

Module Title: Ethical Hacking

Module Code: ACCA7033

Assignment Title:

Strategic Threat Analysis and Practical Penetration Testing Assessment

Task 1:

Strategic Analysis of the M&S and Co-op UK Cyber Campaign

Task 2:

Practical Penetration Testing and Vulnerability Assessment in a Virtual Lab Environment

Submitted to:

Dipo Dunsin

Student Name:

Keval Mahendra Motivaras

Student ID:

2515743

MSc Cyber Security and Digital Forensics

Institution:

University of Wales Trinity Saint David (UWTSD) London

Submission Date:

[June 30, 2026]

Word Count:

[4800]

Contents

Task 1: Strategic Threat Analysis of the M&S and Co-op UK Cyber Campaign.....	4
Introduction	4
Incident summary and timeline	4
Adversary TTP Mapping	7
Root Cause and Security Control Failures	9
Threat Actor Profile and Detection Response Analysis.....	10
Strategic Recommendations	11
TASK 2 — Practical Penetration Testing and Vulnerability Assessment.....	15
1. Introduction	15
2. Lab Environment Setup	16
3. Tools Used During Assessment.....	18
4. Attack 1 – Reachability Testing.....	18
5. Attack 2 — Service Discovery	19
6. Attack 3 — Anonymous FTP Access.....	21
7. Attack 4 – Validation of VSFTPD vulnerability.....	22
8. Attack 5 – Web Vulnerability Enumeration.....	23
9. Attack 6 — SMB Enumeration	26
10. Nessus Vulnerability Assessment	29
11. Recommendations.....	30
12. Conclusion	31
References and Appendices	32

Abstract

In this report, the cyber incidents experienced by Marks & Spencer and the Co-Operative Group in 2025 will be analyzed as a probable single campaign, while maintaining the uncertainties regarding the evidence. Such a claim is backed up by the public statement from the Cyber Monitoring Centre that the cyber incidents experienced by the two companies represent “a single combined cyber event.” This is supplemented by reports indicating that both companies have suffered from similar or nearly identical tactics, and a threat actor has even claimed responsibility for both incidents. While combining data theft, business disruption, and, at least in the case of M&S, ransomware-type effects, the cyber campaign has become a system-wide shock in UK retailing. In its report to the Parliament, M&S has admitted that the initial entry into their system occurred on 17 April 2025 using social engineering methods in collaboration with a third party. Co-Op CEO revealed that Co-Op has experienced a multi-stage attack on 25 April 2025. Available evidence strongly indicates attribution of Scattered Spider/UNC3944 operations in collaboration with DragonForce ransomware campaign [1], [2], [3].

The key takeaway from the analysis is that the campaign succeeded less because of defeating perimeter technology and more through defeating the trust and assurance mechanisms of identity. The key underlying factors that contributed to success include ineffective helpdesk identity verification, susceptibility to password/MFA reset attacks, reliance on third parties with over-trust, inadequate segmentation and lack of detection of abuse of a legitimate account. Co-op appears to have mitigated any potential for damage to a larger portion of their infrastructure by isolating and segregating more aggressively, while M&S was more heavily impacted in terms of operational dysfunction due to their highly interdependent systems in the retail, fulfillment, and online worlds being harder to isolate and more difficult to recover from [4], [5].

Furthermore, this report incorporates a realistic penetration testing and vulnerability assessment carried out within a safe virtual lab setting with the help of Kali Linux, Metasploitable 2, OWASP BWA, and Windows 7. Various penetration testing methodologies such as host discovery, service enumeration, authentication testing, vulnerability testing, SMB enumeration and scanning using Nessus Essentials have been implemented to discover services that are visible on the network, insecure settings and any vulnerabilities.

Task 1: Strategic Threat Analysis of the M&S and Co-op UK Cyber Campaign

Introduction

What makes the M&S and Co-op incidents strategically significant is that they represent an example of the way in which cyber crime may lead to a disruption visible at the national level in a non-critical infrastructure industry through the exploitation of enterprise identity processes. In June 2025, the Cyber Monitoring Centre categorised the combined disruption as a Category 2 systemic event with estimated financial losses ranging between £270 million and £440 million. M&S independently estimated its 2025/26 operating profit losses at about £300 million, while Co-op estimated a total financial impact of £107 million in profitability losses and £285 million in revenue losses due to deliberate restrictions placed upon its own IT systems.

From a methodology point of view, the present report places importance upon the official victim statement, UK public sector guidelines, parliamentary evidence, and vendor threat intelligence reports. As complete forensic information was not made publicly available, the TTP matrix included below explicitly distinguishes between confirmed actions, likely actions and actor consistent inferences. This is relevant to postgraduate research: based on publicly available information, it can be concluded that the campaign relied upon social engineering of identity processes, but not every single step in the post-exploitation phase can be conclusively reconstructed.

Incident summary and timeline

According to public information, the two campaigns unfolded rapidly but required quite some time to be mitigated successfully. M&S told the parliament that the attackers penetrated the company network on 17 April 2025, that M&S discovered the intrusion on 19 April and held its first crisis meeting on the same day, informed the appropriate authorities and announced the incident to the public on 22 April. The company disclosed its operational disruptions caused by the cyber-attack on 23 April, when the problem affected contactless payments and Click & Collect service, and suspended all online orders and the app on 25 April. On 13 May, the company notified their customers that their personal data were compromised but no card details and passwords were stolen. M&S stated that it was attacked by deceiving its contractors' employees on 21 May and allowed limited orders on 10 June [4], [5].

Co-op was less detailed in its public account but equally serious in terms of losses suffered. According to Co-op's CEO, the company was subjected to a multi-stage cyber-attack on 25 April 2025. On 2 May, Co-op disclosed to the public that its system was penetrated and personal data were extracted. Co-op entered recovery phase of the

incident, having restored its systems in a controlled fashion, after having taken early and decisive action to restrict the access to its systems. Later in 2025 and early in 2026, Co-op disclosed the material financial consequences of the said decision[1], [2].

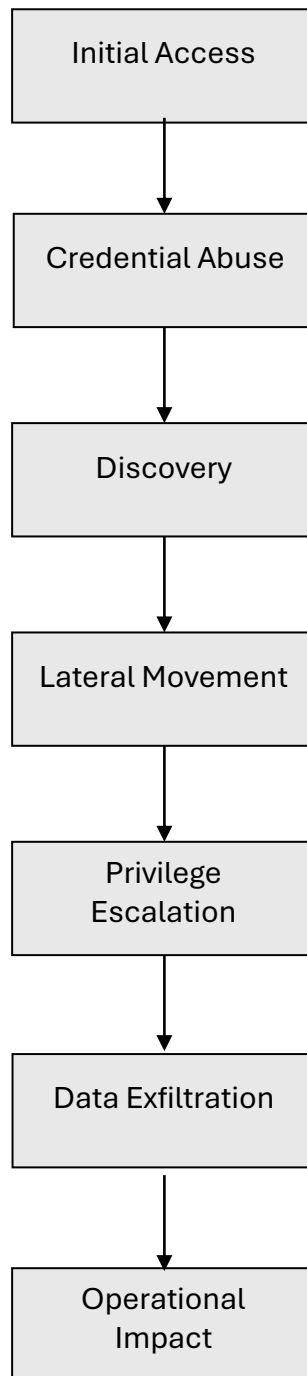


Diagram 1: Cyber Attack Chain Overview

Date	Organisation	Event	Evidence
17 Apr 2025	M&S	Initial entry through sophisticated social engineering involving a third party	[4]
19 Apr 2025	M&S	Intrusion recognised; crisis management team convened that evening	[2], [6]
22 Apr 2025	M&S	Public disclosure	[2]
23 Apr 2025	M&S	Contactless issues, Click & Collect pause, some processes moved offline	[2], [6]
25 Apr 2025	M&S	Online and app orders paused	[2]
25 Apr 2025	Co-op	Multi-stage attack date later disclosed by CEO	[3], [6]
2 May 2025	Co-op	Data extraction from one system confirmed	[3]
4 May 2025	Sector-wide	NCSC warns retailers to review helpdesk reset processes and monitor account misuse	[1]
13 May 2025	M&S	Customer data theft disclosed; no usable payment data or passwords	[2]
14 May 2025	Co-op	Recovery phase announced	[3], [6]
21 May 2025	M&S	Third-party contractor social-engineering vector confirmed; £300m impact estimated	[6], [4]
,10 Jun 2025	M&S	Limited online orders resumed	[2]
20 Jun 2025	Campaign	CMC treats incidents as one combined event	[7]
10 Jul 2025	Campaign	NCA arrests four suspects in connection with M&S, Co-op and Harrods attacks	[4], [6]

Table 1: Incident Summary

Adversary TTP Mapping

The following ATT&CK mapping utilizes official MITRE ATT&CK Enterprise technique identifiers and distinguishes between proven and inferred tradecraft. The logic of evidence here is clear – public reports confirm social engineering driven account takeover, data theft and ransomware impact; vendor/government reports on UNC3944/Scattered Spider offer the most reasonable explanations for the intervening steps, including helpdesk abuse, MFA exploitation, cloud account misuse and lateral movement.

