Information Gathering Using Metasploit

Overview
Metasploit Framework facilitates the tasks of attackers, exploit writers and payload writers. A major advantage of the framework is the modular approach i.e. allowing the combination of any exploit with any payload. Metasploit Framework operates as an open-source project and accepts contributions from the community through GitHub.com pull requests.

Lab Objectives
The objective of this lab is to demonstrate how to identify vulnerabilities and information disclosures using Metasploit Framework. Students will learn how to:

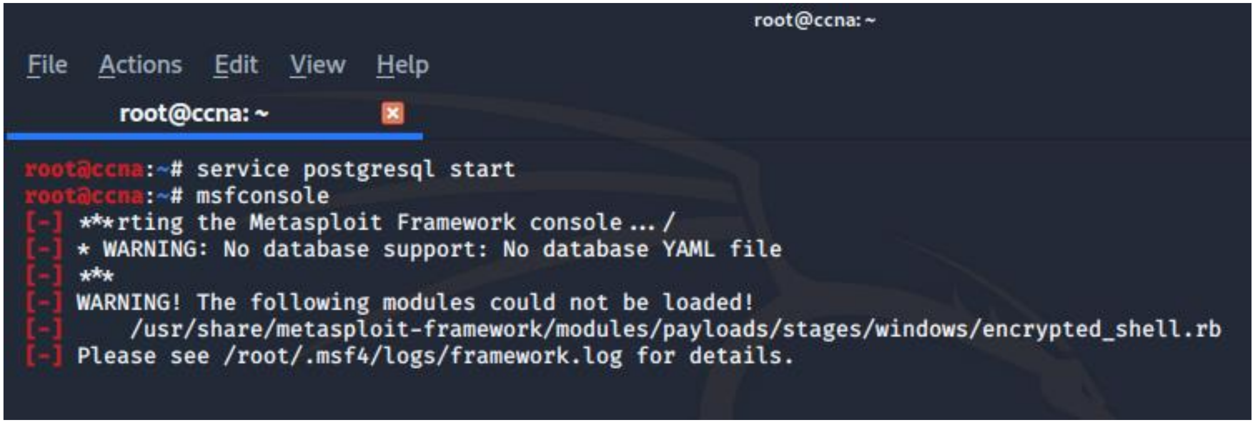
- Extract accurate information about a network using Metasploit Framework.

Lab Scenario
As a professional ethical hacker, you should be able to extract information on the target using an automated tool such as Metasploit. Metasploit can be used to test the vulnerability of computer systems or to break into remote systems. This lab will demonstrate extracting information using Metasploit Framework.

1. The Kali Linux desktop appears, click the Terminal icon in the Favourites bar on the upper-left side

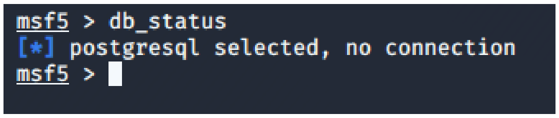
2. In the terminal window, type service postgresql start and press Enter.

3. Type msfconsole and press Enter. Wait for the Metasploit Framework to launch.



```
root@ccna:~# service postgresql start
root@ccna:~# msfconsole
[-] ***rting the Metasploit Framework console.../
[-] * WARNING: No database support: No database YAML file
[-] ***
[-] WARNING! The following modules could not be loaded!
[-]     /usr/share/metasploit-framework/modules/payloads/stages/windows/encrypted_shell.rb
[-] Please see /root/.msf4/logs/framework.log for details.
```

4. In the msf command line, type db_status and press Enter. If you get the postgresql selected, no connection message, then the databse was not initiated.

