruder has entered his predictions, the attack is started, and it tries every combination.

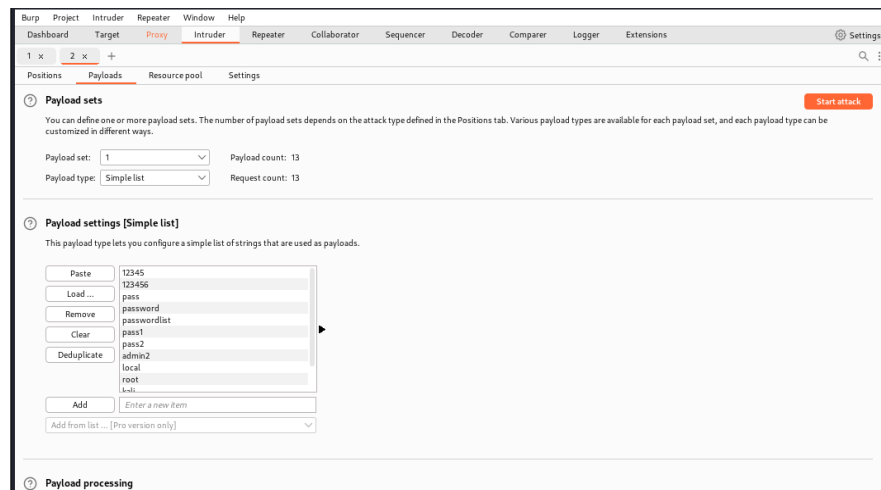


Figure 11. Payload settings list in Burpsuite

Intruder checks the value of every password. In order to check the correct password, intruder checks the response tab to find the successful login response, as seen below.

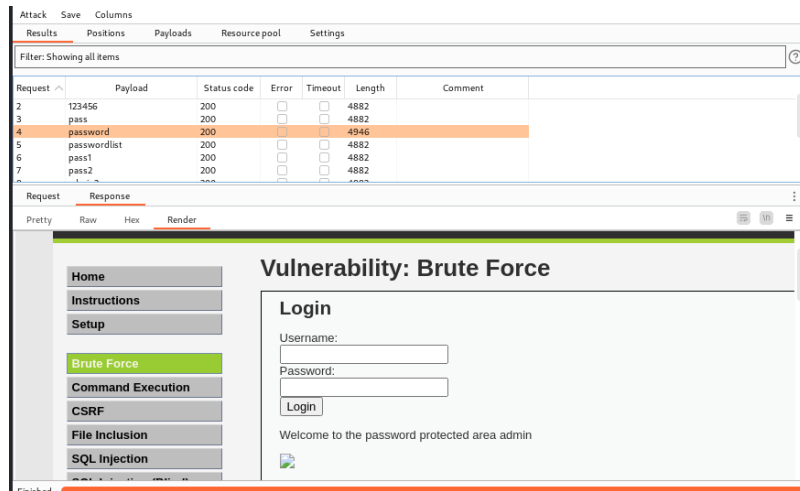


Figure 12. Log-in tab in Burpsuite

Once the correct password is found, the intruder can gain access to the account with the credentials found.

6.3 Phishing Attack Simulation

There are a number of ways to test for phishing attacks. One way is to use a phishing simulation tool, which can send fake emails or text messages to employees and then track who clicks on the links. Another way to test for phishing attacks is to use a phishing awareness training program, which can teach employees how to identify and avoid phishing attacks.

Social Engineering Toolkit [50] or SET for short is the standard for social engineering testing among security professionals and even beginners must have a basic idea about using the tool. Basically, it implements a computer-based social engineering attack.

To initiate the phishing attack, intruder makes use of Kali Linux SET and gains root access in the terminal. After gaining root access, intruder runs Social Engineering

Tools through the terminal. The most common used phishing attack is website attack vectors.

```
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2
```

Figure 13. SET attack vectors

This tool gives a variety of attack types to the intruder. Credential Harvester Attack Method is the method used to perform a phishing attack to steal the victims credentials.

```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

Figure 14. Web attack methods in SET

Now, the attacker has a choice to either craft a malicious web page on their own or to just clone an existing trustworthy site. In most cases the intrudred clone and existing trustworthy site because is it easier and with an higher success rate for their purpose.

```
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>
```

Figure 15. Website clone methods

SET will ask intruder to provide an IP where the credentials captured will be store. This attack performs on local host 0.0.0.0 is added as IP address.

