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

A Practical Investigation into Network Vulnerabilities and Exploitation Techniques Using Kali Linux in a Controlled Lab Environment

Student Name:	MD Monsuruzzaman
Student ID:	2504658
Programme:	MSc Cybersecurity and Digital Forensics
Institution:	University of Wales Trinity Saint David London
Module:	Ethical Hacking
Module Code:	ACCA7033
Lecturer:	Anum Paracha
Submission Date:	1st May 2026

Table of Contents

Abstract 3

1. Introduction 3

2. Task 1 – Strategic Threat Analysis 4

2.1 Incident Overview 4

2.2 Timeline of Attack 5

2.3 MITRE ATT&CK Mapping 6

2.4 Root Cause Analysis 7

2.5 Threat Actor Analysis 7

2.6 Detection & Response 8

2.7 Recommendations 8

3. Task 2 – Red Team Engagement 9

3.1 Rules of Engagement 9

3.2 Threat Emulation Plan 9

3.3 Penetration Testing Methodology 10

3.4 Lab Environment Setup 13

3.5 Tools Used 14

3.6 Attack Execution 15

3.7 SQL Injection 16

3.8 IRC Exploit 19

3.9 Social Engineering 20

3.10 Post Exploitation 21

3.11 Vulnerability Scanning 22

3.12 MITRE Mapping 22

3.13 Detection Gap Analysis 22

4. Analysis of Attack Techniques 23

5. Conclusion 28

6. References 29

Abstract

This report explores offensive cybersecurity practices through two main components: a strategic analysis of recent cyber attacks affecting UK organisations (Task 1) and a practical red team engagement conducted within a controlled lab environment (Task 2). The first part examines real-world incidents, focusing on attacker behaviour, techniques used, and the security weaknesses that enabled these attacks. It also considers how these attacks align with recognised frameworks such as the Cyber Kill Chain and MITRE ATT&CK.

The second part demonstrates a full penetration testing process using tools such as Nmap, Metasploit, Burp Suite, SQLMap, and the Social Engineering Toolkit. The assessment includes reconnaissance, scanning, exploitation, and post-exploitation activities performed on a vulnerable system. Several attack scenarios were successfully executed, including SQL injection, IRC backdoor exploitation, and a social engineering simulation, highlighting how different vulnerabilities can be exploited in practice.

The findings identify key security issues, including poor input validation, outdated services, and insufficient monitoring. Overall, this report demonstrates how theoretical concepts and practical skills can be combined to understand modern cyber threats and emphasises the importance of strong security practices, user awareness, and continuous monitoring.

1. Introduction

Ethical hacking, also known as penetration testing, is a proactive cybersecurity approach used to identify and mitigate vulnerabilities before they can be exploited by malicious actors. It involves simulating real-world attack scenarios within a controlled environment to evaluate an organisation's security posture and resilience.

With the increasing prevalence of Advanced Persistent Threats (APTs), cyber attacks have become more sophisticated, targeting not only technical systems but also human behaviour and organisational processes. In this context, red teaming extends beyond traditional penetration testing by emulating real attackers' tactics, techniques, and procedures (TTPs), providing a more comprehensive assessment of security weaknesses.

This assessment is divided into two main components. Task 1 focuses on the analysis of real-world cyber incidents affecting UK retail organisations, examining how attacks occur, the techniques used by adversaries, and the underlying security failures. Task 2 involves the design and execution of a full red team engagement within a controlled virtual lab environment, simulating realistic attack scenarios.

The objective of this report is to develop both strategic and technical understanding of modern cyber threats, while demonstrating practical skills in vulnerability identification, exploitation, and post-exploitation analysis. Additionally, the report aims to evaluate the effectiveness of existing

security controls and provide recommendations to enhance organisational resilience against evolving cyber threats.

2. Task 1 – Strategic Threat Analysis

2.1 Incident Overview

Recent cyber incidents affecting major UK retail organisations such as Marks & Spencer (M&S) and the Co-operative Group (Co-op) highlight the increasing sophistication of modern cyber threats targeting critical commercial infrastructure. These attacks demonstrate how threat actors leverage a combination of technical vulnerabilities, social engineering, and supply chain weaknesses to achieve their objectives [1].

Retail organisations are particularly attractive targets due to the large volume of sensitive customer data they process, including payment details, personal information, and supply chain data. Additionally, their reliance on interconnected digital systems increases the attack surface, making them vulnerable to multi-stage cyber attacks. In both cases, publicly available reports suggest that attackers exploited weaknesses in authentication mechanisms and potentially leveraged phishing-based initial access vectors. Phishing remains one of the most common attack vectors due to its effectiveness in bypassing technical controls by targeting human vulnerabilities. Once initial access is achieved, attackers typically deploy malware or establish persistence mechanisms to maintain long-term access within the compromised network. The incidents affecting M&S and Co-op are believed to follow patterns consistent with ransomware or financially motivated cybercrime campaigns. These campaigns often involve data exfiltration followed by extortion, where attackers threaten to release sensitive data unless a ransom is paid. This aligns with broader trends in cybercrime, where ransomware-as-a-service (RaaS) models enable even less technically skilled attackers to conduct sophisticated attacks [2] - [5].

Furthermore, these incidents demonstrate how attackers increasingly combine multiple techniques, including credential harvesting, privilege escalation, and lateral movement, to compromise entire organisational infrastructures. This multi-stage attack approach is characteristic of Advanced Persistent Threat (APT) like behaviour, even when conducted by financially motivated groups [6].

2.2 Timeline of Attack

A structured timeline of cyber attacks is essential to understanding how adversaries progress through different stages of compromise. Based on industry frameworks such as the Cyber Kill Chain and MITRE ATT&CK, the attack lifecycle can be broken down into several key phases.

- **Initial Access**

  The attack typically begins with initial access, often achieved through phishing emails, compromised credentials, or exploitation of publicly exposed services. Phishing attacks may include malicious links or attachments designed to trick users into revealing credentials or executing malware.

- **Execution**

  Once access is obtained, attackers execute malicious code within the target environment. This may involve running scripts, deploying malware, or exploiting vulnerabilities in applications.

- **Persistence**

  To maintain access, attackers establish persistence mechanisms such as backdoors, scheduled tasks, or registry modifications. These techniques ensure that attackers can regain access even if the system is restarted.

- **Privilege Escalation**

  Attackers then attempt to elevate their privileges to gain administrative access. This is often achieved by exploiting system vulnerabilities or misconfigurations.

- **Lateral Movement**

  After gaining higher privileges, attackers move laterally across the network using tools such as remote desktop protocols, credential reuse, or pass-the-hash attacks.

- **Data Exfiltration**

  Sensitive data is collected and transferred outside the organisation. This may involve encrypted channels or disguised traffic to avoid detection.

- **Impact**

  Finally, attackers execute their primary objective, which may include data encryption (ransomware), system disruption, or financial theft.

This structured progression demonstrates how attackers systematically compromise organisations while avoiding detection [1] - [4], [7].

2.3 MITRE ATT&CK Mapping

The MITRE ATT&CK framework provides a comprehensive model for analysing adversary behaviour based on observed tactics and techniques. Mapping the attack to this framework enables a deeper understanding of how each stage contributes to the overall compromise.

Table 1: Mapping of identified attack techniques to the MITRE ATT&CK framework, illustrating the relationship between adversary tactics, techniques, and corresponding technique IDs used during the attack lifecycle.

Tactic	Technique	ID	Explanation
Initial Access	Phishing	T1566	Users are tricked into revealing credentials or executing malware
Execution	Command-Line Interface	T1059	Attackers execute malicious commands
Persistence	Registry Run Keys / Startup Folder	T1547	Ensures continued access
Privilege Escalation	Exploitation for Privilege Escalation	T1068	Exploits system vulnerabilities
Credential Access	Credential Dumping	T1003	Extracts stored credentials
Discovery	Network Service Scanning	T1046	Identifies services and systems
Lateral Movement	Remote Services	T1021	Moves across systems
Collection	Data from Local System	T1005	Gathers sensitive data
Exfiltration	Exfiltration Over Web Services	T1041	Transfer data externally
Impact	Data Encrypted for Impact	T1486	Encrypts systems (ransomware)

Each of these techniques has been widely observed in real-world attacks, making MITRE ATT&CK a critical framework for both offensive and defensive cybersecurity strategies [1].