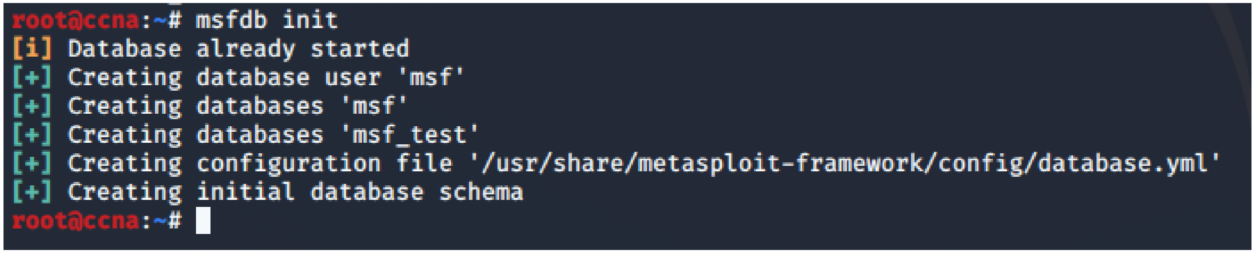


```
msf5 > db_status
[*] postgresql selected, no connection
msf5 > 
```

Note: If you get the postgresql connected to msf message, then skip to Step 10.

5. Exit metasploit by typing exit and press Enter.

6. To initialize the database type msfdb init and press Enter.



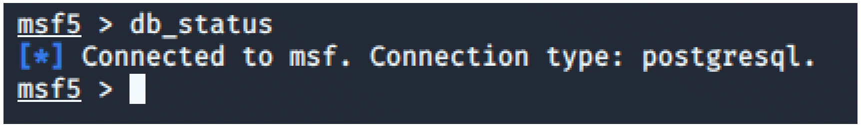
```
root@ccna:~# msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
root@ccna:~# 
```

7. Now restart the postgresql service by typing service postgresql restart and press Enter.

8. Relaunch metasploit framework by typing msfconsole and press Enter. Wait till the metasploit framework starts and gives you the msf command line.

9. Recheck if the database is connect to metasploit by typing db_status and press Enter.

This time you should get the postgresql conncted to msf message.

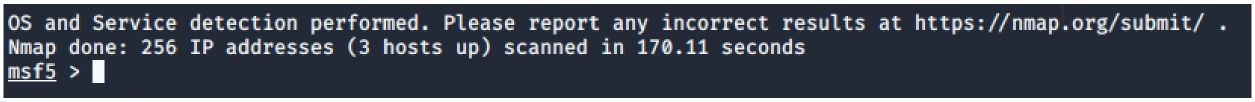


```
msf5 > db_status
[*] Connected to msf. Connection type: postgresql.
msf5 > 
```

10. Type nmap –T4 -A -oX Test 172.16.17.0/24 and press Enter. It takes approximately 5 to 10 minutes for nmap to complete scanning the subnet.

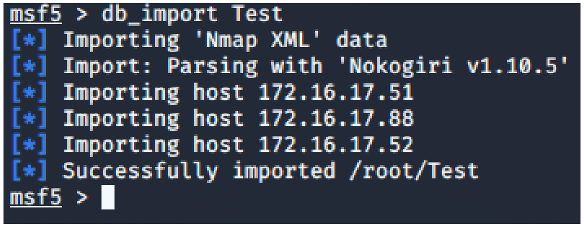
    nmap -Pn -sS -A -oX Test 172.16.17.0/24 – is another option, however it will take more time, why? Use the Man page in Linux to find the explanation of –Pn and –sS options.

On completion you will get a Nmap done message with nmap showing the total number of hosts active in the subnet.



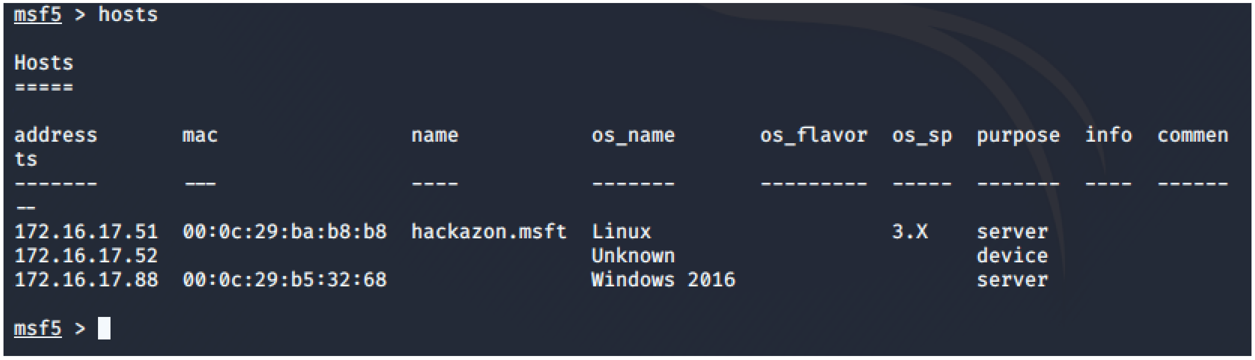
```
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 170.11 seconds
msf5 > 
```

