

Ethical Hacking (ACCA7033)

Cyber Security attacks and Penetration testing for a virtualise simulated company Website

Name: Riddhi Damjibhai Mendpara

Student ID: 2518862

Lecturer Name: Assoc. Professor Carlene Campbell

Submission Date: 12th May 2026

Table of Contents

1. Abstract.....	4
2. Introduction.....	5
3. Task-1 Strategic Threat Analysis	5
3.1 Incident Overview	5
3.2 Incident Timeline.....	6
3.3 Timeline Analysis.....	7
3.4 Adversary TTP Mapping (MITRE ATTACK).....	7
3.5 MITRE ATTACK Mapping Table	7
3.6 Analysis.....	8
4. Root Cause and Security Control Failures.....	8
4.1 Human Element – Social Engineering of IT Support Desk.....	8
4.2 Risk from External Parties and Supply Networks	8
4.3 Inadequate Active Directory Security	9
4.4 MFA Circumvention	9
4.5 Extended Stay Duration	9
5. Profile and Motivation of the Threat Actor	9
6. Identification and Reaction Assessment.....	10
6.1 Detection Errors	10
6.2 Feedback – What Was Successful	10
6.3 Reaction – What Went Wrong.....	10
7. Tactical Suggestions.....	10
8. Task 2: Red Team Assessment.....	11
8.1 Lab Environment Design	12
8.2 Rules Engagement.....	13
8.3 Threat Emulation Plan.....	13
8.4 Reconnaissance Phase	14
8.5 Port and Service Enumeration	14
8.6 Exploitation – Finding 1: Default Credentials.....	15
8.7 Exploitation – Finding 2: Broken Access Control Command Injection.....	17
8.8 Exploitation – Finding 3: Cross-Site Scripting XSS.....	18
8.9 Exploitation – Finding 4: SQL Injection	19

8.10 Vulnerability Summary Table	20
9. Conclusion	21
10. References	22

1. Abstract

This report conducts an in-depth analysis of two major aspects of offensive cybersecurity. Task 1 performs a strategic evaluation of the synchronized ransomware assaults that affected Marks and Spencer and the Co-operative Group in the UK in April 2025, linked to the financially driven threat group Scattered Spider. The examination aligns the opponent's campaign with MITRE ATTACK Enterprise Matrix, investigates underlying causes and shortcomings in security controls, profiles the threat actor, assesses detection and response abilities, and offers strategic suggestions for prevention. Task 2 outlines a comprehensive red team penetration testing exercise targeting ABCD Ltd, a fictitious retail company based in the UK, carried out in a controlled virtualised lab environment. Utilizing Parrot OS 7.1 as the offensive platform against two virtual machine targets, several significant vulnerabilities were identified, such as default login credentials, cross-site scripting, SQL injection, command injection and compromised access control. All results are aligned with the MITRE ATTACK framework and backed by peer-reviewed studies. Both tasks collectively showcase the fundamental skill of an offensive security specialist – the capacity to convert real-world threat intelligence into thorough, evidence-based security evaluations that achieve significant risk reduction results.

2. Introduction

The United Kingdom retail sector has become one of the most heavily targeted industries in today's cyber threat landscape. Organisations in this sector process millions of customer transactions, store sensitive personal data, and rely on complex digital infrastructure – characteristics that make them highly attractive targets for financially motivated threat actors [1] [2].

The 2025 ransomware attacks on Marks and Spencer and the Co-operative Group demonstrated this reality with easting consequences. Attributed to the criminal collective Scattered Spider, the attacks exploit preventable weaknesses including weak helpdesk identity verification, insufficient multi-factor authentication and poor Active Directory protection. Combined financial losses exceeded pound 500 million, and the personal data of millions of customers was compromised [1] [2] [9]. These incidents serve as the central case study for Task 1 of this report.

Offensive security – the practice of simulating adversary behaviour to identify and remediate vulnerabilities before real attackers exploit them – has become an essential component of modern organisational cybersecurity strategy [10]. Penetration testing a dried team operations translate threat intelligence into actionable security improvement, these engagements become significantly more targeted and valuable [9].

This report addresses both dimensions of offensive security. Task 1 critically analyses the M&S and Co-op attacks using the MITRE ATTACK Enterprise Matrix as the primary analytical framework, drawing on peer-reviewed literature, NCSC guidance and authoritative industry reporting [1] [2] [9].

Task 2 applies the insights developed in Task 1 to a practical red team engagement against ABCD Ltd, a simulated UK retail company. The engagement was conducted in an isolated virtual laboratory using Parrot OS 7.1, targeting a Node.js web application at 192.168.56.40 and an internal windows server at 192.168.56.50, following a formally agreed Rules of Engagement document and a MITRE ATTACK mapped Threat Emulation Plan [9] [10].

Together, both tasks present a logical and integrated approach to offensive security that moves beyond individual vulnerability identification towards a comprehensive understanding of how advanced threats operate, how they can be ethically emulated, and how findings can be translated into concrete, prioritised security improvements for organisations operating in today's challenging digital environment [9] [8].

3. Task-1 Strategic Threat Analysis

3.1 Incident Overview

The incidents involving M&S and Co-op took place over several months, beginning with secret infiltration long before any signs of trouble were visible to customers or management [1][2].

February 2025 - Subtle First Arrival

The agreement with Marks & Spencer began in February 2025. Unauthorized users accessed the retailer's network and retrieved the ntds.dit file from the windows domain controller, which is the Critical Active Directory database that holds password hashes for all traverse the network without triggering any alarms [1][5].

Easter Weekend – April 19 to 21, 2025

Shoppers nationwide began experiencing problems in M&S stores. Contactless card payments and click-and-collect services unexpectedly encountered issues at various sites. By Monday, April 21, the entire chain's contactless payment systems and order pickup services were out of service [1][2].

22 April 2025 — M&S Formal Announcement

M&S issued an official announcement to the stock market, acknowledging a cyber incident but stressing that stores remained open. The company notified the UK's National Cyber Security Centre regarding the breach and brought in external experts to handle the situation[2][9].

22–30 April 2025 — Collaborative Assault

On 30 April 2025, the Co-op was required to shut down its IT systems after identifying unauthorised access that occurred on 22 April. On April 25, they commenced their initial extortion outreach via Microsoft Teams and directly reached out to Co-op's security head, insisting on payment for the stolen data [1][2].

2 May 2025 — NCSC Recognises Involvement

The National Cyber Security Centre has stated that it is assisting M&S, Co-op and Harrods due to increasing worries among UK retailers [9].

