



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

**Strategic Threat Analysis of the M&S and Co-op
Campaign and a Full Penetration Test of ABCD Ltd**

Name: Dipkumar Hemantkumar patel

Student Id: 2535265

Course: MSc Cybersecurity and Digital Forensics

Module: Ethical Hacking

University: University of Wales, Trinity Saint David

TABLE OF CONTENTS

Abstract	3
1 · Introduction.....	3
2 · Task 1 — Strategic Threat Analysis: The M&S and Co-op Campaign.....	4
2.1 · Incident summary and timeline	4
2.2 · Adversary TTP mapping to MITRE ATT&CK	7
2.3 · Root cause and security-control failures	9
2.4 · Threat-actor profile and motive	10
2.5 · Detection and response analysis	11
2.6 · Strategic recommendations.....	12
2.7 · Synthesis and critical reflection.....	14
3 · Task 2 — Red Team Engagement: ABCD Ltd.....	15
3.1 · Rules of Engagement (RoE)	15
3.2 · Threat Emulation Plan	16
3.3 · Lab Environment Design.....	18
3.4 · Exploitation – Three Distinct Exploits	22
3.4.1 · Exploit A – Web Application Exploitation (VM-2).....	22
3.4.2 · Exploit B – Vulnerable Network Service (VM-2).....	25
3.4.3 · Exploit C – Windows 7 Target (VM-3).....	27
3.4.4 · Overall Evaluation of the Three Exploits	29
3.5 · Tools and Techniques.....	30
3.6 · Operational Execution, Containment and Safety	31
3.7 · Detection-Gap Analysis.....	35
5 · Conclusion	36
References.....	37

Abstract

This report comprises of two parts. The first section analyses the cyberattacks which faced Marks & Spencer (M&S) and the Co-operative Group (Co-op), in April 2025. It examines the incident timeline, threat actor reported, MITRE ATT&CK techniques used, security-control failures, and detection and response of both organisations. The essential safety guidelines on secure passwords, login processes, and why we need tough cybersecurity ought to be observed, according to the ESSDA.

The following part describes red-team engagement for a UK retail company called ABCD Ltd. The package consists of the Rules of Engagement, a Threat Emulation Plan, a virtual lab with three virtual machines, and three separate exploits. The security vulnerabilities found in the review in relation to the organisation are analysed and recommendation are provided to improve their security and reduce the risk of future attacks by this report.[8]

Scattered Spider and DragonForce are Using Ransomware to Attack Active Directory via Social Engineering.

1 · Introduction

Cyberattacks are more reliant on identity, genuine credentials, and operational flaws than over-dependence on software vulnerabilities. Given this state of affairs, organisations must assess not only their technical weaknesses but also their ability to detect, respond to and recover from realistic attack activity. Simulating attacker behavior and evaluating security controls across an end-to-end attack chain is paramount for this assessment known as red teaming and adversary emulation.

Cyber attacks targeting Marks and Spencer (M&S) and the Co-operative Group (Co-op) in Apr 2025 showcase how identity compromise can cause major operational disruption. According to public reports, social engineering as well as compromised credentials played an important role in the attacks. These incidents offer some insightful lessons regarding identity security, authentication access controls, network segmentation, and incident response. [8].

The report has been subdivided into two parts. Task 1, which is part of the project, critically analyses two incidents which are M&S and Co-op. The incident timeline, MITRE ATT&CK techniques, security-control failures, threat

actor profile, detection and response given in the report followed by strategic recommendations. The virtual laboratory design, penetration-testing activities, and detection-gap analysis are outlined as well as the Rules of Engagement and Threat Emulation Plan for ABCD Ltd. The assessment utilizes academic literature, government guidance, industry reports, and evidence generated in a practical laboratory exercise, and sources are referenced using the IEEE style.

2 · Task 1 — Strategic Threat Analysis: The M&S and Co-op Campaign

2.1 · Incident summary and timeline

- In April 2025, two UK retailers Marks & Spencer (M&S) and Co-op were affected by related cyber attacks. M&S faced a ransomware assault that interfered with contactless payments, Click & Collect as well as online shopping. Also, Co-op underwent a cyber attack disrupting certain aspect of its IT systems. According to the UK Cyber Monitoring Centre (CMC), the incidents represented a single cyber event as all of them were associated with the same threat actor and utilized similar tactics, techniques and procedures (TTPs) design. According to the CMC, the overall financial impact was £270 million to £440 million [1][8].
- **Discovery**
- In April 2025, M&S discovered a cyber incident after experiencing significant service disruptions identified by internal security monitoring.
- **Initial access**
- According to reports, the M&S network was breached by the attackers who accessed the internal system of a third-party IT help desk in February 2025. Acquiring privileged credentials allowed access to internal systems without a technical vulnerability being exploited. The attack stayed hidden for a few weeks and only became visible in April 2025.
- **Privilege escalation**
- The attackers accessed an administrator account after stealing log-in credentials to enter the network. They traversed the network and commandeered key systems. Installing ransomware allowed them to halt various M&S services. The incident illustrates a lack of security to protect the administrator account of the company.

- **Containment**

In order to restrict the spread of the attack, M&S halted online shopping. The cyber security experts and the NCSC were consulted by the company for help. To curtail the damage, Co-op also disabled elements of its IT systems to defend its IT net.

- **Public disclosure**

On April 22, 2025, M&S publicly declared the cyberattack. The firm contacted clients and investors over the incident and the bank later confirmed that customers' data was stolen. Co-op confirmed its cyber attack, providing updates on the company's response and recovery.

- **Recovery**

After rebuilding its affected systems, M&S gradually restored its online services. The firm also reset customer passwords and keep monitoring its network for any further threats. The organization not only recovered its systems but also improved its security.

The below timeline compiles public reporting and official statements – where a date is reported rather than confirmed this is stated.

Date (2025)	Event	Phase
c. February	Reported earliest suspected initial access to M&S, implying a period of undetected dwell time [2][3]	Initial access (suspected)
19–21 April	M&S disruption becomes visible: contactless payments and Click & Collect fail over the Easter weekend [2]	Impact begins

Date (2025)	Event	Phase
22 April	M&S discloses the incident to the London Stock Exchange [2]	Public disclosure
24 April	DragonForce ransomware reportedly deployed against M&S VMware ESXi hosts, encrypting e-commerce, payment and logistics VMs [3]	Impact / encryption
25 April	M&S suspends online and app ordering [2]	Containment
Late April	Co-op detects intrusion and proactively shuts down parts of its IT estate; attack linked to Scattered Spider [2]	Parallel incident
13 May	M&S confirms theft of customer personal data; up to ~9.4m online customers potentially affected; password resets prompted [2]	Data-theft confirmation
20 June	CMC classifies M&S and Co-op as a single combined cyber event, £270m–£440m impact [1]	Assessment
10 July	Four individuals arrested in connection with the M&S, Co-op and Harrods attacks [3]	Law enforcement
Into July	M&S continues phased restoration of online services [2]	Recovery

Figure 1 (below) renders the same sequence as an attack-flow diagram.

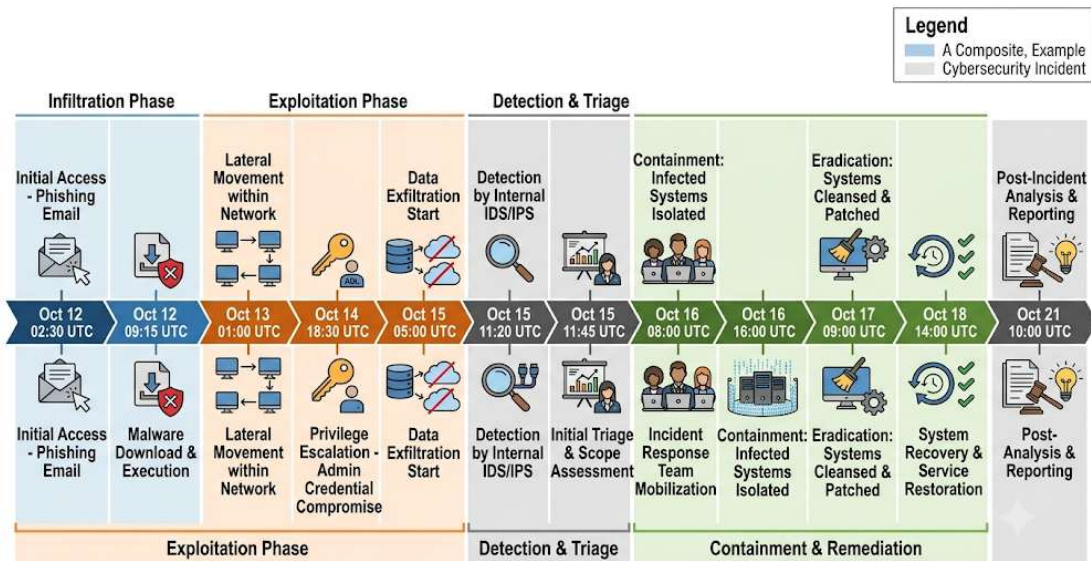


Figure 1. Consolidated Incident Timeline (see Appendix A for source mapping)

2.2 · Adversary TTP mapping to MITRE ATT&CK

According to media reports, threat actors Scattered Spider working in co-operation with Dragon Force ransomware operation were behind the cyber attacks of M&S and Co-op [3][4][5]. Cybercriminals mainly attacked user identities and not software vulnerabilities. Using social engineering, they gained access and stole admin credentials, later moving laterally and deploying ransomware. The MITRE ATT&CK framework specifies the tactics and techniques used at each stage of the attack. According to public reports, some of the techniques indicated below are confirmed while others are based on the known behaviour of the threat actor.

Tactic	Technique (ID)	Justification / evidence
Reconnaissance	Gather Victim Identity Info (T1589)	Actor profiles staff and outsourced help-desk processes to make impersonation credible [4][5].
Resource Development	Acquire Infrastructure: Domains (T1583.001)	Scattered Spider is documented registering look-alike domains for credential harvesting [4][5].

