VNC tunneling over SSH

posted in PENETRATION TESTING on OCTOBER 2, 2017 by RAJ CHANDEL SHARE

In previous article we had perform **VNC penetration testing** and today you will VNC tunneling to connect remote machine with VNC server when they both belongs different network interface.

Basically tunneling is process which allows data sharing or communication between two different networks privately. Tunneling is normally perform through encapsulating the private network data and protocol information inside the public network broadcast units so that the private network protocol information visible to the public network as data.

Let's Begin!!

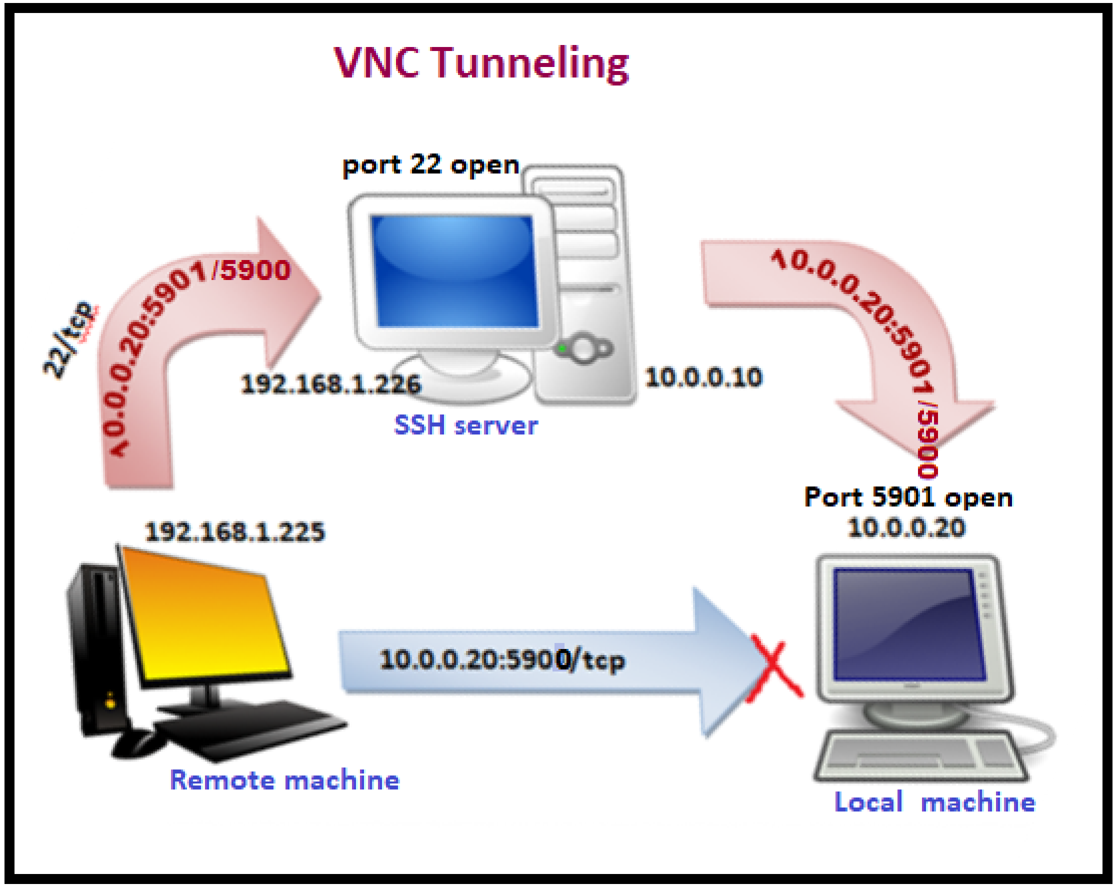
Requiremet:

Server machine(ubuntu): Two network interface with activted SSH service

Local machine (ubuntu): activated VNC service

Remote machine(window): with install tight VNC viewer

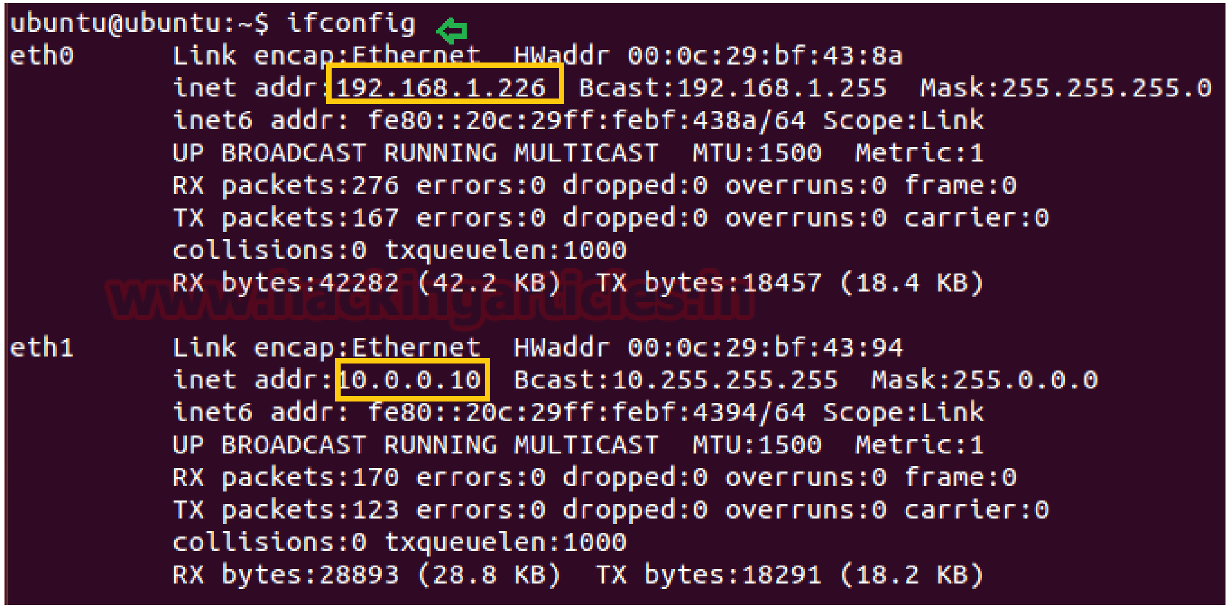
In following image we are trying to explain VNC tunneling process where a remote PC of IP 192.168.1.225 is trying to connect to 10.0.0.20 which is on INTRANET of another network. To establish connection with **local machine**, remote PC will create VNC tunnel which will connect with the **local** system via **SSH server machine**.



Given image below is describing the network configuration for **server machine (SSH)** where it is showing two IP 192.168.1.226 and another 10.0.0.10 as explain above.

Categories

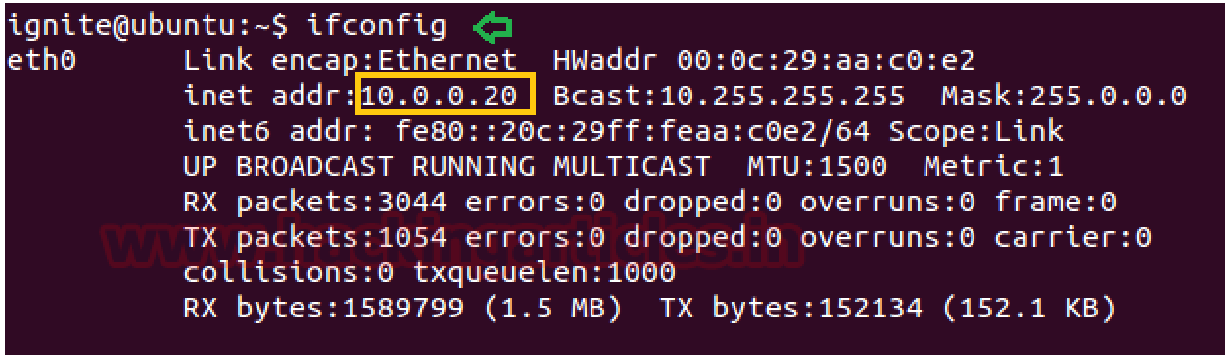
- BackTrack 5 Tutorials
- Best of Hacking
- Browser Hacking
- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Domain Hacking
- Email Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others
- Penetration Testing
- Social Engineering Toolkit
- Trojans & Backdoors
- Website Hacking
- Window Password Hacking
- Windows Hacking Tricks
- Wireless Hacking
- Youtube Hacking



```
ubuntu@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:bf:43:8a
          inet addr:192.168.1.226  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:febf:438a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:276 errors:0 dropped:0 overruns:0 frame:0
          TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:42282 (42.2 KB)  TX bytes:18457 (18.4 KB)

eth1      Link encap:Ethernet  HWaddr 00:0c:29:bf:43:94
          inet addr:10.0.0.10  Bcast:10.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::20c:29ff:febf:4394/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:170 errors:0 dropped:0 overruns:0 frame:0
          TX packets:123 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:28893 (28.8 KB)  TX bytes:18291 (18.2 KB)
```

