SEC285 Final Project

Introduction

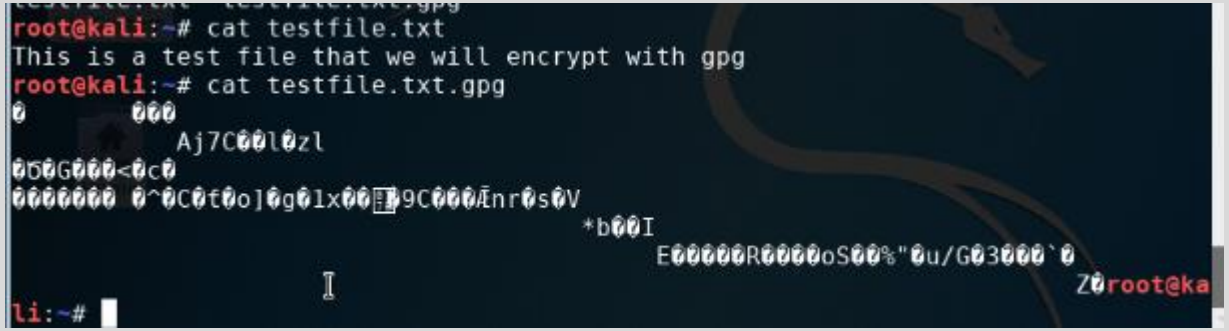
This project includes File encryption, decryption, Nmap scan, my own BYOD policy and a few other things regarding system securities.

Career skills

- File encryption and encryption
- Tool experience Wireshark, Nmap, and nessus
- Working with colleagues and superiors

File Encryption

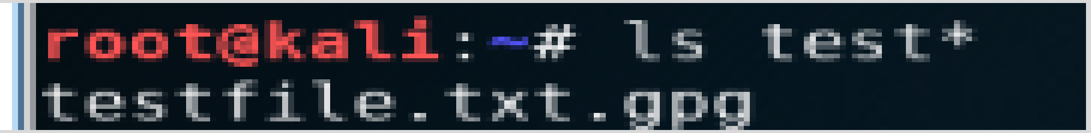
File encryption is way of encoding files, including the sensitive data, in order to send them securely



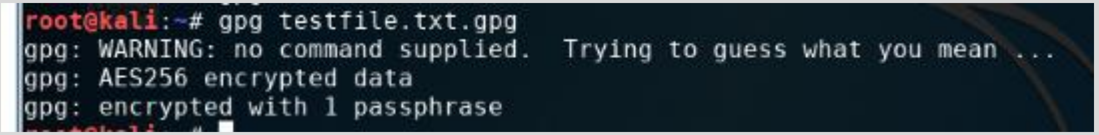
```
testfile.txt  testfile.txt.gpg
root@kali:~# cat testfile.txt
This is a test file that we will encrypt with gpg
root@kali:~# cat testfile.txt.gpg
�       ���
           Aj7C��l�zl
�5�G���<�c�
������� �^�C�t�o]�g�1x��▯9C���Ānr�s�V
                                        *b��I
                                             E�����R����oS��%"�u/G�3���`�
                                                                          Z�root@ka
li:~# 
```

File Decryption

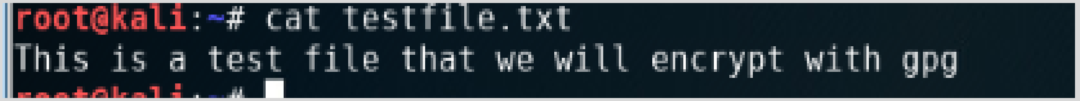
The conversion of encrypted data into its original form is



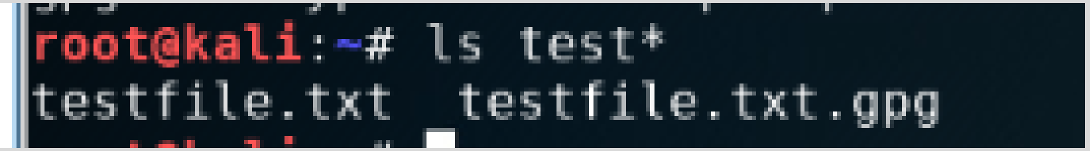
```
root@kali:~# ls test*
testfile.txt.gpg
```



```
root@kali:~# gpg testfile.txt.gpg
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
```



```
root@kali:~# cat testfile.txt
This is a test file that we will encrypt with gpg
```



```
root@kali:~# ls test*
testfile.txt  testfile.txt.gpg
```