2.4 Root Cause Analysis

The success of these cyber attacks can be attributed to a combination of technical, human, and organisational failures.

- **Technical Failures**

  One of the primary technical causes is the presence of unpatched vulnerabilities. Many organisations fail to apply security updates promptly, leaving systems exposed to known exploits [12]. Additionally, weak input validation mechanisms enable attacks such as SQL injection, which can lead to unauthorised database access [4]. Misconfigured systems also contribute significantly to security breaches. Incorrect firewall rules, exposed services, and weak authentication mechanisms increase the likelihood of exploitation [14].

- **Human Factors**

  Human error remains one of the most significant contributors to cyber incidents. Employees may fall victim to phishing attacks, reuse passwords, or fail to recognise suspicious activity [3]. Social engineering techniques exploit psychological factors such as trust and urgency, making them highly effective [15].

- **Organisational Weaknesses**

  Organisational shortcomings include insufficient monitoring, lack of incident response planning, and inadequate security policies. Many organisations lack proper network segmentation, allowing attackers to move freely once inside the network [16].

Additionally, insufficient security awareness training results in employees being unable to identify and respond to threats effectively [17].

2.5 Threat Actor Analysis

The threat actors involved in these incidents are likely financially motivated cybercriminal groups. These groups often operate using organised structures and advanced tools, enabling them to conduct large-scale attacks [5].

Ransomware groups, in particular, have become increasingly sophisticated, using double extortion techniques where data is both encrypted and stolen [4]. This increases pressure on victims to pay ransoms.

In some cases, attackers may also leverage initial access brokers (IABs), who specialise in gaining access to systems and selling it to other cybercriminals [18]. This division of labour within the cybercrime ecosystem increases efficiency and scalability.

The attackers' use of multiple techniques, including phishing, privilege escalation, and lateral movement, indicates a high level of capability and planning. While not necessarily state-sponsored, these actors demonstrate behaviours similar to advanced threat groups.

2.6 Detection & Response

- A critical aspect of these incidents is the failure of detection and response mechanisms.
- Many organisations rely on traditional security tools that are ineffective against modern threats. For example, signature-based antivirus systems may fail to detect new or customised malware [19].
- The absence of Security Information and Event Management (SIEM) systems or improper configuration of logging mechanisms can result in delayed detection of suspicious activity [20]. Without proper visibility, attackers can remain undetected for extended periods.
- Additionally, incident response processes are often slow or poorly coordinated. This allows attackers to escalate their activities before containment measures are implemented [21].
- Another significant issue is alert fatigue, where security teams are overwhelmed by large volumes of alerts and may miss critical threats [22].

2.7 Recommendations

To mitigate future attacks, organisations must implement a comprehensive security strategy that addresses prevention, detection, and response.

Prevention

- Implement Multi-Factor Authentication (MFA) to reduce credential-based attacks [23]
- Apply regular patch management to eliminate known vulnerabilities [12]
- Use secure coding practices to prevent injection attacks [13]

Detection

- Deploy SIEM systems for real-time monitoring [20]
- Enable detailed logging and anomaly detection
- Use Endpoint Detection and Response (EDR) tools

Response

- Develop and regularly test incident response plans [21]
- Conduct security awareness training for employees [17]
- Implement network segmentation to limit lateral movement [16]

These measures provide a layered defence approach, significantly reducing the likelihood and impact of cyber attacks.

3. Task 2 - Red Team Engagement

3.1 Rules of Engagement (RoE)

A Rules of Engagement (RoE) document defines the legal, ethical, and operational boundaries of a penetration testing engagement. It ensures that all testing activities are conducted safely, ethically, and within the agreed scope [1].

For this engagement, the scope was limited to a controlled virtual lab environment representing ABCD Ltd's infrastructure. The lab included three primary systems: a Kali Linux attacker machine, a Metasploitable server, and a vulnerable web application environment. All activities were conducted in isolation using a host-only network configuration to prevent unintended impact on external systems.

The permitted techniques included reconnaissance, vulnerability scanning, exploitation, and post-exploitation activities. However, destructive actions such as denial-of-service (DoS) attacks or permanent system modifications were excluded to maintain system stability [2].

A rollback strategy was implemented through virtual machine snapshots, allowing the environment to be restored in case of failure or instability. This ensures safe experimentation and aligns with ethical hacking best practices [3].

Communication protocols were also defined, ensuring that any critical findings would be documented and reported systematically. This structured approach reflects professional red team engagements, where transparency and accountability are essential.

3.2 Threat Emulation Plan

The threat emulation plan was designed to simulate a realistic attack scenario aligned with known adversary tactics. The objective was to gain unauthorised access to systems and extract sensitive data, thereby demonstrating the effectiveness of offensive security techniques.

The attack was structured into four key phases:

1. **Reconnaissance**

   The first phase involved gathering information about the target systems, including identifying IP addresses, active hosts, and network configurations. Tools such as ARP scan and ping were used to map the network [4].

2. **Scanning and Enumeration**

   Once targets were identified, detailed scanning was performed using Nmap to identify open ports, services, and potential vulnerabilities. Service version detection provided insights into exploitable weaknesses [5].

3. **Exploitation**

   The exploitation phase involved leveraging identified vulnerabilities to gain access to systems. Multiple attack vectors were used, including remote service exploitation and web application attacks.

4. **Post-Exploitation**

   After gaining access, further actions were performed to escalate privileges, gather data, and maintain persistence within the system. This phase demonstrates the full impact of a successful compromise [6].

This structured approach reflects real-world attack methodologies and aligns with frameworks such as the MITRE ATT&CK model [7].

3.3 Penetration Testing Methodology

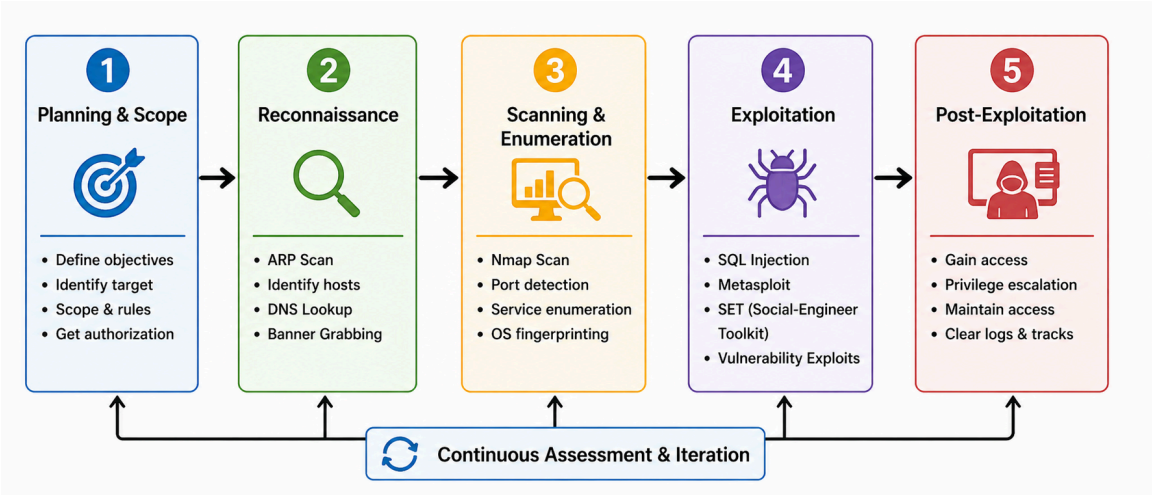

Figure 1: Penetration testing methodology followed in this assessment, aligned with NIST and OWASP testing frameworks.

As illustrated in Figure 1, the penetration testing process followed a structured methodology aligned with industry standards such as NIST and OWASP. This approach ensures a systematic assessment of vulnerabilities and minimizes risks during testing. The process began with planning and scoping, where objectives, target systems, and rules of engagement were defined. This was

followed by reconnaissance to gather information about the target environment. Next, scanning and enumeration were conducted using tools such as Nmap to identify open ports, services, and potential vulnerabilities. Based on these findings, exploitation techniques were applied to gain initial access.

Finally, post-exploitation activities were performed to assess the impact, including privilege escalation and maintaining access. The methodology ensures a complete understanding of system weaknesses and their potential risks.

3.3.I Planning and Scope Definition

The initial phase of the penetration test involved defining the scope, objectives, and boundaries of the assessment. The testing was conducted within a controlled virtual lab environment using Oracle VirtualBox, consisting of a Kali Linux attacker machine and a Metasploitable vulnerable target system. This ensured that all activities were performed ethically and without risk to real-world systems [3], [9].