```
— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * —

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.28.128]:0.0.0.0
```

Figure 16. IP address set

After adding IP address, the intruder can either provide the web page url that he wants to clone or use already provided templates. Provided templates include those of mostly used web pages such as google or Twitter.

```
**** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

/etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

1. Java Required
2. Google
3. Twitter

set:webattack> Select a template:3
```

Figure 17. Templates for website cloning

The setup for a **phishing attack** is complete.

SET display the captured data when a victim enter their credentials like username and password.

```
[*] Cloning the website: http://www.twitter.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
127.0.0.1 - - [22/Nov/2023 11:02:17] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [22/Nov/2023 11:02:38] "GET / HTTP/1.1" 200 -
```

Figure 18. Start of phishing attack

After the site is cloned , the intruder forges a scam email account and sends a scam email to the victim ,while posing as an official support of the cloned web page asking for the victim to confirm their account credentials and provides a link which re-directs to the cloned web page. This link is often disguised in order to not alert the victim.

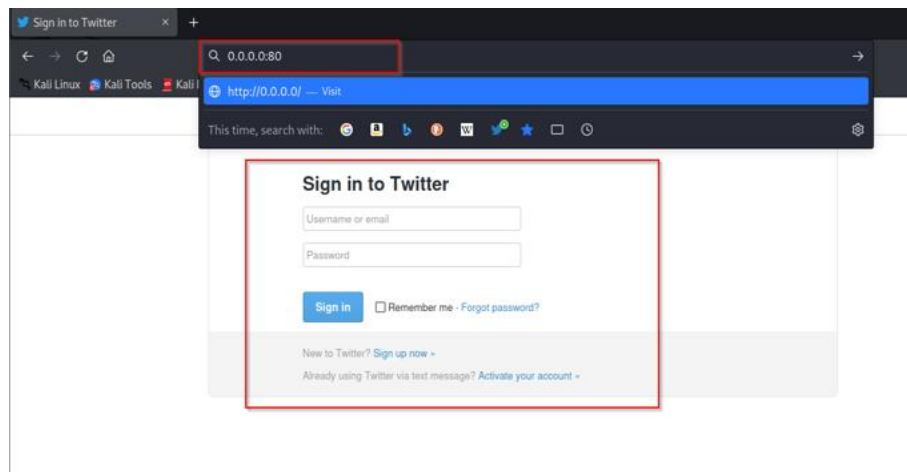


Figure 19. Cloned site for phishing attack

At the moment in which the victim fills in their details and clicks on ‘Log In’, the cloned page takes them to the real web-page login page. Meanwhile as the victim believes that he has confirmed the credentials and doesn’t suspect anything, the intruder get the credentials in his terminal where he has started the attack.

```
[*] Cloning the website: http://www.twitter.com
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
127.0.0.1 - - [22/Nov/2023 11:02:17] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [22/Nov/2023 11:02:38] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=testusername
POSSIBLE PASSWORD FIELD FOUND: session[password]=testpassword6723
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
PARAM: scribe_log=
POSSIBLE USERNAME FIELD FOUND: redirect_after_login=
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