Question

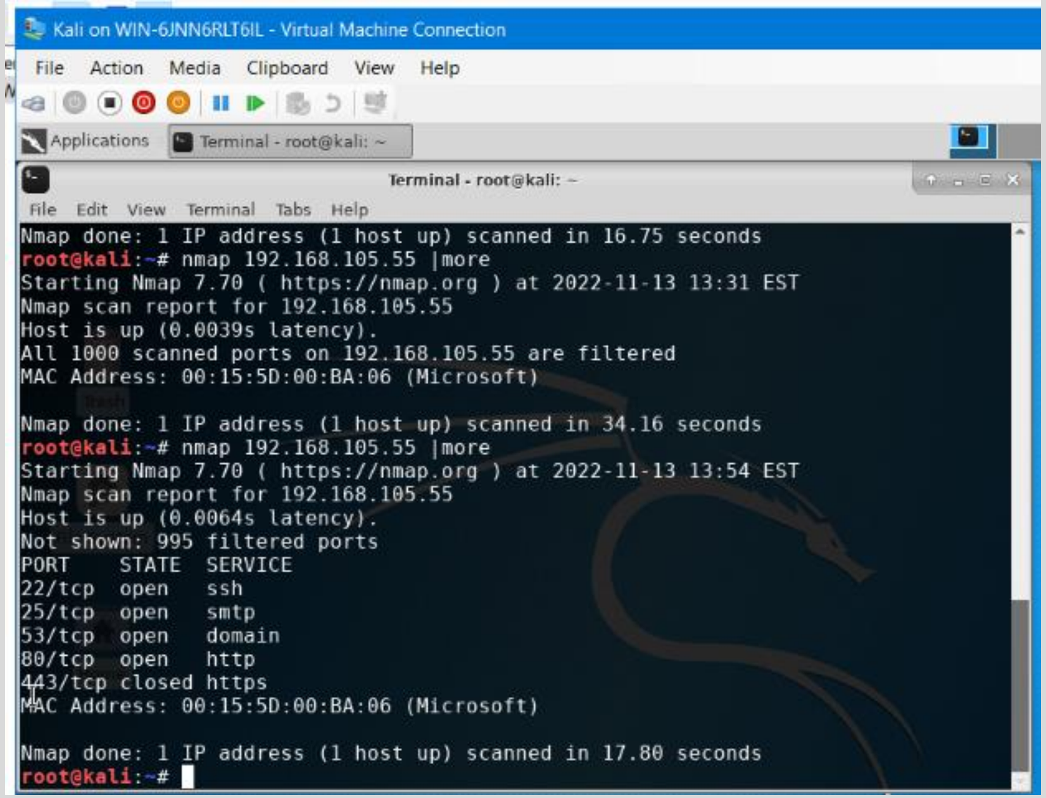
What effect does the sudo iptables --policy INPUT DROP command have on the access to computing resources?

Answer here: It drops a rule regarding incoming traffic the result was I had 0 open ports and everything was filtered

References:
Project video

Nmap Scan

Stands for Network Mapper, is an open source tool that lets you perform scans on local and remote networks.


Kali on WIN-6JNN6RLT6IL - Virtual Machine Connection
File Action Media Clipboard View Help
Applications
Terminal - root@kali: ~
Terminal - root@kali: ~
File Edit View Terminal Tabs Help