Stage	ATT&CK Technique	Description
Initial Access	T1078	Valid accounts abuse
Credential Access	T1556	MFA reset manipulation
Discovery	T1087	Account discovery
Exfiltration	T1567	Data exfiltration

Table 1: Attack-flow table

ATT&CK ID	Technique	Confidence	Campaign Justification
T1591	Gather Victim Org Information	Medium	The actor appears to understand the structure of retail operations and target organisations with large outsourced or support-based attack surfaces, corresponding with Mandiant and NCSC observations regarding modern ransomware targeting strategies [1], [3], [5].
T1589.003	Gather Victim Identity Information:	Medium	Public reporting suggests that attackers impersonated legitimate personnel and presented valid employee details to

ATT&CK ID	Technique	Confidence	Campaign Justification
	Employee Names		helpdesk staff, indicating prior collection of identity information [2], [4], [5].
T1684.001	Social Engineering: Impersonation	High	M&S described the initial breach as sophisticated impersonation, while NCSC guidance highlighted social engineering targeting IT helpdesks [1], [2], [5].
T1598.004	Phishing for Information: Spearphishing Voice	Medium	Public reporting suggests attackers manipulated helpdesk personnel into resetting passwords through social engineering techniques consistent with voice phishing [1], [2], [4].
T1078	Valid Accounts	High	The campaign relied heavily on the abuse of legitimate identities rather than unauthenticated software exploitation. Reuters reported that attackers exploited employees at a third-party contractor [1], [4], [5].
T1556.006	Modify Authentication Process: Multi-Factor Authentication	Medium	NCSC guidance referenced password and MFA reset abuse, while ransomware campaigns increasingly target authentication workflows to maintain persistence [1], [3], [5].
T1098.005	Account Manipulation: Device Registration	Medium-Low	Public reporting does not fully confirm device registration abuse, however ransomware groups commonly register attacker-controlled MFA devices following credential compromise [1], [3], [5].
T1087.004	Account Discovery: Cloud Account	Medium-Low	Public reporting suggests that attackers likely conducted account discovery activities following initial access in order to identify privileged or cloud-based accounts [1], [5].
T1021	Remote Services	Medium	M&S explained that legacy connectivity allowed lateral movement within the environment after initial compromise. Remote administrative services commonly facilitate attacker movement across enterprise networks [1], [3], [5].

ATT&CK ID	Technique	Confidence	Campaign Justification
T1005	Data from Local System	High	Both M&S and Co-op confirmed that customer and organisational data was accessed and extracted from internal systems prior to exfiltration [2], [3], [5].
T1567.002	Exfiltration to Cloud Storage	Low-Medium	Data exfiltration was publicly confirmed, although the exact transfer method was not disclosed. Cloud-based exfiltration methods are common within modern ransomware operations [1], [3], [5].
T1486	Data Encrypted for Impact	High for M&S, Low for Co-op	The M&S incident was publicly associated with ransomware activity and operational disruption. Modern ransomware campaigns frequently combine encryption with extortion and data theft tactics [3], [4], [5].

Mapping demonstrates that the campaign is mainly based on identity-based intrusion, privilege maintenance via authentication workflow exploitation and economic impact. More importantly, it shows why purely malware-focused detection solutions perform worse in this situation – many of attacker advantages come from legitimate authentication events and organizational shortcuts rather than any exploit kits or malicious binaries.

Root Cause and Security Control Failures

The most compelling underlying reason for this incident was the breakdown of identity assurance processes at the helpdesk and administrator boundaries. M&S described the initial attack as using advanced impersonation and involving third parties, and later Reuters reported that the attack involved manipulation of employees at the third party's contractor. NCSC guidelines, issued after the incident, did not emphasize software exploits or patching practices. Rather, they suggested improving the process of password resetting, monitoring risky logins, and reviewing the activity of privilege accounts, which indicates that the main point of the control failure was the social engineering-prone identity verification process [1], [2], [4].

Another issue was the lack of effective third-party identity and access management processes. Public reporting indicated that the attackers took advantage of trust relationships between the retail company and its external partners. It can be assumed that access accounts created by suppliers had too much trust or the power to interfere with identity verification processes in case of insufficient identity assurance measures. It

shows that the supplier and contractor access should be managed as an integral part of identity security strategy rather than an operational problem [1], [4].

Another potential weakness was inadequate network segmentation. M&S revealed that the presence of hybrid environment with modern and legacy systems complicated the containment process and provided easier lateral movement after the initial penetration. Although M&S claimed that a substantial share of systems was isolated from others due to shut down, the incident showed that interconnected retail environments cannot be easily isolated during active attacks. Effective segmentation of the identity systems, fulfillment operations, commerce platform, and administrative systems is vital for restricting the attack surface [1], [4], [5].

The human and organizational factors were also important for this breach. The literature on the subject and the campaign itself have shown that social engineering attacks are successful when organizations prefer operational efficiency and speedy workflows to identity verification measures. Helpdesk employees are especially vulnerable to such attacks, as they are required to grant fast access. Literature on social engineering and ransomware consistently points out that human trust, urgency, and procedural shortcuts are major factors that cause the success of social engineering attacks [2], [3].

Threat Actor Profile and Detection Response Analysis

Most likely scenario includes financially motivated cybercriminal ecosystem with identity theft (Scattered Spider or UNC3944-style) and DragonForce ransomware operation.

Public reports and threat intelligence assessments indicate that the attacks were mostly based on social engineering, compromise of valid accounts and identity-oriented intrusions rather than technical exploit of vulnerabilities. Later Reuters reported that attacks included manipulation of third-party contractors' personnel, while Mandiant detected methods which align with UNC3944's usual tactics. Publicly released reports connected the campaign with the DragonForce ransomware activities and extortion-based motivation [3], [4].

Attribution cannot be taken as completely certain. NCSC noted that it was not in position to confirm that attacks were linked to the same threat actor or campaign. Thus, most academically sound assessment is high level of confidence in similarity of attack method, medium level of confidence in threat actor participation in the same attacks and medium confidence in collaboration of ransomware operators and identity intrusions affiliate in ransomware as a service ecosystem. This scenario corresponds to current model of

cybercriminal ecosystem when access brokers, ransomware operators and extortion groups work in loose associations rather than in strict organizational structure [1], [3].

Detection and response aspects show strong executive mobilization but weak detection of identity-related threats. Public sources indicate that the company has managed to identify suspicious activities and to call for external specialists quickly, but the attacks have been performed by the time the suspicious activity was detected, and the attackers had enough time to obtain access and to learn internal processes for forced containment actions [2], [4], [5].

Public Co-op response appears to be more containment-oriented and resilient to the attacks. Public statements show that quick restriction of systems access, segmentation and isolation helped to avoid larger compromise and allowed to keep operations running despite of data leakage and logistical disruptions. Though the organization suffered operational disruption, the response shows that compartmentalization and quick containment of attackers limited their movements inside the environment [1], [2].

The general strategic lesson learned is that both organizations showed more maturity in crisis response than identity prevention and anomaly detection. NCSC recommendations which were issued after the incidents contain a lot of advice about risky sign-ins, monitoring of privilege accounts, password resets and identity verification processes. It clearly indicates that the major security issue was lack of proper detection of identity-centered methods rather than lack of endpoint protection [1], [3], [5].

Strategic Recommendations

The prevention, detection and response priorities below are ordered by likely risk reduction against this exact campaign class. Effort and cost are expressed as **Low**, **Medium**, or **High** relative to a large UK retail enterprise.