The primary objective of the test was to identify vulnerabilities, exploit them, and assess their impact on system confidentiality, integrity, and availability.

3.3.II Reconnaissance (Information Gathering)

The reconnaissance phase involved identifying active hosts and gathering preliminary information about the target environment. Tools such as ARP scanning were used to discover devices within the local network. This passive and active information gathering process provided essential data required for further analysis [4], [5].

This phase aligns with the “Discovery” stage of penetration testing frameworks, where attackers map the target environment before launching attacks.

3.3.III Scanning and Enumeration

Following reconnaissance, active scanning techniques were used to identify open ports, services, and potential vulnerabilities. The Nmap tool was used to perform service detection and operating system fingerprinting.

The scan results revealed multiple open ports, including FTP (21), HTTP (80), and IRC (6667), indicating the presence of vulnerable services such as vsFTPd and UnrealIRCd. This phase is critical as it identifies entry points for exploitation [4], [5].

3.3.IV Exploitation

The exploitation phase involved actively leveraging identified vulnerabilities to gain unauthorised access to the target system.

Multiple attack techniques were applied:

SQL Injection was used against the Mutillidae web application to bypass authentication and extract database information. Automated tools such as SQLMap were used to enumerate databases and retrieve sensitive data, demonstrating a failure in input validation mechanisms [12].

A remote exploitation attack was conducted using the Metasploit Framework targeting the UnrealIRCd backdoor vulnerability. This resulted in successful remote shell access, confirming full system compromise [13].

Social engineering techniques were also employed using the Social Engineering Toolkit (SET) to create phishing pages and capture user credentials, highlighting human vulnerabilities in cybersecurity [14].

This phase aligns with the "Exploitation" stage in penetration testing frameworks and demonstrates real-world attack scenarios.

3.3.V Post-Exploitation

Once access was gained, post-exploitation activities were performed to assess the impact of the compromise. Commands such as 'whoami' and 'uname -a' were executed to confirm privilege levels and system information.

Additionally, database contents were accessed and credentials were extracted, demonstrating the potential for data breaches and lateral movement within a network. This phase reflects real-world attacker behaviour as described in the MITRE ATT&CK framework [7].

3.3.VI Reporting and Documentation

The final phase involves documenting findings, vulnerabilities, and their impact. This assessment provides a detailed analysis of each attack performed, supported by evidence from the lab environment.

The inclusion of screenshots, tool outputs, and technical explanations ensures that the report meets professional penetration testing standards. Recommendations for mitigation and security improvements are also provided to reduce future risk.

Overall, the methodology used in this assessment reflects a complete penetration testing lifecycle, demonstrating both theoretical understanding and practical application of offensive security techniques in a controlled environment.

3.4 Lab Environment Setup

The lab environment was designed to simulate a realistic corporate network while ensuring complete isolation. The setup included:

- **Kali Linux (Attacker Machine)**
- **Metasploitable (Vulnerable Server)**
- **Mutillidae Web Application (Web Target)**

All systems were configured using a host-only network, enabling secure communication between virtual machines without external connectivity. This ensures compliance with ethical and legal standards [3].

The Metasploitable system was intentionally configured with known vulnerabilities, including outdated services such as FTP, IRC, and web applications. This allowed for controlled testing of exploitation techniques [8].

The use of virtualisation provides flexibility and safety, enabling repeated testing without risk to real-world systems. This approach is widely used in cybersecurity education and professional training environments [9].

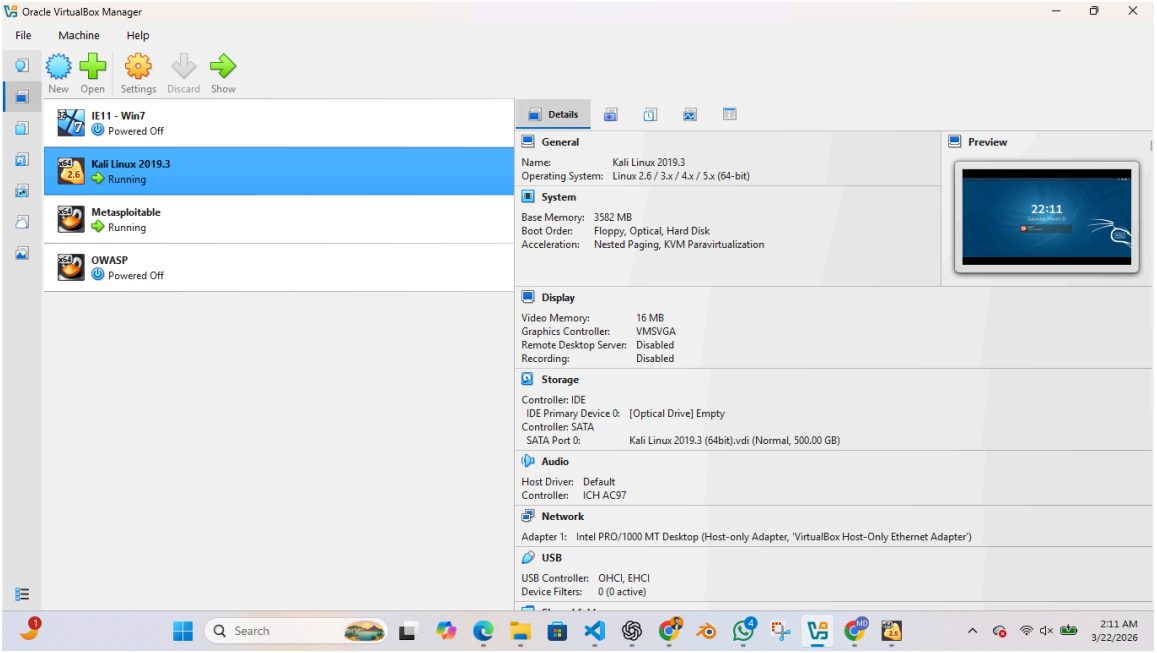

Figure 2: Virtual lab environment configured in Oracle VirtualBox showing Kali Linux attacker and Metasploitable target systems connected via a host-only network.

A controlled virtual lab environment was established to safely conduct penetration testing activities. The lab consisted of two virtual machines configured using Oracle VirtualBox. Kali Linux was used as the attacker machine, while Metasploitable 2 was deployed as the vulnerable target system.

Both machines were connected using a host-only network to ensure isolation from external networks. The assigned IP addresses were 192.168.56.101 for Kali Linux and 192.168.56.102 for Metasploitable 2. This setup allowed secure testing of vulnerabilities such as SQL injection, remote exploitation, and privilege escalation without impacting real-world systems.

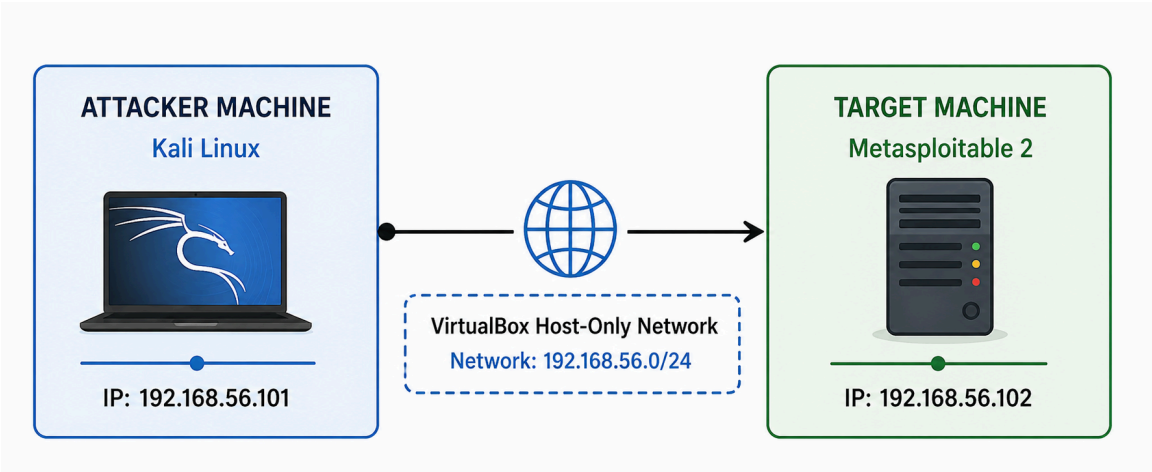

Figure 3: Network architecture of the lab environment showing communication between Kali Linux and Metasploitable via a host-only network.