Tactic	Technique (ID)	Justification / evidence
Initial Access	Phishing: Spearphishing Voice / Vishing (T1566.004)	Attackers phoned the outsourced help desk (reportedly TCS) impersonating IT staff to obtain access [2][3][6].
Initial Access	Valid Accounts: Domain Accounts (T1078.002)	Help-desk-assisted password/MFA resets yielded legitimate domain credentials, bypassing the perimeter [3][6].
Credential Access	MFA Request Generation / bypass (T1621)	MFA was circumvented via help-desk reset rather than a technical MFA flaw [3][6].
Discovery	Account & Domain Discovery (T1087 / T1482)	Reconnaissance of Active Directory to locate privileged accounts and trust structure [3][4].
Credential Access	OS Credential Dumping: NTDS (T1003.003)	Exfiltration of the domain controller NTDS.dit file, exposing all domain credential hashes [3].
Lateral Movement	Remote Services / Use of Legitimate Admin Tools (T1021)	Actors moved laterally with legitimate administrative tooling to avoid raising alerts [3].
Defense Evasion	Living-off-the-Land / valid accounts (T1078)	Use of built-in tooling and stolen credentials reduced malware footprint and detection [3][4].
Collection / Exfiltration	Data from Information Repositories; Exfiltration (T1213 / TA0010)	Customer personal data was staged and exfiltrated prior to encryption (double extortion) [2].

Tactic	Technique (ID)	Justification / evidence
Impact	Data Encrypted for Impact (T1486)	DragonForce ransomware encrypted VMware ESXi-hosted virtual machines [3].
Impact	Service Stop / Inhibit Recovery (T1489 / T1490)	Encryption of e-commerce, payment and logistics systems halted trading operations [2][3].

The mapping demonstrates that the attacker opted for attacks on the identity instead of an attack on software vulnerability. They sidestepped many traditional security measures by employing social engineering and stealing credentials. After gaining access to the network, they traversed various systems, stole sensitive information and deployed ransomware. This shows the need to implement strong identity management, phishing-resistant MFA, monitor the network, and employee training[7].

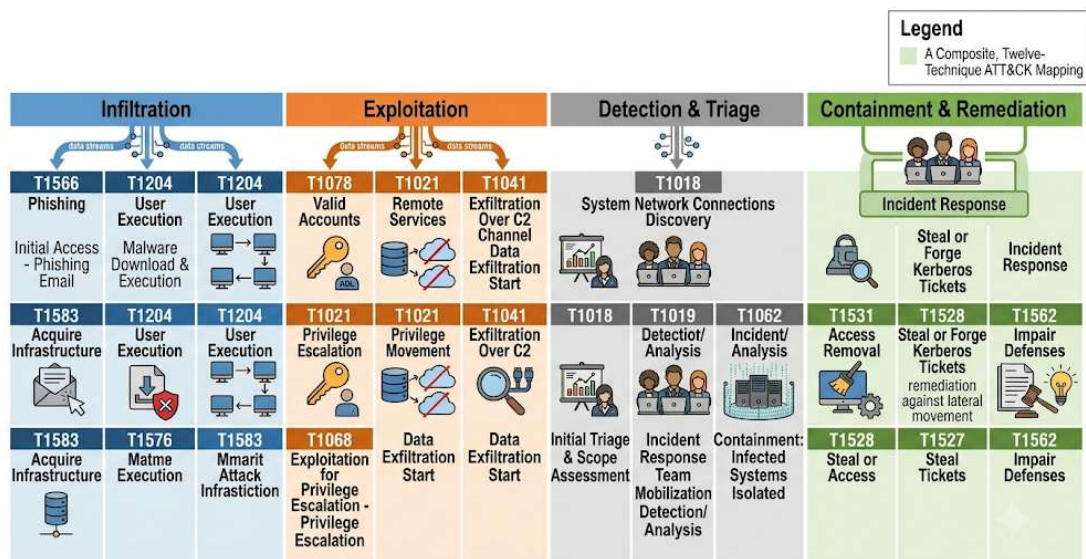


Figure 2: Twelve-technique ATT&CK mapping across the attack chain.

2.3 · Root cause and security-control failures

The main disclosed flaw of the attack was not a security flaw, but rather flaws in identity verification and security processes. Reports indicate that attackers contacted the IT help desk to convince personnel to reset user accounts' passwords or multi-factor authentication (MFA) settings. This gave access without the need to exploit a software bug. An outsourced IT help desk also

increased the attack surface. Third-party personnel became a target for social engineering [2][6].

After the first compromise, weaknesses in security controls were evident. Active Directory protection and monitoring was inadequate. As per some recent reports, the NTDS.dit database was accessed by hackers which has password hashes of domain users. If confirmed, this would indicate weaknesses in the protection of privileged accounts and the monitoring of domain controllers [3]. Secondly, insufficient network separation allowed movement between systems and increased the potential impact of a successful compromise [3]. The consolidation of online shopping, payment, and logistics services within the same VMware ESXi environment creates an increased level of potential business impact upon successful ransomware deployment.

As per the overall situation, incidents occur due to weaknesses in identity verification, privileged access, network separation, and the protection of critical infrastructures can combine to enable an attacker to gain entry. Consequently, the discoveries advocate for more robust identity verification, tighter administrator access controls, improved network segmentation, and enhanced monitoring of critical systems.

2.4 · Threat-actor profile and motive

The main disclosed flaw of the attack was not a security flaw, but rather flaws in identity verification and security processes. Reports indicate that attackers contacted the IT help desk to convince personnel to reset user accounts' passwords or **multi-factor authentication (MFA) settings**. This gave access without the need to exploit a software bug. An outsourced IT help desk also increased the attack surface. Third-party personnel became a target for social engineering [2][6].

After the first compromise, weaknesses in security controls were evident. Active Directory protection and monitoring was inadequate. As per some recent reports, the **NTDS.dit** database was accessed by hackers which has password hashes of domain users. It was if confirmed, weaknesses in the protection of privileged accounts and the monitoring of domain controllers [3]. In the second place, insufficient separation between the networks allowed for movement between systems and contributed to access to the [3]. The consolidation of online shopping, payment, and logistics services within the same VMware **ESXi**

environment creates an increased level of potential business impact upon successful ransomware deployment.

As per the overall situation, incidents occur due to weaknesses in identity verification, privileged access, network separation, and the protection of critical infrastructures can combine to enable an attacker to gain entry. Consequently, the discoveries advocate for more robust identity verification, tighter administrator access controls, improved network segmentation, and enhanced monitoring of critical systems.

2.5 · Detection and response analysis

Cyber attack was unnoticed in the early stages. It is reported that the attackers convinced the IT help desk to reset victims' passwords and multi-factor authentication (MFA) to get valid user accounts.

Due to the involvement of real identities, as opposed to commonly malware infections or software exploits, conventional security controls may have had fewer indicators to raise alerts.

According to reports, the attackers may have accessed the system in February 2025, although the intrusion was not detected until April 2025 [2][3]. The period of time may be several weeks. Throughout this time, hackers are said to have gained access to Active Directory, obtained credentials, traversed the environment, and ultimately deployed Dragon Force ransomware. This delay highlights deficiencies in the identification of identity-based post-compromise activity. Further opportunities for earlier detection could have been identified through monitoring unconventional administrator logins, help-desk password and MFA resets, Active Directory activity, and anomalous lateral movement.

Following discovery of the intrusion, the organisations implemented broader containment and incident-response measures. M&S reached out to the London Stock Exchange and cut off affected systems as a precaution. The firm engaged with security professionals from CrowdStrike, Microsoft, and Fenix24 and received assistance from the NCSC, the Metropolitan Police, and the National Crime Agency [2]. Co-op also restricted the impact by shutting down portions of its IT environment after discovery of suspicious activity [2].

According to the evidence provided, early detection was a serious weakness, containment and external coordination were important parts of the later responses. Nevertheless, it is difficult to determine from public reporting the

extent to which particular monitoring controls failed. This restriction strengthens the call for richer identity and Active Directory telemetry; in particular, to deal with unusual account activity, privileged access, and help-desk authentication changes.

2.6 · Strategic recommendations

The recommendations below are prioritised according to their ability to reduce the attack paths identified in the M&S and Co-op incidents, together with their relative implementation effort.

Priority	Recommendation	Addresses	Effort / cost
1	Harden help-desk identity verification through mandatory callback procedures, management approval for privileged resets, removal of knowledge-based verification, and use of pre-registered contact details.	Vishing (T1566.004), Valid Accounts (T1078)	Low
2	Deploy phishing-resistant MFA, such as FIDO2 security keys, for privileged and remote access, reducing reliance on SMS and push-based authentication.	MFA bypass (T1621)	Low–Medium
3	Enforce Active Directory tiering and privileged-access management, while strengthening protection and monitoring of domain-controller access.	Credential Access (T1003.003)	Medium
4	Implement network micro-segmentation and Zero Trust controls between corporate, e-commerce, and virtualisation environments to restrict lateral movement.	Lateral Movement (T1021)	High
5	Integrate identity and domain-controller telemetry into the SIEM, including anomalous authentication, help-desk	Detection gaps	Medium

Priority	Recommendation	Addresses	Effort / cost
	resets, privileged access, and suspicious activity involving critical infrastructure.		
6	Strengthen third-party and supply-chain security through contractual security requirements, access controls, and assurance of outsourced IT functions.	Third-party risk	Medium
7	Rehearse ransomware response and validate immutable, offline backups of critical systems to improve recovery following successful encryption.	Impact (T1486/T1490)	Medium

Analysis

The highest priority is strengthening **help-desk identity verification** because the reported initial access relied on social engineering and account recovery processes. Stronger verification and controlled approval of privileged resets would directly reduce the likelihood of an attacker obtaining legitimate credentials through impersonation [3][6].

Phishing-resistant MFA is the second priority because it provides stronger protection against credential-based attacks than SMS or push-based authentication. However, MFA alone would not address an attacker who has already obtained authorised access through a compromised account-recovery process. It should therefore complement, rather than replace, stronger help-desk controls.

Active Directory hardening and network segmentation address the later stages of the attack chain. Privileged-access controls can limit the consequences of credential compromise, while segmentation can restrict movement between corporate, e-commerce, and virtualisation environments. These measures require greater implementation effort but provide protection even when initial access controls fail.

The rest of the recommendations deal with detection, third-party risk and recovery. The chance for earlier detection is increased through improved identity and domain-controller telemetry, and stronger assurance of outsourced

IT functions reducing exposure resulting from third-party access. Rehearsed response procedures and immutable offline backups may not prevent compromise, but they can limit operational impact and support recovery following ransomware deployment [2][3].

2.7 · Synthesis and critical reflection

The incidents at M&S and Co-op show that essential business disruption doesn't necessarily require the use of complex software. The use of social engineering and compromised identities indicates that weaknesses in people, the authentication process, and access-control procedures provide an effective route into an organisation. Cyber controls and human controls are two sides of the same coin. We need to incorporate human controls and procedural controls as cyber security controls instead of only relying on technical security controls.