Another image given below is describing network configuration for **local machine** which is showing IP 10.0.0.20



```
ignite@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:aa:c0:e2
          inet addr:10.0.0.20  Bcast:10.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::20c:29ff:feaa:c0e2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3044 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1054 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1589799 (1.5 MB)  TX bytes:152134 (152.1 KB)
```

Checking activated VNC service using following command:

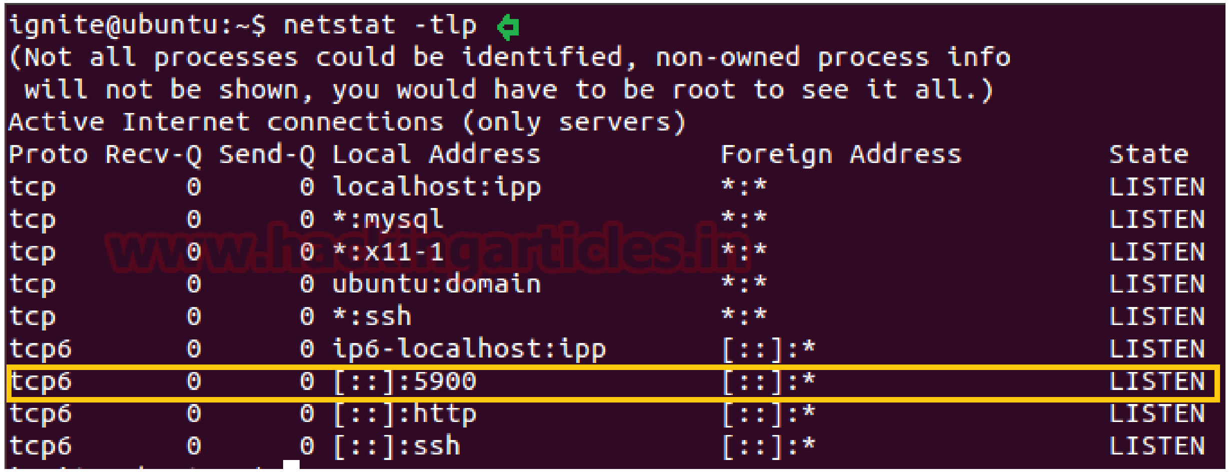
netstat -tlp

Hence from given image you can see the highlighted text is showing 5900 is enabled in local machine.

Articles

Select Month

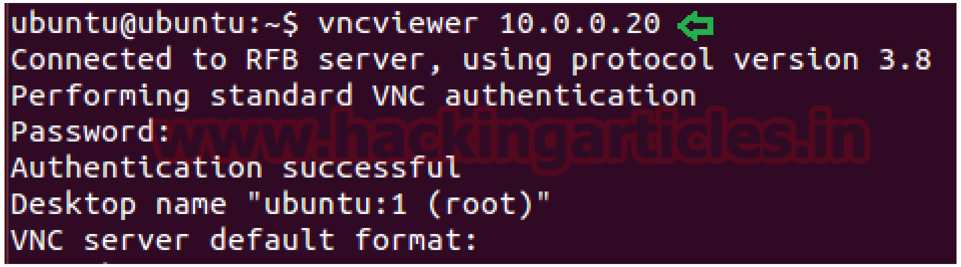
Facebook Page



```
ignite@ubuntu:~$ netstat -tlp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:ipp           *:*                     LISTEN
tcp        0      0 *:mysql                 *:*                     LISTEN
tcp        0      0 *:x11-1                 *:*                     LISTEN
tcp        0      0 ubuntu:domain           *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
tcp6       0      0 [::]:5900               [::]:*                  LISTEN
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
```

