Cybersecurity

Activity File

Activity File: Metasploit Exploitation

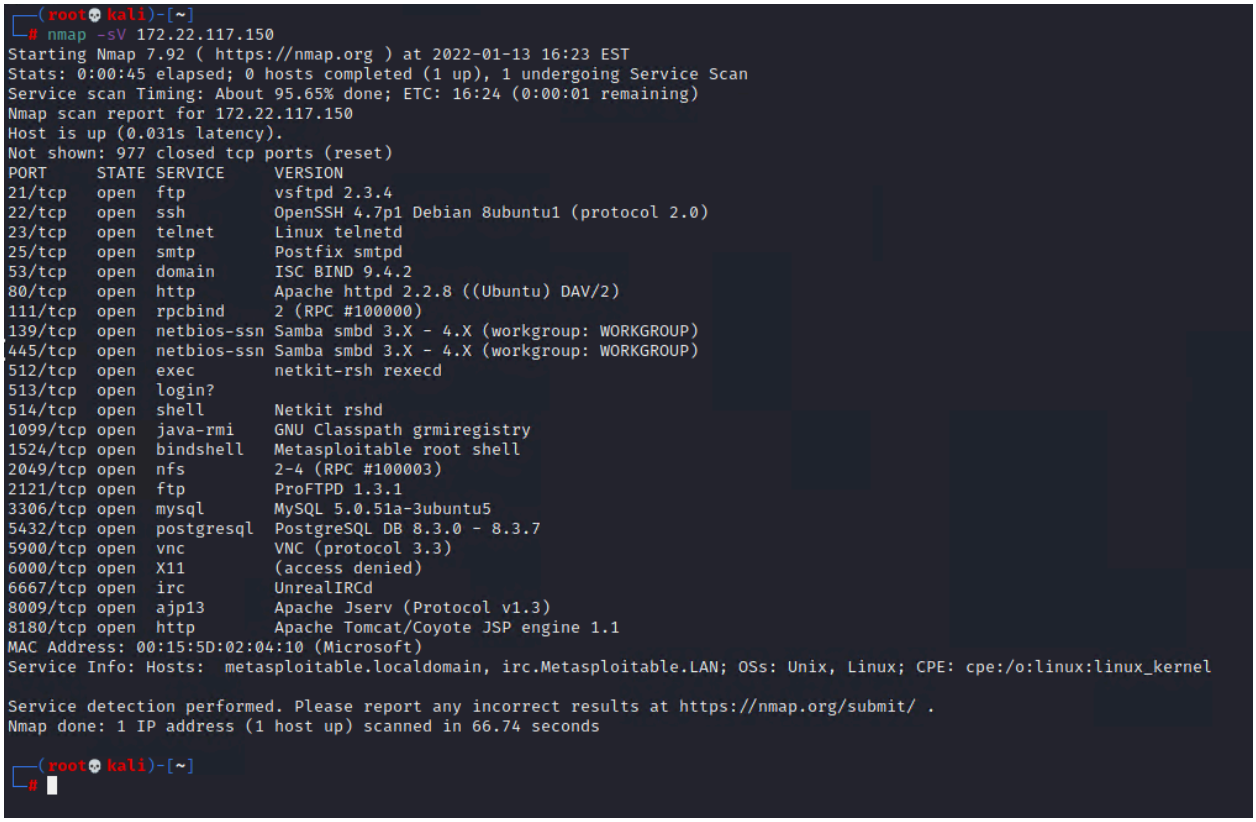
- In this activity, you will continue to play the role of a pen tester conducting an engagement on MegaCorpOne.
- Through our previous Nmap scan, we discovered several exploitable services.
- MegaCorpOne has given you permission to exploit any vulnerable service you find, as long as you document your 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:



- :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

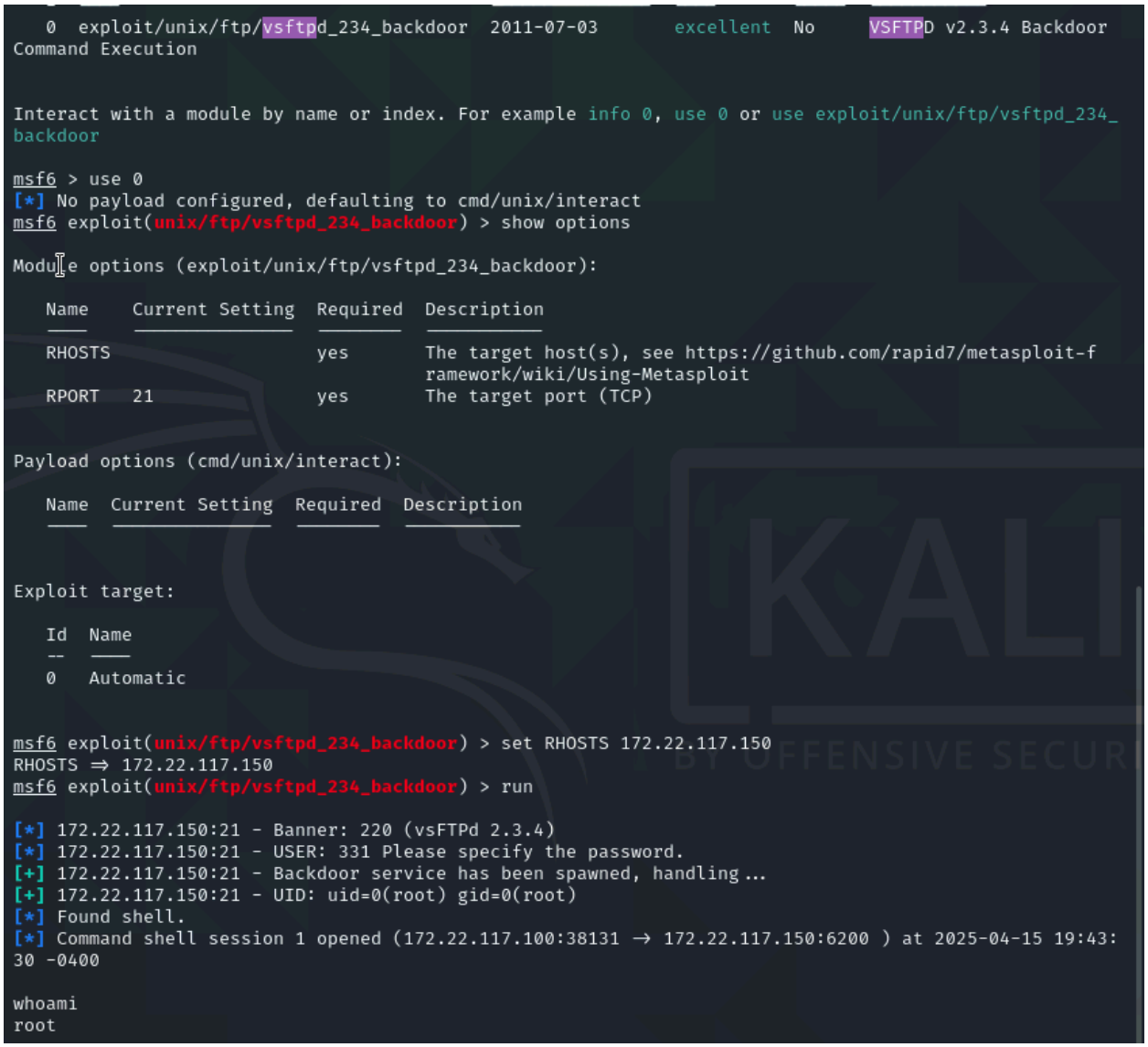
Your task is to use Metasploit to exploit as many services as possible within the time limit.