Type db_import Test and press Enter to import the test results.



```
msf5 > db_import Test
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.10.5'
[*] Importing host 172.16.17.51
[*] Importing host 172.16.17.88
[*] Importing host 172.16.17.52
[*] Successfully imported /root/Test
msf5 > 
```

Type **hosts** and press Enter to display the hosts and their details as collected by nmap.



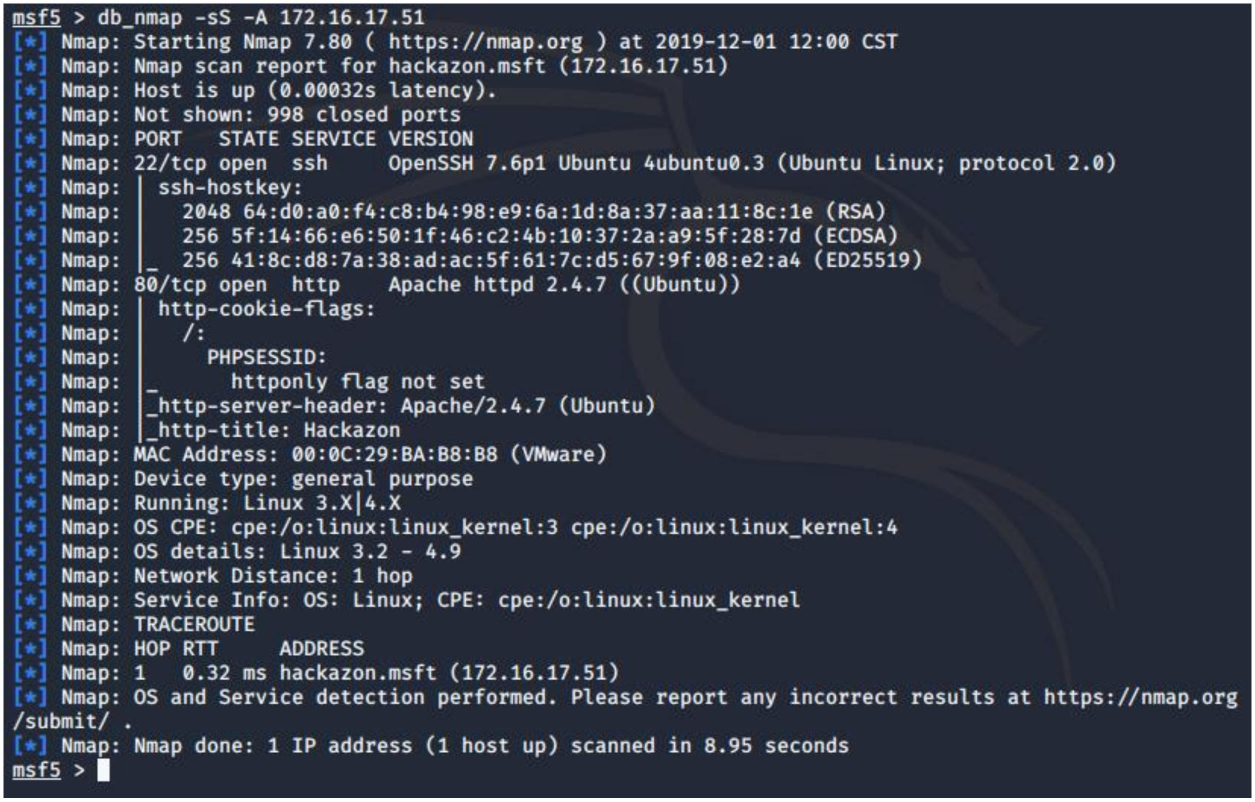
```
msf5 > hosts

Hosts
=====

address       mac                name           os_name        os_flavor  os_sp  purpose  info  commen
ts
-------       ---                ----           -------        ---------  -----  -------  ----  ------
--
172.16.17.51  00:0c:29:ba:b8:b8  hackazon.msft  Linux                     3.X    server
172.16.17.52                                    Unknown                          device
172.16.17.88  00:0c:29:b5:32:68                 Windows 2016                     server

msf5 > █
```