127.0.0.1 - - [22/Nov/2023 11:19:08] "POST /sessions HTTP/1.1" 302 -
```

Figure 20. Results of phishing attack

6.4 Vulnerability Comparisons

How do Albanian institutions perform compared to established institutions world-wide? This comparison contains data gathered using OpenVAS scanner from various higher education institutions domains which are located in:

- Albania
- Montenegro
- Kosovo
- North Macedonia
- Romanian
- Italy
- USA

. The corresponding IP of each higher education institute domain was gained by performing a nslookup command through command prompt.

The first results show the vulnerability report of an Albanian higher education institution.

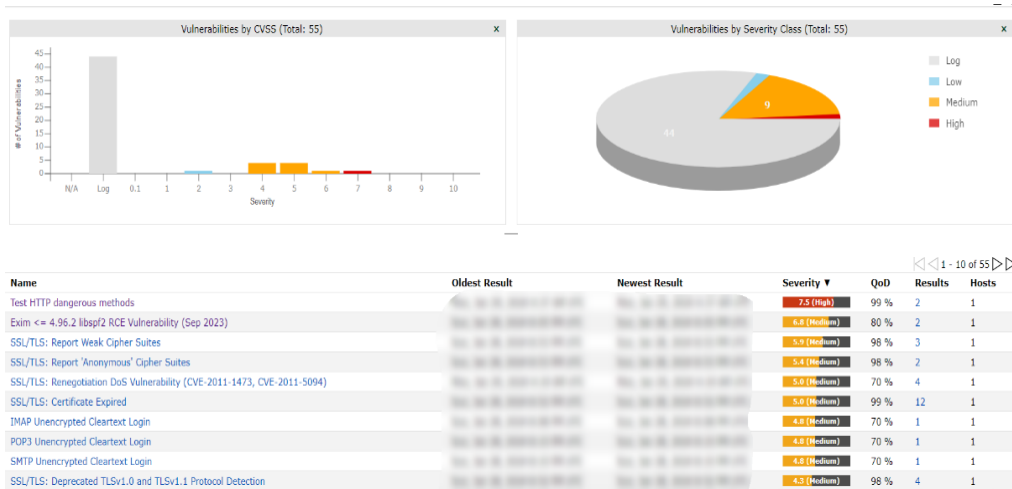


Figure 21 Albanian institution vulnerability report

In total there were 55 vulnerabilities discovered by the scanner. They included 44 in Log severity , 1 low severity, 9 medium severity and 1 high severity level. The most crucial vulnerability discovered is related to HTTP dangerous methods. As seen below the scanner shows the nature of this vulnerability , how an intruder can exploit it and also an suggested method to fix it.

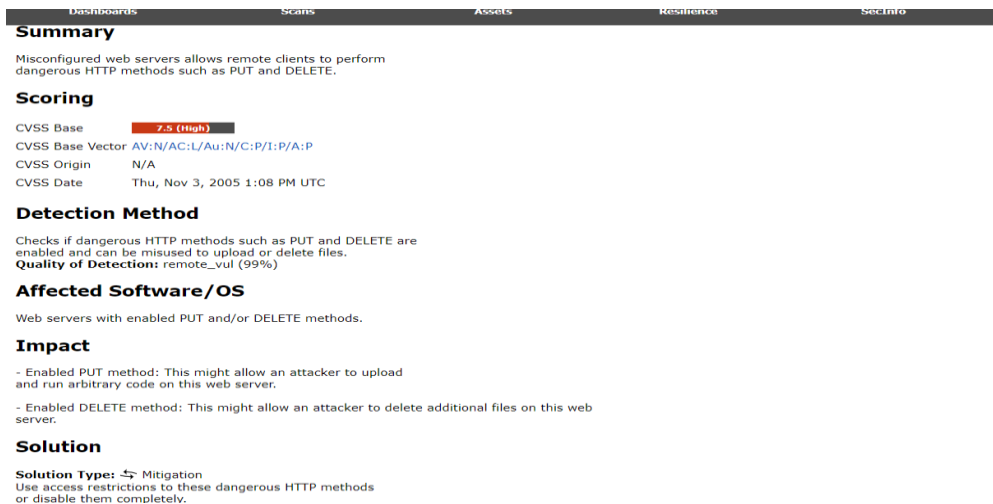


Figure 22 Albanian institution high severity vulnerability

Next it is presented the report of an Montenegro higher education institution. This institution showcased various vulnerabilities in different severities.

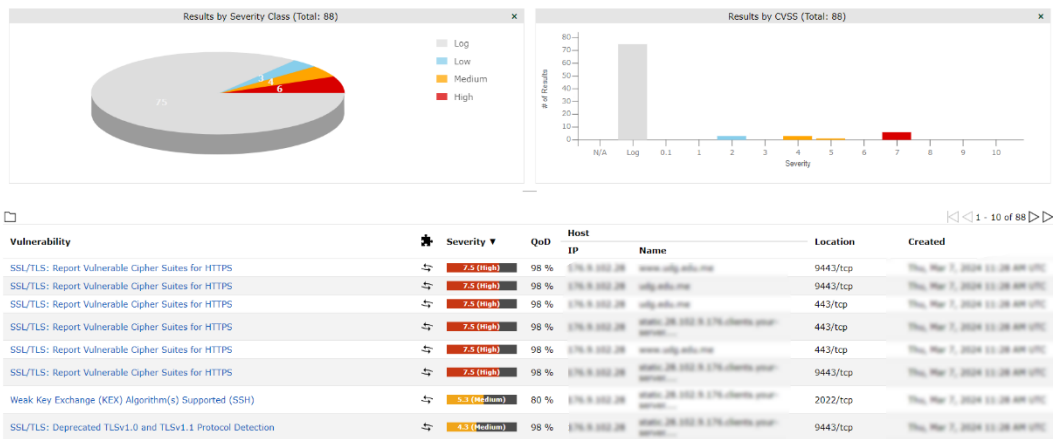


Figure 23 Montenegro institution vulnerability report

As seen in the report this institution showcased a total of 88 vulnerabilities discovered, from which 6 were high severity level vulnerabilities. These were mainly related to SSL/TLS vulnerabilities. In addition there were 4 medium severity level and also 3 low severity level. Below it is demonstrated one of the high severity level vulnerability discovered.

Summary

This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Scoring

CVSS Base **7.5 (High)**
 CVSS Base Vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
 CVSS Origin NVD
 CVSS Date Thu, Jul 28, 2022 11:27 AM UTC

Insight

These rules are applied for the evaluation of the vulnerable cipher suites:
 - 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Detection Method

Quality of Detection: remote_app (98%)

Affected Software/OS

Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Solution

Solution Type: Mitigation
 The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