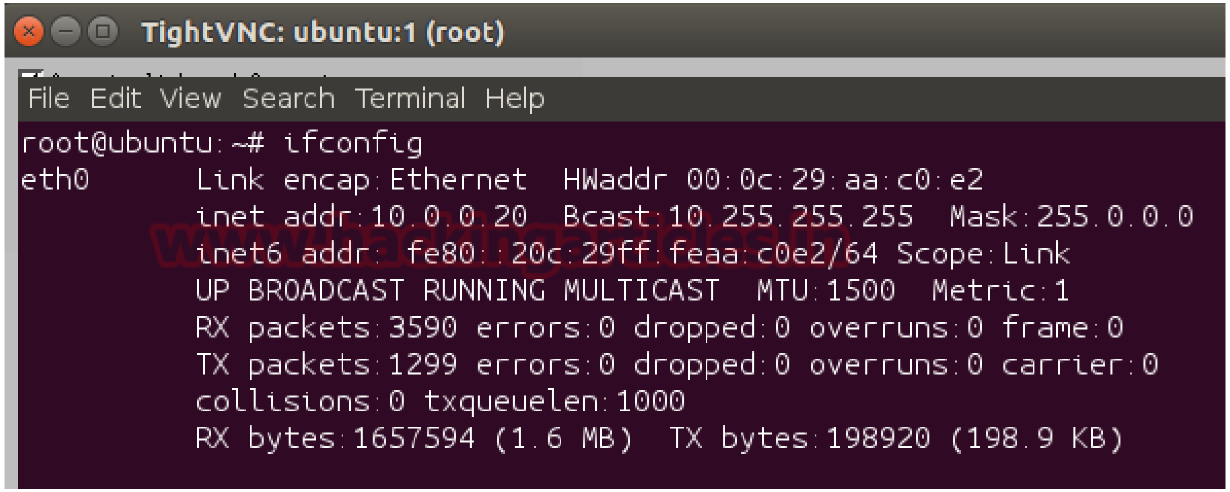
Open the terminal and type using following command to connecting to VNC machine (IP: 10.0.0.20) through server machine (IP: 10.0.0.10).

vncviewer 10.0.0.20



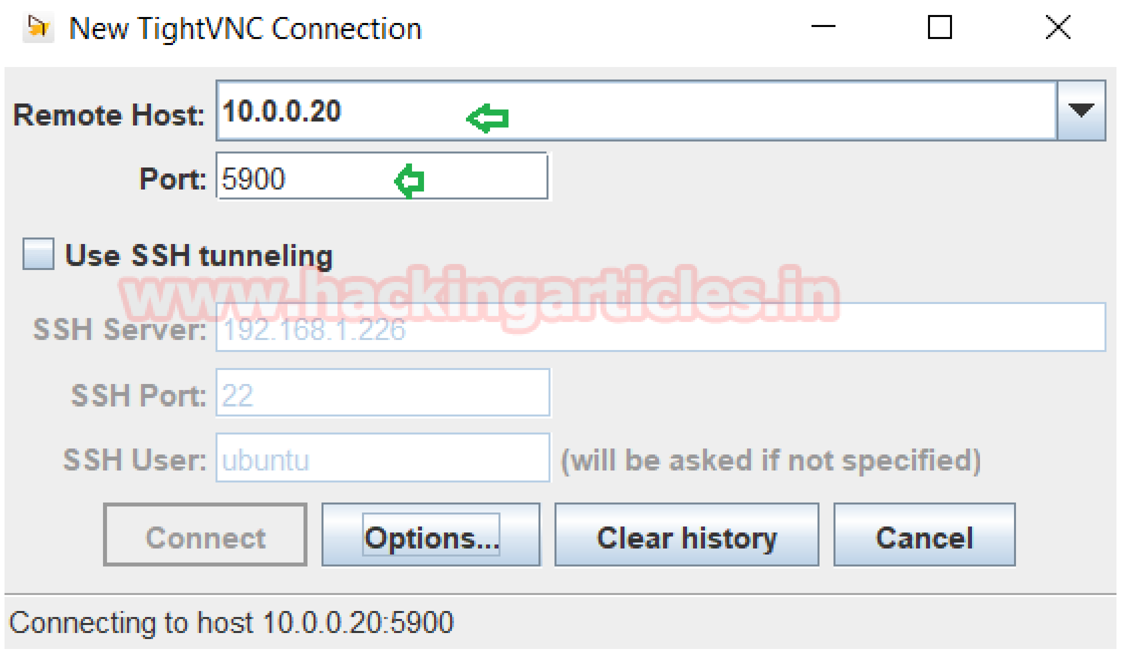
```
ubuntu@ubuntu:~$ vncviewer 10.0.0.20
Connected to RFB server, using protocol version 3.8
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "ubuntu:1 (root)"
VNC server default format:
```