10 July 2025 – Four Persons Apprehended

Officials arrested four youths aged 17 to 20 in London and the West Midlands. They were apprehended on suspicion of breaching the Computer Misuse Act, engaging in blackmail, money laundering funds and participating in an organised crime group [1][2].

3.2 Incident Timeline

Date	Event	Source
April 2025 (Easter)	Initial disruption detected at M&S	[9]
25 April 2025	Co-op confirms cyber attack	[9]
Early May 2025	Ongoing service disruption	[1] [2]
May 2025	Help-desk social engineering identified	[1] [2]
May 2025	Third-party access exploited	[1] [2]
Aug 2025	Services restored gradually	[1] [2]

3.3 Timeline Analysis

The timeline indicates that the assault utilized a strategic, multi-stage method commencing with social engineering tactics to obtain initial entry and advancing to internal system infiltration and prolonged operational disruption. Recent studies indicates that impersonation and credential manipulation are key patterns in social engineering attacks [1] [2]. Moreover, the extended length of the incident highlights potential weaknesses in detection and incident response mechanisms, allowing attackers to maintain access for an extended period [7].

3.4 Adversary TTP Mapping (MITRE ATTACK)

The MITRE Corporation ATT&CK methodology, which offers an organised method for comprehending adversary tactics, methods, and procedures (TTPs) throughout the attack lifecycle, can be used to analyse the cyberattack [9]. This framework is frequently used in red teaming and ethical hacking to mimic actual attack behaviour and enhance detection capabilities [2][9].

3.5 MITRE ATTACK Mapping Table

Tactic	Technique	ID	Description
Initial Access	Phishing/ Social Engineering	T1566	Attackers impersonated employees to gain access [1] [2]
Initial Access	Valid Accounts	T1078	Compromised credentials used for login [1] [2]
Execution	Command Execution	T1059	Malicious commands executed after access [9]
Persistence	Account manipulation	T1098	Accounts modified to maintain access [1] [9]
Privilege Escalation	Exploitation for Privilege Escalation	T1068	Elevated privileges obtained [1] [2]
Credential Access	Credential Dumping	T1003	Sensitive credentials extracted [1] [2]
Discovery	Network Service Discovery	T1046	Internal systems identified [9]
Lateral Movement	Remote Services	T1021	Movement across systems [1] [9]
Command & Control	Encrypted Channel	T1573	Communication hidden from detection [9]
Exfiltration	Data Transfer	T1041	Sensitive data accessed/ exfiltrated [1] [2]

3.6 Analysis

The attack's alignment with the MITRE ATTACK framework illustrates how the attackers employed a combination of credential-based tactics and social engineering techniques to gain initial access and establish network persistence. Impersonation, along with the utilisation of authentic accounts are common tactic exhibited by adversaries in modern cyberattacks [1][2].

Moreover, a standard multi-phase attack lifecycle, where attackers gradually enhance their control over the network, is illustrated by the progression from initial access to lateral movement and data extraction. Research indicates that the ATTACK framework aids organisations in comprehending attacker behaviour and improving detection tactics by aligning security with recognised adversary methods [9], [2].

This systematic study highlights the importance of integrating threat intelligence frameworks into security operations to enhance visibility and reduce the likelihood of enduring undetected attacks.

4. Root Cause and Security Control Failures

The M&S and Co-op breaches occurred not due to the attackers being technically invulnerable, but because several security layers — human, procedural and technical — failed at the same time.

4.1 Human Element – Social Engineering of IT Support Desk

The most critical failure happened on a human level. M&S Chairman Archie Norman noted that attackers impersonated an M&S employee and reached out to the service desk run by an outside company, which executed a password reset for them. This single action gave hackers entry to one of the largest retail networks in the UK. The helpdesk agent, likely following standard procedures lacked the ability to verify the caller's actual identity [1][3].

This failure highlights an important concern: the effectiveness of technical security measures are greatly dependent on the associated human processes. When a helpdesk agent is able to modify any user's credentials without going through identity verification, all technical protections become irrelevant [3][6].

4.2 Risk from External Parties and Supply Networks

The initial breach originated from social manipulation of a third-party supplier. M&S assigned its IT service desk duties to Tata Consultancy Services (TCS). In July 2025, M&S ended its IT service desk contract with TCS following a ten-year collaboration [1][2]. Handing over critical IT responsibilities without ensuring vendors comply with identical security measures poses dangerous risks. When a third party has privileged access to your systems, their vulnerabilities become your vulnerabilities [3][8].

4.3 Inadequate Active Directory Security

With access to the ntds.dit file, threat actors could extract and decrypt these hashes offline, leading to readable credentials for multiple networks [1][2]. It contains the password hashes for every user. Allowing attackers to access this file indicates a critical failure in data classification and access control. Proper network segmentation and controlling privileged access could have either stopped or detected this data exfiltration[1][5][7].

4.4 MFA Circumvention

M&S and Co-op adopted MFA, but it was bypassed. Scattered Spider utilised MFA fatigue tactics by repeatedly sending login requests until a user unknowingly authorised one, highlighting that traditional push notification MFA falls short against relentless adversaries [1][2][3]. Techniques for MFA that are resistant to phishing, such as FIDO2 hardware keys, would have prevented this bypass [3][9].

4.5 Extended Stay Duration

The attack was formally recognised in late April 2025, but it is believed that threat actors infiltrated internal systems as early as February 2025, indicating a prolonged dwell time before the ransomware was executed. Took over two months for the breach to be detected. This indicates a complete absence of effective behavioural oversight, SIEM alerts or threat-hunting capabilities in M&S security operations [1] [7].

5. Profile and Motivation of the Threat Actor

Cybersecurity experts have associated the assault on M&S with a collective named Scattered Spider, which is also referred to as Octo Tempest. This is an informal network of mainly young, English-speaking hackers who employ techniques such as phishing, SIM swapping, and MFA fatigue to infiltrate company systems.

Essential Profile Details:

Operational since: Around 2022

Also known as: Octo Tempest, UNC3944, Muddled Libra, Scatter Swine, Star Fraud [1][2]

Participants: Mainly young people who are English speakers and range in age from 17 to 25.

Motive: Exclusively financial — demands for ransomware and data extortion.

Earlier significant breaches: Twilio (2022), MGM Resorts (2023), Nike, T-Mobile, Vodafone

Ransomware employed: Dragon Force (Ransomware-as-a-Service)

Tim Mitchell, a senior security researcher at SecureWorks, noted that Scattered Spider is distinctive as an unusual hacking group because most cybercriminal organizations usually operate from

countries like Russia, where lenient laws foster and their presence in the UK and US complicate identification – they integrate culturally and linguistically when reaching out of helpdesks.