 Please see the references for more resources supporting you with this task.

Figure 24 Montenegro institution high severity vulnerability

Kosovo higher education institution demonstrate excellent results, with only two low severity vulnerabilities. Despite being a new country which faces a lot of challenges , Kosovo institution demonstrate a high security level.

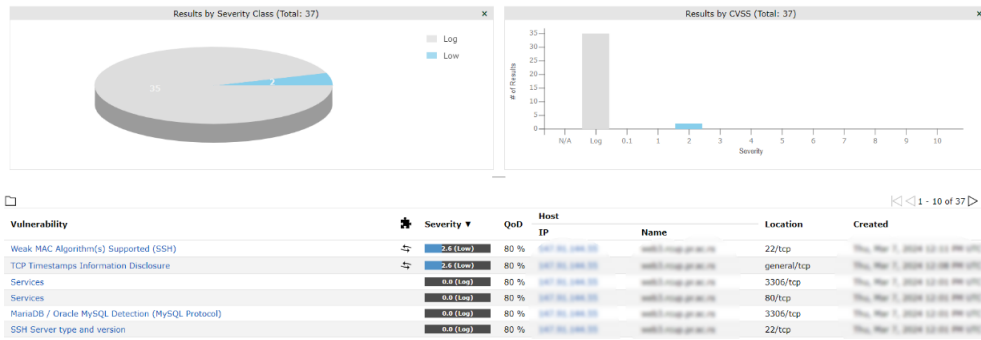


Figure 25 Kosovo institution vulnerability report

North Macedonia higher education institution demonstrates excellent results with only one severity vulnerability.

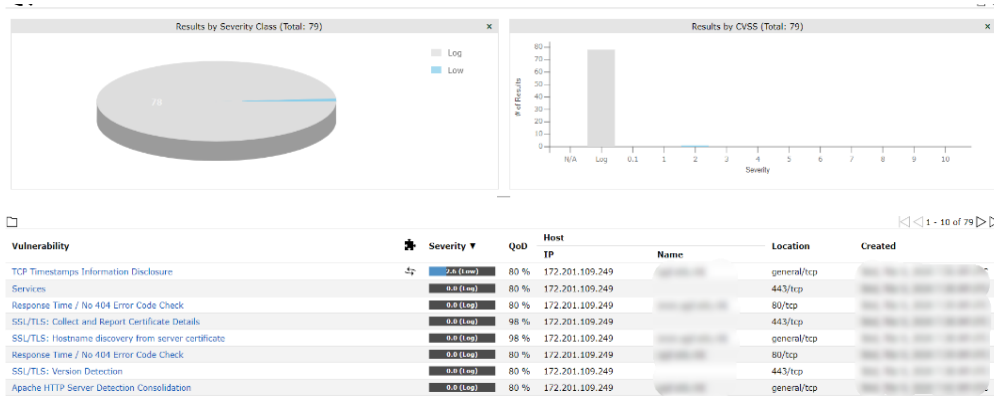


Figure 26 North Macedonian institution vulnerability report

Next it is presented the vulnerability scan report of an Romanian higher education institution.

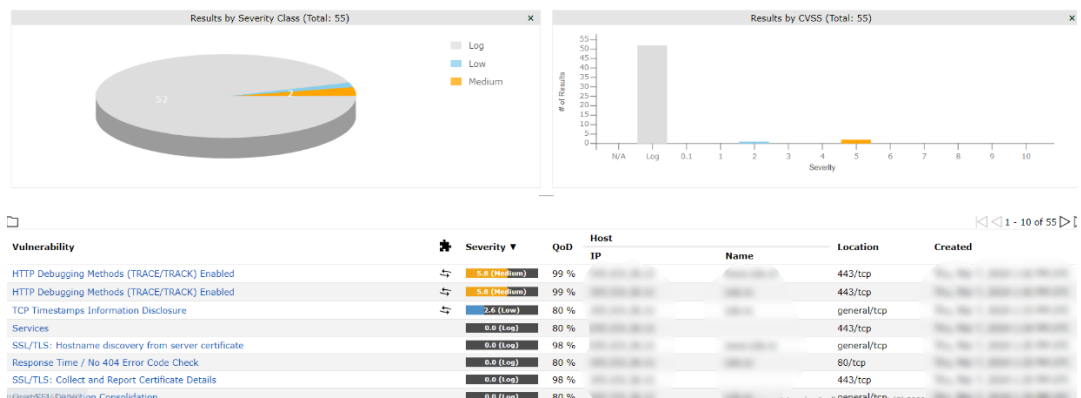


Figure 27 Romanian institution vulnerability report

The results were positive. The report included only two medium severity vulnerability level related to HTTP Debugging Methods and one low severity level related to TCP Timestamps.

Italian higher education institution report consisted of various vulnerability found ,from which six were in medium severity level as seen below.

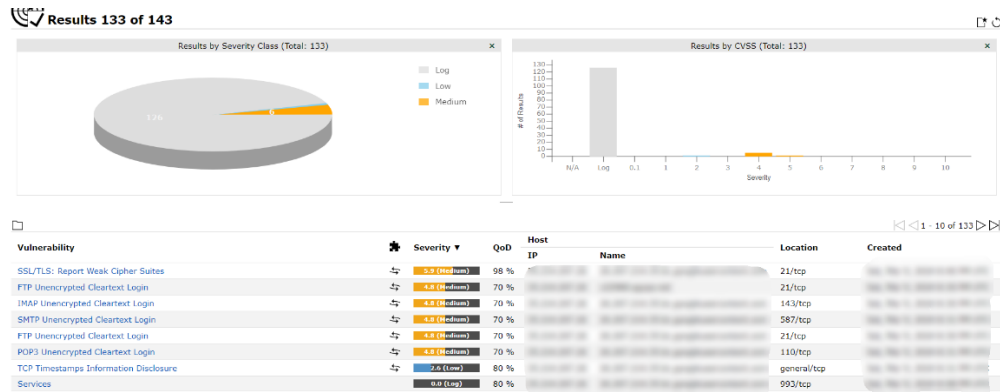


Figure 28 Italian institution vulnerability report

One of the vulnerabilities found is related to IMP unencrypted cleartext login. As seen below the scanner gives detailed description related to this vulnerability found.

Summary

The remote host is running an IMAP daemon that allows cleartext logins over unencrypted connections.

NOTE: Valid credentials needs to given to the settings of 'Login configurations' OID: 1.3.6.1.4.1.25623.1.0.10870.

Scoring

CVSS Base **4.0 (Medium)**
 CVSS Base Vector AV:A/AC:L/Au:N/C:P/I:P/A:N
 CVSS Origin N/A
 CVSS Date Thu, Nov 3, 2005 1:08 PM UTC

Detection Method

Quality of Detection: remote_analysis (70%)

Impact

An attacker can uncover user names and passwords by sniffing traffic to the IMAP daemon if a less secure authentication mechanism (eg, LOGIN command, AUTH=PLAIN, AUTH=LOGIN) is used.

Solution

Solution Type: Mitigation
 Configure the remote server to always enforce encrypted connections via SSL/TLS with the 'STARTTLS' command.

Figure 29 Italian institution medium severity vulnerability

USA higher education institution demonstrated excellent results , which included only one vulnerability found. This vulnerability was placed on low severity level and it was related to TCP timestamps.