Great!! Local machine successfully connected


TightVNC: ubuntu:1 (root)
File Edit View Search Terminal Help

```
root@ubuntu:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:aa:c0:e2
          inet addr:10.0.0.20  Bcast:10.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::20c:29ff:feaa:c0e2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3590 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1299 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1657594 (1.6 MB)  TX bytes:198920 (198.9 KB)
```

Similarly Using tight vnc viewer remote machine (192.168.1.225) now trying to connect local machine (IP: 10.0.0.10) as shown in given image



Remote Host: 10.0.0.20

Port: 5900

□ Use SSH tunneling

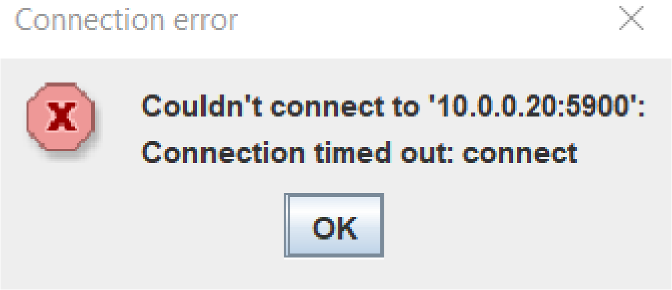
SSH Server: 192.168.1.226

SSH Port: 22

SSH User: ubuntu (will be asked if not specified)

Connecting to host 10.0.0.20:5900

Since they belong to different network therefore he receives network error.