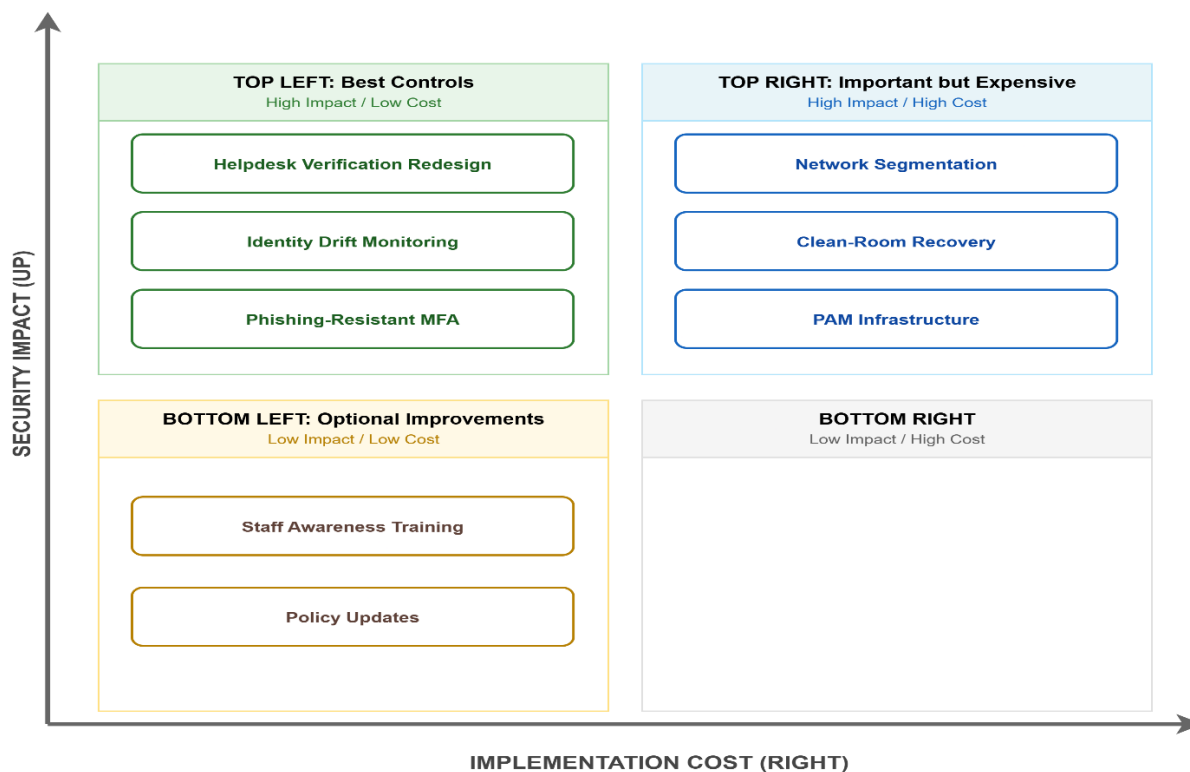


Diagram 2: Security Recommendations Priority Matrix

However, prior to discussing any defensive controls, the first telemetry requirement to be listed must be explicitly stated – defending against ransomware attacks that specifically target identities implies the necessity for comprehensive visibility into authentication and identity events rather than simple malware detection. Specifically, this includes observing password resets, modifications to MFA configuration, privileged role changes, third party access (contractors), risky sign-ins, remote administration, SMB/RDP usage, and unusual access to sensitive customer/operations systems. Service desk engagements and activities should also be treated as security telemetry since the service desk itself was used as an attack vector by the actors during both of these campaigns [1], [3], [5].

Priority Recommendation	Why it matters in this campaign	Effort / Cost Band
Implement phishing-resistant MFA for employees, contractors, administrators, and service desk workflows	NCSC guidance has pointed out that password/MFA reset abuse has been a key risk. Reinforcement of MFA processes directly addresses the identity reset vectors used in the campaign [1], [3].	Medium / Medium

Priority Recommendation	Why it matters in this campaign	Effort / Cost Band
Revise identity verification processes in the helpdesk through callback procedures and approval workflows	The attack flow depended a lot on convincing helpdesk operators to perform legitimate actions. Process revision is therefore more effective than awareness training [1], [2], [4].	Low-Medium / Low-Medium
Remove permanent privileged access for suppliers and support providers through PAM and just-in-time access controls	Public reporting showed that access relationships with third parties played an important role in the initial breach route [3], [4].	Medium / Medium-High
Enhance segmentation between e-commerce, fulfilment, identity systems and corporate infrastructure	There is public evidence that interconnected systems made the containment and recovery after breach more difficult [1], [4], [5].	High / High
Create detections for valid account abuse and identity anomalies	NCSC recommendations have emphasized the importance of detecting risky sign-ins, privileged access changes, MFA modifications and unusual authentication behaviour [1], [3].	Low-Medium / Low-Medium
Create a clean room recovery capability with immutable backups and tested recovery procedures	The incidents have shown that recovery architecture and planning are crucial when there are problems related to ransomware operations [3], [5].	Medium-High / Medium-High
Conduct regular cross-functional cyber incident exercises with suppliers and external stakeholders	Both incidents have demonstrated that ransomware mitigation is an enterprise-wide operation problem rather than strictly an IT problem [1], [5].	Low / Low
Enable rapid incident reporting and sector-wide intelligence sharing	Fast information exchange between organizations and national cyber organizations can decrease the dwell time of the attackers and improve collective	Low / Low

Priority Recommendation	Why it matters in this campaign	Effort / Cost Band
	defence in the retail sector [1], [4].	

Table 3: Strategic Security Recommendations Following the M&S and Co-op Cyber Campaign

Combining all these control strategies implies a clear need to transition from old perimeter-based security strategy to new identity-resilient security architecture. The main security goal should be to make sure that all authentication changes require strong proof of identity, all privileged accesses are isolated, recovery environment is protected, and there is fast information exchange in the sector during incidents [1], [3], [5].

TASK 2 — Practical Penetration Testing and Vulnerability Assessment

1. Introduction

Penetration Testing and Vulnerability Assessment are an indispensable part of contemporary cybersecurity measures. Penetration tests allow organisations to detect their vulnerabilities in advance and prevent potential attackers from exploiting them. In order to conduct a practical assessment, the activity was performed in a controlled environment of VirtualBox.

The aim of the assignment is to identify open ports, configuration vulnerabilities, insecure authentications and vulnerable software through both manual and automated penetration testing approaches. The following three targets located in an isolated VirtualBox environment have been assessed for vulnerabilities:

- Metasploitable 2
- OWASP Broken Web Applications (OWASP BWA)
- Windows 7

Kali Linux OS has been chosen as the attacking machine due to its extensive set of tools for penetration testing and security auditing. Some industry-recognised tools such as Nmap, FTP, Nikto, enum4linux, Metasploit Framework and Nessus Essentials have been employed throughout the assessment.

Penetration testing process includes the following steps:

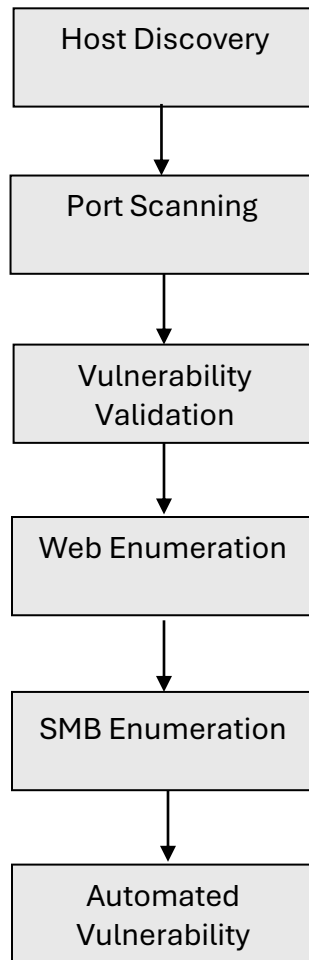


Diagram 3: Practical Assessment Workflow

All testing activities were conducted within an isolated host-only network to ensure that no external systems or public networks were affected during the practical assessment.

2. Lab Environment Setup

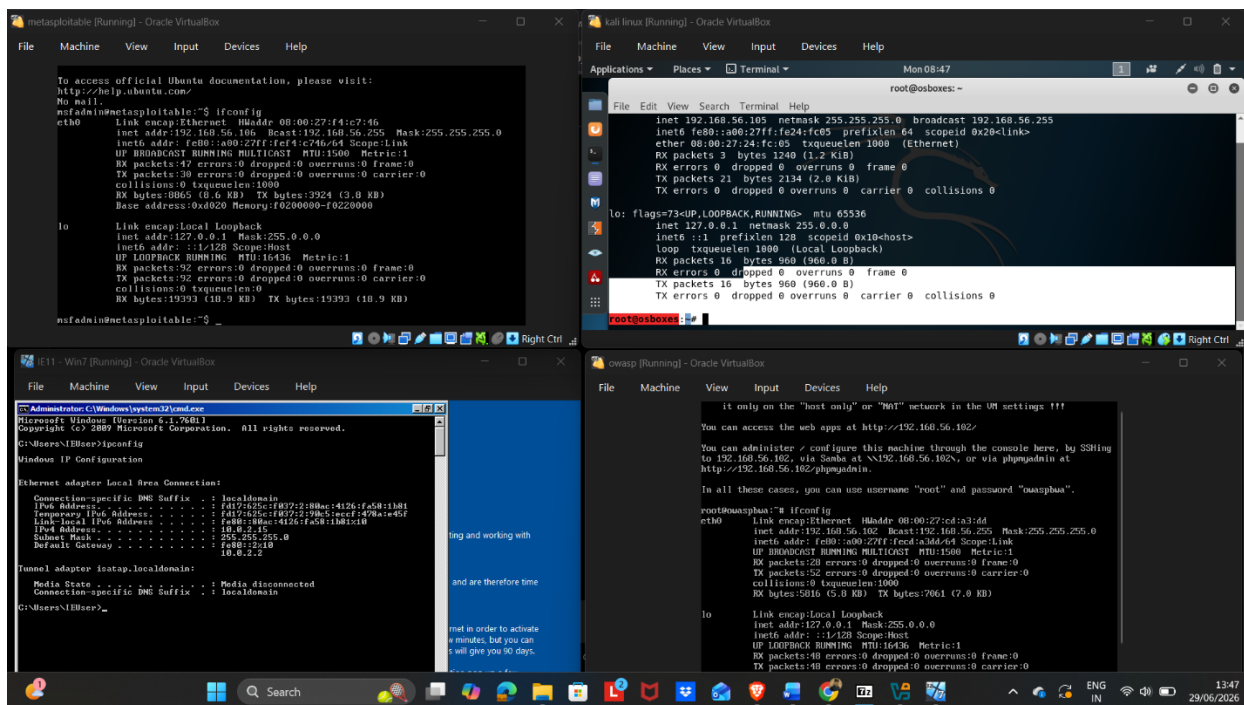


Figure 1: Virtual lab environment setup.

