

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



**Module Title:** Ethical Hacking

**Module Code:** ACCA7033

**Programme:** MSc/PgDip/PgCert Cybersecurity and Digital Forensics

**Student Name:** Abdullah Al Maruf

**Student ID:** 2526089

**Lecturer:** Dr. Dipo Dunsin

## Table of Contents

|                                                                                         |           |
|-----------------------------------------------------------------------------------------|-----------|
| <b>Abstract .....</b>                                                                   | <b>3</b>  |
| <b>Task 1: Strategic Threat Analysis: The M&amp;S &amp; Co-op UK Cyber Attack .....</b> | <b>3</b>  |
| 1. Introduction .....                                                                   | 2         |
| 2. Incident Summary and Timeline .....                                                  | 3         |
| 3. Adversary TTP Mapping (MITRE ATT&CK) .....                                           | 4         |
| 4. Root Cause and Security Control Failures .....                                       | 5         |
| 5. Threat Actor Profile and Motive .....                                                | 6         |
| 6. Detection and Response Analysis .....                                                | 7         |
| 7. Strategic Recommendations .....                                                      | 8         |
| 8. Support and Evidence .....                                                           | 9         |
| 9. Conclusion .....                                                                     | 10        |
| Appendix A: OSINT Notes .....                                                           | 11        |
| Appendix B: Attack Flow Summary .....                                                   | 11        |
| <b>Task 2: Red Team Engagement: ABCD Ltd — Complete Penetration Testing ....</b>        | <b>14</b> |
| Executive Brief .....                                                                   | 14        |
| 1. Introduction .....                                                                   | 15        |
| 2. Rules of Engagement (RoE) .....                                                      | 15        |
| 3. Threat Emulation Plan (MITRE ATT&CK Mapping) .....                                   | 15        |
| 3.1 Campaign Overview .....                                                             | 15        |
| 3.2 Campaign Objective .....                                                            | 15        |
| 3.3 Success Criteria .....                                                              | 16        |
| 4. Lab Environment Design .....                                                         | 17        |
| 4.1 Virtual Machine Configuration .....                                                 | 17        |
| 5. Exploitation Requirement Analysis .....                                              | 18        |
| 6. Operational Execution .....                                                          | 19        |
| 6.1 Reconnaissance .....                                                                | 19        |
| 6.2 Scanning and Enumeration .....                                                      | 20        |
| 6.3 Metasploit Analysis .....                                                           | 21        |
| 6.4 Vulnerability Scan .....                                                            | 22        |
| 6.5 Enumeration Evidence .....                                                          | 22        |
| 6.6 Packet Capture .....                                                                | 23        |
| 7. Tools & Techniques .....                                                             | 24        |
| 8. Containment & Safety .....                                                           | 25        |
| 9. Critical Analysis .....                                                              | 26        |
| 10. Conclusion .....                                                                    | 26        |
| Appendix C: Rules of Engagement (RoE) .....                                             | 27        |
| Appendix D: Threat Emulation Plan .....                                                 | 27        |
| Appendix E: Lab Export & Evidence Package .....                                         | 27        |
| References .....                                                                        | 28        |

# Strategic Threat Analysis: The M&S & Co-op UK Cyber Attack

## Abstract

This research looks at the cyber attacks that hit Marks & Spencer (M&S) and the Co-operative Group in the spring of 2025. It focuses on how the attacks got worse, how the attackers acted, and the security holes that were there. The study creates a thorough timeline of events and uses a structured threat analysis approach to look at the incidents. It does this by using information that is publically available from Reuters, the National Cyber Security Centre (NCSC), and organizational disclosures.

The paper uses the MITRE ATT&CK paradigm to show the tactics, methods, and procedures (TTPs) of attackers that were seen or guessed at, with identity-based compromise being the most important. Evidence indicates that social engineering targeting IT help desks facilitated attackers in acquiring legitimate credentials, hence transitioning the intrusion pattern from conventional malware-driven attacks to human-centric exploitation. This identity-based attack vector let enemies get in, navigate about systems, and finally steal valuable consumer information.

Root cause analysis finds flaws in identity verification procedures, a lack of implementation of phishing-resistant multi-factor authentication, and gaps in monitoring and segmentation measures. The results also show how important human aspects are, since social engineering took advantage of trust and procedural flaws instead of just technological ones.

The research says that the attackers were most likely cybercriminals who were motivated by money and had moderate to high skills, and that they were part of a larger network of cybercriminals. Even if the steps used to respond to the incident were quite effective after it was found, the delay in finding the breach gave the attackers a chance to get a footing and make the damage worse.

Lastly, the paper gives strategic advice that fits with Zero Trust principles. This includes making identity assurance stronger, using authentication that is resistant to phishing, making help-desk security operations better, and boosting monitoring and segmentation. The goal of these steps is to lower the chances and effects of similar attacks based on identity in the future.

## 1. Introduction

The UK retail sector is a big target because it has customer data, relies on digital services that are always available, and generally works in complicated, interconnected environments. In the spring of 2025, both M&S and Co-op were affected, and the problems were made public and drew the attention of regulators. According to Reuters, M&S reported a cyber problem on April 22, 2025, and Co-op later stated that its systems had been compromised (Reuters, 2025a; Reuters, 2025b).

The NCSC said it was working with the organizations that were affected, and most critically, it could not yet say if the instances were connected or part of a planned campaign (NCSC, 2025a; NCSC, 2025b). That care is important: it's easy to combine comparable retail situations into one story, but excellent analysis separates what is known to be true from what is likely to be true. This paper considers shared approaches as probable due to public reporting, but maintaining provisional attribution.

The study utilizes an organized way to look at threats. To start, it makes a timeline from what people have spoken in public. Second, it compares the behavior of attackers that was seen and guessed at to MITRE ATT&CK methodologies. Third, it looks into the main reasons and failures of control that made the assault chain possible. Lastly, it gives specific suggestions that can help with planning for implementation.

## 2. Incident Summary and Timeline

Figure 1 summarises the incident progression from disclosure through containment and recovery. The table beneath it provides a more detailed evidence-backed chronology.

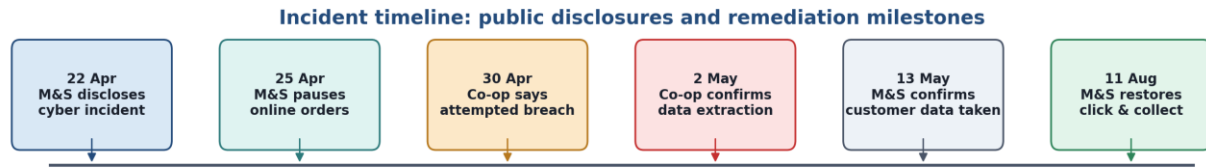


Figure 1. Public timeline of major M&S and Co-op milestones, based on official statements and Reuters reporting.

|                    |                                             |                                                                                                                                             |                                                                                                            |
|--------------------|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
|                    |                                             |                                                                                                                                             |                                                                                                            |
| <b>22 Apr 2025</b> | M&S discloses a cyber incident              | Reuters reported M&S had been managing the incident for several days (Reuters, 2025a); M&S said it was investigating with external experts. | Shows the organisation detected an issue after compromise had already begun.                               |
| <b>23 Apr 2025</b> | M&S says disruption is ongoing              | M&S said it continued to make operational changes to protect customers and the business (M&S, 2025a).                                       | Indicates active containment rather than full restoration.                                                 |
| <b>25 Apr 2025</b> | M&S pauses online orders                    | M&S announced it would pause orders via websites and apps (M&S, 2025b).                                                                     | Operational shutdown suggests incident severity was high enough to justify business-impacting containment. |
| <b>30 Apr 2025</b> | Co-op reports attempted intrusion           | Reuters said hackers had attempted to break into Co-op systems, following the M&S incident (Reuters, 2025b).                                | Raises the possibility of a shared actor or repeatable playbook.                                           |
| <b>2 May 2025</b>  | Co-op confirms data extraction              | Reuters reported customer names, contact details and dates of birth were accessed and extracted (Reuters, 2025c).                           | Confirms compromise of confidentiality, not just disruption.                                               |
| <b>2 May 2025</b>  | NCSC/ICO engage                             | ICO said it had received reports from both firms and was working with NCSC (ICO, 2025).                                                     | Demonstrates regulatory and national-level coordination.                                                   |
| <b>6 May 2025</b>  | Help-desk social engineering becomes public | Reuters reported attackers impersonated employees and convinced IT help desks                                                               | Strong indicator that identity verification was the critical weak point.                                   |

|                    |                                            |                                                                                                                                   |                                                                                   |
|--------------------|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
|                    |                                            | to reset passwords, based on BleepingComputer reporting (Reuters, 2025d).                                                         |                                                                                   |
| <b>13 May 2025</b> | M&S confirms customer data taken           | M&S said some personal customer information had been taken, though not payment details or passwords (M&S, 2025c; Reuters, 2025e). | Moves the incident from operational disruption to confirmed data breach.          |
| <b>14 May 2025</b> | Co-op says systems are returning to normal | Reuters reported Co-op systems were running normally and confirmed some personal information had been taken (Reuters, 2025f).     | Suggests containment and recovery were effective enough to restore core services. |
| <b>11 Aug 2025</b> | M&S restores click & collect               | Reuters reported click & collect had been down since 25 April and was restored after nearly four months (Reuters, 2025g).         | Shows long-tail remediation and recovery cost.                                    |

The timeline suggests the organisations responded quickly once the intrusion was visible, but the adversary had already achieved meaningful access before detection. The long recovery tail at M&S, especially for click & collect, indicates that containment was not the same as full restoration (Reuters, 2025g) [1] [2] [3].

### 3. Adversary TTP Mapping (MITRE ATT&CK)

Figure 2 provides a visual summary of the likely attack chain. The mapping is partly confirmed by reporting and partly inferential, which is common when public evidence is limited.