3.5 Tools Used

A range of industry-standard tools was used during the engagement, each selected based on its capabilities and relevance to the attack scenario.

- **Nmap**: Used for network scanning and service enumeration
- **Metasploit Framework**: Used for exploitation of vulnerabilities
- **Burp Suite**: Used for web application testing
- **SQLMap**: Used for automated SQL injection attacks
- **Social Engineering Toolkit (SET)**: Used for phishing simulation

These tools are widely recognised in penetration testing and are commonly used by both ethical hackers and malicious actors [10].

Additionally, Living-Off-the-Land (LOLBins) techniques were considered, where built-in system tools are used to perform malicious actions without introducing external malware. This helps evade detection and reflects real-world attacker behaviour [11].

3.6 Attack Execution

The attack execution followed a structured methodology, beginning with reconnaissance and progressing through exploitation and post-exploitation.

Reconnaissance

Initial reconnaissance identified the target IP address and confirmed connectivity using ping. ARP scanning revealed active hosts within the network, providing a clear understanding of the attack surface.

Scanning

Nmap scanning revealed multiple open ports, including:

- Port 21 (FTP)
- Port 80 (HTTP)
- Port 6667 (IRC)

Service version detection identified outdated and vulnerable services, making them suitable targets for exploitation [5].

Analysis

The scanning results indicated several potential vulnerabilities, including known backdoors and weak authentication mechanisms. These findings guided the selection of appropriate exploits.

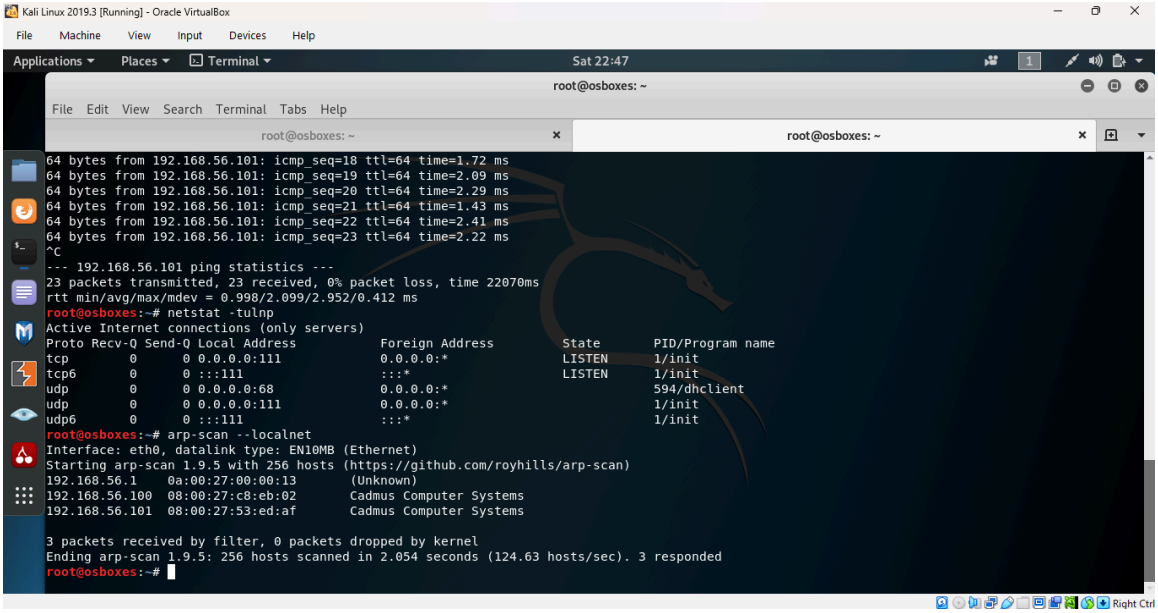

Figure 4: ARP scan results identifying active hosts within the local network, enabling target discovery during the reconnaissance phase.

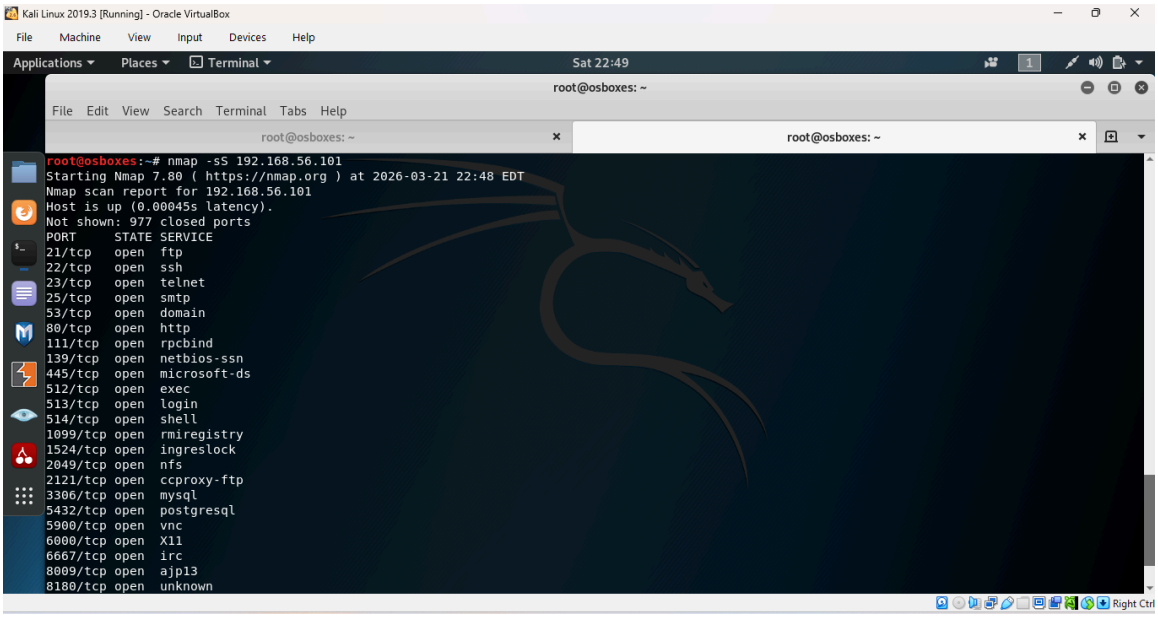

Figure 5: Nmap scan identifying open ports (21, 80, 6667) and vulnerable services, forming the foundation for selecting appropriate exploitation techniques.

3.7 Exploit 1 – SQL Injection

- SQL Injection is a web application vulnerability that allows attackers to manipulate database queries through unsanitised user input [12].
- In this engagement, a vulnerable login form within the Mutillidae web application was targeted. A simple payload (`' OR '1'='1`) was used to bypass authentication, demonstrating a failure in input validation mechanisms.
- Further exploitation was conducted using SQLMap, which automated the process of database enumeration and data extraction. The tool successfully identified available databases, extracted tables, and retrieved user credentials.
- This demonstrates how SQL injection can lead to full database compromise, exposing sensitive information such as usernames and passwords. It highlights the importance of secure coding practices, including parameterised queries and input validation [4].

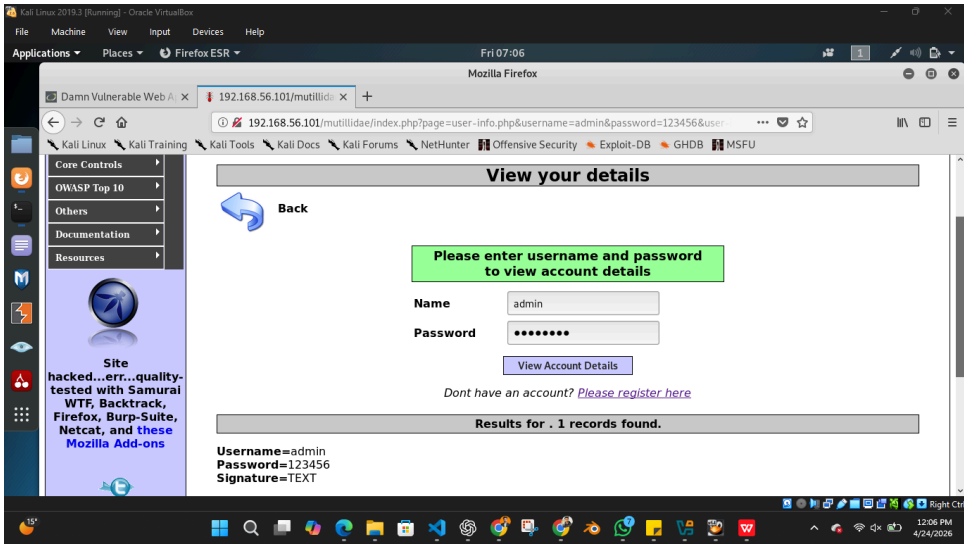

Figure 6: Successful authentication bypass using SQL Injection payload (' OR '1'='1), demonstrating failure in input validation mechanisms.