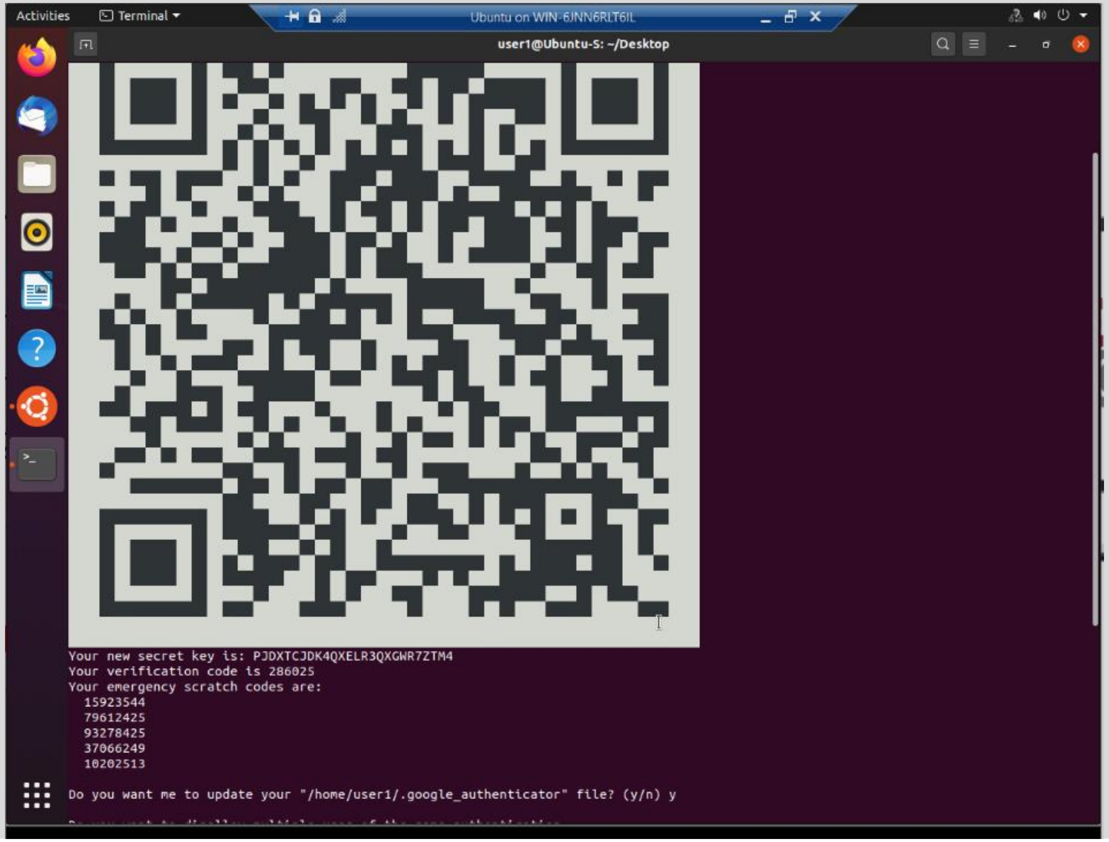
```
Nmap done: 1 IP address (1 host up) scanned in 16.75 seconds
root@kali:~# nmap 192.168.105.55 |more
Starting Nmap 7.70 ( https://nmap.org ) at 2022-11-13 13:31 EST
Nmap scan report for 192.168.105.55
Host is up (0.0039s latency).
All 1000 scanned ports on 192.168.105.55 are filtered
MAC Address: 00:15:5D:00:BA:06 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 34.16 seconds
root@kali:~# nmap 192.168.105.55 |more
Starting Nmap 7.70 ( https://nmap.org ) at 2022-11-13 13:54 EST
Nmap scan report for 192.168.105.55
Host is up (0.0064s latency).
Not shown: 995 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
25/tcp  open   smtp
53/tcp  open   domain
80/tcp  open   http
443/tcp closed https
MAC Address: 00:15:5D:00:BA:06 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 17.80 seconds
root@kali:~#
```

Common-auth Configuration File

The purpose of these files are to provide common interface for all applications and service daemons calling into the PAM library