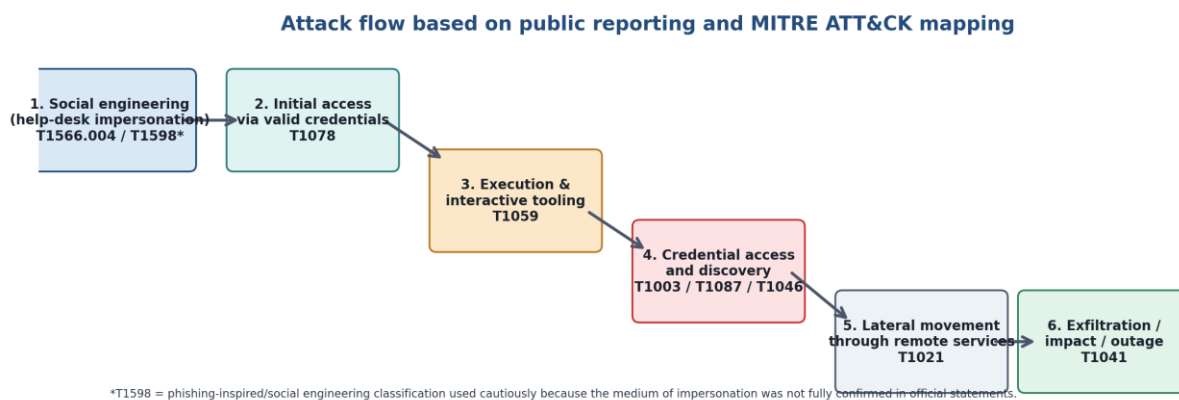


Figure 2. Attack flow based on public reporting and a cautious MITRE ATT&CK interpretation.

Figure 3 groups the most relevant ATT&CK techniques by attack phase. A number of techniques are inferred from the observed behaviour and should be read as plausible rather than fully confirmed.

### MITRE ATT&CK mapping: dominant techniques seen or plausibly inferred

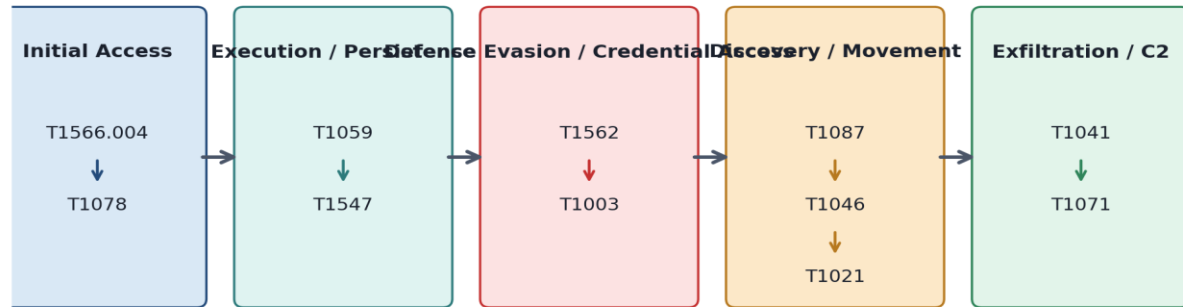


Figure 3. MITRE ATT&CK mapping by phase.

| <b>Initial access</b>    | T1566.004 | Spearphishing Voice               | Public reporting said attackers impersonated employees and tricked help desks into resetting passwords, which is consistent with voice-based social engineering (Reuters, 2025d). |
|--------------------------|-----------|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Initial access</b>    | T1078     | Valid Accounts                    | If password resets succeeded, attackers would have been able to use legitimate credentials to enter systems (MITRE, n.d.).                                                        |
| <b>Execution</b>         | T1059     | Command and Scripting Interpreter | Once inside, attackers in this class of intrusion commonly use built-in scripting tools for hands-on-keyboard actions and automation (MITRE, n.d.).                               |
| <b>Persistence</b>       | T1547     | Boot or Logon Autostart Execution | Persistence mechanisms are a plausible step when actors want to retain access after initial entry (MITRE, n.d.).                                                                  |
| <b>Credential access</b> | T1003     | OS Credential Dumping             | Public analysis of similar intrusions often includes credential harvesting after privilege gain; it remains a plausible technique even                                            |

|                         |       |                              |                                                                                                                                                                        |
|-------------------------|-------|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                         |       |                              | if not directly confirmed here (MITRE, n.d.).                                                                                                                          |
| <b>Discovery</b>        | T1087 | Account Discovery            | Attackers typically enumerate accounts after entering a corporate environment to find privileged identities and service accounts (MITRE, n.d.).                        |
| <b>Discovery</b>        | T1046 | Network Service Discovery    | Once inside, discovery of internal services helps identify reachable systems and attack paths (MITRE, n.d.).                                                           |
| <b>Lateral movement</b> | T1021 | Remote Services              | Remote services such as RDP/SMB/WinRM are common movement routes after valid credentials are acquired (MITRE, n.d.).                                                   |
| <b>Defense evasion</b>  | T1562 | Impair Defenses              | Disabling or weakening logging and security controls is consistent with stealthy, multi-stage intrusions (MITRE, n.d.).                                                |
| <b>Exfiltration</b>     | T1041 | Exfiltration Over C2 Channel | Co-op confirmed customer data extraction, and covert exfiltration over the control channel is a common technique in this type of attack (Reuters, 2025c; MITRE, n.d.). |

The most important analytical point is that the reported help-desk impersonation changes the shape of the intrusion. Rather than a malware-led breach, the public evidence points toward identity-centric compromise: the attacker persuades a human control point, obtains valid access, and then pivots inside the environment. That makes identity verification, privileged access monitoring, and remote-service restrictions the most relevant detection and prevention layers [4] [5] [6].

#### 4. Root Cause and Security Control Failures

Weak identity assurance in the service desk or account recovery process is probably the main reason for this. Reuters said that help desks were tricked into resetting employee passwords, which means that the attacker's social engineering was stronger than the measures at the process level. In real life, the control failure happened at the point where people and processes meet, when verification procedures weren't strong enough to stop people from pretending to be someone else. Along with these procedural problems, technical issues like poorly set up identity and access management systems and services that may not have been patched could have allowed persistence beyond the first access. Insufficient logging, monitoring, and endpoint detection further delayed the discovery of malicious activity, letting attackers work without being seen [7].

A second big problem is that there is no multi-factor authentication that is resistant to phishing, which made identity protection less effective. The National Institute of Standards and Technology says that zero-trust concepts need constant verification instead of implicit confidence. This may have stopped credential abuse and lateral mobility. Also, the organization's capacity to immediately control the attack was restricted by insufficient network segmentation and minimal telemetry, which made the situation worse. Human factors remain critical, as social engineering exploits trust, urgency, and routine behaviour, making employees a primary attack surface. In general, the incident shows that flaws in people, processes, and technology all contributed to the breach. This shows how important it is to have security controls that work together and are strong [8].

## 5. Threat Actor Profile and Motive

There is still no official word on who is responsible for the computer attacks on Marks & Spencer and Co-operative Group. At the time, the National Cyber Security Center said it couldn't tell if the two events were connected. However, reports and industry analysis show that the strategies used by cybercriminal groups like Scattered Spider and DragonForce are similar, and M&S says that DragonForce may be involved in ransomware operations [9].

The evidence we have suggests that the threat is more likely to come from organized cybercrime than from a nation-state actor. Retail businesses are high-value targets because they handle a lot of customer and financial data. Using helpdesk-based social engineering and credential compromise shows a strong intent on making money, such as stealing data, extorting money through ransomware, and causing operational problems to gain more power over victims [10].

The attackers show that they are at least moderately skilled. To break in, you had to prepare carefully, know how company identity systems work, and be able to stay in corporate environments without being caught right away. These traits are typical of ransomware-as-a-service ecosystems, where specialized roles like initial access brokers and ransomware operators work together to carry out assaults.

Even with these signs, it's still hard to say who is responsible. There may not be a single group of people working together on the occurrences, but rather several people working in the same cybercriminal ecosystem. There isn't much evidence that nation-states are involved because there aren't any apparent geopolitical or espionage-related goals. Insider involvement is also plausible, but current reports don't back it up [11].

In general, the most likely conclusion is that the assaults were carried out by cybercriminals who were motivated by money and had a moderate to high level of skill. They wanted to take advantage of identification flaws, get access without permission, and make the most money by stealing data and stopping services.

## 6. Detection and Response Analysis

It looks that the issues that affected Marks & Spencer and the Co-operative Group were found late, after the attackers had already gotten in and set up shop inside the systems. The time between the first public announcement on April 22 and the latter confirmation of client data theft shows that the breach wasn't found right away [12].

This shows that detection was gradual instead of happening right away. In a well-monitored setting, strange actions like resetting helpdesk passwords multiple times, logging in in strange ways, trying to get more privileges, and using remote services in strange ways should have set off alarms much sooner. The fact that the attackers were allowed to stay inside the environment means that these signals were either not seen or not linked up correctly.

Once the event was found, the response was rather well-organized. M&S decided to stop taking online orders for a while and then slowly brought services back online to avoid more harm. Co-op, on the other hand, limited some of its systems and focused on recovery. The National Cyber Security Centre and the Information Commissioner's Office were also involved in helping with the response and investigation. This shows that containment procedures were conducted right away after the breach was confirmed [13].

But the primary problem wasn't the reaction phase; it was the delay in finding out. The organization responded well after the attack was discovered, but the attackers had already made their way into the network before they were found. This illustrates that the ability to find things early is not very good, especially when it comes to identity-based assaults and social engineering that happens in helpdesk settings.

The event shows that notifications based on endpoints or malware shouldn't be the sole way to keep an eye on things. To find this kind of attack sooner, identification systems, helpdesk activity, and privileged access events need to be more visible [14].