Penetration testing lab was developed using Oracle VirtualBox. Host-only network topology was adopted to ensure that the environment is isolated from the internet. Penetration testing lab consisted of one attacker machine and three target machines.

Attacker Machine:

1. Kali Linux 2019.3

Target Machines:

1. Metasploitable 2
2. OWASP Broken Web Applications
3. Windows 7

Host-only network topology was used to allow all virtual machines to communicate with each other without exposing them to the internet. An IP address was assigned to each virtual machine within the 192.168.56.0/24 subnet range.

The above-listed target systems represent vulnerable systems used by cybersecurity professionals for training purposes. This system had old services, insecure configurations, and exposed applications which could be exploited during penetration testing exercises.

3. Tools Used During Assessment

Several penetration testing and vulnerability assessment tools were used throughout the practical investigation.

Tool	Purpose
Nmap	Host discovery and service enumeration
FTP Client	Authentication testing
Metasploit Framework	Vulnerability validation
Nikto	Web server vulnerability scanning
enum4linux	SMB enumeration
Nessus Essentials	Automated vulnerability assessment

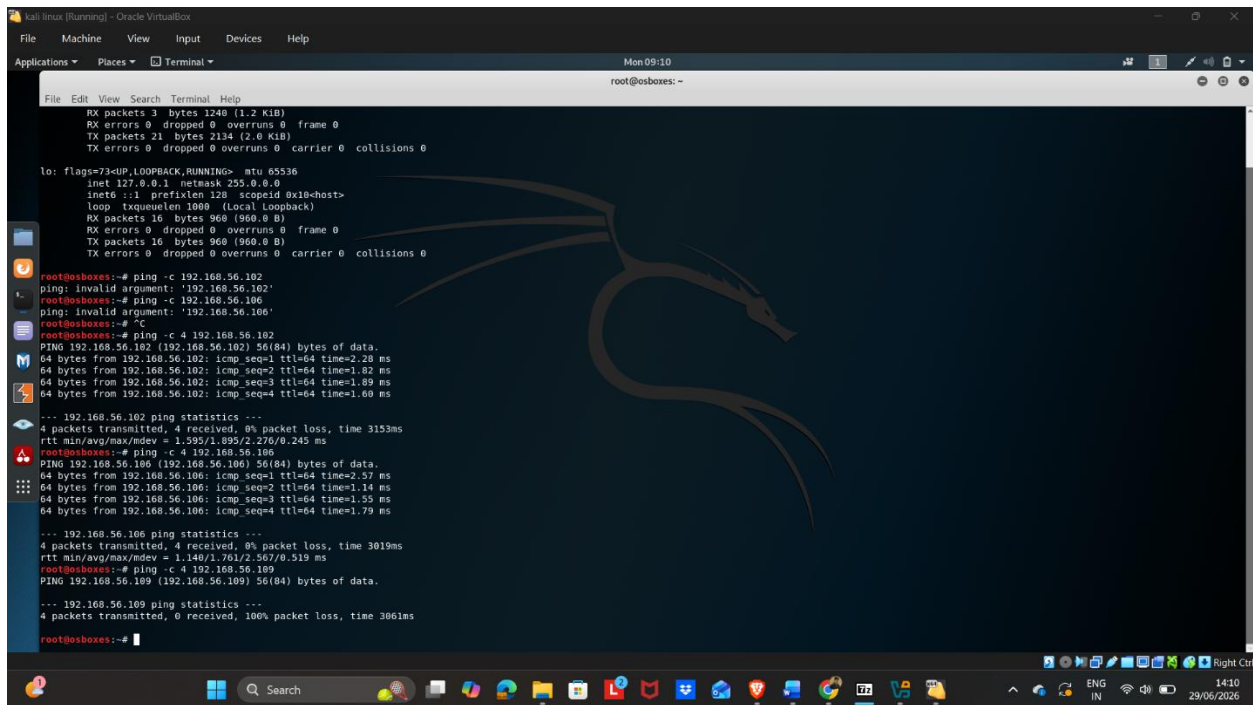
These tools provided both manual and automated methods for identifying vulnerabilities and validating security weaknesses across the target systems.

4. Attack 1 – Reachability Testing

Reachability testing refers to the first step where it was necessary to check whether there was a possibility to connect to the target system. Network reachability testing was conducted by sending ICMP packets to verify reachability of the targets.

The following systems returned ICMP reply message:

- Metasploitable 2
- OWASP BWA



```
kali:linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Places
root@kali:~# cat /dev/null
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 16 bytes 960 (960.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 960 (960.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# ping -c 1 192.168.56.102
ping: invalid argument: '192.168.56.102'
root@kali:~# ping -c 1 192.168.56.106
ping: invalid argument: '192.168.56.106'
root@kali:~# 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=2.28 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=1.82 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=1.89 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=1.60 ms

--- 192.168.56.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3153ms
rtt min/avg/max/mdev = 1.595/1.895/2.276/0.245 ms
root@kali:~# ping -c 4 192.168.56.106
PING 192.168.56.106 (192.168.56.106) 56(84) bytes of data:
64 bytes from 192.168.56.106: icmp_seq=1 ttl=64 time=2.57 ms
64 bytes from 192.168.56.106: icmp_seq=2 ttl=64 time=1.14 ms
64 bytes from 192.168.56.106: icmp_seq=3 ttl=64 time=1.55 ms
64 bytes from 192.168.56.106: icmp_seq=4 ttl=64 time=1.79 ms

--- 192.168.56.106 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3019ms
rtt min/avg/max/mdev = 1.140/1.761/2.567/0.519 ms
root@kali:~# ping -c 4 192.168.56.109
PING 192.168.56.109 (192.168.56.109) 56(84) bytes of data:
64 bytes from 192.168.56.109: icmp_seq=1 ttl=64 time=2.28 ms
64 bytes from 192.168.56.109: icmp_seq=2 ttl=64 time=1.82 ms
64 bytes from 192.168.56.109: icmp_seq=3 ttl=64 time=1.89 ms
64 bytes from 192.168.56.109: icmp_seq=4 ttl=64 time=1.60 ms

--- 192.168.56.109 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3061ms
rtt min/avg/max/mdev = 1.595/1.895/2.276/0.245 ms
root@kali:~#
```

Figure 2: ICMP reachability testing.

The Windows 7 machine did not reply to the ICMP packets sent out, possibly due to the presence of firewall rules or disabled ICMP responses. Nevertheless, the system was still reachable throughout the subsequent enumeration process.

Reachability scanning ensured that the target machines were reachable and active for additional scanning and vulnerability assessment tasks.