The purpose is clearly financial miscount. Investigators found that the M&S attack involved a ransomware incident using a classic double extortion tactic: attackers encrypted company systems, stole data, and then demanded payment for decryption and deleting the stolen files.

6. Identification and Reaction Assessment

6.1 Detection Errors

The most troubling aspect of this breach was the two-month dwell time-attackers explored M&S systems from February until April 2025 without being detected. This emphasizes considerable deficiencies in:

SIEM monitoring — no alerts triggered despite unusual Active Directory access.

Monitoring privileged accounts — the extraction of ntds.dit was not unnoticed [1][2].

Behavioural analysis — no system detected the unusual helpdesk password reset.

Threat hunting — no active searching for signs of breach

6.2 Feedback – What Was Successful

M&S collaborated with the UK's National Cyber Security Centre, law enforcement, CrowdStrike and Microsoft to track threat actor behaviours, assess data exposure, conduct forensics and recover from the breach [1][9].

Co-op demonstrated slightly enhanced operational efficiency. Prompt detection and rapid network disconnection prevented a complete ransomware lockdown at-Co-op, enabling the company to avoid the full systems encryption that affected M&S [1][2].

6.3 Reaction – What Went Wrong

M&S projected the profit loss to be around pound 3000 millions and anticipated that problems with online sales would persist until July. The retailer returned its website to read-only status on 21 may-precisely one month following the public announcement of the attack [1][2]. A recovery time surpassing a month for a major retailer's online site indicates a serious failure in business continuity [7].

7. Tactical Suggestions

Considering the identified root causes and detection shortcomings, the following prioritized suggestions are recommended for organizations aiming to avert similar attacks [1][2][3][7][9]:

Suggestion 1 — Adopt Phishing-Resistant MFA (Prompt, Inexpensive)

Replace push notification MFA with FIDO2 hardware security keys or certificate-based authentication. The NCSC strongly encouraged retailers to activate like risky login attempts. It indicates that MFA fatigue attacks can bypass push-based MFA, but hardware keys are resistant to these attempts [3][9].

Suggestion 2 — Strengthen IT Helpdesk Identity Authentication (Prompt, Inexpensive)

Establish a secondary authorization procedure for all privileged account password resets. Restricting service-desk permissions is crucial to ensure that agents cannot reset credentials for admin or IT-privileged accounts without going through an extra approval process. No single helpdesk staff member should possess the ability to independently reset a domain administrator password [1][3].

Suggestion 3 — Safeguard Active Directory as Valuable Assets (Medium Cost)

Implement strict rules concerning the ntds.dit file. Utilize privileged Access Workstations (PAWs) for all tasks performed by domain administrators. Monitor and alert concerning any attempts to access or replicate the ntds.dit file via SIEM rules [5][7].

Suggestion 4 — Zero Trust Framework (Medium-High Expense, Extended Duration)

Zero Trust architecture limits damage even if an account is compromised. In a zero trust model. Every access request is verified regardless of its source being inside or outside the network. No device or user can be considered trustworthy by default [8][9].

Suggestion 5 — Risk Management for Third-Party Vendors (Moderate Expense)

Conduct regular security evaluations of all external vendors with heightened access. Ensure that outsourced IT functions, such as helpdesks, comply with the same security policies as internal teams. Include security obligations in all vendor contracts [1][3].

Suggestion 6 — Implement Advanced SIEM and Threat Detection (Significant Expense, Great Benefit)

Set up 24/7 security operations centre (SOC) employing SIEM tools capable of detecting lateral movements, unusual Active Directory queries and significant data exfiltration. A wait time of two months is unacceptable and would be noticed with proper supervision [5][7].

Suggestion 7 — Frequent Penetration Testing and Red Team Activities (Moderate Expense)

Commence ongoing penetration testing and red team exercises concentrating on social engineering strategies. Assess helpdesk procedure via simulated impersonation calls to identify weaknesses prior to real attackers taking advantage of them [9][10].

8. Task 2: Red Team Assessment

8.1 Lab Environment Design

The lab setup, constructed virtually with VirtualBox, featured three virtual machines linked via a private internal network utilizing the subnet 192.168.56.0/24. Throughout the testing, external internet access was prohibited, fulfilling the engagement's safety and containment standards.

Parrot OS was selected as the attack platform due to its pre-installed suite of offensive security tools, including Nmap, SQLmap. Lab05-01 ran the ABCD Ltd web application developed on Node.js on port 3000. Lab05-02 functioned as the internal administrative jump host used by the personnel of ABCD Ltd.

All virtual machines were snapshot backed prior to any intrusive testing to facilitate full rollback if needed. This demonstrates responsible operational security and preserve the integrity of the laboratory environment throughout the interaction.

Machine	IP Address	Role
Parrot OS 7.1	192.168.56.10	Attacker machine
LAB05-01	192.168.56.40	Web application server
LAB05-02	192.168.56.50	Internal Windows server