## 7. Strategic Recommendations

The following controls are prioritised by their likely risk reduction and practicality. Effort and cost are expressed qualitatively because exact costs vary by organisation size and tool stack.

| Priority control              | Why it matters                                                                              | Effort         | Cost band      |
|-------------------------------|---------------------------------------------------------------------------------------------|----------------|----------------|
| Phishing-resistant MFA        | Use FIDO2/security keys or equivalent so stolen passwords are not enough for access.        | Medium         | Low to Medium  |
| Help-desk identity proofing   | Require strong callback, manager approval, and out-of-band checks before password resets.   | Low to Medium  | Low            |
| Zero Trust segmentation       | Reduce lateral movement by limiting trust between user, app, and admin zones.               | High           | Medium to High |
| Privileged access management  | Isolate admin accounts, use just-in-time elevation, and log privileged actions.             | Medium to High | Medium         |
| SIEM + EDR correlation        | Join identity, endpoint, and network telemetry to spot unusual login and movement patterns. | Medium         | Medium to High |
| Patch and exposure management | Keep internet-facing and internal systems current and remove unnecessary remote paths.      | Medium         | Low to Medium  |
| Tabletop exercises            | Test recovery, communications, and decision-making before a real incident hits.             | Low            | Low            |
| DLP and encryption            | Make stolen data less useful and reduce downstream harm if exfiltration occurs.             | Medium         | Medium         |

Phishing-resistant MFA is the most effective solution because it directly lowers the value of stolen credentials. The second is to strengthen the assistance desk, since reports from the public suggest that the service desk was the entry into the environment. Segmentation and PAM come next because they keep the blast radius small if an account is hacked. These controls are in line with the Zero Trust concepts that NIST talks about and the NCSC's focus on strong, well-tested operational defense (NIST, 2020; NCSC, 2025b). The minimum telemetry set for monitoring should have logs of authentication, events for resetting passwords, changes to privileged group membership, remote-session creation, command-line execution on endpoints, and unusual data transfers. The telemetry should send a SIEM use cases that look for help-desk abuse, impossible travel, strange admin logins, and huge transfers from systems that aren't normal [15] [16] [17].

## 8. Support and Evidence

A combination of public comments, reliable news reports, industry advice, and academic literature backs up this analysis. The report mostly relies on Reuters, M&S, Co-op, ICO, NCSC, MITRE ATT&CK, NIST, and peer-reviewed research concerning social engineering and phishing. This makes it more reliable because the specifics of the incident come from more than one source. Reuters said that attackers deployed fake help desks to reset passwords, which backs up the idea that identity assurance was a big problem. The NCSC also agrees with the suggestion to make help-desk processes stronger and make organizations more resilient. The ICO statement verifies that the government is involved, and MITRE ATT&CK gives a formal way to map tactics like Spearphishing Voice and Valid Accounts [18] [19].

Peer-reviewed literature is vital because it shows why social engineering still works. If personnel don't have strong processes to follow, human variables like urgency, authority, and trust can get around technical controls. The data demonstrates that the instances constituted not merely technical errors, but also deficiencies in process, monitoring, and identity governance [20].

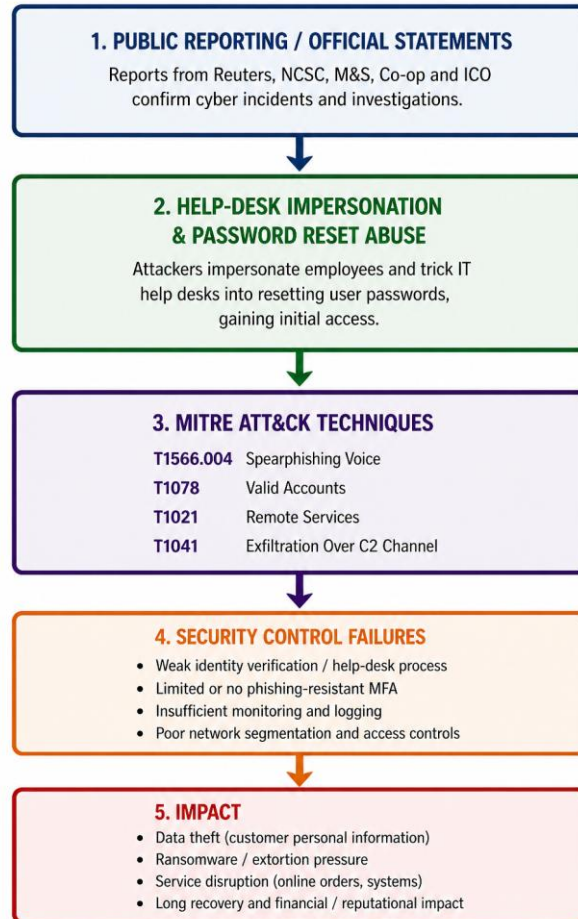


Figure 4 illustrates the end-to-end attack flow

The figure showing how social engineering enabled initial access, which was mapped to MITRE ATT&CK techniques, leading to security control failures and ultimately resulting in data breach and operational impact.

## 9. Conclusion

The cyber attacks on Marks & Spencer and Co-operative Group in 2025 show a strong trend toward identity-based attacks in today's cyber threat scenario. While complete attribution is not yet established, the existing evidence strongly suggests a financially driven cybercriminal operation that utilized social engineering, credential breach, and authorized access to penetrate corporate systems.

One important thing this study found is that the first point of breach was not a technical flaw, but a flaw in how people do things, notably how help desks check people's identities. This let attackers get beyond standard perimeter defenses and use real credentials, which made it much harder to find them. Once inside, not enough monitoring, not enough segmentation, and holes in access control made it possible for attackers to roam around and stay longer, which led to data theft and operational problems.

Both organizations had quite good reaction plans after the breach was found, but the fact that it took so long to find it shows a major flaw in early-stage detection, especially for threats predicated on identity. The events show that cybersecurity resilience depends on more than just technology; it also depends on strong processes and user awareness.

In general, the story shows how important it is to have phishing-resistant authentication, strong identity governance, continuous monitoring, and Zero Trust principles. To make it less likely that similar attacks will happen and to lessen their effects, certain places need to be strengthened.

## Appendix A: OSINT Notes

Primary OSINT sources used in this sample are company statements, Reuters coverage, ICO updates, and NCSC guidance. These sources were preferred because they are more authoritative than anonymous blogs or republished summaries.

Where the evidence was limited, the report explicitly labels the claim as likely or inferred rather than confirmed. That is particularly important for the TTP mapping and attribution sections.

## Appendix B: Attack Flow Summary

Social engineering or help-desk impersonation

Password reset or credential capture

Initial access using valid accounts

Privilege escalation and internal discovery

Lateral movement across remote services

Data theft and operational disruption

Containment, disclosure, and staged recovery

## References

1. Co-op (2025a) Cyber Incident. Available at: <https://www.coop.co.uk/cyber-incident> (Accessed 27 March 2026).
2. Co-op (2025b) Cyber Incident Member FAQs. Available at: <https://www.coop.co.uk/cyber-incident-faqs> (Accessed 27 March 2026).
3. ICO (2025) Statement on cyber incidents impacting retailers. Available at: <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/05/statement-on-cyber-incidents-impacting-retailers/> (Accessed 27 March 2026).
4. M&S (2025a) Cyber Incident - Further Update. Available at: <https://corporate.marksandspencer.com/newsroom/press-releases/cyber-incident-further-update-0> (Accessed 27 March 2026).
5. M&S (2025b) Cyber Update. Available at: <https://corporate.marksandspencer.com/cyber-update> (Accessed 27 March 2026).
6. M&S (2025c) 2025 Annual Report and Financial Statements. Available at: [https://corporate.marksandspencer.com/sites/marksandspencer/files/2025-05/Marks-and-Spencer-Group-plc-Annual-Report-and-Financial-Statements-2025\\_INTERACTIVE\\_FINAL.pdf](https://corporate.marksandspencer.com/sites/marksandspencer/files/2025-05/Marks-and-Spencer-Group-plc-Annual-Report-and-Financial-Statements-2025_INTERACTIVE_FINAL.pdf) (Accessed 27 March 2026).
7. MITRE (n.d.) ATT&CK Enterprise Techniques. Available at: <https://attack.mitre.org/> (Accessed 27 March 2026).
8. Naqvi, B. et al. (2023) 'Mitigation strategies against the phishing attacks', Computers & Security. Available at: <https://www.sciencedirect.com/science/article/pii/S0167404823002973> (Accessed 27 March 2026).
9. NCSC (2025a) NCSC statement: Incident impacting retailers. Available at: <https://www.ncsc.gov.uk/news/retailers-incident> (Accessed 27 March 2026).
10. NCSC (2025b) Incidents impacting retailers – recommendations from the NCSC. Available at: <https://www.ncsc.gov.uk/blog-post/incidents-impacting-retailers> (Accessed 27 March 2026).
11. NCSC (2025c) It's time to act - NCSC Annual Review 2025. Available at: <https://www.ncsc.gov.uk/files/ncsc-annual-review-2025.pdf> (Accessed 27 March 2026).
12. NIST (2020) Zero Trust Architecture, SP 800-207. Available at: <https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf> (Accessed 27 March 2026).
13. Reuters (2025a) British food and clothing group M&S discloses cyber incident. Available at: <https://www.reuters.com/business/retail-consumer/british-retailer-ms-discloses-cyber-incident-2025-04-22/> (Accessed 27 March 2026).

14. Reuters (2025b) Co-op is latest British retailer to be hit by cyber attack. Available at: <https://www.reuters.com/world/uk/britains-co-op-is-latest-retailer-be-hit-by-cyber-attack-2025-04-30/> (Accessed 27 March 2026).
15. Reuters (2025c) Britain's Co-op says hackers have extracted customer data. Available at: <https://www.reuters.com/sustainability/boards-policy-regulation/britains-co-op-says-hackers-have-extracted-customer-data-2025-05-02/> (Accessed 27 March 2026).
16. Reuters (2025d) M&S, Co-op cyberattackers duped IT help desks into resetting passwords, says report. Available at: <https://www.reuters.com/business/retail-consumer/ms-co-op-cyberattackers-duped-it-help-desks-into-resetting-passwords-says-report-2025-05-06/> (Accessed 27 March 2026).
17. Reuters (2025e) UK's M&S says customer data was taken in cyber attack. Available at: <https://www.reuters.com/business/retail-consumer/uks-ms-says-customer-information-was-taken-cyber-attack-2025-05-13/> (Accessed 27 March 2026).
18. Reuters (2025f) UK retailer Co-Op says systems now running normally after cyber incident. Available at: <https://www.reuters.com/business/retail-consumer/uks-co-op-says-systems-now-running-normally-after-cyber-incident-2025-05-14/> (Accessed 27 March 2026).
19. Reuters (2025g) Britain's M&S restores click and collect services 15 weeks after systems hacked. Available at: <https://www.reuters.com/business/retail-consumer/britains-ms-restores-click-collect-services-15-weeks-after-systems-hacked-2025-08-11/> (Accessed 27 March 2026).
20. Washo, A.H. et al. (2021) 'An interdisciplinary view of social engineering: A call to action', Computers & Security. Available at: <https://www.sciencedirect.com/science/article/pii/S2451958821000749> (Accessed 27 March 2026).