The events also suggest that limiting the consequences of the first compromise is essential. Once attackers accessed the enterprise, weaknesses in the company's identity protections networks separations and monitoring allowed them to move against critical business systems. This means that if the malware attack had stronger identity check, better segmentation and earlier detection of anomalous activity, the impact could be lesser.

The key strategic insight is that security investment must address the whole attack chain, not just more security technology. While preventing compromise of identities is essential, organisations must also plan for the eventuality that some measure or control might fail, hence limiting lateral movement, detecting suspicious activity and sustaining effective capability to recover. The results discussed above lead us on to **Task 2** which is a practical evaluation. This evaluation studies how weaknesses can be chained into end-to-end attack path in a controlled overall virtual environment.

3 · Task 2 — Red Team Engagement: ABCD Ltd

The task presents a red-team assessment of a virtualised laboratory emulating ABCD Ltd, a UK-based medium-sized online retailer. The goal is to assess the organisation's ability to prevent, detect and respond to a credible attack chain.

The evaluation applies lessons learned from Task 1, particularly initial access and credential use, privilege escalation, lateral movement and data access. The assessment includes Rules of Engagement, a Threat Emulation Plan based on MITRE ATT&CK, a laboratory with three target virtual machines serving

different roles, and three distinct exploits targeting different services or attack surfaces. Screenshots, command output, logs and other practical evidence are used to support the findings [7].

3.1 Rules of Engagement (RoE)

The Rules of Engagement for the red-team assessment of ABCD Ltd cover the scope and objectives of the assessment, permitted and prohibited activities, communication procedures, safety controls and evidence-handling requirements. Client authorisation is assumed for this simulated engagement, and all testing is restricted to the laboratory environment.

Clause	Definition
Client / Sponsor	ABCD Ltd, represented by the designated authorising officer.
Engagement type	Objective-based red-team and threat-emulation exercise conducted within the authorised laboratory.
Primary objective	Determine whether an attacker can progress through an attack chain and access an agreed sample of synthetic customer data under controlled conditions.
In scope	The isolated laboratory subnet and the three target VMs defined in Section 3.3.
Explicitly excluded	Production systems, public internet hosts, real customer data, denial-of-service activity and destructive ransomware execution.
Permitted techniques	Web application testing, authorised credential testing, vulnerability exploitation, privilege escalation, lateral movement, approved LOLBin techniques and controlled C2 activity within the laboratory.
Time window	Testing is restricted to the agreed assessment period, with significant activity recorded in the evidence log.
Safe-word / kill switch	The word “ BLACKOUT ” immediately terminates offensive activity and initiates rollback procedures.
Escalation and communications	Unexpected activity, genuine data exposure or loss of laboratory control is reported immediately through the designated communication channel.
Legal / ethical basis	Written authorisation is assumed, and testing is restricted to the authorised laboratory with no real personal data processed.

Evidence handling	Logs, screenshots, packet captures and other evidence are stored securely and sanitised before inclusion in the report.
Sign-off	ABCD Ltd Authorising Officer: _____ Red Team Specialist: _____ Date: _____ _____

The isolated laboratory boundary prevents assessment activities from affecting external infrastructure. Snapshots help maintain the stability of the virtual machines, while the kill switch and rollback procedures support safe recovery and evidence preservation.

3.2 Threat Emulation Plan

The red-team assessment will be conducted against the ABCD Ltd virtual laboratory according to the Threat Emulation Plan. The attack pattern identified in Task 1, including initial access, credential use, privilege escalation, lateral movement and data access, is applied. However, the practical laboratory does not contain a Windows Active Directory domain or a human IT help desk, so these elements are not directly reproduced. Instead, controlled exploitation of deliberately vulnerable web and network services is conducted within the isolated laboratory.

The engagement is considered successful when the following objectives are achieved:

- **Initial access:** Gain controlled access to the vulnerable web application in the OWASP Broken Web Apps environment.
- **Further exploitation:** Identify and exploit a second distinct vulnerability on an authorised laboratory system where technically appropriate.
- **Privilege escalation or lateral movement:** Determine whether initial access can be used to obtain higher privileges or access another authorised target.
- **Data access:** Where the attack path permits, access the agreed synthetic data on the Windows 7 test system.
- **Evidence collection:** Gather screenshots, command output, logs and other telemetry to verify the assessment findings.
- **Detection assessment:** Identify security controls that detect the tested activities and document observable detection gaps [7].

These criteria provide a framework for evaluating the three distinct exploits and determining whether they can contribute to a wider attack path within the laboratory.

Attack Sequence and MITRE ATT&CK Mapping

Phase	Planned action	MITRE ATT&CK technique
1. Reconnaissance	Identify live hosts, open ports, services and application versions within the isolated laboratory.	Active Scanning (T1595)
2. Initial Access	Assess the OWASP Broken Web Apps environment for a deliberately vulnerable web application and test the confirmed vulnerability.	Exploit Public-Facing Application (T1190)
3. Execution	Execute controlled commands on a successfully compromised system where permitted by the confirmed vulnerability.	Command and Scripting Interpreter (T1059)
4. Credential / Access Assessment	Assess the compromised environment for authorised credentials, exposed configuration information or other relevant access paths.	Unsecured Credentials (T1552), only if demonstrated
5. Lateral Movement	Test whether authorised access can be used to reach another laboratory system, such as Metasploitable or Windows 7.	Valid Accounts (T1078) / Remote Services (T1021), if demonstrated
6. Privilege Escalation	Assess the compromised target for a confirmed local privilege-escalation weakness.	Exploitation for Privilege Escalation (T1068), only if confirmed
7. Collection / Data Access	Access the agreed synthetic customer data without modifying or deleting it.	Data from Local System (T1005), or another technique confirmed by practical evidence
8. Completion and Recovery	Stop testing, preserve evidence and restore the laboratory where required. No destructive activity is performed.	N/A – safety requirement

3.3 Lab Environment Design

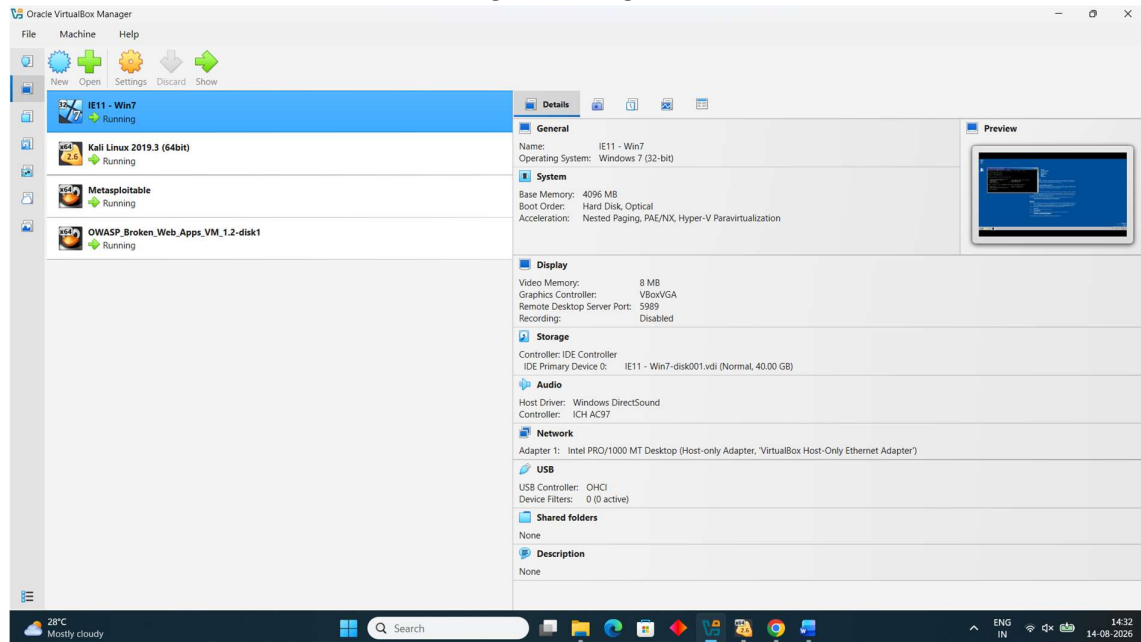
The main systems of ABCD Ltd have been represented by a virtual laboratory for a small retail organisation. Kali Linux acts as the red-team machine, supported by three target virtual machines with different roles and attack surfaces. This configuration meets the requirement

for three target VMs representing different systems and provides a controlled environment for the security assessment.

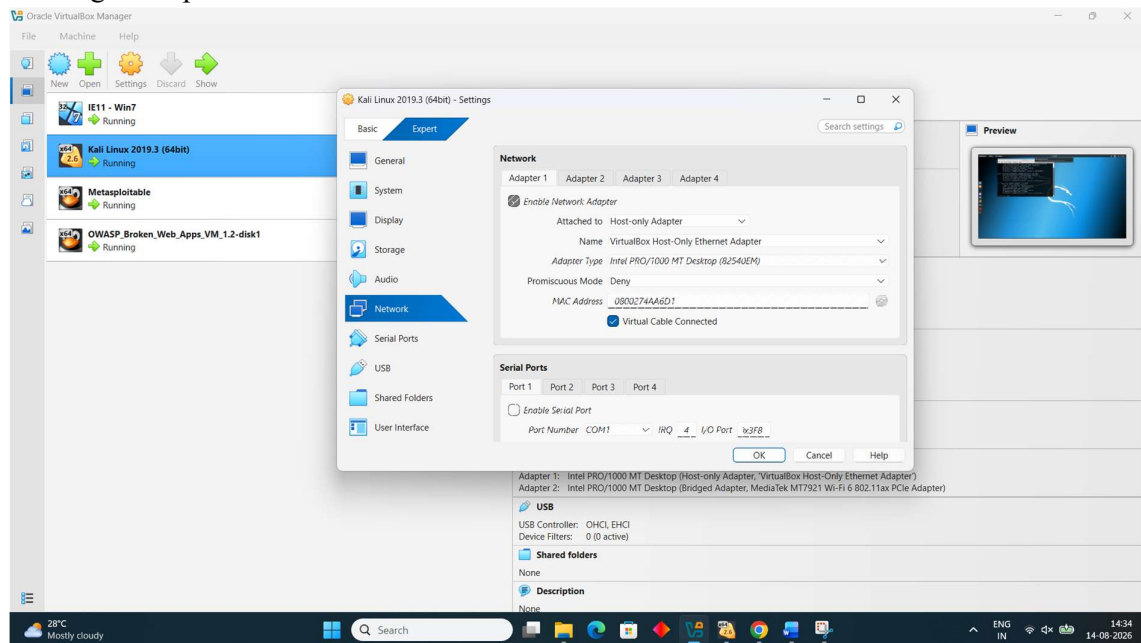
VM	Role / Configuration	IP Address	Main Services	Purpose
VM-1	OWASP Broken Web Apps Linux virtual machine	192.168.56.101	HTTP/HTTPS and deliberately vulnerable web applications	Primary web-application attack surface and initial-access target.
VM-2	Metasploitable Linux virtual machine	192.168.56.103	Multiple intentionally vulnerable network services	Vulnerable service environment for controlled exploitation and further attack-path testing.
VM-3	Windows 7 IE11 virtual machine containing synthetic test data	192.168.56.104	Windows networking services and authorised test services	Internal Windows endpoint providing the controlled environment for the final data-access objective.
Kali Linux	Red-team/attacker machine	192.168.56.102	Nmap, Burp Suite, Metasploit and other approved assessment tools	Platform for reconnaissance, exploitation and controlled post-exploitation activities.