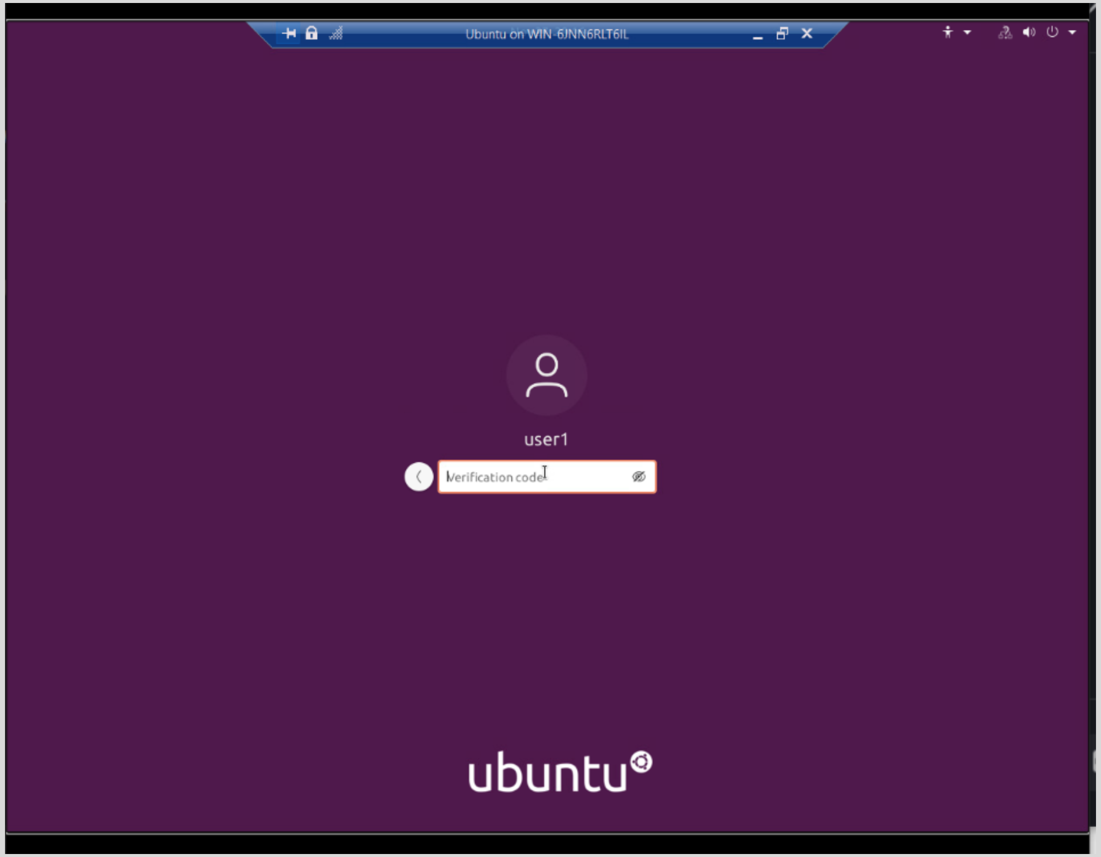


```
Your new secret key is: PJDXTCJDK4QXELR3QXGWR7ZTM4
Your verification code is 286025
Your emergency scratch codes are:
  15923544
  79612425
  93278425
  37066249
  10202513

Do you want me to update your "/home/user1/.google_authenticator" file? (y/n) y
```