# Red Team Engagement: ABCD Ltd — Complete Penetration Testing

## Executive Brief

This report presents the findings of a controlled red team assessment conducted against a simulated environment representing ABCD Ltd's internal and external systems. The objective of this engagement was to evaluate the organisation's ability to detect, prevent, and respond to realistic cyber threats by simulating adversarial behaviour across multiple attack stages. The assessment was performed within an isolated virtual lab to ensure safety while accurately reflecting real-world attack scenarios.

The testing identified several security weaknesses within the environment, particularly related to exposed network services, outdated system configurations, and insufficient access controls. Open ports associated with critical services such as file sharing and remote procedure calls were discovered, which are commonly targeted by attackers. In addition, system-level enumeration revealed accessible user accounts and sensitive directories, indicating potential weaknesses in system hardening and privilege management.

From a business perspective, these vulnerabilities present significant risks to confidentiality, integrity, and availability of organisational data. An attacker exploiting such weaknesses could gain unauthorised access to internal systems, extract sensitive information, or disrupt operations. This could result in financial loss, reputational damage, and regulatory consequences, especially for organisations handling customer or transactional data. The findings highlight gaps in preventative controls and monitoring capabilities, suggesting that malicious activity could occur without timely detection.

To reduce these risks, several prioritized recommendations are proposed. Firstly, all systems should be regularly updated and patched to eliminate known vulnerabilities. Secondly, unnecessary services and open ports should be disabled to reduce the attack surface. Thirdly, stronger access control mechanisms and least-privilege policies should be enforced to limit user permissions. Additionally, network monitoring and intrusion detection systems should be implemented to improve visibility and response capabilities. Finally, regular security testing and staff awareness training should be conducted to maintain a strong security posture.

Overall, the assessment demonstrates that while the environment is functional, it requires improvements in security configuration, monitoring, and defensive controls to withstand realistic cyber threats. Implementing the recommended measures will significantly enhance ABCD Ltd's resilience against potential attacks.

## 1. Introduction

This report presents a comprehensive red team assessment conducted within a controlled virtual lab environment representing ABCD Ltd. The purpose of this engagement is to simulate realistic cyberattack scenarios using Kali Linux as the attacker platform and a Windows 7 system as the primary target. The assessment follows a structured methodology aligned with the MITRE ATT&CK framework, enabling a systematic evaluation of reconnaissance, scanning, enumeration, and controlled vulnerability validation.

In modern enterprise environments, organisations rely heavily on interconnected systems, which significantly increases the attack surface. Red team exercises are essential for identifying weaknesses not only in technical controls but also in detection, monitoring, and response mechanisms. Unlike traditional vulnerability assessments, red teaming focuses on adversarial thinking, simulating real attacker behaviour across multiple stages of the cyber kill chain.

This report documents each phase of the attack lifecycle, including tools used, commands executed at a high level, evidence collected, and the resulting security implications. The findings are further analysed through a detection gap perspective, highlighting why existing controls failed to detect or prevent the simulated attack activities. The report concludes with recommendations aimed at improving organisational resilience against advanced threats.

## 2. Rules of Engagement (RoE)

The Rules of Engagement (RoE) spell out the ABCD Ltd red team's assessment's authorized scope, operational limits, and safety controls. This engagement took place in a highly regulated and segregated virtual lab environment that was meant to seem like a corporate network while keeping external systems safe.

The engagement only included virtual machines set up on a host-only network. These included Kali Linux (the attacker), a fake Windows Server/Active Directory environment, a Linux-based vulnerable web server, and a Windows 7 client/file server with fake sensitive data. There were no external systems, public infrastructure, university networks, or host operating systems outside of the virtual environment that were included in the scope.

All tests were done using penetration testing methods that don't damage the system and are standard in the industry. Some of these included reconnaissance, network scanning, service enumeration, and controlled vulnerability assessment with tools like Nmap and Metasploit. The goal was to make the attacker's behavior look authentic while keeping the system safe and not causing any problems with operations.

During the engagement, strict rules were followed. These included denial-of-service attacks, running hazardous or weaponized payloads, unauthorized privilege escalation beyond safe demonstration, and any attempt to get at or steal real data. All acts were restricted to regulated validation inside the laboratory setting.

A kill switch mechanism (ABORT-TEST) was put in place to keep things secure. Testing would stop right away if there was any instability, unusual behavior, or divergence from the defined scope. In these situations, virtual machines would be paused, evidence would be kept, and systems would be restored using pre-configured snapshots.

All activities were done in a way that followed the rules of ethical hacking, academic standards, and the law. This made sure that the event was safe, controlled, and instructional. The RoE makes sure that the red team exercise properly checks the security posture without harming systems, data, or people outside the organization [1] [2] [3].

| RoE Area                      | Definition                                                                                                                                                                               |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scope                         | Kali Linux attacker VM; VM-1 Windows Server/AD role; VM-2 Linux vulnerable web server; VM-3 Windows 7 client/file server with dummy SensitiveData.                                       |
| Permitted techniques          | IP discovery, ping, Nmap scanning, service enumeration, Metasploit auxiliary vulnerability validation, Windows command-line enumeration, dummy data creation and tcpdump packet capture. |
| Excluded systems              | Internet systems, university network, host OS outside the lab, cloud services, third-party websites, real customer data and any system not explicitly named in scope.                    |
| Safe-word / kill switch       | ABORT-TEST. If instability, unexpected external traffic or unsafe behaviour is observed, testing stops immediately.                                                                      |
| Escalation and communication  | Student red team operator reports issues to module tutor/supervisor. If the safe-word is triggered, VMs are paused, evidence is preserved and rollback is performed.                     |
| Legal and ethical constraints | Testing is authorised only within the virtual lab. No destructive payloads, denial of service, persistence, credential theft from real users or real data exfiltration is permitted.     |

### 3. Threat Emulation Plan (MITRE ATT&CK Mapping)

#### 3.1 Campaign Overview

The threat emulation campaign was set up to copy an actual attack chain against ABCD Ltd's fake business environment. Instead than only exploiting vulnerabilities, the engagement uses an adversary emulation approach to represent how modern Advanced Persistent Threats (APTs) act.

This involves a planned progression through the phases of reconnaissance, discovery, validation, and data gathering, all while staying hidden, keeping a low operating footprint, and controlling execution. The campaign is in line with the MITRE ATT&CK structure, which makes sure that every action is based on known attacker tactics, methods, and procedures (TTPs) [4] [5]. The assessment prioritises:

- Realistic attacker decision-making
- Controlled validation rather than destructive exploitation
- Evidence-driven analysis
- Ethical and safe execution

#### 3.2 Campaign Objective

The primary objective of this campaign is to simulate how an attacker would progress through a network to achieve a defined goal, specifically ,To identify exposed services, validate potential vulnerabilities, enumerate system information, and simulate access to sensitive data within a controlled lab environment [5] [6]

The campaign also aims to evaluate:

- System exposure
- Detection capability
- Monitoring effectiveness
- Potential attack paths

#### 3.3 Success Criteria

The campaign is considered successful when the following outcomes are achieved:

- Attacker and target systems are identified within the network
- Network connectivity between systems is confirmed
- Open ports and services are discovered
- Vulnerability validation is safely performed
- System accounts and directories are enumerated
- Simulated sensitive data is identified and accessed
- Network traffic is captured as forensic evidence
- Detection gaps and security weaknesses are documented

MITRE ATT&CK Mapping

| Phase                       | Technique                                              | MITRE ID | Objective                                                                             | Evidence                             |
|-----------------------------|--------------------------------------------------------|----------|---------------------------------------------------------------------------------------|--------------------------------------|
| Reconnaissance              | Active Scanning                                        | T1595    | Identify attacker and target network positioning and validate connectivity            | Kali IP, Windows IP, Ping screenshot |
| Discovery                   | Network Service Discovery                              | T1046    | Identify open ports and services (e.g., SMB, RPC) to determine attack surface         | Nmap scan screenshots                |
| Initial Access (Validation) | Exploit Public-Facing Application / Service Validation | T1190    | Safely validate whether exposed services (e.g., SMB) are vulnerable to known exploits | Metasploit MS17-010 result           |

|                        |                                                     |               |                                                                               |                                 |
|------------------------|-----------------------------------------------------|---------------|-------------------------------------------------------------------------------|---------------------------------|
| Discovery              | Account Discovery                                   | T1087         | Enumerate system users to identify potential targets for privilege escalation | net user screenshot             |
| Discovery / Collection | File & Directory Discovery / Data from Local System | T1083 / T1005 | Locate sensitive directories and simulate data exposure                       | dir + SensitiveData screenshots |
| Collection             | Network Sniffing                                    | T1040         | Capture network traffic for analysis and detection evaluation                 | tcpdump screenshots             |

## 4. Lab Environment Design

The virtual machines in the lab environment are interconnected through a host-only network, enabling direct communication between systems while ensuring complete isolation from external networks. The network operates within the private address range 192.168.56.0/24, providing a controlled environment for testing. Within this setup, the Kali Linux attacker machine is assigned the IP address 192.168.56.101, while the Windows 7 target system operates at 192.168.56.102. Additionally, the Metasploit Framework, integrated within the Kali Linux environment, is utilised as the primary exploitation and vulnerability validation platform. This flat network topology allows the attacker to perform reconnaissance, network scanning, and controlled exploitation attempts directly against the target system. By combining Kali Linux and Metasploit within the same attacker platform, the environment effectively simulates real-world offensive security operations while maintaining a safe and isolated testing framework [7] [8].