- The three target machines provide different attack surfaces, with **VM-1** hosting vulnerable web applications, **VM-2** providing vulnerable network services, and **VM-3** representing an internal Windows endpoint containing synthetic test data. This separation allows the assessment to determine whether weaknesses across different systems can contribute to an attack path.
- **Kali Linux**, serving as the assessment machine, and the three target VMs representing the ABCD Ltd infrastructure operate on the same isolated **Host-only network**.

Screenshot 1: VirtualBox Manager showing all four machines.



- **Screenshot 2:** Network adapter settings showing Host-only networking and no NAT or bridged adapter used for the assessment.



- **Screenshot 3:** IP configuration from each VM showing the actual laboratory addresses.

```
OWASP_Broken_Web_Apps_VM_12-disk1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

You can administer / configure this machine through the console here, by SSHing
to 192.168.56.101, via Sshs at 192.168.56.101, or via phpmyadmin at
http://192.168.56.101/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbun".

root@owaspbun:~# ifconfig
No command 'ifconfig' found, did you mean:
Command 'ifconfig' from package 'net-tools' (main)
ifconfig: command not found
root@owaspbun:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a1:96:fe
          inet addr: 192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8a:320/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:38 errors:0 dropped:0 overruns:0 frame:0
          TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7510 (7.3 KB)  TX bytes:6719 (6.7 KB)

lo        Link encap:Local Loopback
          inet addr: 127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:42 errors:0 dropped:0 overruns:0 frame:0
          TX packets:42 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:14609 (14.6 KB)  TX bytes:14609 (14.6 KB)

root@owaspbun:~# "12"

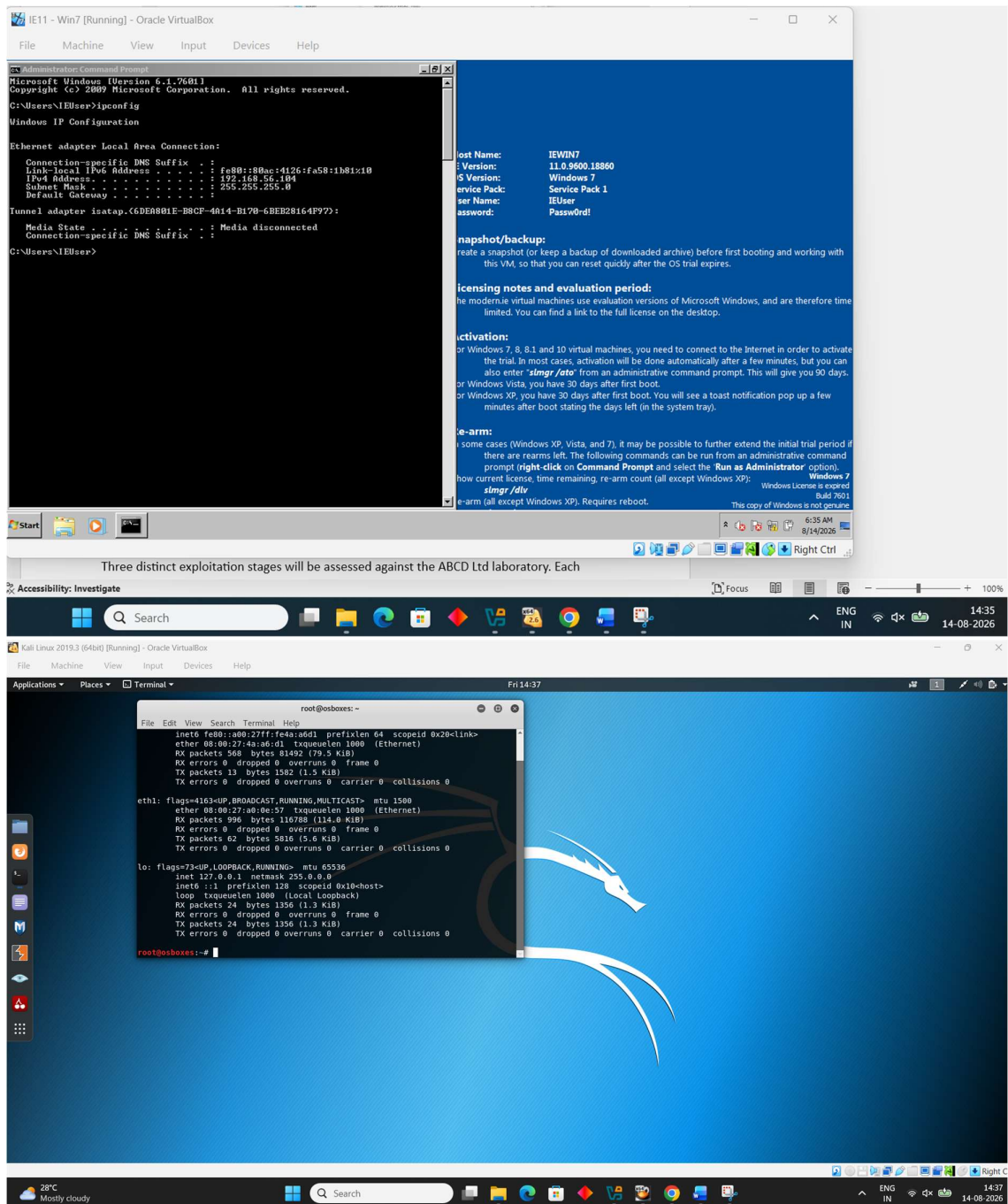
Metasploitable (Running) - Oracle VM VirtualBox
28°C Mostly cloudy 14:36 14-08-2026

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:8a:03:20
          inet addr:192.168.56.103  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8a:320/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:98 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15659 (15.2 KB)  TX bytes:3638 (3.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$ _

28°C Mostly cloudy 14:36 14-08-2026
```



- **Screenshot 4:** Connectivity test between Kali Linux and the three target VMs.

```

Kali Linux 2019.3 (64bit) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Applications Places Terminal
File Edit View Search Terminal Help

Fri 14:40
root@osboxes: ~

eth0: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 01<host>
    loop txqueuelen 1000 (local loopback)
    RX packets 24 bytes 1356 (1.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 1356 (1.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 01<host>
    loop txqueuelen 1000 (local loopback)
    RX packets 24 bytes 1356 (1.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 1356 (1.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@osboxes:~# ping -c 4 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data:
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=1.83 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.68 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.454 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.747 ms

--- 192.168.56.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3038ms
rtt min/avg/max/mdev = 0.454/3.159/9.598/3.753 ms
root@osboxes:~# ping -c 4 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data:
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=29.9 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=9.59 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=11.6 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=20.6 ms

--- 192.168.56.103 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 9.598/17.915/29.873/8.864 ms
root@osboxes:~# ping -c 4 192.168.56.104
PING 192.168.56.104 (192.168.56.104) 56(84) bytes of data:
64 bytes from 192.168.56.104: icmp_seq=1 ttl=128 time=11.0 ms
64 bytes from 192.168.56.104: icmp_seq=2 ttl=128 time=1.02 ms
64 bytes from 192.168.56.104: icmp_seq=3 ttl=128 time=0.938 ms
64 bytes from 192.168.56.104: icmp_seq=4 ttl=128 time=1.09 ms

--- 192.168.56.104 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 0.938/3.505/10.970/4.310 ms
root@osboxes:~#

```

Assessment of the Laboratory Design

- The main benefit of the design is the separation of attack stages across different systems. This allows the assessment to determine whether compromising one service can provide a pathway to another system and supports evaluation of the required multi-stage attack chain.
- Overall, the laboratory provides a controlled and observable environment for collecting evidence of attack-chain activity without affecting external infrastructure.

3.4 Exploitation – Three Distinct Exploits

The ABCD Ltd laboratory was assessed using three distinct exploitation scenarios, each targeting an authorised VM, service or attack surface defined in the Threat Emulation Plan. For each exploit, the confirmed vulnerability, method, evidence, result and security impact are considered. The technical detail is limited to what is required to demonstrate and evaluate the practical findings.

3.4.1 Exploit A – Web Application Exploitation (VM-2)

Target: VM-2 – Metasploitable

Target IP: 192.168.56.103

Attack type: Web application exploitation

MITRE ATT&CK: Exploit Public-Facing Application (T1190)

Precondition:

The Metasploitable VM was reachable through the isolated Host-only network and exposed deliberately vulnerable web services.

Vulnerability:

Service enumeration identified the vulnerable DVWA web application and its command-execution functionality. The vulnerability was verified before exploitation.