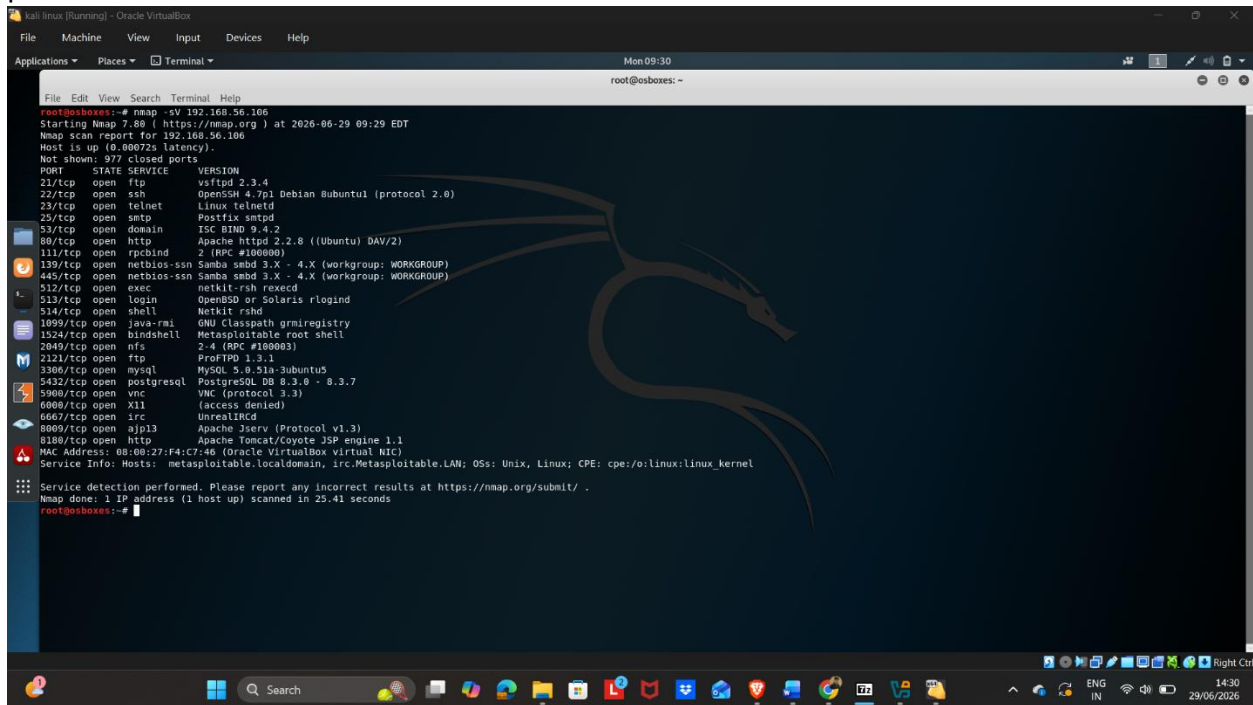
Security Analysis

ICMP replies can help the attacker in conducting reconnaissance by locating the active machines on the network. Most companies block ICMP replies through the firewall policy in order to minimise their exposure.

5. Attack 2 — Service Discovery

Service discovery was done via Nmap after verifying the availability of hosts. Service enumeration provides information about open ports, services, and the software version that runs on the targeted systems. This is an important step since services usually act as

possible vectors for attacks.



```
root@kali:~# nmap -sV 192.168.56.106
Starting Nmap 7.80 ( https://nmap.org ) at 2026-06-29 09:29 EDT
Nmap scan report for 192.168.56.106
Host is up (0.00072s latency).
Not shown: 972 closed ports
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 6ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain         ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind        2 (RPC #100000)
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec           netkit-rsh rshcd
513/tcp   open  login          OpenBSD or Solaris rlogind
514/tcp   open  shell          Netkit rshd
1099/tcp  open  java-rmi       GNU Classpath grmiregistry
1324/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
8080/tcp  open  ajp13          Apache jkerv (Protocol v1.3)
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:F4:C7:46 (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 25.41 seconds
root@kali:~#
```

Figure 3: Nmap scan on Metasploitable 2.

The above-mentioned command was run:

`nmap -sV <target IP>`

Multiple vulnerable and outdated services discovered by the Metasploitable system included:

- FTP (vsftpd 2.3.4)
- Telnet
- Apache HTTP Server
- Samba
- MySQL
- PostgreSQL
- IRC
- VNC

The following services were found to be exposed in the OWASP BWA system:

- Apache HTTP Server

- Samba
- SSH
- Tomcat services

Windows 7 system disclosed only the SSH services through scanning.

Security Analysis

The discovery of various services proved that there were some outdated and insecure services that would help to make the systems vulnerable to any attack. Legacy protocols and outdated FTP services are risky in nature since they usually have known security issues.

Services are very important for the attacker because they give them knowledge about the operating system and applications.

6. Attack 3 — Anonymous FTP Access

Authentication test was conducted against the FTP service in the Metasploitable system.

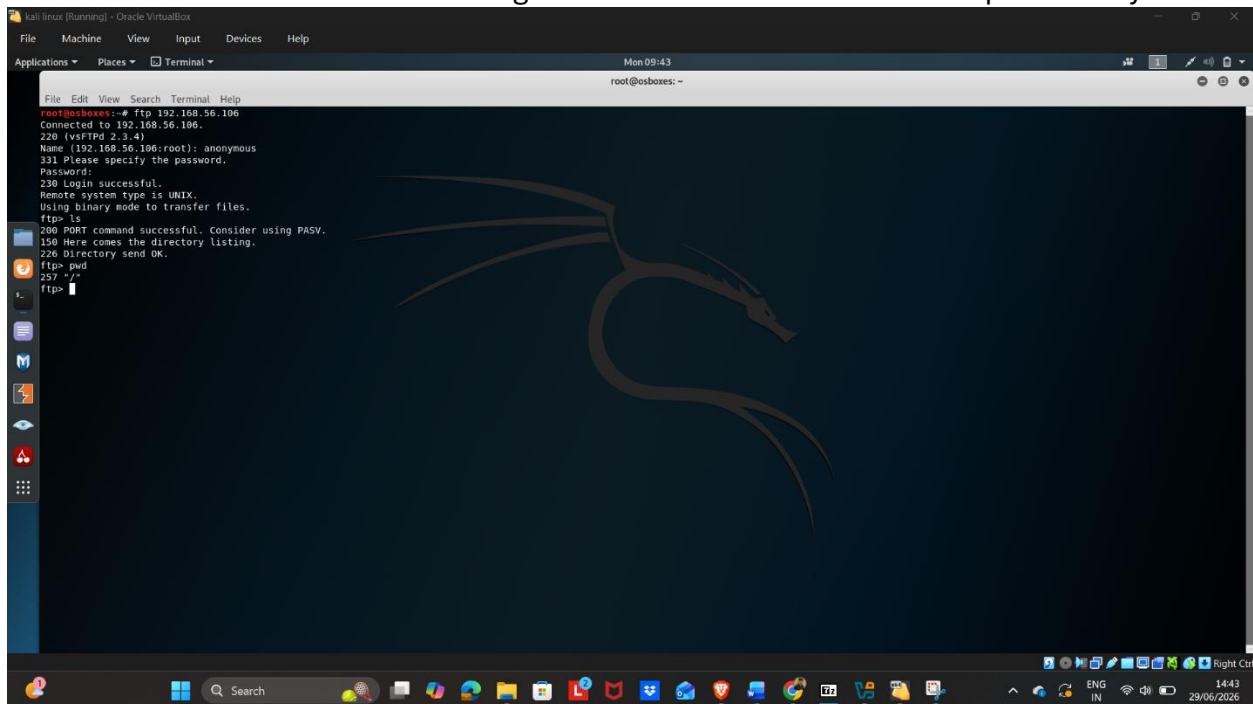


Figure 4: Anonymous FTP authentication.

The following command was used:

ftp 192.168.56.106

Login was successful with the username:

anonymous

The server permitted listing of directories after logging in.

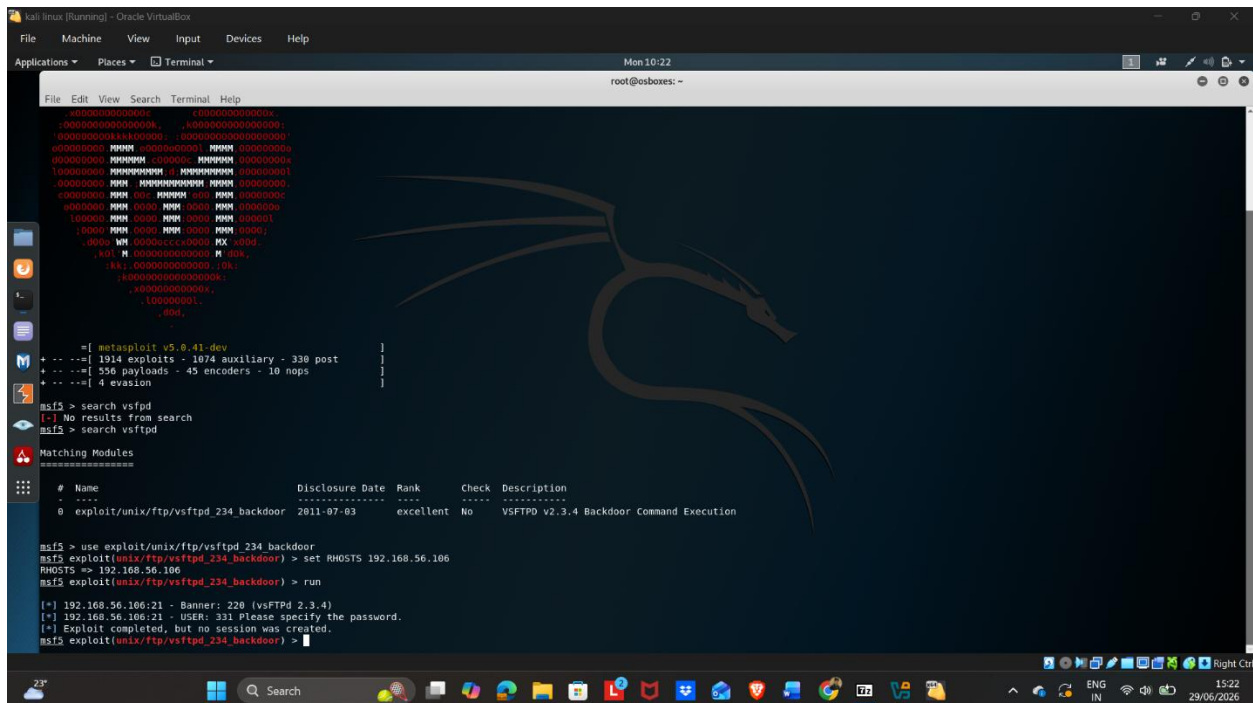
Security Analysis

The practice of allowing anonymous FTP login is a poor authentication mechanism since unauthorised users have access to the files present on the server. The consequences of misconfigured FTP server include:

- Information exposure
- File access by an unauthorised individual
- Malware distribution
- Leakage of data

Anonymous logins must be prevented from accessing the server unless absolutely required for public file exchange.