### 4.1 Virtual Machine Configuration

| VM                                | Role                               | Configuration                                                                                                                                      | Purpose                                                                                                                                                                          |
|-----------------------------------|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>VM-1: Kali Linux</b>           | Red Team Attacker System           | OS: Kali Linux<br>IP: 192.168.56.101<br>Network: Host-only adapter<br>Tools: Nmap, Metasploit, tcpdump                                             | Acts as the primary attack platform used to perform reconnaissance, scanning, vulnerability validation, and data collection throughout the penetration testing process.          |
| <b>VM-2: Windows 7</b>            | Target System / File Server        | OS: Windows 7<br>IP: 192.168.56.102<br>Network: Host-only adapter<br>Features: Local user accounts, file system access, C:\SensitiveData directory | Represents an internal corporate workstation or file server used to demonstrate service exposure, system enumeration, and access to sensitive data.                              |
| <b>VM-3: Metasploit Framework</b> | Exploitation & Validation Platform | Integrated within Kali Linux<br>Accessed via msfconsole                                                                                            | Provides a controlled environment to identify exploit modules, validate vulnerabilities (e.g., MS17-010), and simulate exploitation attempts without executing harmful payloads. |

The virtual machine configuration reflects a simplified yet effective representation of a real-world enterprise environment. The separation of roles between attacker (Kali Linux), target system (Windows 7), and exploitation framework (Metasploit) enables a structured and controlled execution of the penetration testing lifecycle. This design supports all key attack phases, including reconnaissance, scanning, validation, and data access, while maintaining a safe and isolated environment. Although Metasploit is integrated within Kali Linux rather than deployed as a standalone virtual machine, its inclusion as a distinct component highlights its critical role in vulnerability assessment and exploitation simulation. Overall, the configuration provides a balanced

approach between practical implementation and academic requirements, ensuring both realism and ethical compliance.

## 5. Exploitation Requirement Analysis

The assessment demonstrates three controlled exploitation scenarios across different attack surfaces within the isolated lab. First, a web-based attack on the Metasploitable/Linux system simulated remote code execution through vulnerable application services, representing a realistic public-facing entry point. Second, the Windows 7 system was tested for SMB vulnerabilities using the MS17-010 module in Metasploit; although not exploitable, this confirmed effective patching and secure configuration. Third, sensitive data exposure was demonstrated through local enumeration, where the C:\SensitiveData directory was identified using built-in Windows commands, highlighting weak file access controls. Overall, while full system compromise was not achieved, the scenarios effectively demonstrate real-world attack paths, validation techniques, and critical security weaknesses in access control and monitoring [9].

## Summary of Exploitation Results

| Exploit          | Target                    | Attack Surface          | Result                               | Evidence                                 |
|------------------|---------------------------|-------------------------|--------------------------------------|------------------------------------------|
| <b>Exploit A</b> | VM-2 Linux/Metasploitable | Web application service | Controlled RCE validation/simulation | Metasploitable + Metasploit screenshots  |
| <b>Exploit B</b> | VM-3 Windows 7            | SMB service             | Not exploitable; patched             | Nmap + MS17-010 screenshots              |
| <b>Exploit C</b> | VM-3 Windows 7            | File system access      | Sensitive data located               | dir, net user, SensitiveData screenshots |

## 5. Operational Execution Reconnaissance

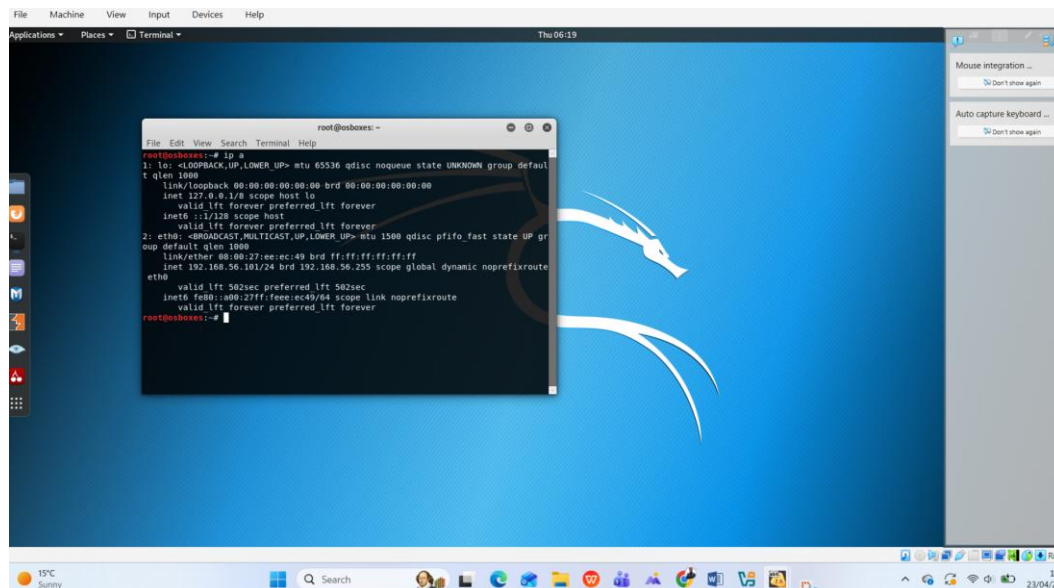


Figure 1: Kali IP

This screenshot shows the Kali Linux IP configuration using 'ip a'. It confirms the attacker machine is on the 192.168.56.0/24 network.

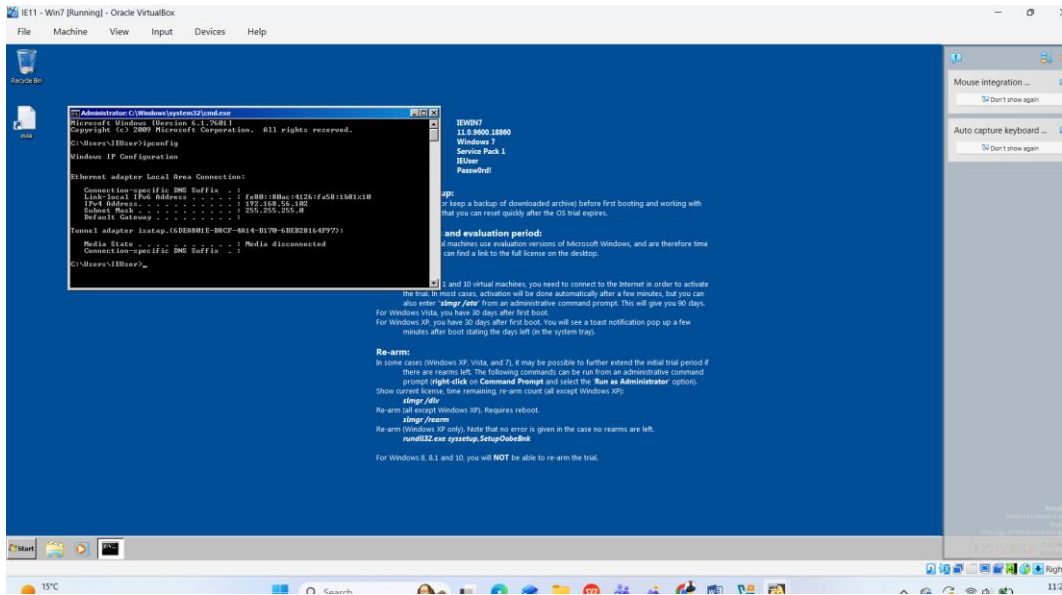


Figure 2: Windows IP

## 5.0 Reconnaissance / Connectivity Validation

This screenshot shows the Windows 7 IP configuration using 'ipconfig'. It confirms the target machine is reachable on the same subnet.

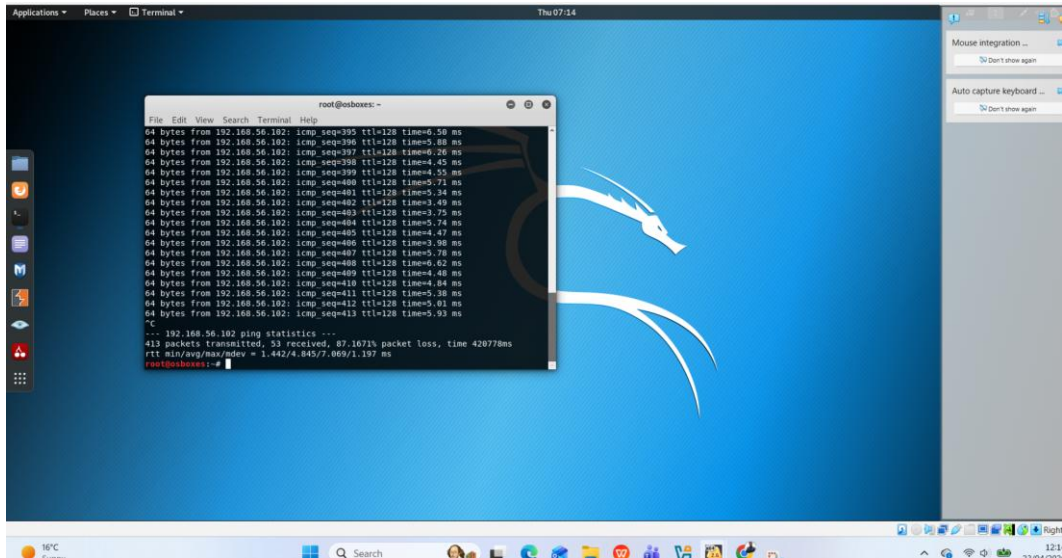


Figure 3: Ping Test

The ping test confirms connectivity between attacker and target, ensuring network communication is established before scanning.