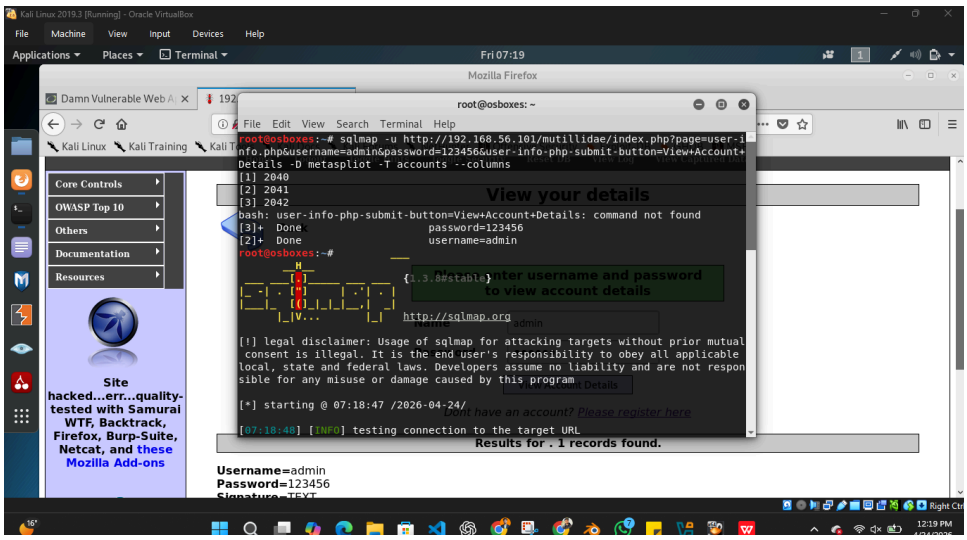

Figure 7: SQLMap identifying SQL Injection vulnerability in the web application, confirming exploitable input fields.

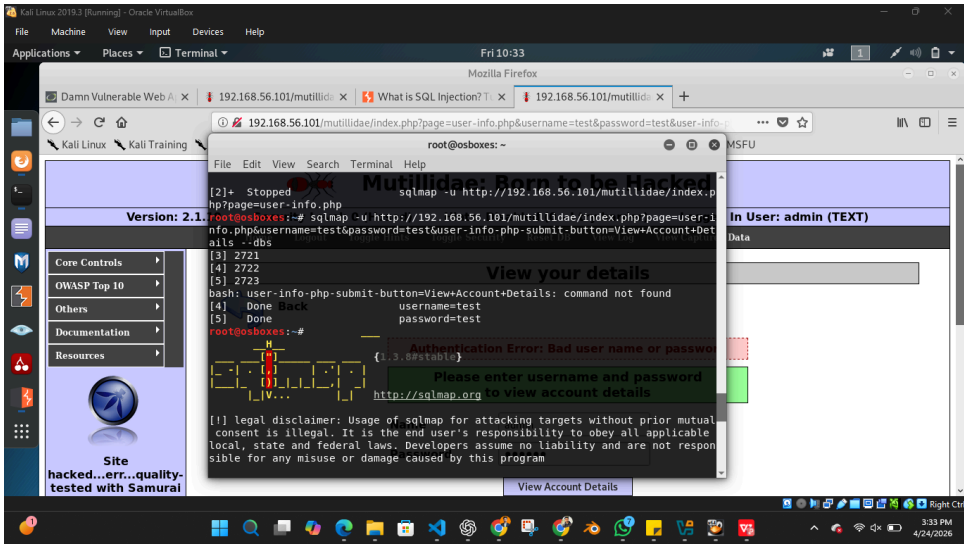

Figure 8: SQLMap enumerating databases and extracting sensitive data, demonstrating full database compromise.

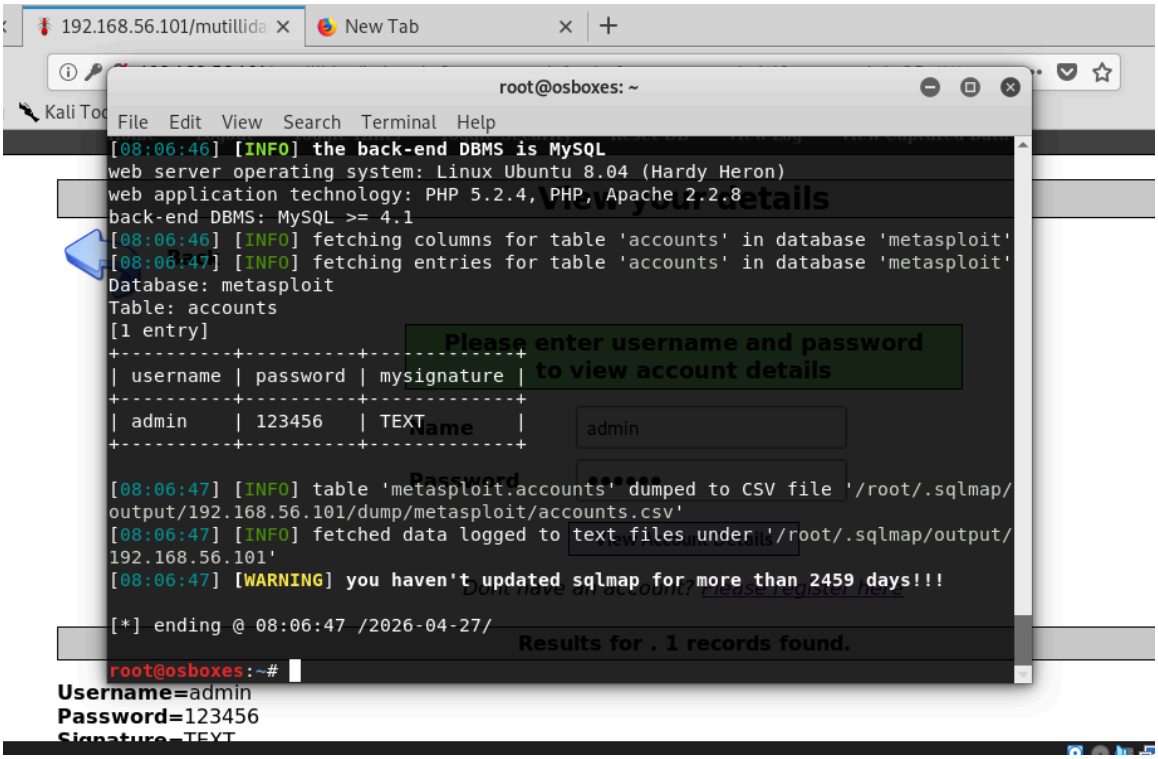

Figure 9: Extracted user credentials from the database, confirming successful exploitation and breach of data confidentiality.

3.8 Exploit 2 - Metasploit IRC Exploit

The second exploit targeted the UnrealIRCd service running on port 6667. This service is known to contain a backdoor vulnerability that allows remote command execution.

An initial attempt using an FTP-based exploit (vsftpd) was unsuccessful, demonstrating that not all vulnerabilities are exploitable in practice. However, an alternative exploit targeting the IRC service was successfully executed using the Metasploit Framework.

The exploit resulted in a remote command shell, providing full control over the target system. Commands such as `whoami` confirmed root-level access, indicating a complete system compromise.

This demonstrates the importance of adaptability in penetration testing, where multiple attack vectors may need to be explored to achieve success [7].