7. Attack 4 – Validation of VSFTPD vulnerability



```
kali linux [running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Mon 10/22
root@usbboxes: ~
File Edit View Search Terminal Help
[ASCII art of a dragon]
msf5 > search vsftpd
[*] No results from search
msf5 > search vsftpd
Matching Modules
=====
#  Name                                     Disclosure Date  Rank   Check  Description
#  ----                                     -
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent No      VsFTPd v2.3.4 Backdoor Command Execution

msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.106
RHOSTS => 192.168.56.106
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.56.106:21 - Banner: 220 (VsFTPd 2.3.4)
[*] 192.168.56.106:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf5 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Figure 5: VSFTPD vulnerability validation.

The following Metasploit module was used:

```
exploit/unix/ftp/vsftpd_234_backdoor
```

The vulnerability verification process has determined that the FTP service is using the vulnerable version of VSFTPD 2.3.4.

Security analysis

The VSFTPD 2.3.4 contains an interesting backdoor vulnerability that could be potentially exploited to execute commands remotely if certain conditions are met. Outdated and unsupported software still poses significant risks when exploited by attackers.

Failure to update or patch the software leads to increased exposure to attack.

8. Attack 5 – Web Vulnerability Enumeration

Nikto web vulnerability scanning tool was used to analyse the vulnerabilities of the web services installed on the target machine.

The following command was used:

```
nikto -h <target IP>
```

The Metasploitable system returned the following:

- Outdated version of the Apache web server
- The absence of any security headers
- Directory indexing is on
- phpMyAdmin page is exposed

- Sensitive PHP files are exposed

```

root@osboxes:~# nikto -h 192.168.56.106
-----
Nikto v2.1.6
-----
+ Target IP: 192.168.56.106
+ Target Hostname: 192.168.56.106
+ Target Port: 80
+ Start Time: 2020-06-29 10:52:45 (GMT-4)
-----
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The x-content-type-options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Uncommon header 'tcn' found, with contents: List
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /*=PHPBB5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /*=PHE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /*=PHE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /*=PHE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ Server may leak inodes via ETags. header found with file /phpMyAdmin/changelog, inode: 92462, size: 40540, mtime: Tue Dec 9 12:24:00 2008
+ OSVDB-3092: /phpMyAdmin/changelog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting.
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin: phpMyAdmin directory found
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3092: /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ 8726 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time: 2020-06-29 10:53:17 (GMT-4) (32 seconds)
-----
+ 1 host(s) tested
root@osboxes:~#

```

Figure 6: Nikto scan on Metasploitable 2.

The OWASP BWA system revealed:

- Outdated Apache and PHP versions
- Missing X-Frame and XSS protection headers
- TRACE HTTP method enabled
- Directory indexing vulnerabilities
- Exposed phpMyAdmin directories

```
kali linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Mon 10:56
root@osboxes: ~

File Edit View Search Terminal Help
+ Start Time: 2020-06-29 10:54:54 (GMT-4)
+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-lubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
+ Server may leak inodes via ETags, header found with file //, inode: 286483, size: 28067, mtime: Thu Jul 30 22:55:52 2015
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ OSVDB-3268: /cgi-bin/: Directory indexing found.
+ /crossdomain.xml contains a full wildcard entry. See http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ Uncommon header 'tcn' found, with contents: List
+ Apache mod negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.css, index.html
+ OSVDB-39272: /favicon.ico file identifies this app/server as: owasp.org
+ IP address found in the 'location' header. The IP is '127.0.1.1'
+ OSVDB-638: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is '127.0.1.1'.
+ OpenSSL/0.9.8k appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0a and 0.9.8z are also current.
+ mod_ssl/2.2.14 appears to be outdated (current is at least 2.0.3) (may depend on server version)
+ PHP/5.3.2-lubuntu4.30 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.
+ Perl/v5.10.1 appears to be outdated (current is at least v5.29.0)
+ proxy_html/3.0.1 appears to be outdated (current is at least 3.1.2)
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Phusion Passenger/4.0.38 appears to be outdated (current is at least 4.0.53)
+ mod_mono/2.4.3 appears to be outdated (current is at least 2.8)
+ Python/2.6.5 appears to be outdated (current is at least 2.7.8)
+ mod_perl/2.0.4 appears to be outdated (current is at least 2.0.8)
+ mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1 - mod_ssl 2.0.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. http://cve.mitre.org/cve-bin/cvname.cgi?name=CVE-2002-0082, OSVDB-756.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Retrieved x-powered-by header: PHP/5.3.2-lubuntu4.30
+ Cookie phpbb2owaspbwa data created without the httponly flag
+ Cookie phpbb2owaspbwa did created without the httponly flag
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ 8877 requests: 1 error(s) and 35 item(s) reported on remote host
+ End Time: 2020-06-29 10:56:02 (GMT-4) (68 seconds)
+ 1 host(s) tested
root@osboxes:~#
```

Figure 7: Nikto scan on OWASP BWA.

The Windows 7 system did not expose an active web service.

```
kali linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Mon 10:58
root@osboxes: ~

File Edit View Search Terminal Help
root@osboxes:~# nikto -h 192.168.56.109
- Nikto v2.1.6
+ No web server found on 192.168.56.109:80
+ 0 host(s) tested
root@osboxes:~#
```

Figure 8: Nikto scan on Windows 7.

Security Analysis

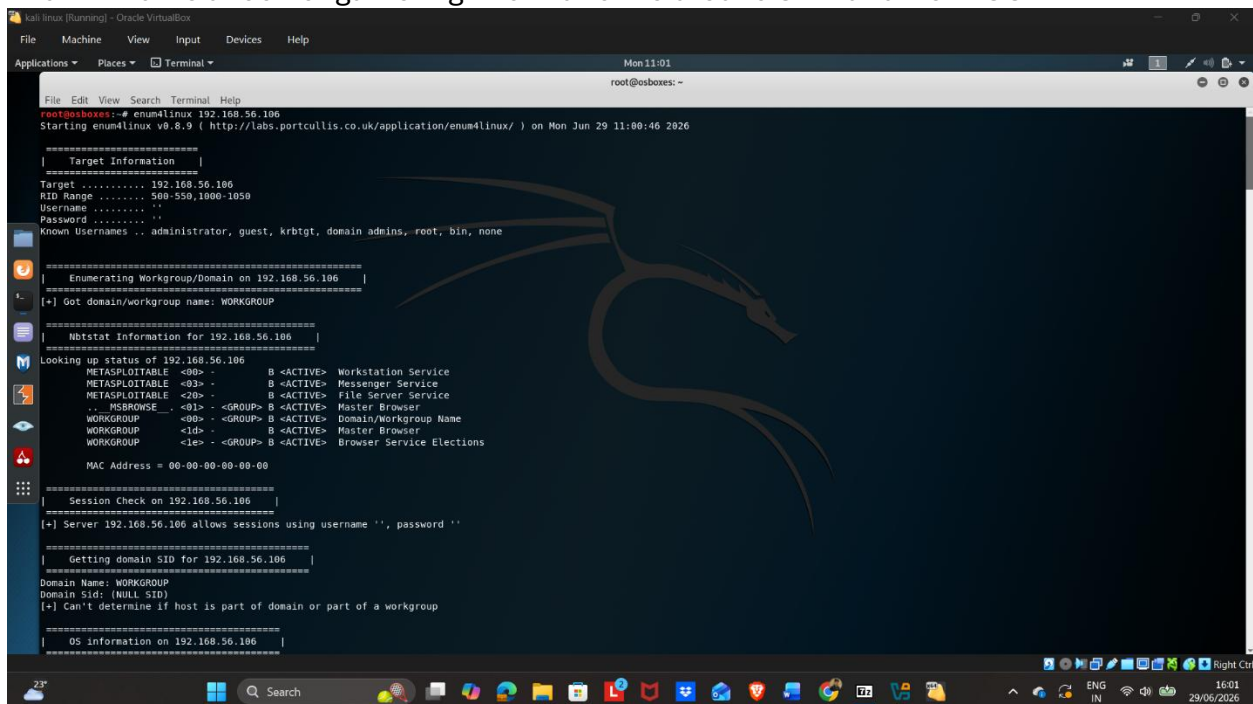
Nikto scan revealed a number of vulnerabilities in web servers that can be used by an attacker in case of web application attacks. Lack of HTTP security headers may result in vulnerabilities in terms of:

- Cross-Site Scripting (XSS)
- Clickjacking
- MIME Type Attacks

Also, directory indexing and visible administrative pages may give attackers valuable information about the structure of the web application.

9. Attack 6 — SMB Enumeration

Enum4linux is a tool for gathering information related to SMB and NetBIOS.