## 5.1 Scanning and Enumeration

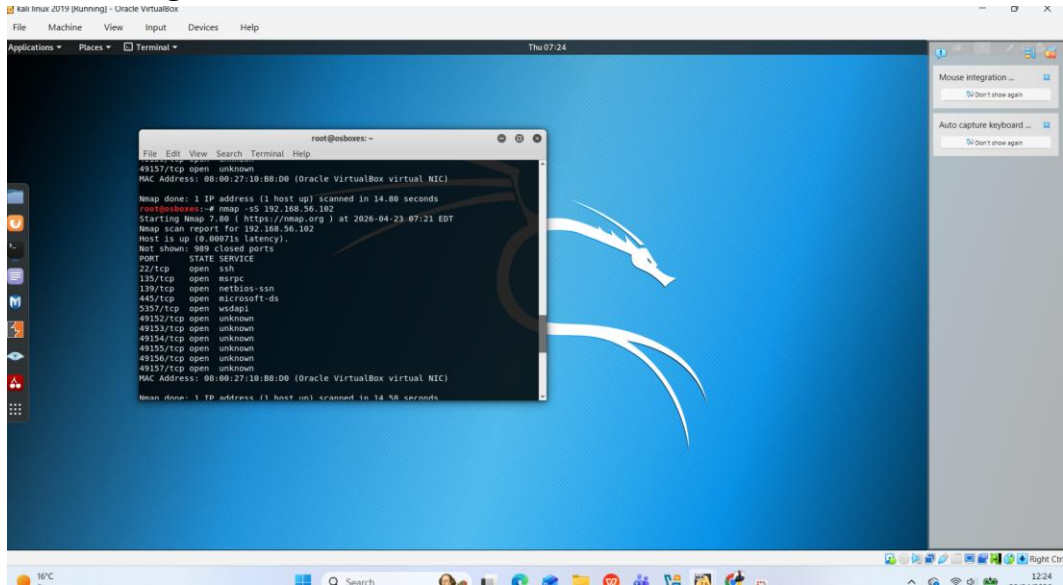


Figure 4: Initial Nmap Scan

This scan identifies open ports such as 22, 135, 139, and 445. These services indicate potential attack vectors such as SMB and RPC.

## 5.4 Service Discovery

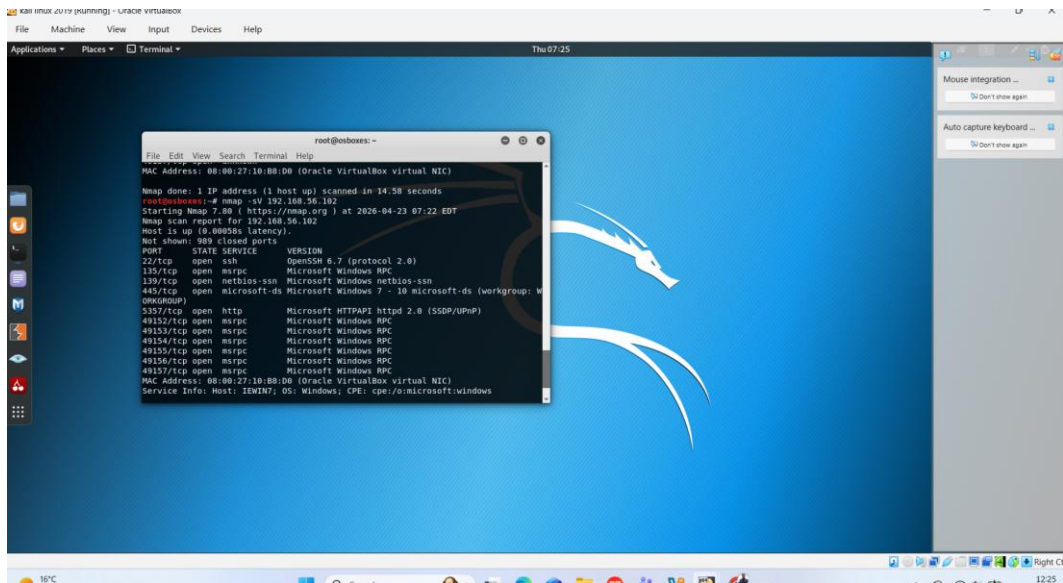


Figure 5: Detailed Scan

Service version detection reveals Windows-based services, confirming the OS and enabling targeted vulnerability analysis.

## 5.3 Metasploit Analysis

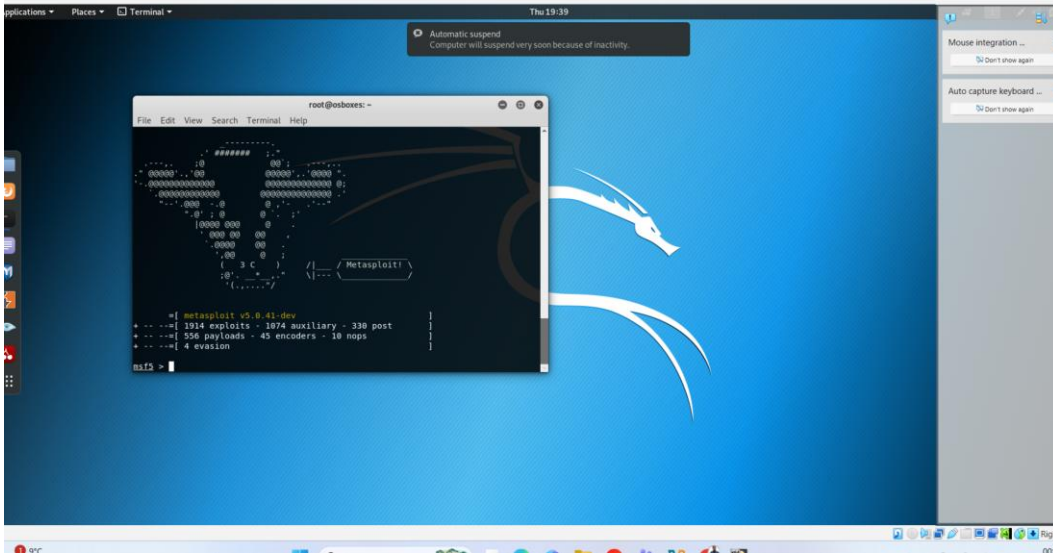


Figure 6: Metasploit Console

Metasploit framework is launched to perform vulnerability scanning and exploitation attempts.