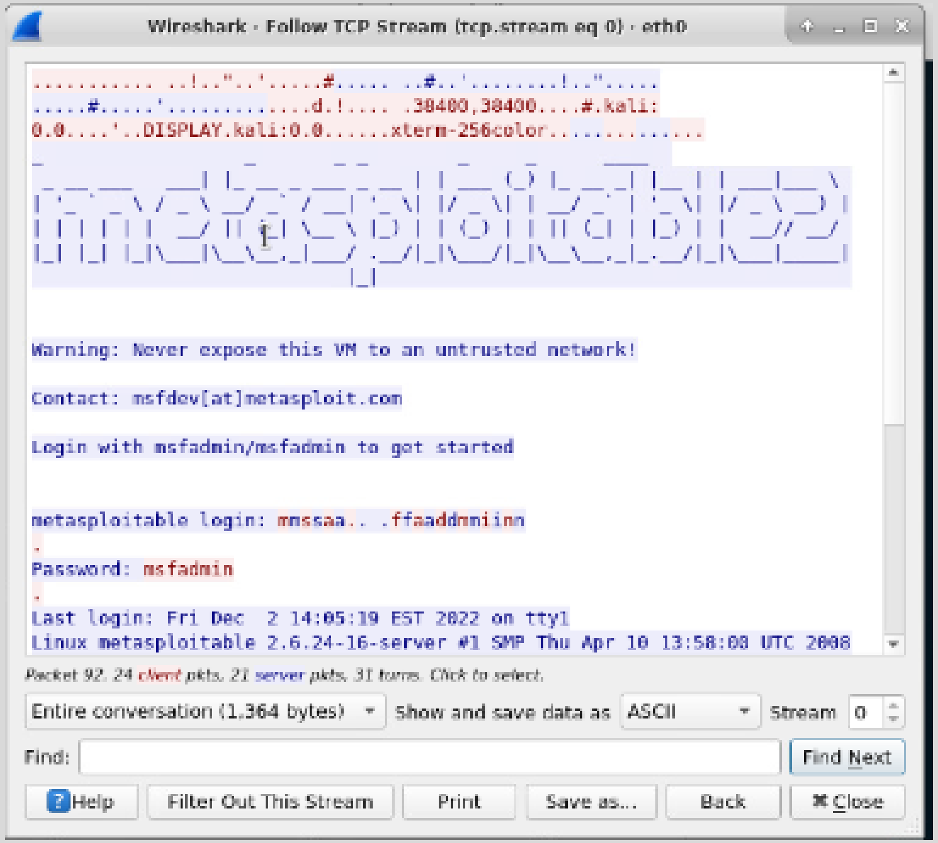
MFA Logon Screen

Multi-factor Authentication method requires the user to provide two or more authentication.



Wireshark

Is an open source tool for profiling network traffic and analyzing packets



```
........... ..!..".."......#..... ..#..'........!.."....
.....#.....'.............d.!.... .38400,38400....#.kali:
0.0....'..DISPLAY.kali:0.0......xterm-256color.............
_                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: mmssaa.. .ffaaddmmiinn
.
Password: msfadmin
.
Last login: Fri Dec  2 14:05:19 EST 2022 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008
```

Packet 92. 24 client pkts, 21 server pkts, 31 turns. Click to select.

Entire conversation (1,364 bytes) · Show and save data as: ASCII · Stream: 0

Overview:
According to a study about 73% of workers are using a laptop, tablet, smartphone, or a combination of these. With the vast majority of a company using these devices so do cyber threats like, social engineering, spyware, lost or stolen mobile devices and many more.

- 2. Purpose:
- IT security policy is to protect confidentiality and availability of data. Devices can bring an unnecessary threat to the network, also devices without security measures such as Antivirus and firewall can be used to gain access to the confidential information from company’s servers. With the BYOD policy we can reduce the attack vector on the organization’s computing resources.

3. Scope:
Employees may use their own electronic devices if they met this criteria. Only certain employees may use their devices, devices must meet security requirements, personal electronic devices include tablets, smartphones, and laptops. Devices will be allowed anytime unless supervisor says otherwise. All activity is allowed as long as it is work appropriate and no pictures or recording of any kind.

- 4. Policy:
- ALL BYOD devices are subject to security assessments prior to the corporation’s network. Devices that are compliant are as such, must have antivirus, mobile device management software installed, windows 10 and 8 installed and everything MUST be up to date with the most recent patches. Noncompliance devices are required to follow remediation which will be done by management.

- 5. Policy Compliance:
- If employees do not follow the security policy disciplinary action will take place, possible termination pending on the infraction.

- 6. Related Standards, Policies, and Processes:
- HIPAA regulations allow healthcare organizations to create BYOD polices to direct and control the use of personal devices to store patient information.

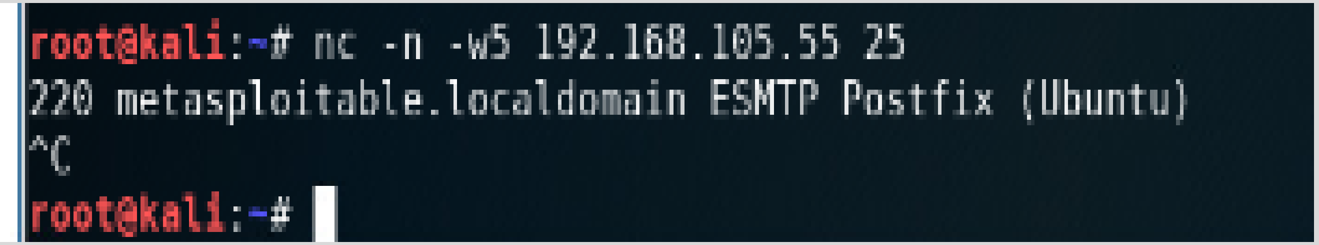
- 7. Definitions and Terms:
- BYOD is bring your own device. mobile devices such as smartphones, tablets, etc. CIA is a certification offered to accountants who conduct internal audits.