```
kali linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Mon 11:01
root@osboxes: ~

File Edit View Search Terminal Help
root@osboxes:~# enum4linux 192.168.56.106
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Jun 29 11:00:46 2026

=====
| Target Information |
=====
Target ..... 192.168.56.106
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 192.168.56.106 |
=====
[+] Got domain/workgroup name: WORKGROUP

=====
| Nbtstat Information for 192.168.56.106 |
=====
Looking up status of 192.168.56.106
METASPLOITABLE <00> - B <ACTIVE> Workstation Service
METASPLOITABLE <03> - B <ACTIVE> Messenger Service
METASPLOITABLE <20> - B <ACTIVE> File Server Service
.._MSBROWSE_ <01> - <GROUP> B <ACTIVE> Master Browser
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP <1d> - B <ACTIVE> Master Browser
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections

MAC Address = 00-00-00-00-00-00

=====
| Session Check on 192.168.56.106 |
=====
[+] Server 192.168.56.106 allows sessions using username '', password ''

=====
| Getting domain SID for 192.168.56.106 |
=====
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

=====
| OS information on 192.168.56.106 |
=====
```

Figure 9: SMB enumeration on Metasploitable 2.

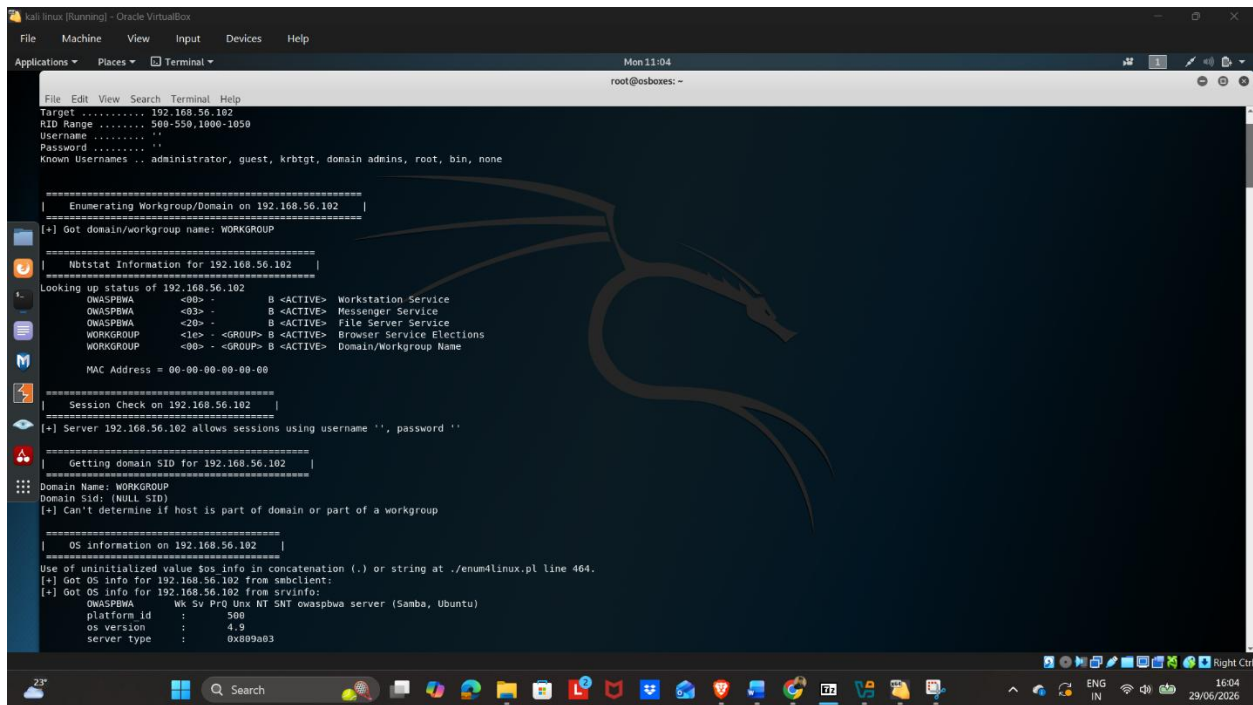


Figure 10: SMB enumeration on OWASP BWA.

The following command was used:

enum4linux <target IP>

The Metasploitable and OWASP systems disclosed:

- Workgroup information
- Server names
- Operating system details
- SMB service information

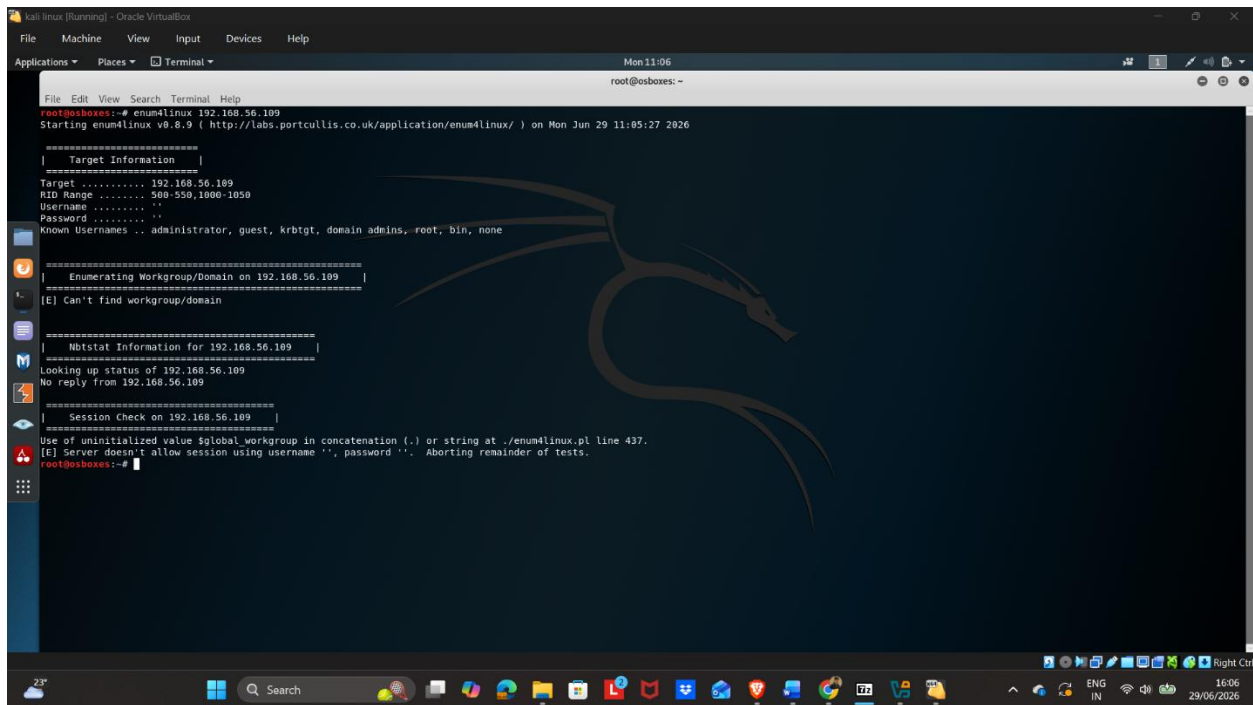


Figure 11: SMB enumeration on Windows 7.

Windows 7 had limited the ability to enumerate anonymously via SMB.

Security Analysis

SMB enumeration can provide useful information to be used in the later stages of an attack. The information that may leak from an SMB scan includes the following:

- Domains
- SMB shares
- Accounts
- Hostnames
- Operating system version

Limiting the ability to enumerate anonymously via SMB is regarded as good security.

10. Nessus Vulnerability Assessment

Nessus Essentials was employed to conduct automated vulnerability scans and confirm manual testing results.

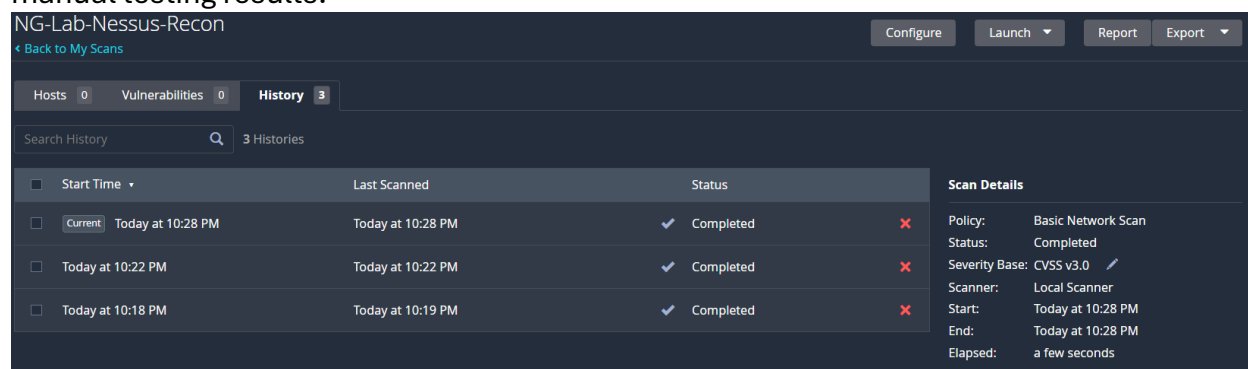


Figure 12: Nessus scan history.

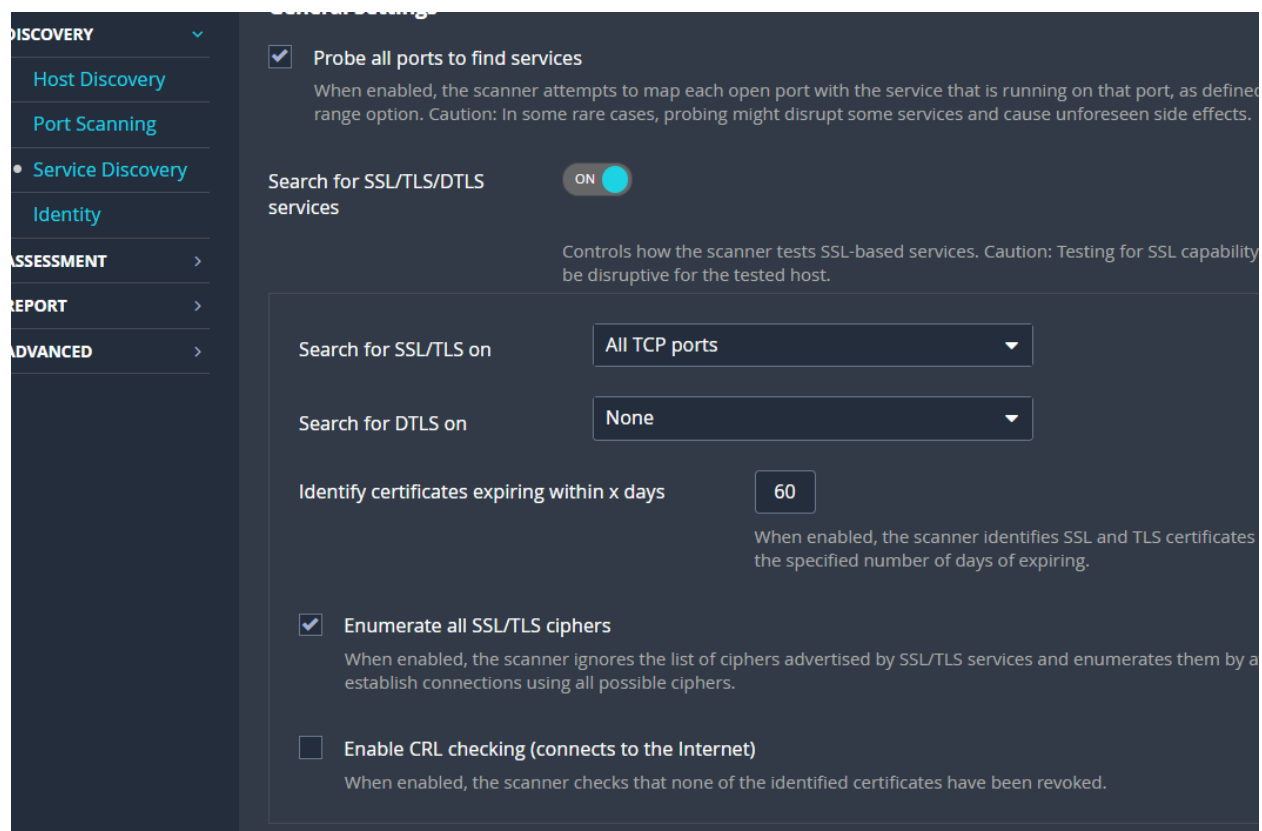


Figure 13: Nessus scan configuration.

Nessus Scans were performed to:

- Port scanning
- Discover running services
- SSL/TLS configuration check
- Vulnerability detection

Nessus scans have successfully confirmed the existence of exposed services and discovered several outdated software versions on the lab environment.

Security Analysis

Automatic scanners such as Nessus increase the awareness about existing system vulnerabilities and allow security analysts to discover known vulnerabilities faster. Nessus helped to validate the discovery of the exposed services and confirmed the presence of insecure configurations.

It is important to combine the automated scanning with the manual testing techniques for the most comprehensive security assessment.

11. Recommendations

Several security recommendations have been suggested:

- Anonymous FTP authentication should be disabled
- Telnet services should be removed or disabled
- All security patches and updates should be applied
- SMB enumeration and anonymous access should be restricted
- Insecure services and open ports should be closed
- Secure HTTP headers should be implemented
- PHPMyAdmin access should be restricted
- Periodic vulnerability assessments should be conducted
- The network segmentation and firewall filtering should be implemented