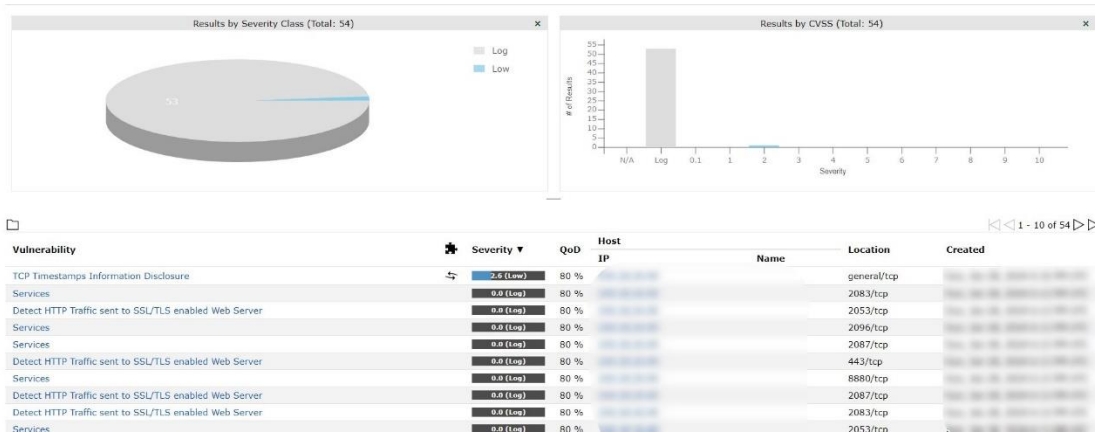
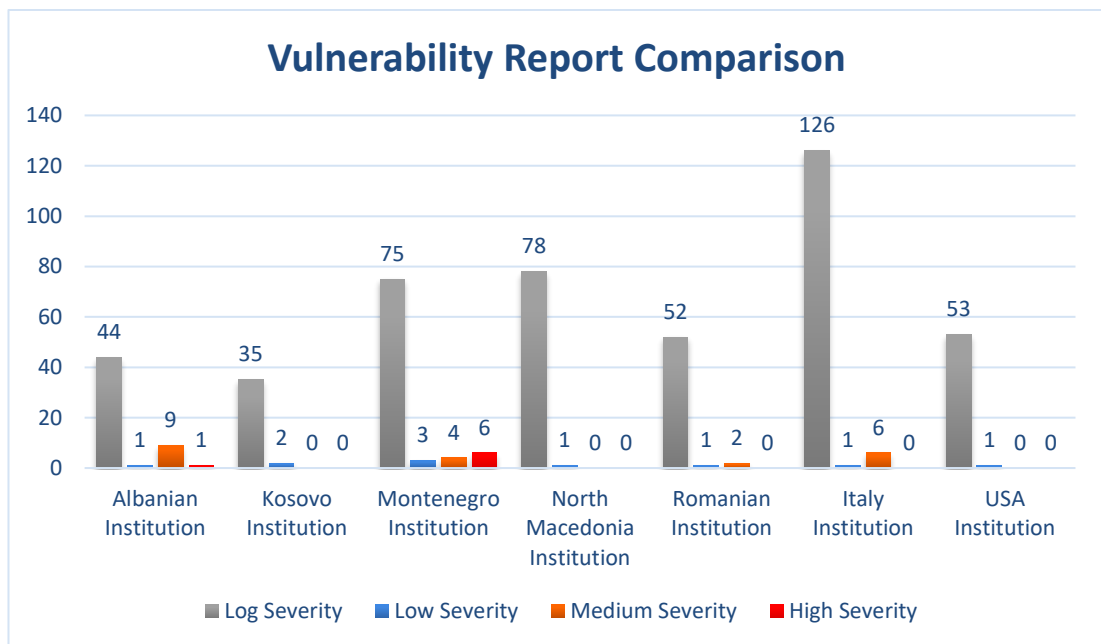


Figure 30 USA institution vulnerability report

Table below consists of a comparison between the vulnerability reports of each institution.

Table 7 Vulnerability reports comparison



Chapter 7

Conclusion

As cyber attack become more advanced, ethical hacking becomes an essential skill in network security. There is a huge demand in this industry to hire specialists, which is perceived as a great career opportunity by anyone who aspires to continue their career in this field. In Albania it is essential to produce specialists and security systems, to prevent malicious attacks which have been constantly targeting this country and its organizations.

Despite its benefits, ethical hacking is not without challenges. One key concern is the ethical dilemma it presents; ethical hackers must navigate the thin line between testing security measures and violating privacy or legal boundaries. Additionally, there is the risk of inadvertently causing system disruptions or data loss during testing. Thus, ethical hacking must be conducted with utmost caution and professionalism.

The integration of ethical hacking into network security is a crucial strategy in today's digital age. By understanding and replicating the methods of malicious actors, ethical hackers provide invaluable insights into security weaknesses, enabling organizations to fortify their defences proactively. As cyber security threats evolve, so too must the techniques and strategies employed to combat them, with ethical hacking at the forefront of this endeavour.

References

- [1] Arctic Wolf, "A Brief History of Cybercrime," 16 November 2022. [Online]. Available: <https://arcticwolf.com/resources/blog/decade-of-cybercrime/#:~:text=Technically%2C%20the%20first%20cyber%20attack,accessing%20the%20French%20telegraph%20system..>
- [2] The Tech, "Internet Archive," 20 November 1963. [Online]. Available: <https://web.archive.org/web/20160314083748/http://tech.mit.edu/V83/PDF/V83-N24.pdf>.
- [3] Wikipedia, "Creep and Reaper," Wikipedia, 8 May 2010. [Online]. Available: https://en.wikipedia.org/wiki/Creep_and_Reaper.
- [4] Federal Bureau of Investigation, "Morris Worm - 30 Years Since First Major Attack on the Internet," 2 November 2018. [Online]. Available: <https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218>.