Method:

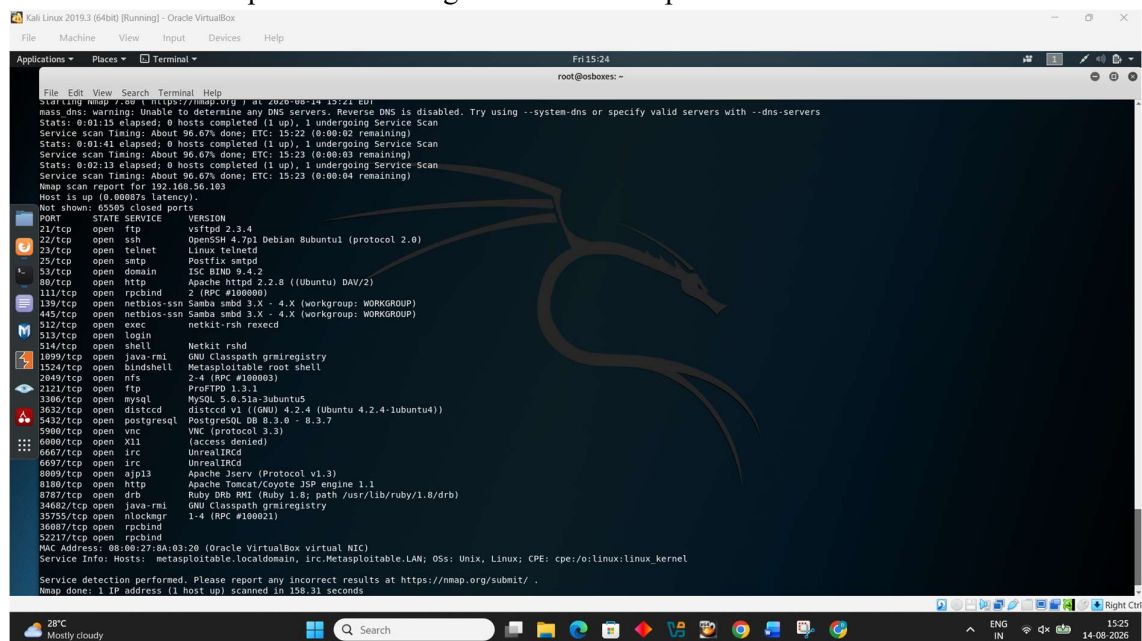
Kali Linux was used to enumerate the target and identify exposed services. The DVWA command-execution function was then tested in the authorised laboratory environment. No destructive activity was performed [9].

Example reconnaissance command:

```
nmap -sV -p- 192.168.56.103
```

Evidence:

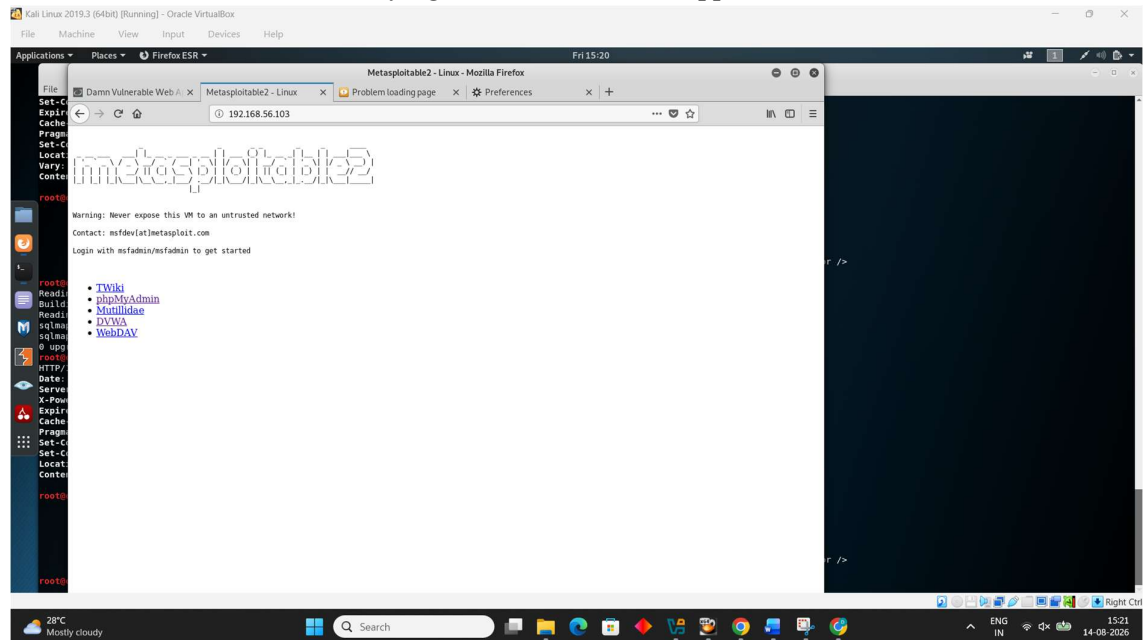
- **Screenshot 5:** Nmap results showing the services and ports identified.



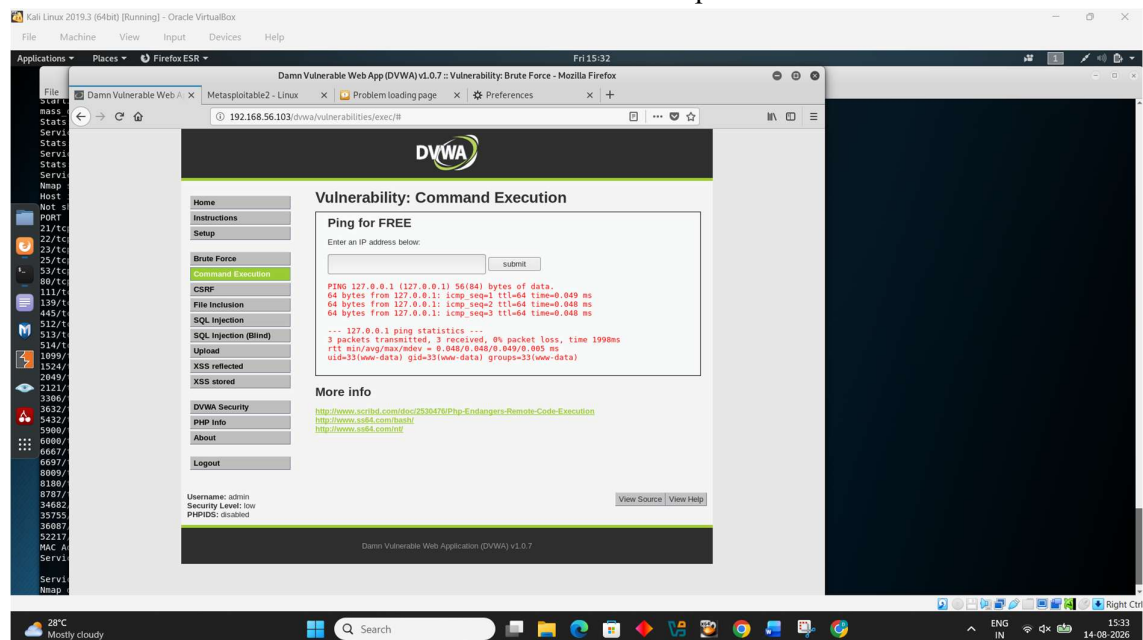
```
root@kali:~# nmap -sV -p- 192.168.56.103
Nmap scan report for 192.168.56.103
Host is up (0.0007s latency).
Not shown: 65535 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC BIND 9.4.2
80/tcp    open  http     Apache/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 rshexec
513/tcp   open  login    netkit-rshd
514/tcp   open  shell    Netkit rshd
1099/tcp  open  java-rmi GNU Classpath gmrregistry
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
3632/tcp  open  distccd  distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc      Apache Xserv (Protocol v1.3)
8080/tcp  open  ajp13    Apache Tomcat/Coyote JSP engine 1.1
8180/tcp  open  drb      Ruby DRB RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
34082/tcp open  java-rmi GNU Classpath gmrregistry
35755/tcp open  nlockmgr 1-4 (RPC #100021)
36087/tcp open  rpcbind
5221/tcp  open  rpcbind
MAC Address: 08:00:27:8A:03:20 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: 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 158.31 seconds
```

- **Screenshot 6:** Evidence identifying the vulnerable web application/version.



- **Screenshot 7:** Evidence of successful or unsuccessful exploitation.



Result

- The command-injection test on DVWA at **192.168.56.103** successfully executed an operating-system command. The output indicated that **www-data** was the execution context (**UID 33, GID 33**). This demonstrates web-server-level access rather than root or administrator-level access.
- **Analysis**
- The ability to execute operating-system commands through the vulnerable web function provides an initial access vector to the web server. However, the evidence

demonstrates only www-data access and does not establish system-level compromise, privilege escalation, lateral movement or access to other laboratory systems. Further testing would be required to determine whether this foothold could support progression through the authorised attack path.

3.4.2 Exploit B – Vulnerable Network Service (VM-2)

Target: VM-2 – Metasploitable2

Target IP: 192.168.56.103

Attack type: Network-service exploitation

Service: FTP

Port: 21/tcp

Detected version: vsFTPD 2.3.4

MITRE ATT&CK: Exploitation for Client Execution (T1203)

Precondition:

The isolated Host-only network allowed access to VM-2, where Nmap identified an FTP service on TCP port 21 running **vsFTPD 2.3.4**.

Vulnerability:

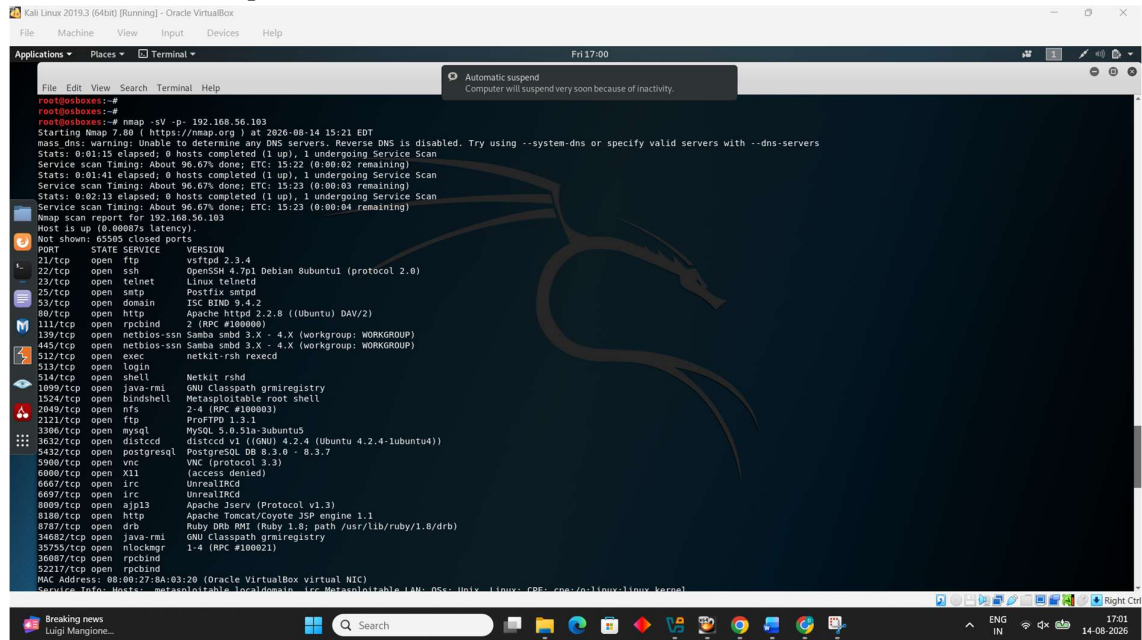
Metasploitable2 contained a deliberately vulnerable version of **vsFTPD 2.3.4**. Controlled testing confirmed that the backdoor could be triggered to obtain a shell.