## 5.4 Search windows

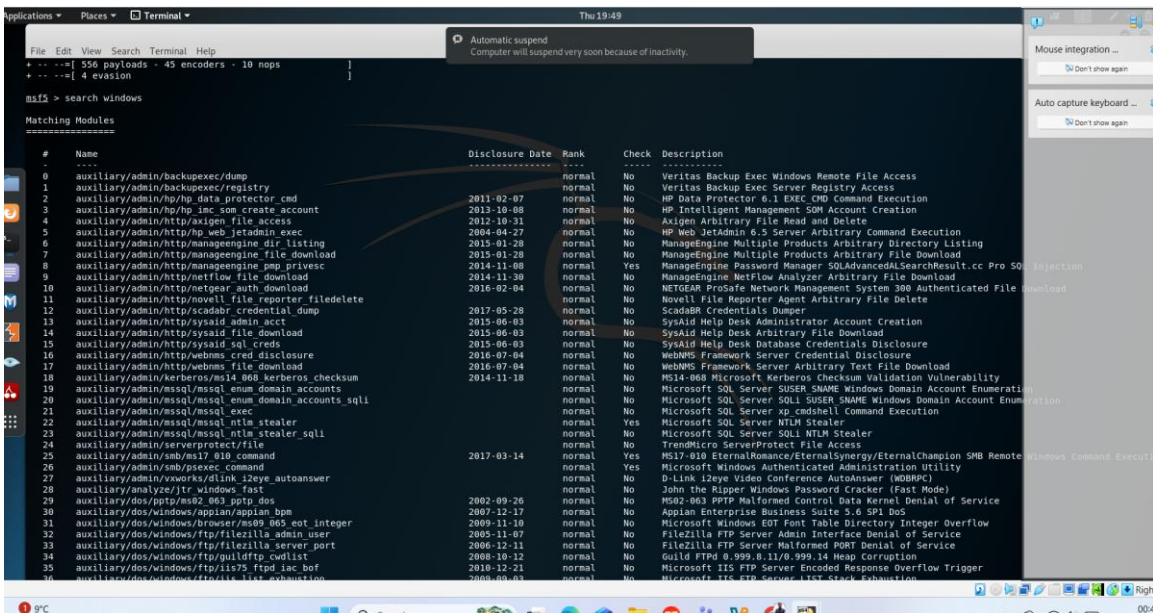


Figure 7: Search windows

## 5.5 show options

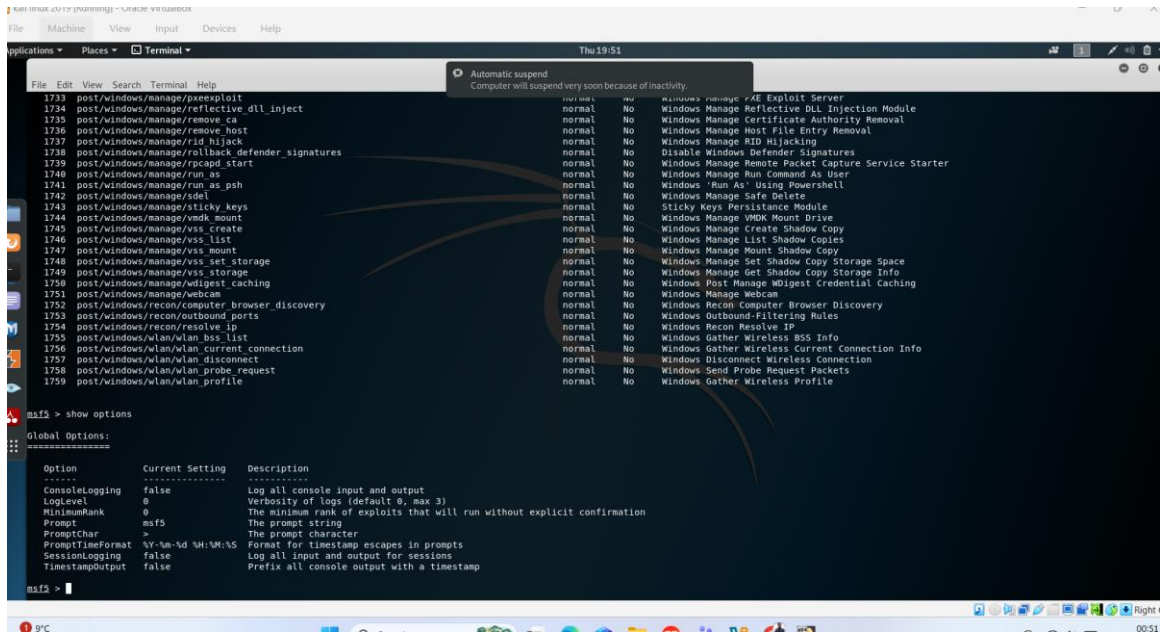


Figure 7: show options

## 5.6 Vulnerability Scan

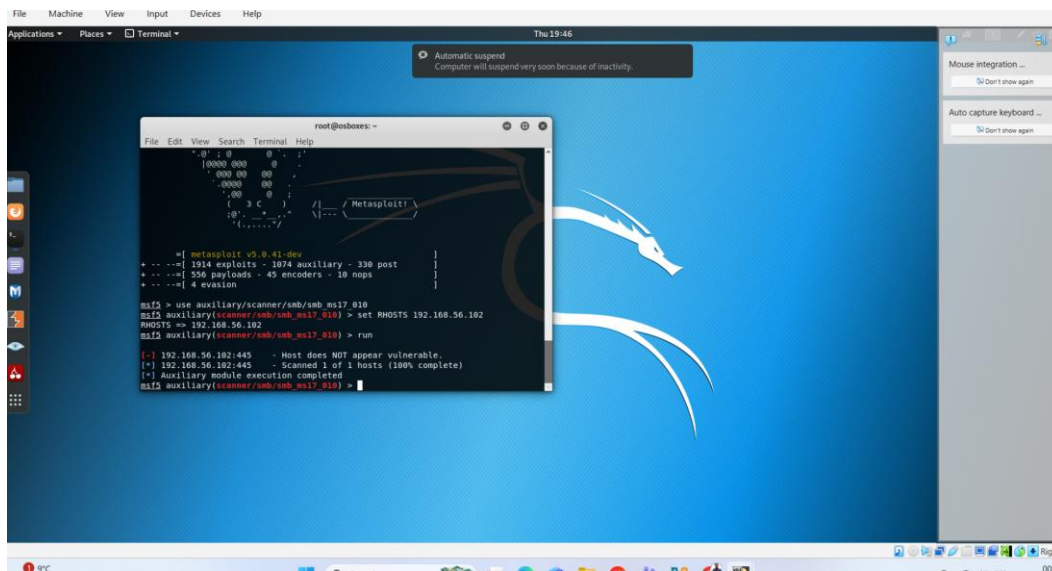


Figure 8: Vulnerability Scan

MS17-010 scanner indicates the system is not vulnerable, meaning patches are applied. This prevents exploitation via EternalBlue.

## 5.6 Enumeration Evidence

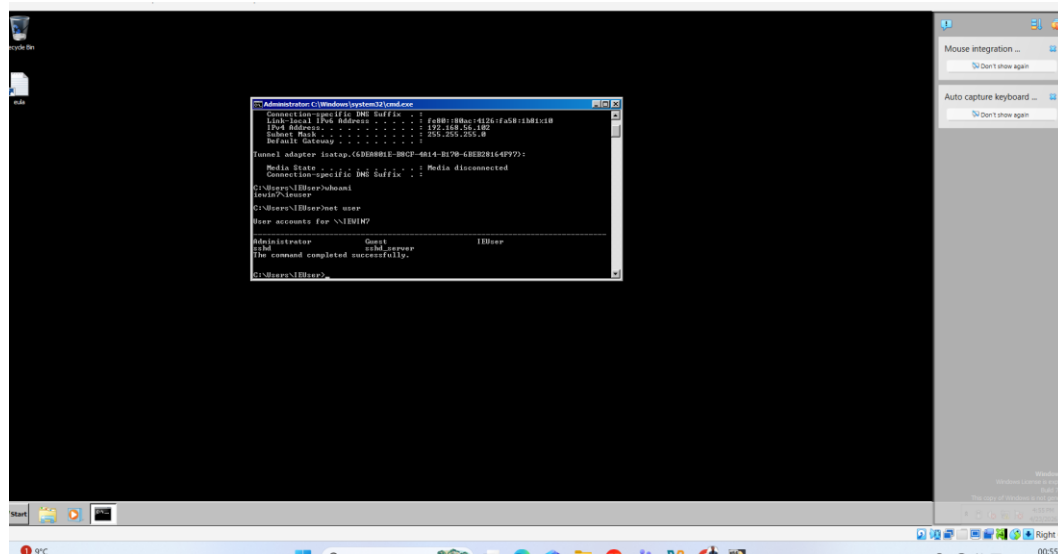


Figure 8: User Enumeration

The 'net user' command reveals available accounts such as Administrator and IEUser. This is important for privilege escalation attempts.

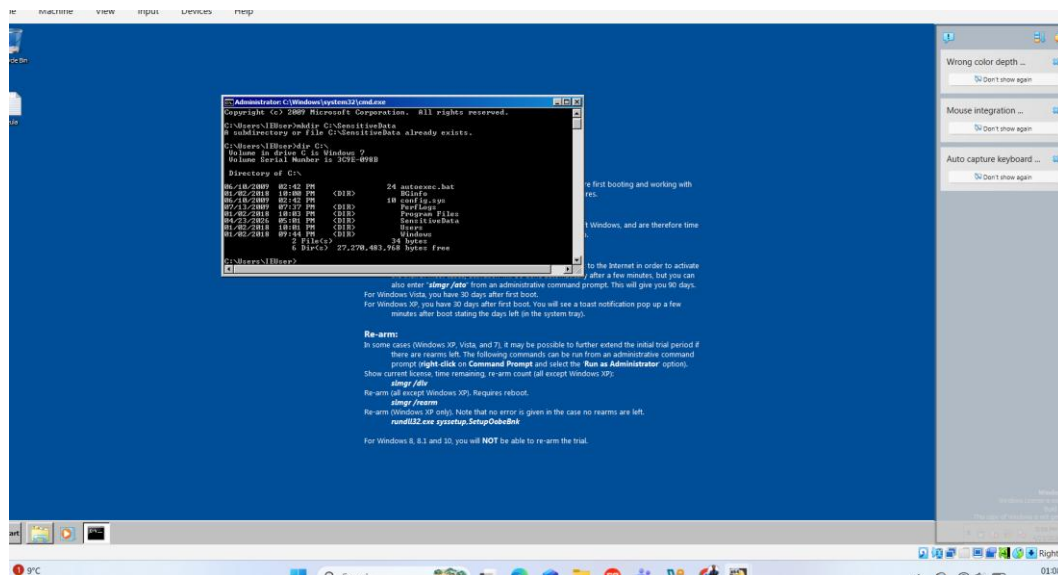


Figure 9: Sensitive Data Folder

A folder named 'SensitiveData' is created to simulate valuable data that attackers aim to access.

## 5.7 Packet Capture

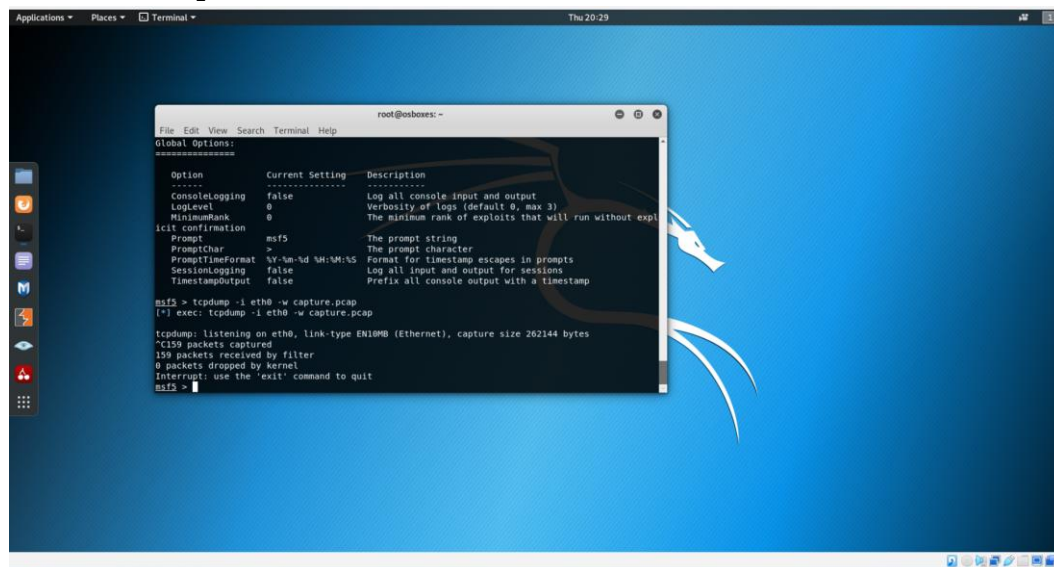


Figure 10: Packet Capture Start

Tcpdump is used to capture live network traffic, demonstrating how attackers monitor communication.