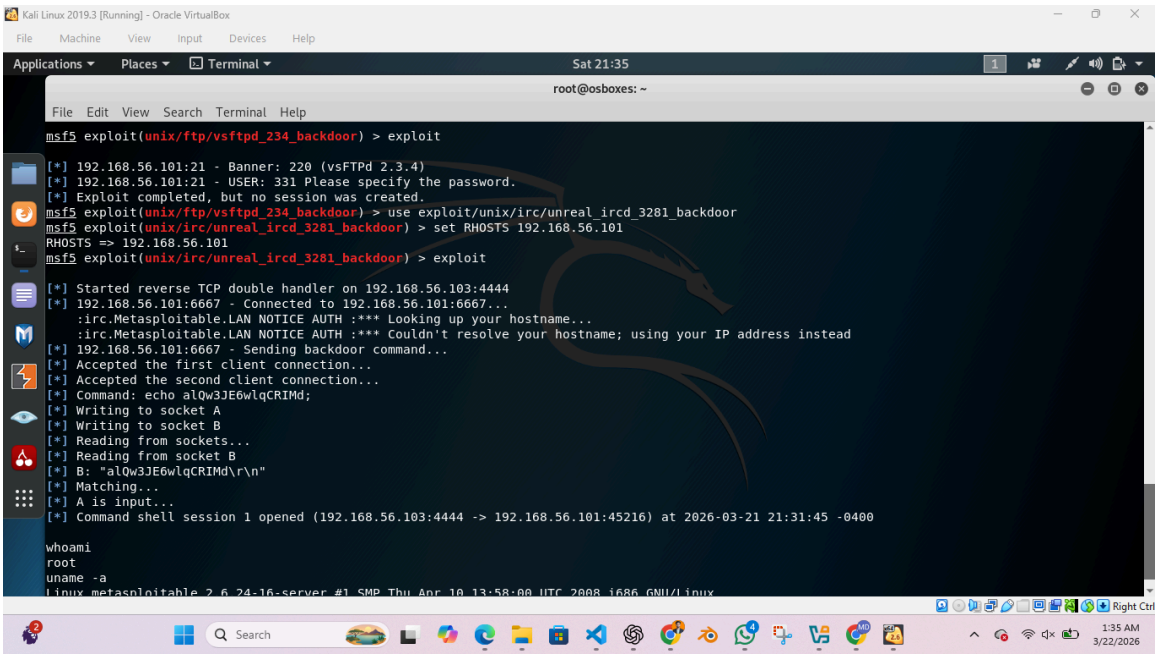

Figure 10: Metasploit module configured to exploit the UnrealIRCd backdoor vulnerability on port 6667.

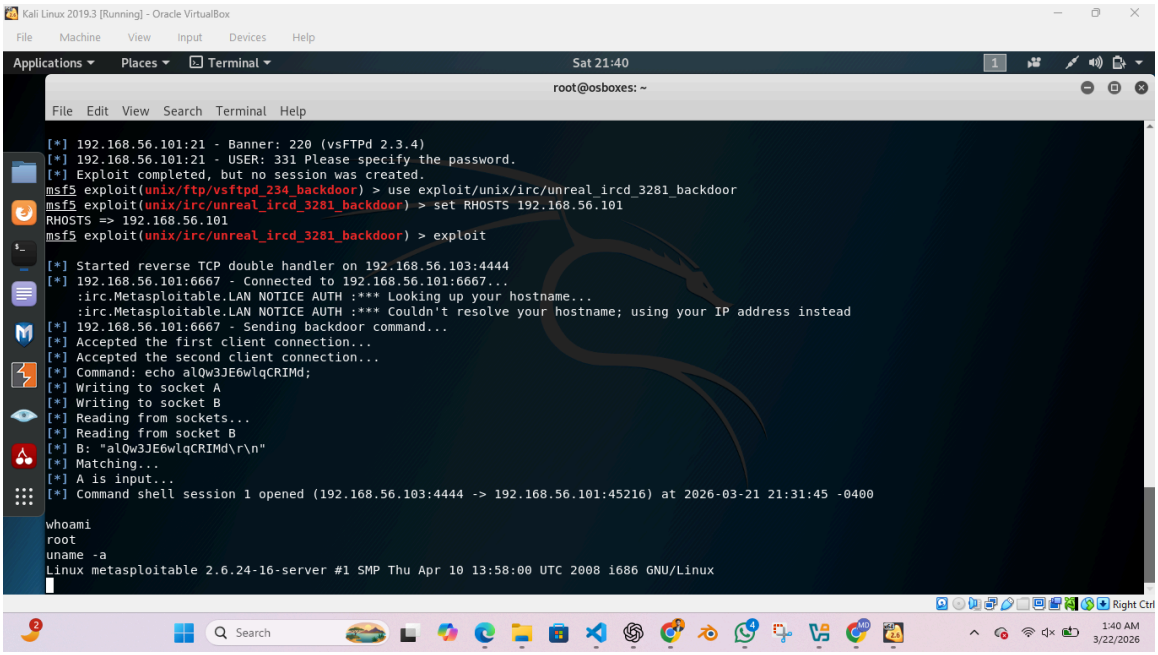

Figure 11: Successful remote shell access obtained via Metasploit, confirming full system compromise with root-level privileges.

3.9 Exploit 3 - Social Engineering Attack

Social engineering attacks target human vulnerabilities rather than technical systems. In this engagement, the Social Engineering Toolkit (SET) was used to simulate a phishing attack.

A cloned login page was created to mimic a legitimate website. When users entered their credentials, the information was captured by the attacker system.

This demonstrates how attackers can bypass technical security controls by exploiting human behaviour. Even well-secured systems can be compromised if users are deceived into revealing sensitive information [10].

It is important to note that this activity was conducted in a controlled lab environment for educational purposes.

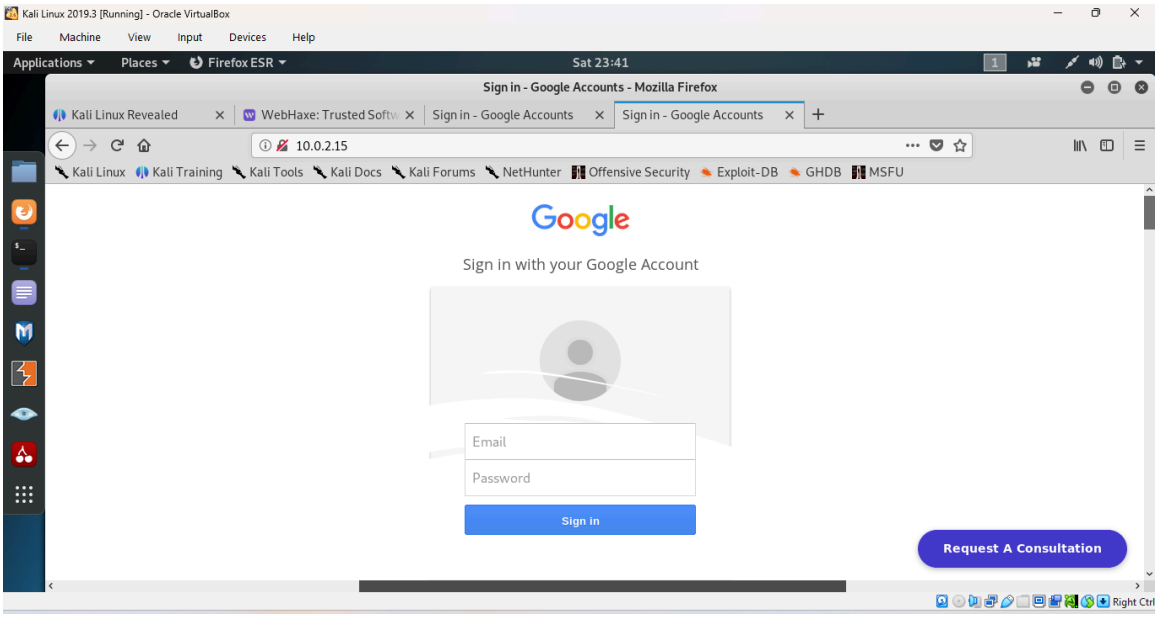

Figure 12: Cloned phishing login page created using the Social Engineering Toolkit (SET), demonstrating credential harvesting through social engineering.

3.10 Post Exploitation

Following successful exploitation, post-exploitation activities were conducted to assess the extent of system compromise.

These included:

- **Privilege Escalation**: Confirming root-level access
- **System Enumeration**: Identifying active services and processes
- **Data Collection**: Accessing sensitive files

Commands such as `whoami` and `netstat` were used to verify system control and identify active network connections.