Method:

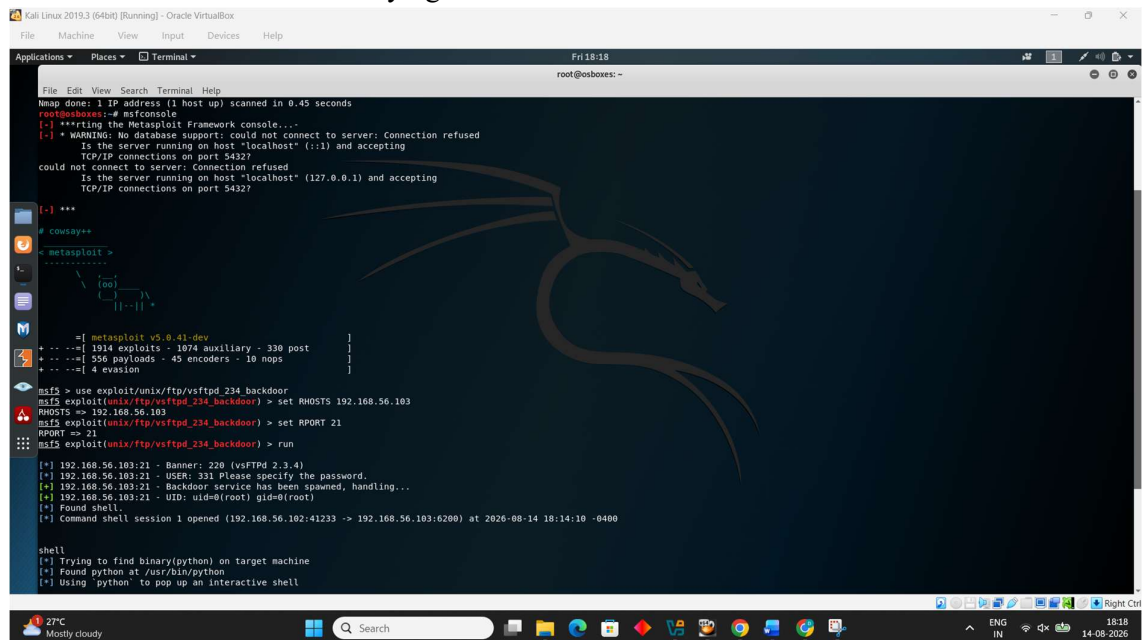
Nmap was used to identify the FTP service and version. The Metasploit Framework was then used from Kali Linux to test the vsftpd_234_backdoor module against 192.168.56.103. The first attempt did not establish a session; a subsequent attempt detected the open backdoor listener and successfully established a command shell.

Evidence:

- **Screenshot 8:** Nmap/service enumeration.



- **Screenshot 9:** Evidence identifying the vulnerable service.



- **Screenshot 10:** Evidence of the exploitation result.

```

msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.56.103:21 - Banner: 220 (vsftpd 2.3.4)
[*] 192.168.56.103:21 - USER: 331 Please specify the password.
[*] 192.168.56.103:21 - Backdoor service has been spawned, handling...
[*] 192.168.56.103:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.102:41233 -> 192.168.56.103:6200) at 2020-08-14 18:14:10 -0400

shell
[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using 'python' to pop up an interactive shell

sh-3.2#
sh-3.2# ls
ls
bin  dev  initrd  lost+found  nohup.out  root  sys  var
boot  etc  initrd.img  media  opt  sbin  tmp  vmlinuz
cdrom  home  lib  mnt  proc  srv  usr
sh-3.2# cd usr
cd usr
sh-3.2# ls
ls
X11R6  bin  games  include  lib  lib64  local  sbin  share  src
sh-3.2#

```

Result

- The VM-2 backdoor at **192.168.56.103** was successfully exploited. Metasploit established **Command Shell Session 1**, returning:
- uid=0(root) gid=0(root)
- The successful execution of directory-listing and navigation commands confirmed root-level access to the Metasploitable2 host.
- **Examination**
- The most serious verified result among the three exploits was the vulnerable network service providing root-level access to the host. The vsFTPD attack achieved the highest available privilege level on the Linux system, unlike the DVWA exploit, which provided only www-data access.
- The finding demonstrates how exploitation of a single vulnerable network service can result in complete host compromise. An attacker with root access could access system files, credentials and application data available to the operating system. In a corporate environment, this level of access could support further reconnaissance and potentially enable lateral movement.

3.4.3 Exploit C – Windows 7 Target (VM-3)

Target: VM-3 – Windows 7

Target IP: 192.168.56.104

Attack type: SMB/file-share access assessment

Precondition:

VM-3 was connected to the isolated Host-only network at 192.168.56.104 and provided the deliberately configured **CustomerData** SMB share for authorised testing.

Vulnerability:

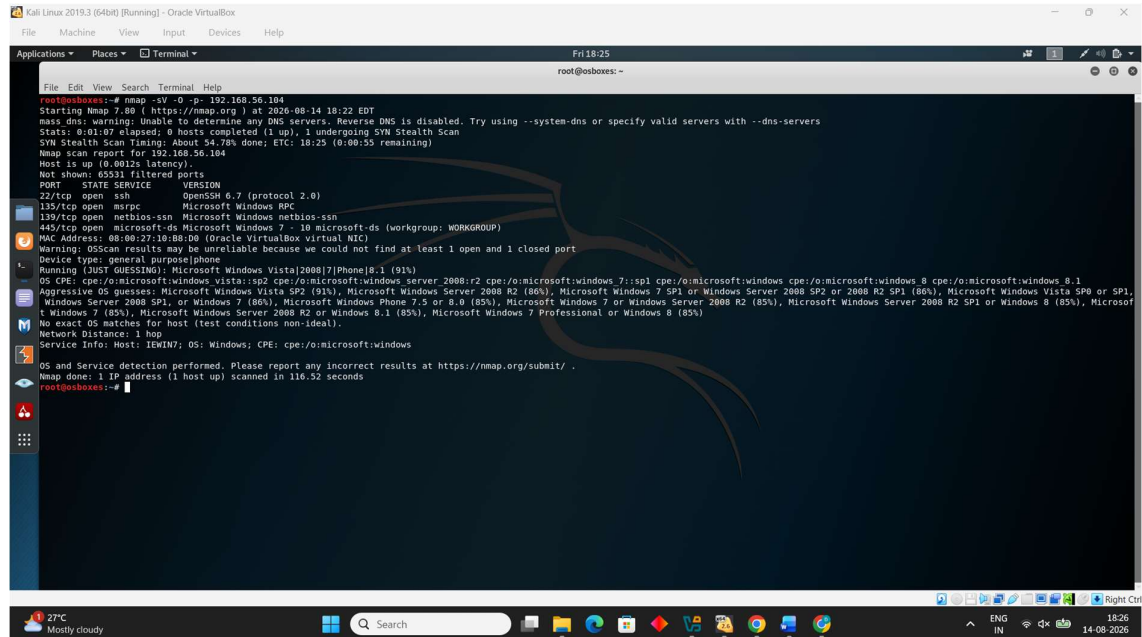
The CustomerData share had excessive permissions that allowed the authorised labtest account to access synthetic customer data. This represented a weakness in access control and least-privilege enforcement.

Method:

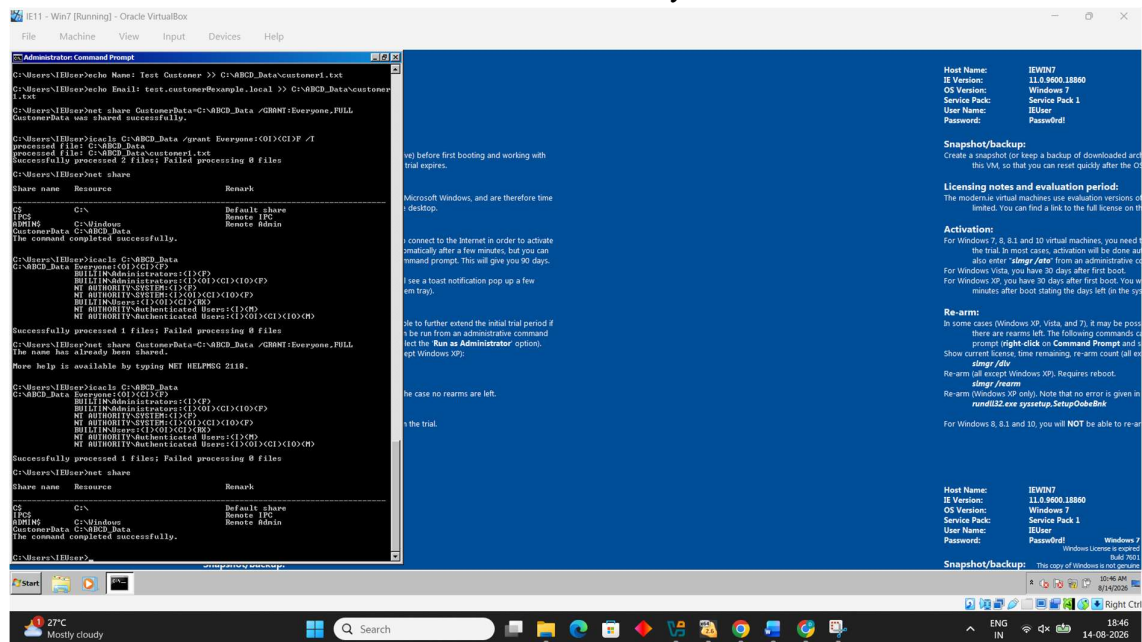
Kali Linux was used to assess the Windows 7 SMB services and access the authorised share using smbclient. The CustomerData share was enumerated, and the customer1.txt test file was retrieved without modifying or deleting the data.