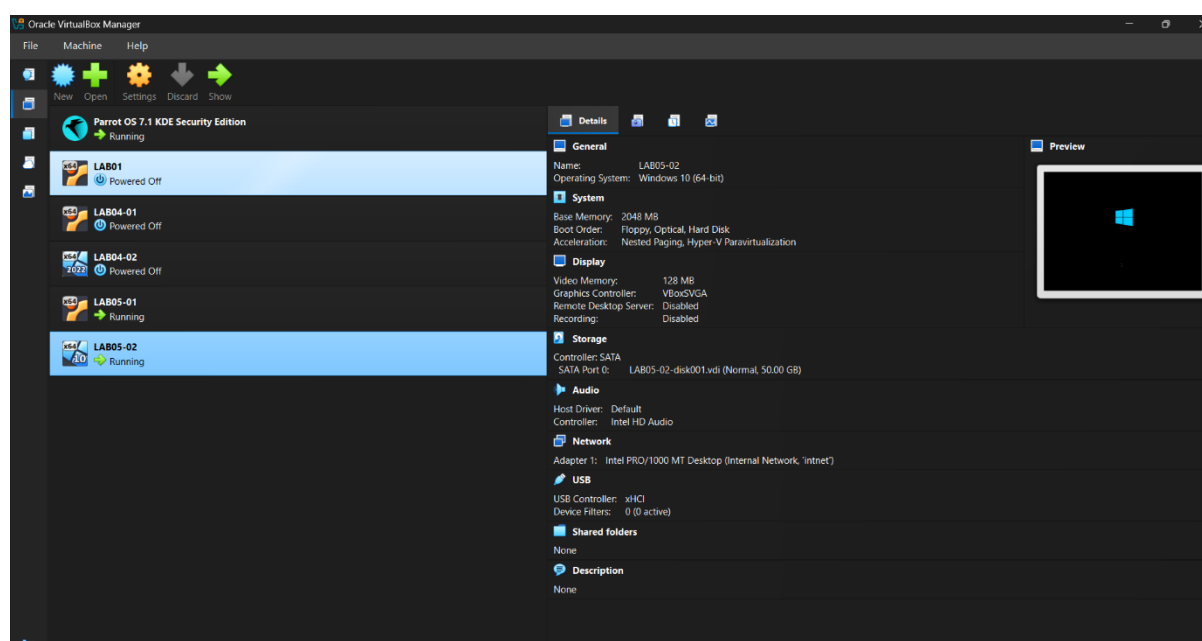


Figure 1 – VirtualBox showing Parrot OS, LAB05-01 AND LAB05-02 all running

Figure 1 illustrates the VirtualBox environment used throughout this engagement, confirming that all three virtual machines – Parrot OS 7.1 as the attacker machine, LAB05-01 as the web application server and LAB05-02 as the internal Windows server were simultaneously running and connected on the isolated internal network during testing [10].

8.2 Rules of Engagement

RULES OF ENGAGEMENT – ABCD LTD	
Tester	Riddhi Mendpara 2518862
Date	April 2026
Client	ABCD Ltd (Simulated)

Scope	
Web application	192.168.56.40
Internal server	192.168.56.50

Permitted:
Port scanning
Web application testing
SQL injection testing
XSS testing
Default credential testing

Not Permitted:
Deleting data
Attacking real external systems
Publishing passwords

Safe Word: Stop-Test
This is an isolated academic lab.
No real systems were harmed.

8.3 Threat Emulation Plan

The assault initiative was correlated with the MITRE ATTACK Enterprise Matrix [9]. The table below displays the scheduled phases of the attack.

Phase	What I Did	Tool	MITRE ID
1 — Reconnaissance	Pinged targets to confirm they are alive	Nmap	T1595
2 — Port Scanning	Scanned for open ports and services	Nmap	T1046
3 — Initial Access	Logged in using default password	Browser	T1078

Phase	What I Did	Tool	MITRE ID
4 — Discovery	Found admin panel and user data	Browser	T1083
5 — Exploitation	Injected XSS script into feedback	Browser	T1059.007
6 — Exploitation	Tested SQL injection on login	SQL map	T1190
7 — Command Injection	Found vulnerable export function	Browser	T1059

8.4 Reconnaissance Phase

Before machines responded successfully with 0% packet loss, confirming they were active and reachable on the internal network.

```

~ : bash — Konsole
File Edit View Bookmarks Plugins Settings Help
See the output of nmap -h for a summary of options.
[user@parrot]~$ ping -c 192.168.56.40
ping: invalid argument: '192.168.56.40'
[user@parrot]~$ ping -c 4 192.168.56.40
PING 192.168.56.40 (192.168.56.40) 56(84) bytes of data:
64 bytes from 192.168.56.40: icmp_seq=1 ttl=64 time=1.29 ms
64 bytes from 192.168.56.40: icmp_seq=2 ttl=64 time=1.73 ms
64 bytes from 192.168.56.40: icmp_seq=3 ttl=64 time=4.65 ms
64 bytes from 192.168.56.40: icmp_seq=4 ttl=64 time=1.74 ms

--- 192.168.56.40 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3013ms
rtt min/avg/max/mdev = 1.285/2.351/4.654/1.342 ms
[user@parrot]~$ ping -c 4 192.168.56.50
PING 192.168.56.50 (192.168.56.50) 56(84) bytes of data:
64 bytes from 192.168.56.50: icmp_seq=1 ttl=128 time=8.71 ms
64 bytes from 192.168.56.50: icmp_seq=2 ttl=128 time=8.76 ms
64 bytes from 192.168.56.50: icmp_seq=3 ttl=128 time=4.23 ms
64 bytes from 192.168.56.50: icmp_seq=4 ttl=128 time=8.69 ms

--- 192.168.56.50 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3009ms
rtt min/avg/max/mdev = 4.226/7.597/8.759/1.946 ms
[user@parrot]~$

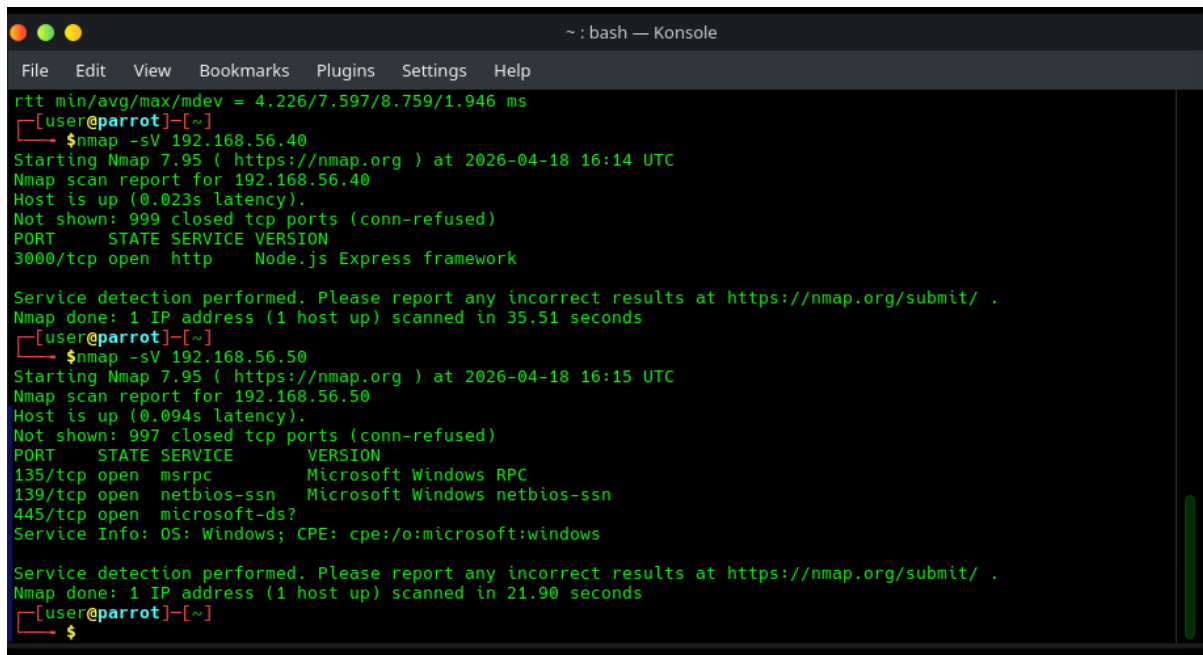
```

Figure 2 – ping results confirming lab05-01 (192.168.56.40) and lab05-02 (192.168.56.50) are online

Figure 2 presents the ping results confirming network connectivity between the Parrot OS attack machine and both target systems. LAB05-01 at 192.168.56.40 responded with 0% packet loss and an average latency of 2.3 milliseconds, while LAB05-02 at 192.168.56.50 responded with 0% packet loss and an average latency of 7.5 milliseconds [9].