- [5] Federal Bureau of Investigation, "A Byte out of History : \$10 Million Hack, 1994-Style," 31 January 2014. [Online]. Available: <https://www.fbi.gov/news/stories/a-byte-out-of-history-10-million-hack>.
- [6] Andrew Froehlich, "white hat hacker," Wikipeida, [Online]. Available: <https://www.techtarget.com/searchsecurity/definition/white-hat>.
- [7] EC-Council, "EC-Council," EC-Council, [Online]. Available: <https://www.eccouncil.org/>.
- [8] T. Ostrand, "White-Box Testing," 15 January 2002. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/0471028959.sof378>.
- [9] M. E. Khan, "Different Approaches to Black Box Testing Technique for Finding Errors," Al Musanna College of Technology, 21 July 2021. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3890672.
- [10] Wikipedia, "Gray-box testing," Wikipedia, 15 October 2011. [Online]. Available: https://en.wikipedia.org/wiki/Gray-box_testing.

- [11] R. P. Goldberg, "Architecture of virtual machines," 26 March 1973. [Online]. Available: <https://dl.acm.org/doi/abs/10.1145/800122.803950>.
- [12] L. a. P. R. a. F. R. G. a. B. D. Martignoni, "Testing system virtual machines," 2010. [Online]. Available: <https://doi.org/10.1145/1831708.1831730>.
- [13] R. Balzer, "Process Virtual Machine," 1991. [Online]. Available: <https://doi.ieeecomputersociety.org/10.1109/ISPW.1991.637520>.
- [14] R. P. Petar Cisar, "Some ethical hacking possibilities in Kali Linux environment," *Journal of Applied Technical and Educational SciencesJATES*, vol. 9, pp. 129-149, 4 November 2019.
- [15] H. Anderson, "Introduction to Nessus," SecurityFocus, 2003.
- [16] M. M. a. A. Saktiansyah, "Analysis of Vulnerability Assessment Technique Implementation on Network Using OpenVas," *International Journal of Engineering and Computer Science Applications (IJECSA)*, vol. 2, no. 2, pp. 51-58, 2023.
- [17] R. A. Grimes, "Brute-Force Attacks," 2020.
- [18] Y. I. a. A. J. M. Khonji, "Phishing Detection: A Literature Survey," *IEEE Communications Surveys & Tutorials*, vol. 15, pp. 2091-2121, 2013.
- [19] C. Brooks, "For Cyber security Awareness Month (and Halloween) - Some Scary Cyber Threat Stats," Forbes, 2022.
- [20] ICO, "TalkTalk cyber-attack - how the ICO's investigation unfolded," [Online]. Available: <https://ico.org.uk/about-the-ico/media-centre/talktalk-cyber-attack-how-the-ico-investigation-unfolded/>.