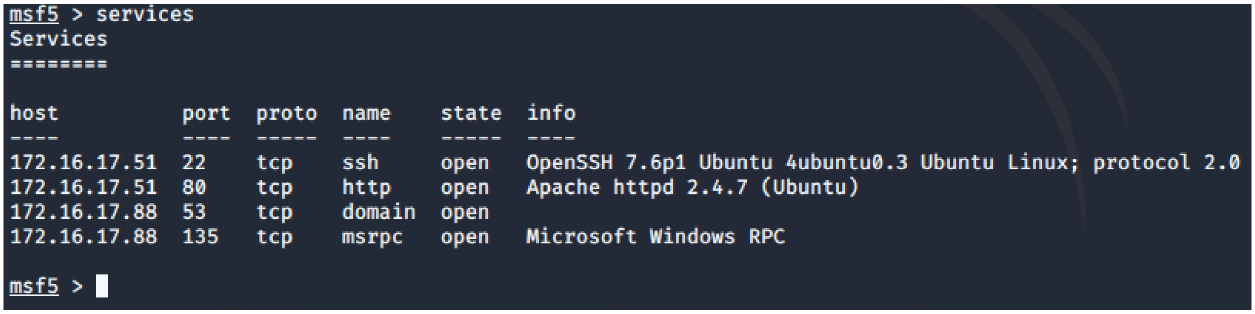
Type db_nmap -sS -A 172.16.17.51 and press Enter.
Nmap scans the Linux machine and gives you the details of the services running in the machine.



```
msf5 > db_nmap -sS -A 172.16.17.51
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-01 12:00 CST
[*] Nmap: Nmap scan report for hackazon.msft (172.16.17.51)
[*] Nmap: Host is up (0.00032s latency).
[*] Nmap: Not shown: 998 closed ports
[*] Nmap: PORT   STATE SERVICE VERSION
[*] Nmap: 22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
[*] Nmap: | ssh-hostkey:
[*] Nmap: |   2048 64:d0:a0:f4:c8:b4:98:e9:6a:1d:8a:37:aa:11:8c:1e (RSA)
[*] Nmap: |   256 5f:14:66:e6:50:1f:46:c2:4b:10:37:2a:a9:5f:28:7d (ECDSA)
[*] Nmap: |_  256 41:8c:d8:7a:38:ad:ac:5f:61:7c:d5:67:9f:08:e2:a4 (ED25519)
[*] Nmap: 80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
[*] Nmap: | http-cookie-flags:
[*] Nmap: |   /:
[*] Nmap: |     PHPSESSID:
[*] Nmap: |_      httponly flag not set
[*] Nmap: |_http-server-header: Apache/2.4.7 (Ubuntu)
[*] Nmap: |_http-title: Hackazon
[*] Nmap: MAC Address: 00:0C:29:BA:B8:B8 (VMware)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 3.X|4.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
[*] Nmap: OS details: Linux 3.2 - 4.9
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT     ADDRESS
[*] Nmap: 1   0.32 ms hackazon.msft (172.16.17.51)
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org
/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 8.95 seconds
msf5 > █
```

This is how you can find services on individual machine.

To get the services information of all the active machines in the subnet type **services** and press Enter.



```
msf5 > services
Services
========

host          port  proto  name    state  info
----          ----  -----  ----    -----  ----
172.16.17.51  22    tcp    ssh     open   OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 Ubuntu Linux; protocol 2.0
172.16.17.51  80    tcp    http    open   Apache httpd 2.4.7 (Ubuntu)
172.16.17.88  53    tcp    domain  open
172.16.17.88  135   tcp    msrpc   open   Microsoft Windows RPC

msf5 > 
```

In this lab you have learned how to extract information about a network using Metasploit Framework.