- 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 `vsftp`, `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**

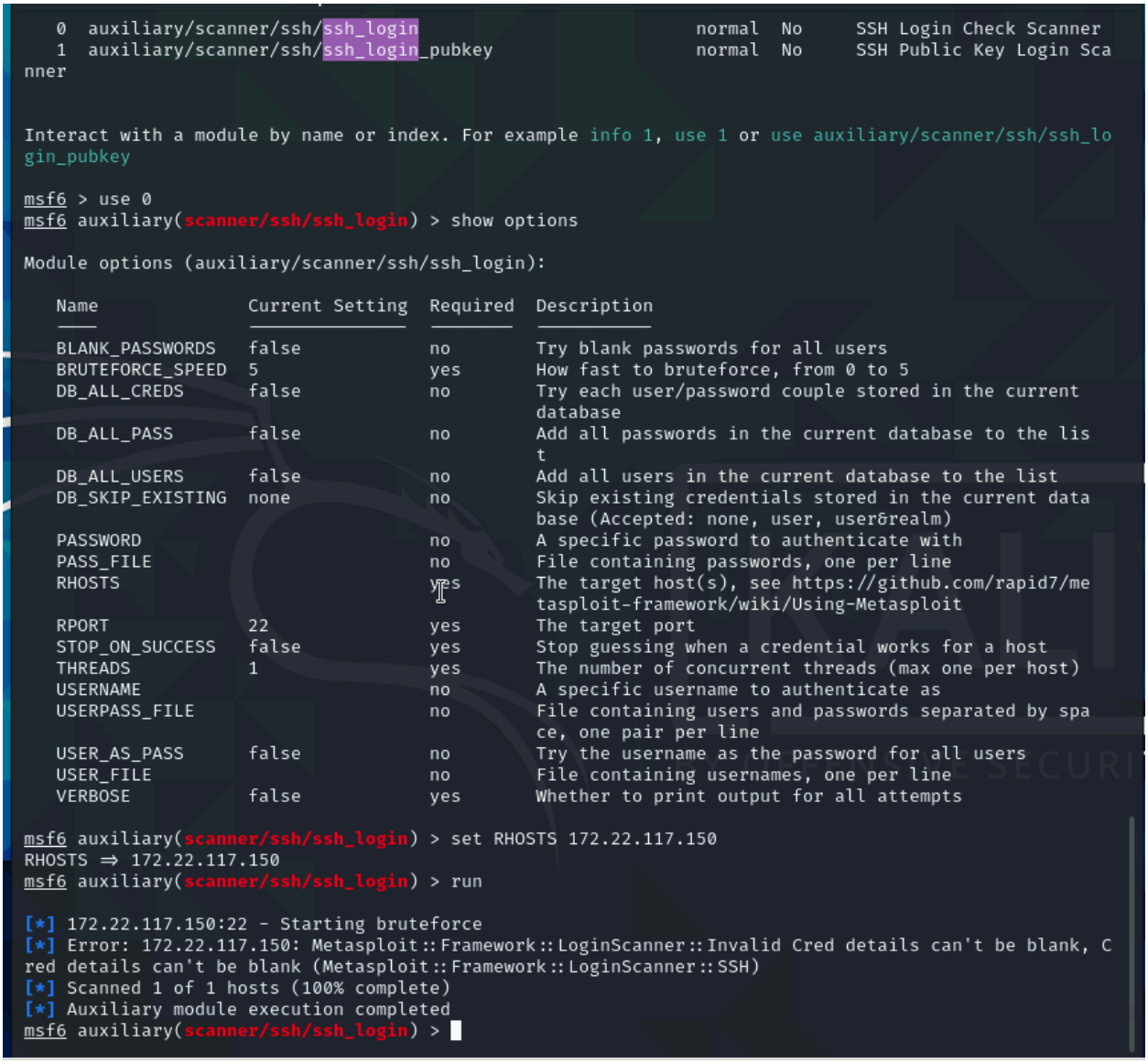
- **Exploit outcome: Success**



- **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                                  yes       The target host(s), see https://github.com/rapi
                                                     d7/metasploit-framework/wiki/Using-Metasploit
   RPORT      25                           yes       The target port (TCP)
   THREADS    1                            yes       The number of concurrent threads (max one per h
                                                     ost)
   UNIXONLY   true                         yes       Skip Microsoft bannered servers when testing un
                                                     ix users
   USER_FILE  /usr/share/metasploit-frame  yes       The file that contains a list of probable users
              work/data/wordlists/unix_us              accounts.
              ers.txt

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 ESMTP Postfix (Ub
untu)
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 ESMTP Postfix (Ub
untu)
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**



- **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**