Post-exploitation demonstrates the potential impact of a breach, where attackers can access sensitive data and maintain persistent access within the system [6].

3.11 Vulnerability Scanning (Nessus)

Vulnerability scanning tools such as Nmap were used to identify weaknesses within the system. The results revealed multiple exposed services and outdated software versions.

These vulnerabilities provide entry points for attackers and highlight the importance of regular security assessments. Automated scanning tools are essential for identifying and prioritising risks within an organisation [15].

3.12 MITRE ATT&CK Mapping

Table 2: The attack can be mapped to the MITRE ATT&CK framework as follows:

Phase	Technique	ID
Reconnaissance	Network Scanning	T1046
Initial Access	SQL Injection	T1190
Execution	Command Shell	T1059
Persistence	Backdoor Access	T1547
Privilege Escalation	Exploitation	T1068

This mapping provides a structured understanding of attacker behaviour and supports the development of defensive strategies [7].

3.13 Detection Gap Analysis

The engagement revealed several critical detection gaps:

- Absence of intrusion detection systems (IDS)
- Lack of log monitoring and analysis
- Weak input validation in web applications
- No alerting mechanisms for suspicious activity

The SQL injection attack went undetected due to poor input validation, while the Metasploit exploit succeeded due to unpatched vulnerabilities.

These findings demonstrate how attackers can operate undetected in poorly secured environments, emphasising the need for improved monitoring and detection capabilities [16].

4. Analysis of Attack Techniques

The attack techniques demonstrated in this assessment illustrate how multiple vulnerabilities can be systematically exploited and chained together to achieve full system compromise. The attack progression aligns closely with established frameworks such as the Cyber Kill Chain and the MITRE ATT&CK model, highlighting how attackers move from initial reconnaissance to achieving complete control over a target system.

This section provides a critical analysis of each stage of the attack lifecycle, linking practical findings from the lab environment to real-world cyber attack methodologies.

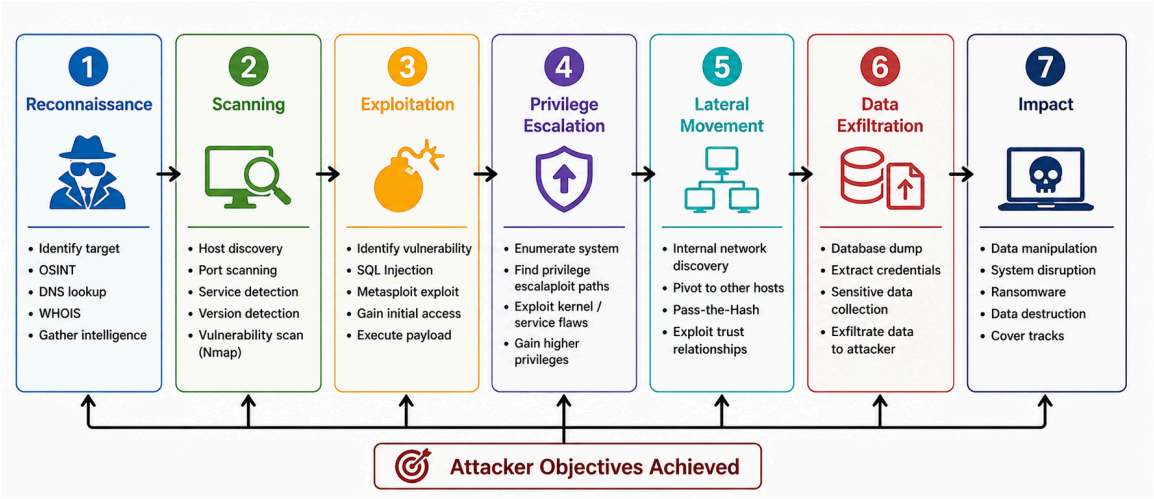

Figure 13: Illustrates the attack progression based on the Cyber Kill Chain model, demonstrating how an attacker moves systematically from reconnaissance to full system compromise and data exfiltration.

Limitations of this assessment include the use of a controlled lab environment (Metasploitable), which intentionally contains vulnerabilities. In real-world environments, additional security controls such as IDS, WAF, and EDR solutions may reduce the effectiveness of these attacks.

4.1 Reconnaissance and Information Gathering

Reconnaissance represents the foundational phase of any cyber attack, where attackers gather intelligence about the target environment before launching active exploitation. In this assessment, reconnaissance was performed using techniques such as ARP scanning and basic network probing to identify active hosts within the virtual lab environment.

The ARP scan results (see Figure 4) revealed active devices within the network, including the target system (Metasploitable 2). This phase is critical because it allows attackers to map the network topology and identify potential targets without triggering significant security alerts.

From a real-world perspective, reconnaissance may involve both passive and active techniques. Passive reconnaissance includes gathering publicly available information (OSINT), such as domain records, DNS information, and employee details, while active reconnaissance involves direct interaction with the target network. The techniques used in this assessment simulate active reconnaissance, which is commonly used once attackers have initial network access.

The effectiveness of reconnaissance lies in its ability to reduce uncertainty. By identifying live hosts and network structure, attackers can focus their efforts on high-value targets, increasing the efficiency and success rate of subsequent attack stages.

4.2 Scanning and Vulnerability Identification

Following reconnaissance, the scanning and enumeration phase was conducted using Nmap to identify open ports, running services, and potential vulnerabilities. The scan results revealed several open ports, including FTP (21), HTTP (80), and IRC (6667), each representing a potential attack vector.

This phase is crucial because it transforms raw network information into actionable intelligence. For example, identifying an open IRC port led directly to the discovery of the UnrealIRCd backdoor vulnerability, which was later exploited using Metasploit.

From a security perspective, exposed services significantly increase the attack surface of a system. Each open port represents an entry point that attackers can probe for weaknesses. Service version detection further enhances this process by allowing attackers to match identified services with known vulnerabilities in public exploit databases.

The findings in this assessment demonstrate how outdated or vulnerable services can be easily identified through automated scanning tools. In real-world environments, attackers often rely on similar tools to perform large-scale scanning across thousands of systems, highlighting the importance of minimizing exposed services and maintaining up-to-date systems.

4.3 Exploitation Techniques

The exploitation phase represents the transition from passive analysis to active compromise. In this assessment, multiple exploitation techniques were successfully executed, including SQL Injection and remote exploitation using the Metasploit Framework.

4.3.I SQL Injection Attack

The SQL Injection attack targeted a vulnerable login form within the Mutillidae web application. By injecting a simple payload (`' OR '1'='1`), authentication controls were bypassed, allowing unauthorized access to the system.

This vulnerability arises due to improper input validation and the failure to use parameterised queries. When user input is directly incorporated into SQL queries without sanitisation, attackers can manipulate the query logic to execute unintended commands.

Further exploitation using SQLMap demonstrated how automated tools can escalate the attack, enabling database enumeration and data extraction. The successful retrieval of user credentials highlights the severity of this vulnerability, as it compromises the confidentiality of sensitive information.

In real-world scenarios, SQL Injection remains one of the most critical web application vulnerabilities, as reflected in the OWASP Top 10. Despite being well understood, it continues to persist due to poor secure coding practices.

4.3.II Metasploit IRC Exploit

The second major exploit targeted the UnrealIRCd service running on port 6667. This service contains a known backdoor vulnerability that allows attackers to execute arbitrary commands remotely.

Using the Metasploit Framework, a remote shell was successfully obtained, providing direct control over the target system. This demonstrates how publicly available exploit frameworks can significantly reduce the complexity of attacks.

An important observation from this phase is that not all vulnerabilities are equally exploitable. The initial attempt to exploit the FTP service (vsftpd) was unsuccessful, highlighting the need for adaptability in penetration testing. Attackers must often test multiple vectors before identifying a successful exploitation path.

This reflects real-world attack behaviour, where attackers continuously adjust their approach based on system responses and available vulnerabilities.

4.3.III Social Engineering Attack

The use of the Social Engineering Toolkit (SET) demonstrated how attackers can bypass technical security controls by exploiting human vulnerabilities. A cloned login page was used to capture user credentials, simulating a phishing attack.

This highlights a critical insight: even if technical systems are secure, human factors can still lead to compromise. Social engineering attacks are particularly effective because they rely on psychological manipulation rather than technical flaws.

In real-world environments, phishing remains one of the most common initial access vectors, often serving as the starting point for larger attack campaigns.