Evidence:

- **Screenshot 11: Windows 7 service/port enumeration.**



- **Screenshot 12: Evidence of the confirmed vulnerability.**



- **Screenshot 13:** Evidence of successful or unsuccessful exploitation and resulting access.

```

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.95 seconds
root@osboxes:~# smbclient -L //192.168.56.104 -N
Anonymous login successful

Sharename      Type            Comment
-----
smbcli1 req writev submit: called for dialect[SMB2 10] server[192.168.56.104]
Error returning browse list: NT_STATUS_REVISION_MISMATCH
Reconnecting with SMB1 for workgroup listing.
do connect: Connection to 192.168.56.104 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Failed to connect with SMB1 -- no workgroup available
root@osboxes:~# smbclient //192.168.56.104/CustomerData -N -u SMB2
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED
root@osboxes:~# smbclient //192.168.56.104/CustomerData -U labtest -m SMB2
Enter WORKGROUP\labtest's password:
session setup failed: NT_STATUS_LOGON_FAILURE
root@osboxes:~# smbclient //192.168.56.104/CustomerData -U labtest -m SMB2
Enter WORKGROUP\labtest's password:
Try "help" to get a list of possible commands.
smb: > ls
.                D          0  Fri Aug 14 13:42:43 2026
..               D          0  Fri Aug 14 13:42:43 2026
customer1.txt    A         100  Fri Aug 14 13:42:45 2026

10485247 blocks of size 4096, 6601022 blocks available
smb: > exit
root@osboxes:~# cat customer1.txt
cat: customer1.txt: No such file or directory
root@osboxes:~# smbclient //192.168.56.104/CustomerData -U labtest -m SMB2
Enter WORKGROUP\labtest's password:
session setup failed: NT_STATUS_LOGON_FAILURE
root@osboxes:~# smbclient //192.168.56.104/CustomerData -U labtest -m SMB2
Enter WORKGROUP\labtest's password:
Try "help" to get a list of possible commands.
smb: > ls
.                D          0  Fri Aug 14 13:42:43 2026
..               D          0  Fri Aug 14 13:42:43 2026
customer1.txt    A         100  Fri Aug 14 13:42:45 2026

10485247 blocks of size 4096, 6601490 blocks available
smb: > get customer1.txt
getting file \customer1.txt of size 106 as customer1.txt (4.1 KiloBytes/sec) (average 4.1 KiloBytes/sec)
smb: >

```

Result

- The test accessed the deliberately created **CustomerData SMB share** on the **Windows 7 VM (192.168.56.104)** using the laboratory account labtest. The customer1.txt file was visible in the share and was successfully retrieved using smbclient. The test revealed that a normal authenticated account had access beyond its intended privileges.
- **Examination**
- The outcome demonstrates a weakness in access control and least-privilege enforcement. An ordinary authenticated user was able to retrieve a sensitive file from the share because excessive permissions had been assigned. The confirmed impact was unauthorised access to shared synthetic test data. However, the test did not demonstrate administrator- or SYSTEM-level compromise.

3.4.4 Overall Evaluation of the Three Exploits

The practical assessment demonstrated three distinct attack surfaces within the ABCD Ltd laboratory. The first exploit used the command-execution function in DVWA, hosted on Metasploitable, to execute operating-system commands. It resulted in www-data access (UID 33, GID 33) rather than root-level access.

The second exploit targeted the vsFTPD 2.3.4 backdoor on 192.168.56.103. The Metasploitable host was compromised at root level, with a command shell returning uid=0(root) gid=0(root).

The third test used the authorised labtest account to access the Windows 7 CustomerData SMB share. The customer1.txt file was successfully listed and retrieved, demonstrating excessive file-share permissions and a weakness in least-privilege enforcement. The test did not demonstrate unauthenticated SMB access or Windows administrator-level compromise.

Overall, the three exploits produced different levels of access: web-server-level access through DVWA, root-level access through vsFTPD, and authenticated access to deliberately exposed Windows test data. The results are supported by Nmap enumeration, application output, Metasploit session output, Windows configuration evidence, SMB commands and retrieved test data. No separate privilege-escalation or lateral-movement technique is claimed because the practical evidence does not demonstrate those activities.

3.5 Tools and Techniques

The assessment stages necessitated the deployment of various security-analysis and penetration-testing tools. All tests were carried out in the authorized ABCD Ltd laboratory, and only the tools that were utilized during the practical assessment have been reported.

Tool	Purpose	Use
Nmap	Identify live hosts, open ports, services, versions and operating-system information.	Reconnaissance and vulnerability identification.
Metasploit Framework	Conduct controlled exploitation of confirmed vulnerable services.	Exploitation of the vsFTPD 2.3.4 backdoor.
smbclient	Connect to and interact with authorised SMB shares.	Windows SMB/share assessment and controlled file-access testing.
Windows Command Prompt	Configure and verify the Windows laboratory environment and collect evidence.	Windows-side configuration and access-control assessment.
Mozilla Firefox	Access and interact with the deliberately vulnerable DVWA application.	Web-application testing.

Tool Usage and Evidence

Nmap identified the FTP service **vsFTPD 2.3.4** on TCP port 21 and SMB services on ports 139 and 445 on the target machine. An exploit for the vsFTPD backdoor was available in Metasploit, which successfully established a root command shell. The **CustomerData** share was accessed using smbclient to retrieve customer1.txt. Windows Command Prompt was

used to create the synthetic test data and configure the SMB share, while Firefox was used to test the DVWA command-execution function, resulting in www-data access.

The tools therefore supported different assessment stages: **Nmap** for reconnaissance, **Metasploit** for exploitation, **Firefox** for web-application testing, and **Windows command-line tools with smbclient** for the SMB assessment.

3.6 Operational Execution, Containment and Safety

The attack sequence defined in the Threat Emulation Plan guided the practical assessment. Testing was restricted to authorised laboratory systems, with screenshots, command output and relevant system evidence collected during the assessment.

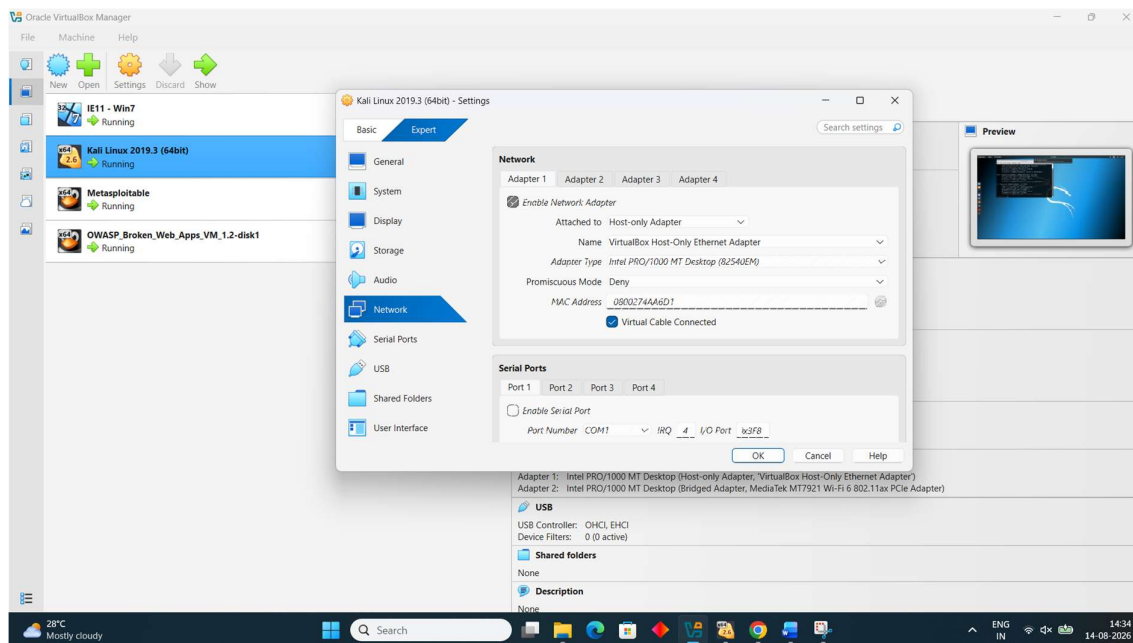
Virtual-machine snapshots were created before exploitation so that the laboratory could be restored if testing caused instability. The VMs operated on a **Host-only network**, and the configuration was checked to ensure that there was no unintended route to external systems.

The verified laboratory IP addresses were:

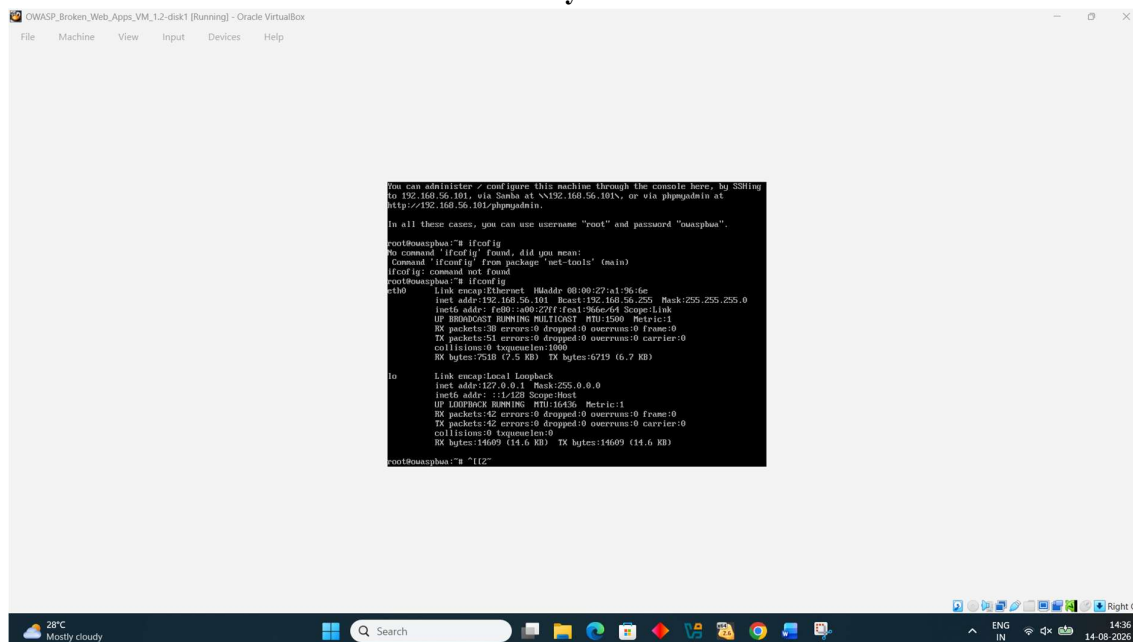
- **Kali Linux:** 192.168.56.102
- **Metasploitable2:** 192.168.56.103
- **Windows 7:** 192.168.56.104
- **OWASP Broken Web Apps:** 192.168.56.101