- [21] K. K. a. Y. D. E. Goncharov, "Five ICS cyber security myths based on Kaspersky Lab ICS CERT experience," *Automatisierungstechnik*, vol. 67, no. 5, pp. 372-382, 2019.
- [22] Deloitte, "Building consumer trust Protecting personal data in the consumer product industry," [Online]. Available: https://www2.deloitte.com/content/dam/insights/us/articles/consumer-data-privacy-strategies/DUP_970-Building-consumer-trust_MASTER.pdf.

- [23] technoaretepublication.org, "The Process of Providing Security Protection in the Amazon E-Commerce System," 2022. [Online]. Available: <https://technoaretepublication.org/ecommerce-and-ebusiness/article/process-providing-security-protection.pdf>.
- [24] DHS, "Cyber security - Homeland Security," 26 November 2023. [Online]. Available: <https://www.dhs.gov/topics/cybersecurity>.
- [25] sciarc, "Family Educational Rights and Privacy Act (FERPA)," [Online]. Available: https://www.sciarc.edu/institution/resources/policies-and-disclosures/ferpa?gad_source=1&gclid=Cj0KCQiA67CrBhC1ARIsACKAa8THCleItjhYYOmzcIztMM8svsNO2zAk1fOv9pRkmVoCRWTgE1qrVi4aAi9gEALw_wcB.
- [26] VicOne, "The Road Ahead Is Paved With Risky Data : VicOne Automotive Cybersecurity Report 2023," VicOne, 2023.
- [27] S. K. P. S. A. P. a. R. C. M. K. Variralkar, "Creating Password Protector Application for Preventing Unauthorised Hackers Using Java," *Cyber Security, Privacy Issues and Challenges*, vol. 2, no. 1, pp. 26-29, 2023.
- [28] SANS , "Ethical Hacking Training - SANS Institute," [Online]. Available: <https://www.sans.org/mlp/ethical-hacking/>.
- [29] K. C. M. G. S. K. S. Joshi, "Cybersecurity in the modern world : Ethical Hacking," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 5, no. 9, September 2023.
- [30] ACM, "Association for Computing Machinery (ACM)," 2022.
- [31] P. Robinson, "Can PCI DSS 4.0 reverse the decline in compliance?," 2022.
- [32] A. Sharma, "The Role of Data Privacy Compliance in Safeguarding Trust - DATAVERSITY," DATAVERSITY, 29 September 2023. [Online]. Available: <https://www.dataversity.net/the-role-of-data-privacy-compliance-in-safeguarding-trust/>.
- [33] W. Kenton, "Memorandum of Understanding (MOU) Defined," 2 May 2023. [Online]. Available: <https://www.investopedia.com/terms/m/mou.asp>.

- [34] "An Exploration of the Ideologies of Software Intellectual Property: The Impact on Ethical Decision Making on JSTOR," jstor, [Online]. Available: <https://www.jstor.org/stable/25075433>.