4.4 Privilege Escalation and System Control

Once initial access was obtained, privilege escalation techniques were used to gain higher levels of access within the system. Commands such as `whoami` confirmed root-level privileges, indicating full system compromise.

Privilege escalation is a critical step in the attack lifecycle, as it allows attackers to move beyond limited access and gain control over the entire system. With elevated privileges, attackers can modify system configurations, install backdoors, and access sensitive data.

In many cases, privilege escalation exploits leverage system misconfigurations or unpatched vulnerabilities. The success of this phase in the assessment demonstrates how insufficient system hardening can significantly increase the impact of an attack.

4.5 Post Exploitation Activities and Impact Analysis

Post-exploitation activities provide insight into the full extent of a security breach. In this assessment, actions such as system enumeration, credential extraction, and data access were performed to evaluate the impact of the compromise.

These activities demonstrate how attackers can maintain persistence within a system and expand their control. Similar behaviour is widely observed in advanced threat campaigns, where attackers prioritise persistence and long-term access within compromised environments [19].

The impact of such activities is significant, as it affects all three pillars of information security:

- **Confidentiality:** Sensitive data is exposed
- **Integrity:** System data can be modified
- **Availability:** Systems can be disrupted or controlled

This highlights the importance of considering not only how attacks occur, but also their broader organisational impact.

4.6 Lateral Movement and Attack Expansion

Although limited in the controlled lab environment, the techniques demonstrated in this assessment provide a foundation for lateral movement within a network. Once attackers gain access to a system, they can use stolen credentials and network information to move across other systems.

Techniques such as pass-the-hash, remote service exploitation, and credential reuse are commonly used to expand access. The absence of network segmentation in many environments allows attackers to move freely once inside the network.

This stage is particularly dangerous because it enables attackers to escalate a single compromised system into a full organisational breach.

4.7 Detection Failures and Security Gaps

A critical finding of this assessment is the absence of effective detection mechanisms. The attacks conducted were not detected or blocked, highlighting several security weaknesses:

- Lack of intrusion detection systems (IDS)
- Absence of real-time monitoring
- Weak input validation in web applications
- Unpatched vulnerabilities in services

The SQL Injection attack succeeded due to poor input validation, while the Metasploit exploit was successful due to outdated and vulnerable services. These issues are common in real-world organisations, where security controls are often insufficient or poorly configured.

Additionally, the lack of logging and alerting mechanisms means that attackers can operate undetected for extended periods, increasing the potential damage. This observation is consistent with modern threat intelligence findings, where attackers maintain persistence due to insufficient monitoring and detection capabilities [19], [20].

4.8 Critical Evaluation of Attack Techniques

While the attacks were successful in this controlled environment, it is important to critically evaluate their effectiveness in real-world scenarios.

Modern systems often implement security controls such as Web Application Firewalls (WAFs), intrusion detection systems, and multi-factor authentication. These controls can significantly reduce the effectiveness of attacks such as SQL Injection and credential-based exploits.

However, attackers continuously adapt their techniques to bypass these defences, as highlighted in modern threat intelligence reports analysing evolving attacker methodologies and tactics [20].

This highlights the need for a layered security approach, combining technical controls, user awareness, and continuous monitoring.

4.9 Summary of Attack Chain

The overall attack chain demonstrates how multiple vulnerabilities can be combined to achieve full system compromise:

1. Reconnaissance identifies targets
2. Scanning reveals vulnerabilities
3. Exploitation provides initial access

4. Privilege escalation grants full control
5. Post-exploitation enables data extraction
6. Lateral movement expands the attack

This structured progression reflects real-world cyber attacks, where attackers follow a systematic approach to maximise impact.

5. Conclusion

This assessment has demonstrated both the theoretical and practical dimensions of ethical hacking through a combination of strategic threat analysis and hands-on penetration testing. Task 1 highlighted how modern cyber attacks exploit interconnected weaknesses across technical systems, human behaviour, and organisational processes, reflecting the complexity of real-world threat environments.

Task 2 successfully simulated a full red team engagement within a controlled lab environment, where multiple attack techniques including SQL injection, remote exploitation, and social engineering were executed. The results demonstrated that even well-known and relatively simple vulnerabilities can lead to full system compromise when appropriate security controls are not in place.

The findings emphasise the importance of adopting a layered security approach that integrates secure coding practices, network segmentation, continuous monitoring, and user awareness. Additionally, the use of frameworks such as the Cyber Kill Chain and MITRE ATT&CK supports a structured understanding of attacker behaviour and enhances defensive capabilities.

Overall, this study demonstrates how theoretical knowledge can be effectively applied in practical scenarios, providing valuable insight into modern attack methodologies. It reinforces the need for organisations to continuously assess, adapt, and strengthen their security posture in order to remain resilient against evolving cyber threats.

6. References

[1] MITRE, "MITRE ATT&CK Framework," 2024. [Online]. Available: https://attack.mitre.org/ [Accessed: Apr. 2026].

[2] Lockheed Martin, "Cyber Kill Chain Model," 2022. [Online]. Available: https://www.lockheedmartin.com/ [Accessed: Apr. 2026].

[3] OWASP Foundation, "OWASP Top 10 Web Application Security Risks," 2023. [Online]. Available: https://owasp.org/ [Accessed: Apr. 2026].

[4] OWASP Foundation, "SQL Injection Prevention Cheat Sheet," 2023. [Online]. Available: https://owasp.org/ [Accessed: Apr. 2026].

[5] Nmap Project, "Nmap Official Documentation," 2024. [Online]. Available: https://nmap.org/docs.html [Accessed: Apr. 2026].

[6] G. F. Lyon, *Nmap Network Scanning*, Insecure, 2022. [Online]. Available: https://nmap.org/book/ [Accessed: Apr. 2026].

[7] Rapid7, "Metasploit Framework Documentation," 2024. [Online]. Available: https://docs.rapid7.com/metasploit/ [Accessed: Apr. 2026].

[8] Offensive Security, "Metasploitable 2," 2023. [Online]. Available: https://sourceforge.net/projects/metasploitable/ [Accessed: Apr. 2026].

[9] SANS Institute, "Post-Exploitation Techniques," 2023. [Online]. Available: https://www.sans.org/ [Accessed: Apr. 2026].

[10] C. Hadnagy, *Social Engineering: The Art of Human Hacking*, 2nd ed., Wiley, 2022.

[11] CrowdStrike, "Lateral Movement Techniques," 2023. [Online]. Available: https://www.crowdstrike.com/ [Accessed: Apr. 2026].

[12] Palo Alto Networks, "Data Exfiltration Techniques," 2023. [Online]. Available: https://www.paloaltonetworks.com/ [Accessed: Apr. 2026].

[13] Microsoft, "Privilege Escalation Techniques," 2024. [Online]. Available: https://learn.microsoft.com/security/ [Accessed: Apr. 2026].

[14] Cybersecurity and Infrastructure Security Agency (CISA), "Vulnerability Management Guide," 2023. [Online]. Available: https://www.cisa.gov/ [Accessed: Apr. 2026].

[15] SANS Institute, "System Misconfiguration Risks," 2022. [Online]. Available: https://www.sans.org/ [Accessed: Apr. 2026].

[16] Verizon, "2024 Data Breach Investigations Report," 2024. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/ [Accessed: Apr. 2026].

[17] European Union Agency for Cybersecurity (ENISA), "Ransomware Threat Landscape," 2023. [Online]. Available: https://www.enisa.europa.eu/ [Accessed: Apr. 2026].

[18] Europol, "Internet Organised Crime Threat Assessment (IOCTA)," 2023. [Online]. Available: https://www.europol.europa.eu/ [Accessed: Apr. 2026].

[19] FireEye (Mandiant), "APT Trends Report," 2023. [Online]. Available: https://www.mandiant.com/ [Accessed: Apr. 2026].

[20] Recorded Future, "Initial Access Brokers Report," 2023. [Online]. Available: https://www.recordedfuture.com/ [Accessed: Apr. 2026].

[21] Red Canary, "Living-Off-the-Land Techniques," 2023. [Online]. Available: https://redcanary.com/ [Accessed: Apr. 2026].

[22] Splunk, "SIEM Best Practices," 2023. [Online]. Available: https://www.splunk.com/ [Accessed: Apr. 2026].

[23] IBM Security, "Security Operations Report," 2024. [Online]. Available: https://www.ibm.com/security/ [Accessed: Apr. 2026].