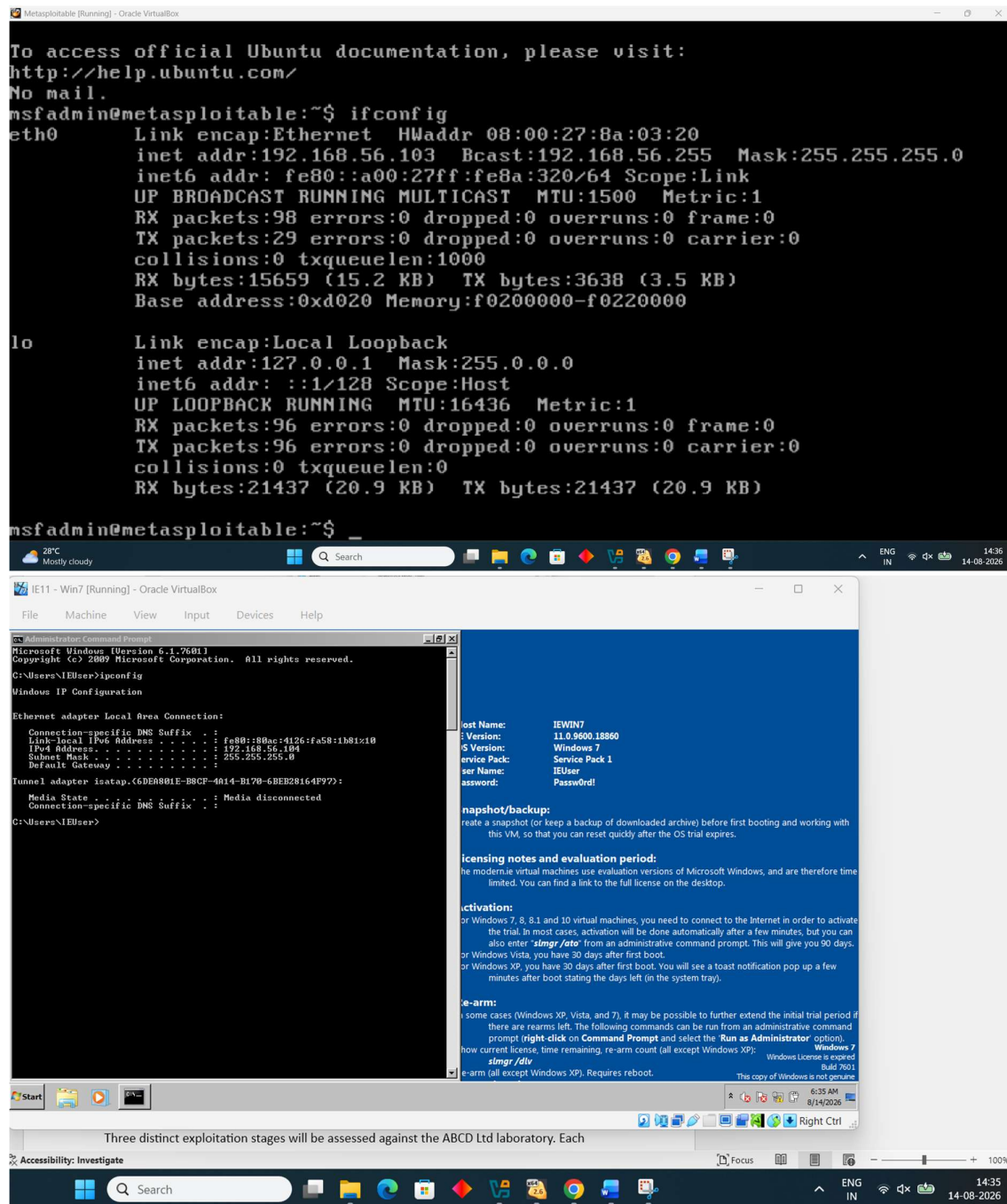
The operational objective was to maintain control of the laboratory while producing reliable evidence of the assessment activities. Tests that were not performed or were interrupted are reported as such, allowing the final evaluation to distinguish between intended actions and demonstrated outcomes [10].

Screenshot 14: VirtualBox network configuration showing the Host-only network used to isolate the ABCD Ltd laboratory.



Screenshot 15: IP configuration of the laboratory virtual machines showing addresses within the isolated 192.168.56.0/24 Host-only network.





Attack phase	Observed result	Security weakness	Recommended detection/control
Web application	DVWA command-injection testing achieved OS command execution under the www-data account.	Vulnerable web functionality permitted operating-system command execution.	Secure application configuration, input validation, WAF controls, web-server monitoring and endpoint monitoring.
Credential access	No separate credential-dumping attack was demonstrated during the three confirmed exploit stages.	Credential-access weakness was not independently demonstrated.	Strong credential controls, secure credential storage and authentication monitoring.
Privilege escalation	The vsFTPD 2.3.4 exploit produced a shell with uid=0(root). This represents root-level host compromise, although a separate privilege-escalation technique was not demonstrated.	A vulnerable network service allowed direct root-level compromise.	Security patch management, service hardening, least privilege, host-based monitoring and vulnerability management.
Lateral movement	No separate lateral-movement technique between the laboratory VMs was demonstrated.	Lateral-movement weakness was not independently demonstrated.	Network segmentation, authentication monitoring and remote-service monitoring.
Sensitive-data access	The labtest account accessed the CustomerData SMB share and retrieved the synthetic customer1.txt file.	Excessive SMB/file-share permissions allowed an ordinary authenticated account to access the test data.	File auditing, least privilege, SMB access monitoring and regular permission reviews.

Analysis of Prevention and Detection

The assessment identified three confirmed prevention weaknesses: DVWA allowed operating-system command execution, vsFTPD 2.3.4 allowed root-level shell access, and the misconfigured SMB share allowed an ordinary authenticated user to retrieve synthetic customer data.

The main detection opportunities concern activities that should be observable through host and network telemetry. Web-server logs could identify unusual requests and command execution, while authentication and SMB logs could record access to the CustomerData

share. Host monitoring could also identify unusual processes or root-level activity resulting from exploitation.

The critical detection gap is therefore the **absence of demonstrated monitoring evidence for the assessed activities**, rather than a proven failure of a specific SIEM or EDR product. This distinction ensures that the assessment does not overstate what the laboratory evidence demonstrates.

5 · Conclusion

This report has made an analysis of the **cyber attack on M&S** and Co-op and applied the lessons learnt to a practical red-team assessment of **ABCD Ltd**. According to task 1, it is important to secure identity, protect Active Directory, segment the network, use a least-privilege access model and be able to detect and respond effectively. These lessons applied to a controlled virtual laboratory set up to test how weaknesses in different systems could generate both security and business risks.

The laboratory had three security vulnerabilities as demonstrated in **task 2**. The first test executed commands on the operating system via the vulnerable **DVWA web application** which led to www-data account access. An exploit against the **vsFTPD 2.3.4** service on **Metasploitable2** successfully created a command shell with root access. The third proved to be excessive SMB file-share permissions on **Windows 7**. The laboratory account labtest was able to access and retrieve the customer1.txt record.

The practical test thus showed weaknesses in application security, management of vulnerable services and access rights. However, it did not exhibit a distinct lateral-movement assault between the systems of the lab or an entire end-to-end breach. The distinction is important. The access demonstrated should be the basis for assessing the severity of each finding, not what was originally intended.

In conclusion, the assessment illustrates that effective cybersecurity requires layers of complementary controls. Services that have vulnerabilities must be patched or removed, web applications must be securely configured, sensitive file shares must be subject to least-privilege controls, unnecessary legacy protocols must be restricted, and security monitoring must provide visibility into malicious activity. Conducting penetration testing and managed red-team exercises on a routine basis helps to uncover weaknesses prior to their combination into a more serious one.

References

[1] Cyber Monitoring Centre, “Statement on ransomware incidents in the retail sector,” Jun. 20, 2025. [Online]. Available:

[2] Cyber Management Alliance, “Cyber-attack timeline: Marks & Spencer,” 2025. [Online]. Available: [Cyber Management Alliance](#)

[3] M. White, “M&S ransomware hack: Service desk & Active Directory security lessons,” Specops Software, 2025. [Online]. Available: [Specops Software](#)

- [4] Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation, “Scattered Spider,” Joint Cybersecurity Advisory AA23-320A, 2023. [Online]. Available: [CISA advisory AA23-320A](#)
- [5] Irish Information Security Forum, “Scattered Spider and the Marks & Spencer cyber incident,” Technical Guide, 2025. [Online]. Available: [IISF Technical Guide](#)
- [6] R. Lakshmanan, “Scattered Spider behind cyberattacks on M&S and Co-op, causing up to \$592M in damages,” The Hacker News, Jun. 21, 2025. [Online]. Available: [The Hacker News](#)
- [7] MITRE, “MITRE ATT&CK Enterprise Matrix,” MITRE Corporation. [Online]. Available: [MITRE ATT&CK Enterprise Matrix](#). The current Enterprise Matrix covers tactics and techniques including Initial Access, Execution, Privilege Escalation, Credential Access, Lateral Movement, Collection and Impact.
- [8] BleepingComputer, “Marks & Spencer breach linked to Scattered Spider ransomware attack,” Apr. 30, 2025. [Online]. Available: [BleepingComputer](#)
- [9] OWASP Foundation, “OWASP Top 10: 2021,” 2021. [Online]. Available: [OWASP Top 10:2021](#). The source specifically covers risks such as Broken Access Control, Injection, Security Misconfiguration, Vulnerable and Outdated Components, and Security Logging and Monitoring Failures.
- [10] National Cyber Security Centre, “Mitigating malware and ransomware attacks,” NCSC. [Online]. Available: [NCSC guidance](#). The guidance supports recommendations around patching, least privilege, MFA, segmentation, obsolete platforms, backups and monitoring.