8.5 Port and Service Enumeration

The analysis of lab05-01 showed port 3000 operating the Node.js Express framework – the warehouse web app. The examination of lab05-02 showed windows services on ports 135, 139 and 445, verifying it as a Windows-based internal server operating Microsoft RPC and SMB service [9][10].



```
~ : bash — Konsole
File Edit View Bookmarks Plugins Settings Help
rtt min/avg/max/mdev = 4.226/7.597/8.759/1.946 ms
[user@parrot]-[~]
$ nmap -sV 192.168.56.40
Starting Nmap 7.95 ( https://nmap.org ) at 2026-04-18 16:14 UTC
Nmap scan report for 192.168.56.40
Host is up (0.023s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
3000/tcp  open  http    Node.js Express framework

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.51 seconds
[user@parrot]-[~]
$ nmap -sV 192.168.56.50
Starting Nmap 7.95 ( https://nmap.org ) at 2026-04-18 16:15 UTC
Nmap scan report for 192.168.56.50
Host is up (0.094s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc    Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.90 seconds
[user@parrot]-[~]
$
```

Figure 3 – Nmap port scan showing Node.js on lab05-01 and Windows services on lab05-02

It displays the complete Nmap output for both target machines, showing the specific port numbers, their states and the identified service versions running on each system [9][10].

8.6 Exploitation – Finding 1: Default Credentials

The login page displayed a typical form for username and password as illustrated in figure 4 below

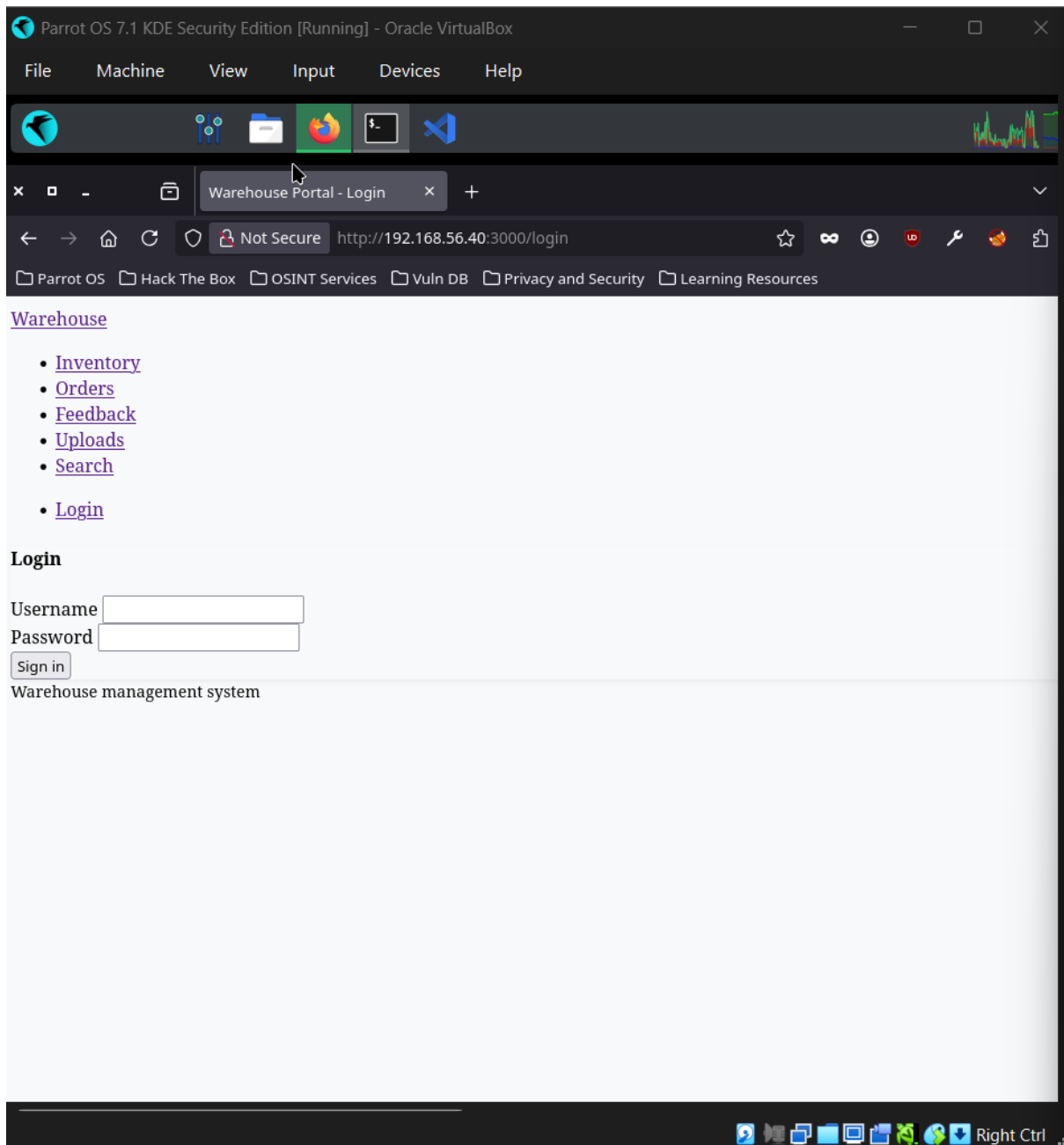


Figure 4 – Warehouse Portal login page before authentication

I experimented with the typical default credential pair: username “admin” and password “admin123”. The system promptly accepted these credentials and provided complete administrative access without any alerts, lockout or extra verification. After logging in successfully, the admin dashboard appeared, showcasing all user accounts within the system, including admin, manager1 and clerk1 – as illustrated in figure 5.