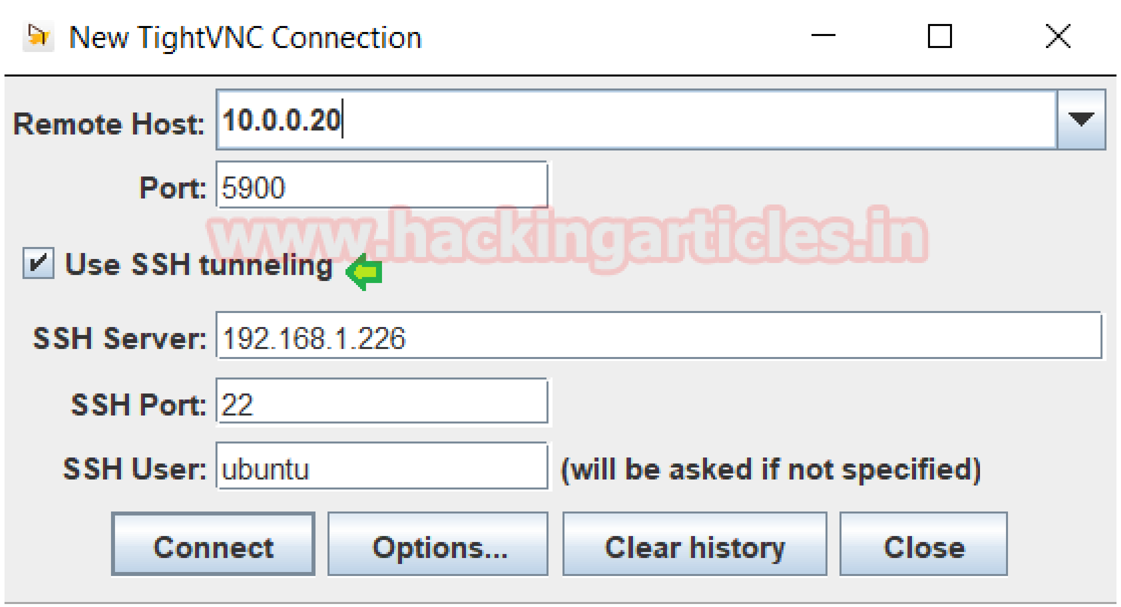


Connection error

Couldn't connect to '10.0.0.20:5900': Connection timed out: connect

Follow given below step to connect remote machine to local machine via ssh server.

- Open tightVNC connection and enter the local machine IP: **0.0.20** with port **5900.**
- **Enable** SSH tunneling
- Now enter ssh server IP: **168.1.226** with port **22** and ssh server username: **ubutnu.**



New TightVNC Connection

Remote Host: 10.0.0.20

Port: 5900

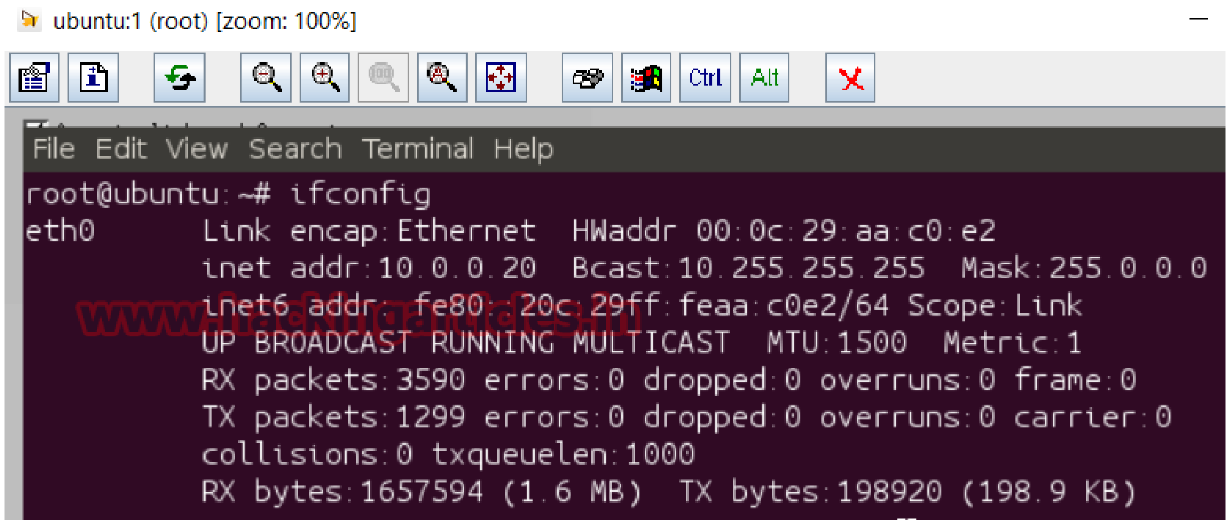
☑ Use SSH tunneling

SSH Server: 192.168.1.226

SSH Port: 22

SSH User: ubuntu (will be asked if not specified)

Congrats!!! Remote machine had successfully connected with local machine through VNC.


ubuntu:1 (root) [zoom: 100%]
Ctrl
Alt
File Edit View Search Terminal Help

```
root@ubuntu:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:aa:c0:e2
          inet addr:10.0.0.20  Bcast:10.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::20c:29ff:feaa:c0e2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3590 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1299 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1657594 (1.6 MB)  TX bytes:198920 (198.9 KB)
```

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 PENETRATION TESTING (PORT 5901)

NEXT POST

VNC PIVOTING THROUGH METERPRETER →

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.