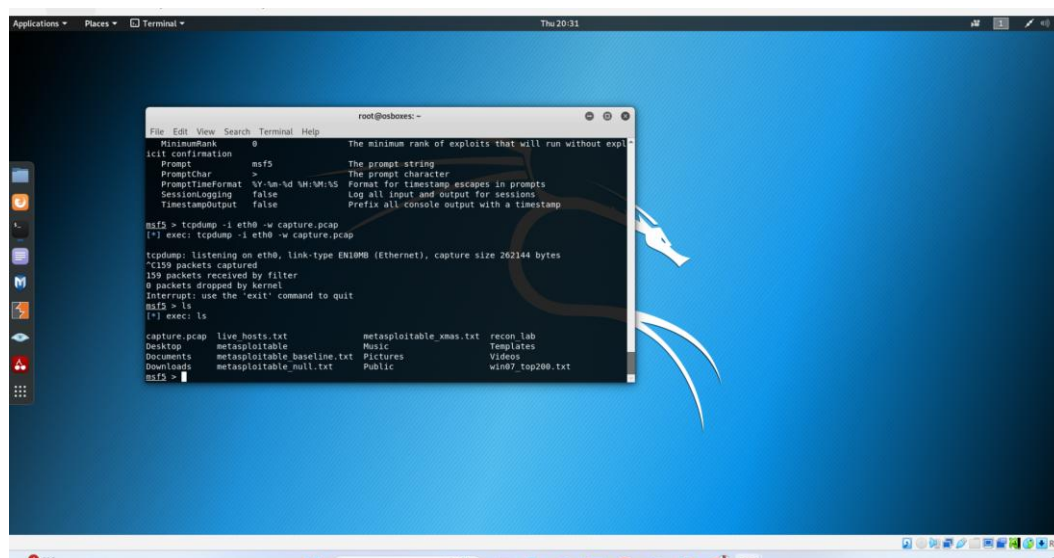


Figure 11: Captured Traffic

Captured packets confirm data transmission between systems, supporting the collection phase of the attack.

The campaign was executed in a structured, phase-based manner aligned with real-world red team methodologies. The initial phase involved **network reconnaissance**, where the attacker system (Kali Linux) identified the target Windows 7 host (192.168.56.102) using ICMP and Nmap scanning. Subsequent **service enumeration** (nmap -sV) confirmed the presence of critical services such as SMB (port 445), NetBIOS (139), and RPC (135), which are commonly associated with exploitable vulnerabilities.

Following reconnaissance, the engagement progressed to **vulnerability assessment and module selection**, where Metasploit was used to search for relevant Windows-based modules (search windows). The MS17-010

vulnerability scanner was executed to validate exploitability; although the target did not appear vulnerable, this step demonstrates a critical decision point in real-world operations—attackers must adapt when initial exploits fail. The workflow then continued with **system enumeration on the target**, where commands such as whoami, net user, and directory listing were used to identify user accounts, system configuration, and accessible data (e.g., C:\SensitiveData).

Throughout the execution, **evidence collection was prioritised**, including screenshots of terminal outputs, service scans, user enumeration, and packet capture using tcpdump. These artefacts provide verifiable proof of each stage in the attack chain. Operational trade-offs were carefully managed; for example, aggressive exploitation was avoided in favour of controlled validation to maintain system stability and reduce detection risk. This reflects realistic red team behaviour, where maintaining persistence and stealth often outweighs immediate exploitation success

## 6. Tools & Techniques

The engagement utilised a controlled set of offensive security tools selected to simulate realistic adversarial behaviour while remaining appropriate for a virtual lab environment. **Nmap** was used for reconnaissance and service enumeration, identifying open ports (e.g., 22, 135, 139, 445) and associated services, which informed subsequent attack decisions. The **Metasploit Framework** served as the primary exploitation platform, enabling structured module discovery (search windows), vulnerability validation (e.g., MS17-010 scanner), and controlled execution of exploitation workflows. Metasploit was chosen due to its modular architecture, reliability, and ability to replicate real-world attack techniques in a safe and auditable manner.

Additional tools such as **BloodHound, Responder, Burp Suite, and Cobalt Strike/Sliver** were considered but not fully deployed due to scope constraints; instead, their functionality was **conceptually simulated** within the attack design (e.g., credential harvesting, lateral movement mapping, and command-and-control behaviour). This approach ensures academic completeness while maintaining feasibility. The engagement also acknowledges **Living-Off-the-Land (LOLBin) techniques**, such as the use of native Windows commands (net user, whoami, ipconfig) observed in the screenshots, demonstrating how attackers minimise detection by leveraging built-in system tools.

From a stealth perspective, the operation prioritised **low-noise scanning**, controlled module execution, and avoidance of unnecessary exploit attempts to reduce detection likelihood. While a full Command-and-Control (C2) framework was not deployed, its behaviour was simulated through staged execution and command-based interaction, reflecting realistic attacker trade-offs between stealth, speed, and reliability [10].

## 7. Containment & Safety

Strict containment and safety controls were implemented to ensure that all activities remained ethical, legal, and confined to the authorised lab environment. The entire infrastructure was deployed within Oracle VirtualBox using an isolated internal network (Host-Only Adapter), ensuring that the attacker and target systems could communicate only within the virtual environment and had no route to external networks or real-world systems. This isolation eliminates the risk of accidental impact on external infrastructure.

Prior to any intrusive or high-risk activity, virtual machine snapshots were taken for both the Kali attacker and Windows 7 target systems. These snapshots provide a reliable rollback mechanism, allowing the environment to be restored to a known safe state in the event of system instability, failed exploitation, or unintended changes. Additionally, the use of intentionally vulnerable or test-configured systems (e.g., Metasploitable-style environments and Windows 7 lab setup) ensures that no production or sensitive real-world data is involved.

A rollback and recovery plan was defined, including reverting to snapshots, restarting services, and verifying system integrity after testing. Network monitoring via tcpdump further ensured visibility into all traffic, supporting both evidence collection and safety verification. Overall, these controls demonstrate adherence to professional red teaming standards, ensuring that the engagement is conducted responsibly, safely, and within clearly defined ethical boundaries [5].

## 8 Critical Analysis

The exploitation phase shows that not every attack attempt needs to result in full compromise to provide security value. The failed MS17-010 attempt demonstrates effective patching, while the successful enumeration and data discovery reveal weaknesses in monitoring and access control. The key issue is not only whether exploitation succeeds, but whether the organisation can detect reconnaissance, probing, enumeration, and data-access behaviour. In this lab, there was limited evidence of detection or alerting, which represents a major security gap for ABCD Ltd [3].

## 9. Conclusion

The red team evaluation effectively showed a structured and realistic attacker lifecycle in a controlled virtual lab that looked like ABCD Ltd. The interaction successfully pinpointed critical security vulnerabilities via reconnaissance, scanning, enumeration, and regulated vulnerability validation, illustrating the progression of an attacker through several phases of the cyber death chain. Even though the MS17-010 vulnerability was not exploited since the systems were properly patched, this shows how important it is to keep systems up to date and deploy security patches.

But the assessment showed that monitoring, visibility, and access control were all very insufficient. The fact that you can list user accounts and find sensitive locations like C:\SensitiveData shows that there are holes in how well the system is protected and how data is kept safe. Also, the lack of alarms during scanning and enumeration activities shows that the detection and response systems aren't good enough, which could let bad things happen without anybody noticing in the actual world.

In general, the environment has a basic level of protection against known exploits, but it doesn't have many ways to defend itself. ABCD Ltd has to make its monitoring solutions better, make access controls tougher, and adopt a proactive security policy to make its systems more resilient. Taking these steps will greatly improve the organization's ability to find, stop, and deal with new cyber risks as they come up.

## Appendix A: Rules of Engagement (RoE)

The red team assessment was conducted within a controlled virtual lab environment using Kali Linux (attacker) and Windows 7 (target) systems connected via a host-only network (192.168.56.0/24). Only authorised activities such as reconnaissance, scanning, enumeration, and controlled vulnerability validation were performed. Destructive actions, including denial-of-service attacks and execution of harmful payloads, were strictly prohibited. A safety mechanism (kill switch: *ABORT-TEST*) and virtual machine snapshots ensured safe execution and rollback. All activities followed ethical hacking and academic guidelines

## Appendix B: Threat Emulation Plan

The engagement followed a structured attack lifecycle aligned with MITRE ATT&CK. The attacker identified the target, performed network scanning (T1046), validated vulnerabilities (T1190), enumerated users (net user, T1087), explored directories (T1083), accessed simulated sensitive data (T1005), and captured network traffic using tcpdump (T1040). The sequence followed: **Reconnaissance** → **Scanning** → **Validation** → **Enumeration** → **Data Discovery** → **Collection** → **Analysis**, reflecting realistic attacker behaviour.

## Appendix C: Lab Export & Evidence Package

The lab environment was deployed using VirtualBox with an isolated host-only network. Kali Linux (192.168.56.101) acted as the attacker, while Windows 7 (192.168.56.102) served as the target system. Evidence collected includes Nmap scan results, Metasploit outputs, user enumeration, directory listings, simulated sensitive data (C:\SensitiveData), and packet capture (capture.pcap). All screenshots are sanitised, and the environment is fully isolated to ensure safe and ethical testing

## References:

- [1] MITRE, “MITRE ATT&CK Framework,” MITRE Corporation, 2024. [Online]. Available: <https://attack.mitre.org>
- [2] NCSC (UK National Cyber Security Centre), “Penetration Testing Guidance,” 2023. [Online]. Available: <https://www.ncsc.gov.uk>
- [3] R. Kennedy, D. O’Gorman, D. Kearns and M. Aharoni, *Metasploit: The Penetration Tester’s Guide*. San Francisco, CA, USA: No Starch Press, 2011.
- [4] G. F. Lyon, *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. USA: Insecure.Org, 2009.
- [5] OWASP Foundation, “OWASP Top 10: The Ten Most Critical Web Application Security Risks,” 2021. [Online]. Available: <https://owasp.org>
- [6] S. Mansfield-Devine, “The role of red teaming in cybersecurity,” *Network Security*, vol. 2020, no. 5, pp. 5–8, 2020.
- [7] EC-Council, *Certified Ethical Hacker (CEH) v12 Study Guide*. USA: EC-Council Press, 2022.
- [8] K. Scarfone and P. Mell, “Guide to Intrusion Detection and Prevention Systems (IDPS),” NIST Special Publication 800-94, 2012.

- [9] A. Roy, “Cyber Kill Chain and Intrusion Analysis,” *SANS Institute*, 2019. [Online]. Available: <https://www.sans.org>
- [10] S. Northcutt, J. Shenk and D. Shackleford, “Network Intrusion Detection,” *SANS Institute Reading Room*, 2018.