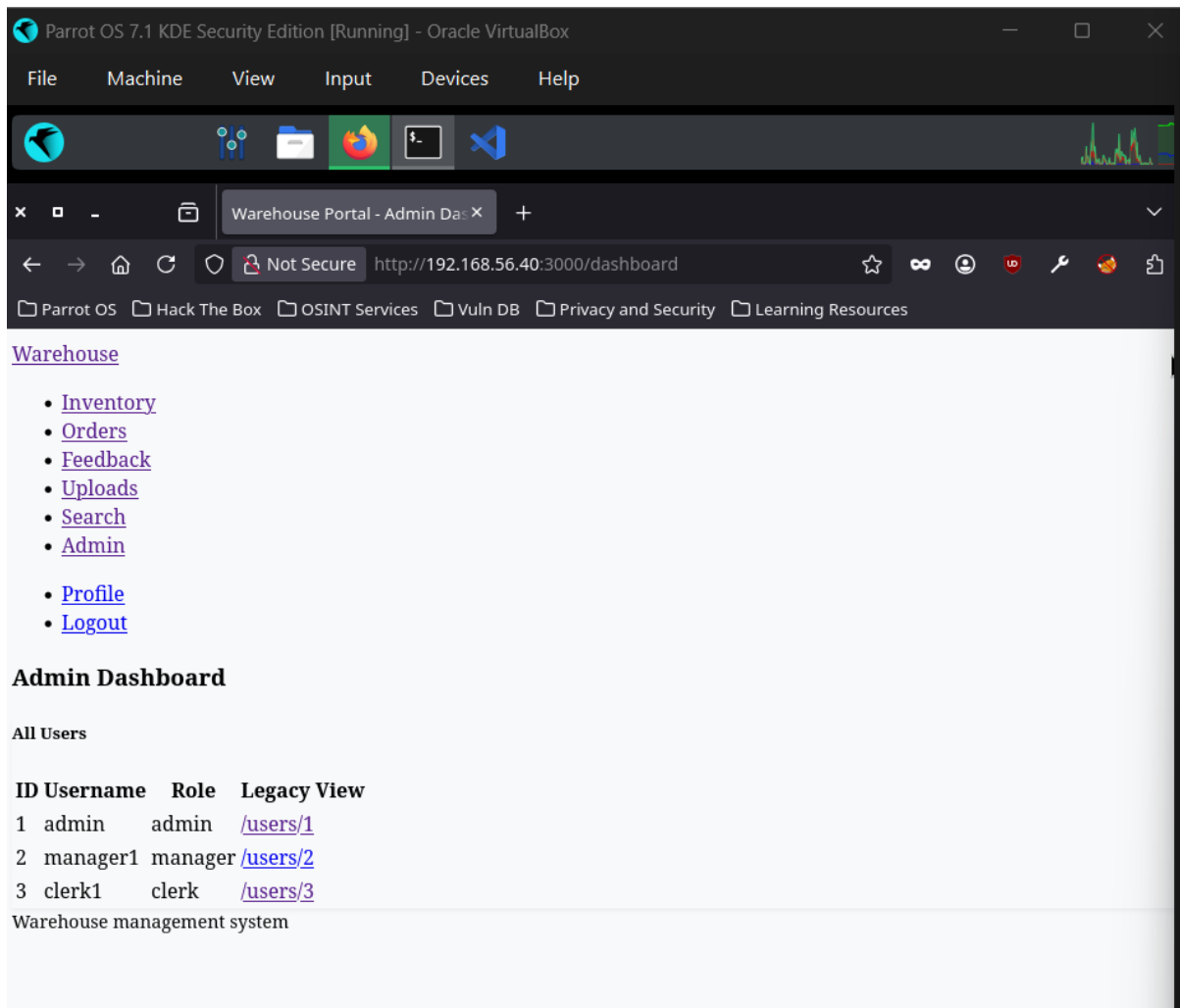


Figure 5 – Admin Dashboard showing all user accounts after login with default credentials

This confirms that a default credential vulnerability (CWE-798) exists. One of the worst weaknesses is that anybody who knows the default password may quickly gain full administrator access to the whole system. Rate limitation, account lockout and multi-factor authentication were not in place [10].

8.7 Exploitation – Finding 2: Broken Access Control Command Injection

After successfully logging in, the administrative panel was accessed by navigating to <http://192.168.56.40:3000/admin>. The whole user management interface, including all registered usernames and their designated roles, was shown as soon as the site loaded without the need for any further verification challenges. This validates a Broken Access Control vulnerability (CWE-284), which allows any authorised user to access the administrative system without any further restrictions [10].