- [35] National Academies Press eBooks, "Computers at Risk," 1991. [Online]. Available: <https://doi.org/10.17226/1581>.
- [36] Balbix, "8 Common Types of Cyber Attack Vectors and How to Avoid Them," BalBix, 2023.
- [37] C. H. L. N. a. I. K. Z. Alkhalil, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," Frontiers in computer science, 2021.
- [38] Rapid7, "What Is a Malware Attack? Definition & Best Practices," [Online]. Available: <https://rapid7.com/fundamentals/malware-attacks/#:~:text=A%20malware%20attack%20is%20a,command%20and%20control%2C%20and%20more..>
- [39] Jnguyen, "Ransomware Attack- What is it and How Does it Work?," Check Point Software, 5 June 2023. [Online]. Available: <https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/#:~:text=Ransomware%20is%20a%20malware%20designed,regain%20access%20to%20their%20files..>
- [40] Radware, "What is the Difference Between DoS and DDoS Attacks".
- [41] T. Stansfield, "Q3 2023 Phishing and Malware Report: Phishing and Malware Threats increase 173% and 110%," vade, 2023.
- [42] Sangfor Technologies, "A comprehensive List of Top Ransomware Attacks in 2023," Sangfor Technologies, 2023.
- [43] S. D. a. S. Rath, "A Retrospective on DDoS Trends in 2023 and Actionable Strategies for 2024," 2024.
- [44] Instat, "Statistika te regjisstrimeve ne arsim," Instat, Tirane, 2023.
- [45] CISA, "Iranian State Actors Conduct Cyber Operations Against the Government of Albania," CISA, 2022.
- [46] DOJ, "Thirty-six Defendants Indicted for Alleged Roles in Transnational Criminal Organization Responsible for More than \$530 Million in Losses from

- Cybercrimes," 7 February 2018. [Online]. Available: <https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible>.
- [47] Top Channel, "Fier Hacker arrested on international order," 13 February 2018. [Online]. Available: <https://top-channel.tv/english/fier-hacker-arrested-on-international-order/>.
- [48] J. Tidy, "Lapsus\$: GTA 6 hacker handed indefinite hospital order," BBC, 2023.
- [49] Cyber Safety Review Board, "Review of the Attacks Associated with LAPSUS\$ and Related Threat Groups," CISA, 2023.
- [50] N. P. a. L. Perkoy, "Social Engineering Toolkit — A systematic approach to social engineering," IEEE, 2011.
- [51] J. S. e. al., "Establishing a Traceability and Quality System for U.S. Ballistics Identification Using NIST SRM Standard Bullets and Cartridge Cases," pp. 53-55, 2012.