- Systems should be monitored for any suspicious activity

12. Conclusion

The practical pen test assessment has successfully found several vulnerabilities, insecure configurations, and exposed services of the target systems. The combination of the manual reconnaissance, enumeration, vulnerability validation, and automated scanning has given the full picture of security status of the lab environment.

The Metasploitable and OWASP BWA systems have exposed several outdated and vulnerable services including FTP, Apache, Samba, and PHP web applications. Insecure authentication and information disclosure vulnerabilities have been discovered.

The usage of the Nmap, Metasploit, Nikto, enum4linux, and Nessus tools has shown that the combination of manual and automated testing techniques plays an important role in the modern cybersecurity.

Overall, the practical assessment has highlighted the crucial importance of:

- system configuration security,
- vulnerability management,
- patch management,
- service hardening,
- penetration testing.

References and Appendices

References

- [1] S. C. National Cyber, "Incidents impacting retailers – recommendations from the NCSC," 2025.
- [2] F. Salahdine and N. Kaabouch, "Social Engineering Attacks: A Survey," vol. 11, no. 4, 2019,
- [3] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak and M. K. Khan, "Ransomware: Recent advances, analysis, challenges and future research directions," *Comput.Secur.*, vol. 111, 2021,
- [4] Reuters, "M&S says cyber hackers broke in through third-party contractor," 2025.
- [5] a. T. National Institute of Standards, "Computer Security Incident Handling Guide," 2012.
- [6] Marks & Spencer, "Cyber incident – further update," 2025.
- [7] The Co-operative Group, "Cyber Incident Update," 2025.
- [8] MITRE ATT&CK, "Enterprise Matrix and ATT&CK Technique Entries," 2026.

Appendix A — Timeline Source Notes

The most authoritative dates regarding the M&S intrusion timeline, including initial access, detection, and public disclosure, were derived primarily from official company statements and Reuters reporting rather than early customer-facing service notices, which initially focused more on operational disruption than intrusion chronology. Co-op's timeline regarding data exposure and operational response was primarily based on the organisation's official public statements and NCSC guidance. The decision to analyse the incidents as part of a broader coordinated campaign was supported through similarities in identity-focused intrusion behaviour, ransomware-related operational disruption, and public reporting concerning third-party access abuse and social engineering techniques [1], [4], [6], [7].

Appendix B — OSINT Confidence Notes

The following findings were assessed with high confidence based on official statements and multiple corroborating public sources: operational disruption at M&S, social-engineering-based intrusion activity, third-party involvement, Co-op data exposure, and ransomware-related operational impact. Findings assessed with medium confidence included overlap between the threat actors involved in both incidents and the use of shared identity-focused intrusion methodologies. Findings assessed with lower confidence included the exact cloud identity modifications, lateral movement techniques, and specific exfiltration channels used during the campaign. This confidence assessment reflects the distinction between confirmed public reporting and inferred attacker tradecraft analysis, which is methodologically preferable to treating all TTPs as equally verified [1], [3], [4], [8].