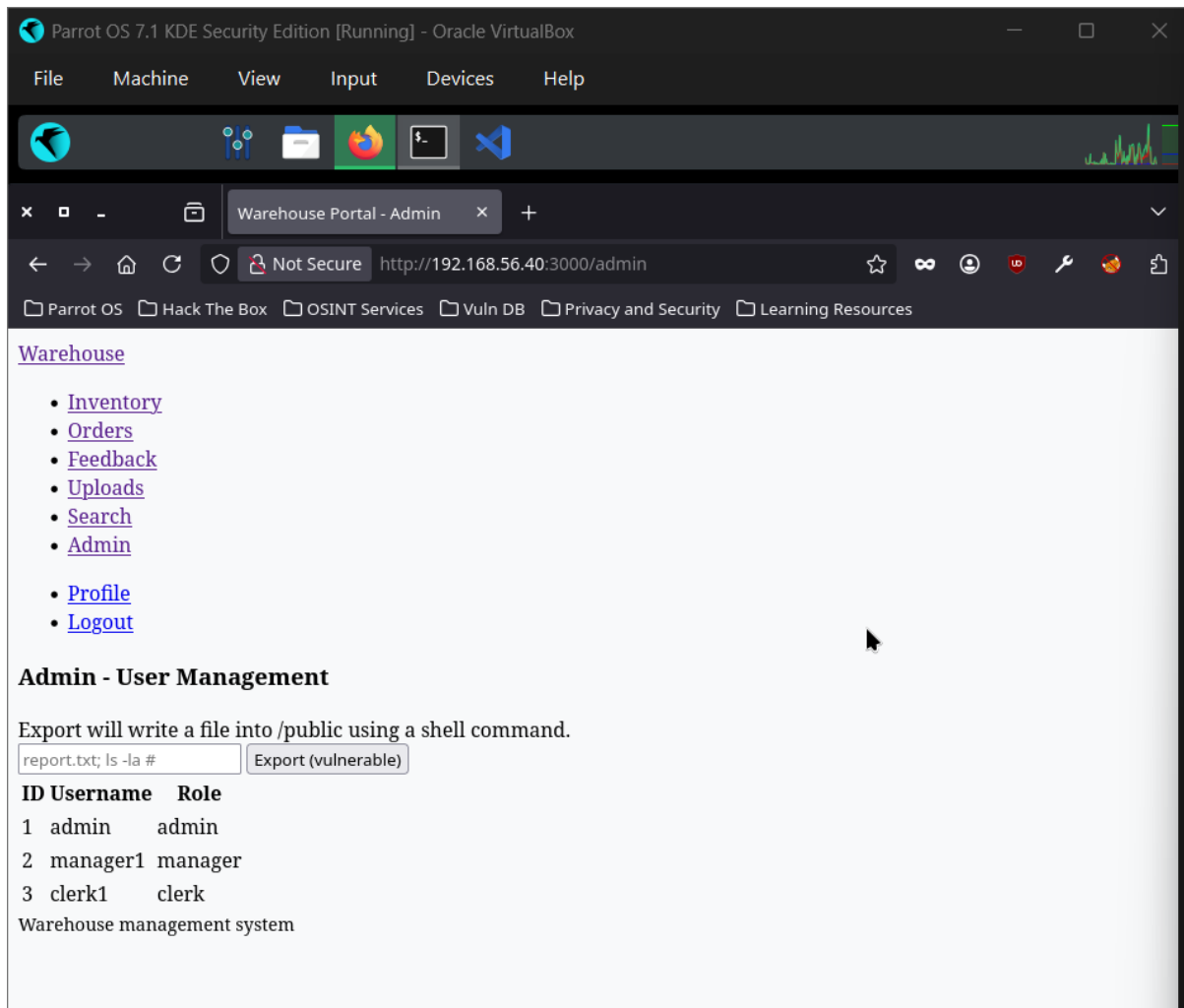


Figure 6 – Admin panel showing exposed shell command export function with prefilled payload

This discovery concurrently highlights two vulnerabilities: Command Injection (CWE-78), which occurs when user input is sent straight to a shell command without sanitisation and Broken Access Control (CWE-284), which occurs when no further authentication is needed to access the admin panel [10].

8.8 Exploitation – Finding 3: Cross-Site Scripting XSS

I went to the feedback page at <http://192.168.56.40:3000/feedback>. In the text input box, I typed the subsequent XSS payload:

```
<script> alert ('XSS found')</script>
```

Upon form submission the browser swiftly ran the injected JavaScript and presented a popup alert indicating XSS detected – coming from the domain 192.168.56.40:3000, as illustrated in Figure 7.

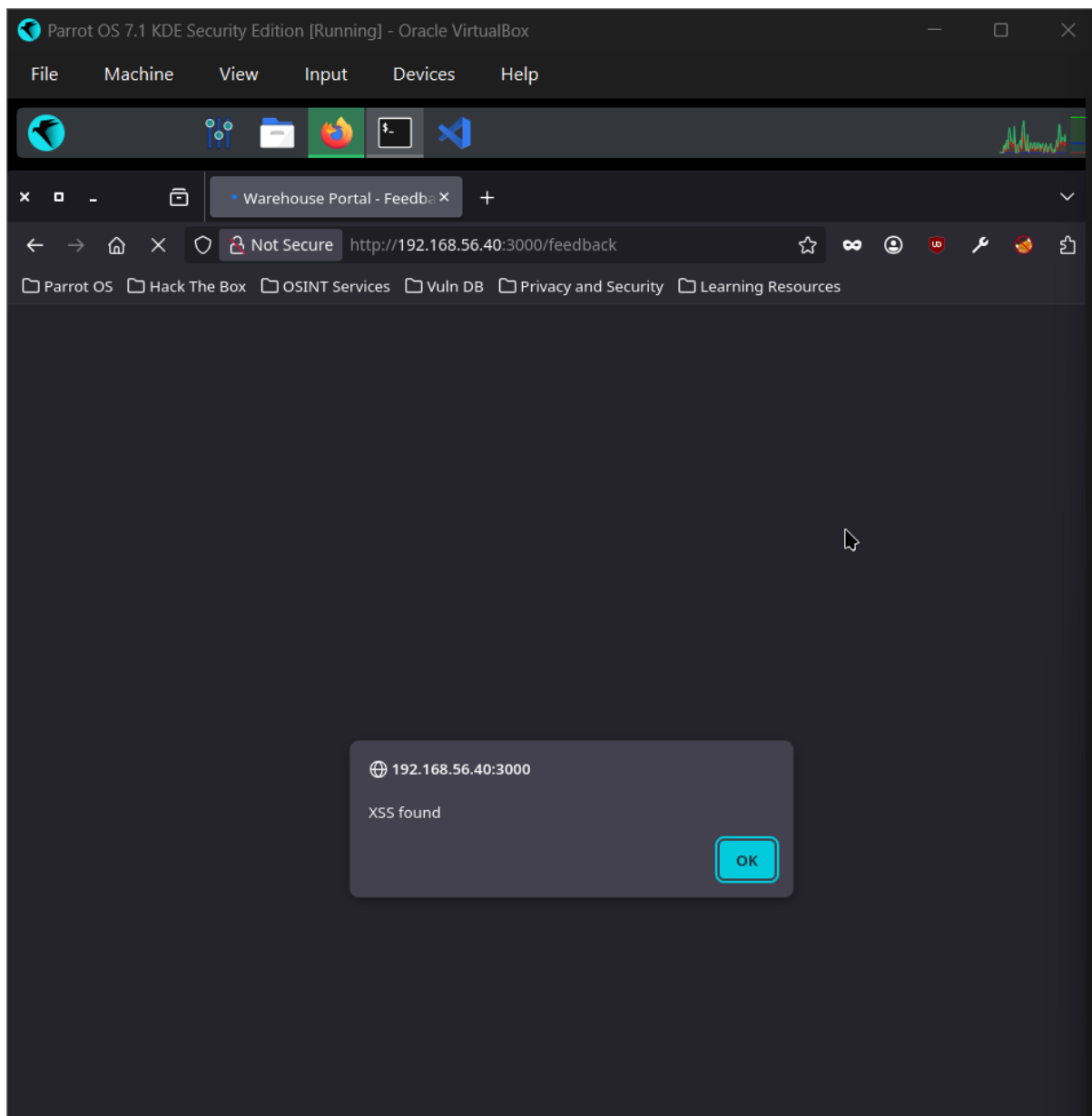


Figure 7 – XSS popup alert confirming successful script injection on the feedback page

A cross-Site Scripting vulnerability (CWE-79) is confirmed by this. Without any input sanitisation encoding, the program accepted and ran dangerous JavaScript. This might be used in a genuine attack to collect session cookies from other users who are signed in, send victims to phishing websites of clients without their knowledge [8][10].

8.9 Exploitation – Finding 4: SQL Injection

I employed the automated SQL injection testing tool SQL map to evaluate the login endpoint for SQL injection weaknesses. The command that was utilized was:

```
sqlmap -u "http://192.168.56.40:3000/login" --data="username=admin&password=admin123" --batch --level=2
```

Figure 8 shows that SQLmap began assessing the login parameters.” The tool identified that the server was redirecting POST requests to the dashboard, confirming that authentication was occurring. The tool then began analysing the username parameter for Boolean-based blind SQL injection.

```

~ : sqlmap — Konsole
File Edit View Bookmarks Plugins Settings Help
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.90 seconds
[user@parrot]~$ sqlmap -u "http://192.168.56.40:3000/login" --data="username=admin&password=admin123" --batch --level=2
• Login
[1.9.6#stable]
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the
end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability
y and are not responsible for any misuse or damage caused by this program
admin 2026-04-18 15:23:12
[*] starting @ 16:25:08 /2026-04-18/
admin 2026-04-17 20:55:05
[16:25:09] [INFO] testing connection to the target URL
got a 302 redirect to 'http://192.168.56.40:3000/dashboard'. Do you want to follow? [Y/n] Y
redirect is a result of a POST request. Do you want to resend original POST data to a new location? [Y/n] Y
you have not declared cookie(s), while server wants to set its own ('connect.sid=s%3A-QDVQqX...g531D8Za8Q'). D
o you want to use those [Y/n] Y
[16:25:09] [INFO] testing if the target URL content is stable
[16:25:10] [WARNING] POST parameter 'username' does not appear to be dynamic
[16:25:10] [WARNING] heuristic (basic) test shows that POST parameter 'username' might not be injectable
[16:25:10] [INFO] testing for SQL injection on POST parameter 'username'
[16:25:10] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'

```

Figure 8 – sqlmap testing the login page for SQL injection vulnerabilities

SQL injection flaws enable attackers to later database queries, possibly retrieving all client records, user credentials and order information from the database without permission. SQL injection regularly ranks among the OWASP Top 110 most severe web vulnerabilities and poses a significant threat to any application that stored data [8][10].

8.10 Vulnerability Summary Table

Vulnerability	Location	Severity	MITRE ID
Default Credentials	Login page	Critical	T1078
Broken Access Control	Admin page	Critical	T1548
Command Injection	Admin export	Critical	T1059
Cross-Site Scripting	Feedback page	High	T1059
SQL Injection	Login endpoint	Critical	T1190
No Rate Limiting	Login page	Medium	T1110

9. Conclusion

This report investigated offensive cybersecurity via strategic threat evaluation and hands-on red team assessment, illustrating how actual attack data can be converted into practical security enhancement. The research emphasizes the necessity of combining insights from major cyber incidents with practical penetration testing to enhance organizational resilience against contemporary threats, alighting theoretical understanding with real-world application [1] [2].

The examination of the 2025 ransomware incidents targeting Marks & Spencer and the Co-operative Group indicated that these breaches resulted not from sophisticated zero-day vulnerabilities but from avoidable flaws in human, procedural and technical safeguards. Threat actors took advantage of inadequate identity verification, feeble multi-factor authentication, and lack of sufficient monitoring, demonstrating that even, well-funded organizations are at risk when fundamental security measures are not properly implemented [1] [2] [9].

The report utilized the MITRE ATTACK framework to chart the entire attack lifecycle, from initial access to ransomware deployment, emphasizing a significant gap in detection and response abilities. The extended duration of attacker presence showed that organizations need to enhance not just prevention but also ongoing monitoring and threat detection to recognize harmful activities promptly [1] [7] [9].

The operational and financial repercussions of these events highlighting the need for cybersecurity to be a kept business focus. Considerable financial setbacks, interruptions in service and harm to reputation demonstrated that lagging detection and response directly amplify the extent of the impact, underlining the necessity for proactive and well-organized security approaches [1] [2].

The hands-on red team assessment in Task 2 conformed these results by revealing significant vulnerabilities like default credentials, flawed access control, command injection. Cross-site scripting and SQL injection. These vulnerabilities revealed how effortlessly attackers can obtain enforced [8] [10].

In summary, the report asserts that successful cybersecurity necessitates a comprehensive strategy that combines people, processes and technology. Ongoing surveillance, robust authentication methods, secure system architecture and frequent penetration testing are crucial to mitigate risk. Utilizing frameworks like MITRE ATTACK and embracing a proactive security approach, organizations can greatly enhance their capacity to safeguard against emerging cyber threats [1] [2] [7] [9] [10].

10. References

- [1] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, "Ransomware: Recent advances, analysis, challenges and future research directions," *Computers & Security*, vol. 111, p. 102490, 2021, doi: 10.1016/j.cose.2021.102490
- [2] Sooraj Sudheer, "Ransomware Attacks and Their Evolving Strategies: A Systematic Review of Recent Incidents," *International Journal of Technology and Systems (IJT)*, vol. 6, no. 7, pp. 32-59, 2024,
- [3] D. Pi, J. Liu, and Y. Wang, "Optimized Iterative Algorithm to Generate Computer-Generated Holograms Based on the Intermediate Angular-Spectrum Method," *IEEE Photonics Journal*, vol. 14, no. 3, June 2022, doi: 10.1109/JPHOT.2022.3162632.
- [4] M. Aldhaheeri, I. Manikas, R. Sharma, and B. Sundarakani, "An investigation of the effect of supply chain digitalization and sustainability on food security through improved forecasting capabilities," *IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD) 2023*, pp. 1-6, 2023, doi: 10.1109/ICTMOD59086.2023.10438117.
- [5] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures," *Sensors*, vol. 21, pp. 1-28, 2021, doi: 10.3390/s21144759.
- [6] Takuma Watanabe, "Image-Based Radar Cross Section Synthesis for a Cluster of Multiple Static Targets," *IEEE Transactions on Instrumentation and Measurement*, vol. 72, 2023, doi: 10.1109/TIM.2023.3246489.
- [7] J. Manzoor, A. Waleed, A. F. Jamali and A. Masood, "Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs," *PLOS ONE*, vol. 19, no. 3, Art. no. e0301183, 2024, doi: 10.1371/journal.pone.0301183.
- [8] J. R. Tadhani, V. Vekariya, V. Sorathiya, S. Alshathri and W. El-Shafai, "Securing web applications against XSS and SQLi attacks using a novel deep learning approach," *Scientific Reports*, vol. 14, no. 1, Art. no. 48845, 2024.
- [9] MITRE Corporation, "MITRE ATT&CK Enterprise Matrix," MITRE, 2024. [Online]. Available: <https://attack.mitre.org>
- [10] OWASP Foundation, "OWASP Top Ten Web Application Security Risks," *Open Web Application Security Project*, 2021. [Online]. Available: <https://owasp.org/www-project-top-ten/>