8. Revision History:

Date of change	Responsible	Summary of change
August 2019	SANS policy team	Updated and converted to new format
November 2022	Brady Sisk	Updated BYOD policy

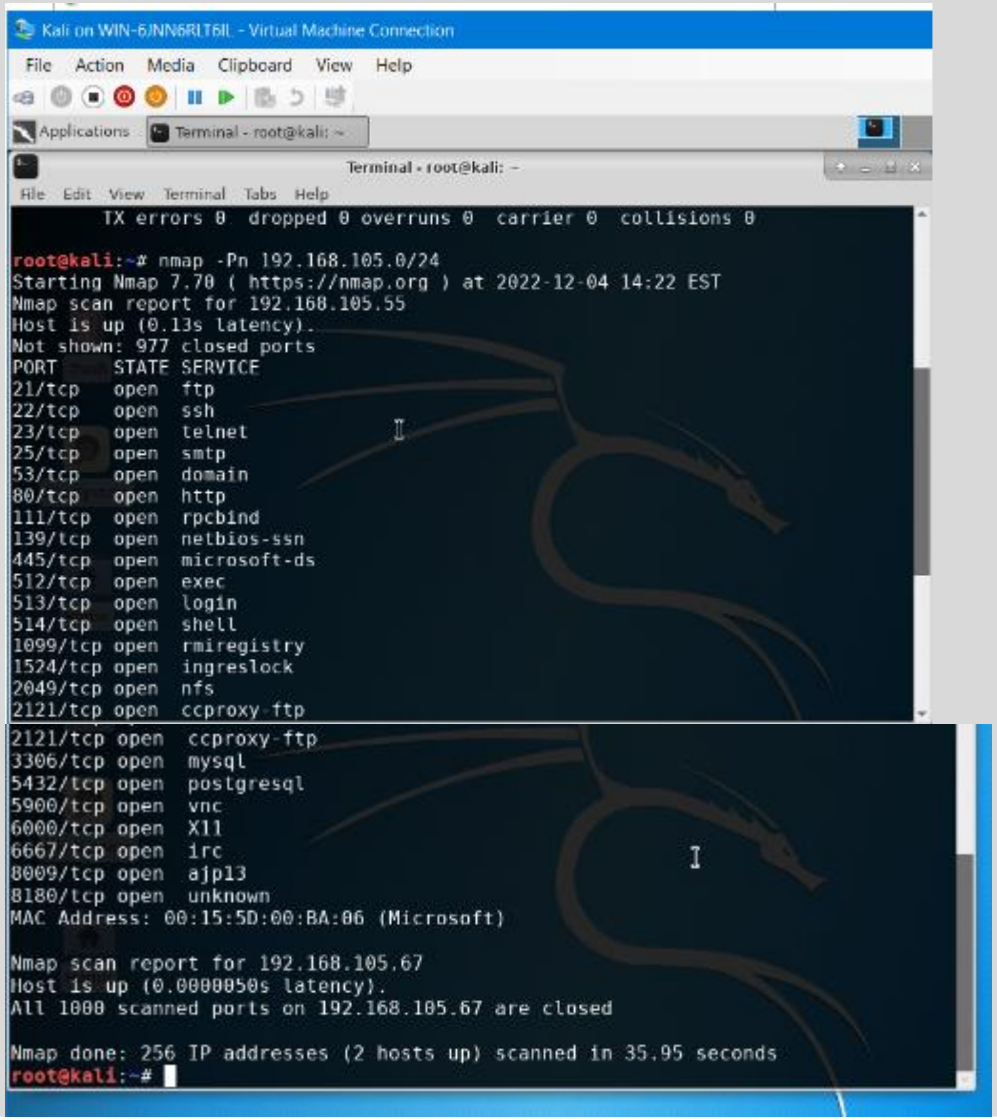
Netcat

Is a utility that uses TCP and UDP connections to read and write in a network.



```
root@kali:~# nc -n -w5 192.168.105.55 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
^C
root@kali:~# 
```

Nmap



```
          TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# nmap -Pn 192.168.105.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2022-12-04 14:22 EST
Nmap scan report for 192.168.105.55
Host is up (0.13s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
```

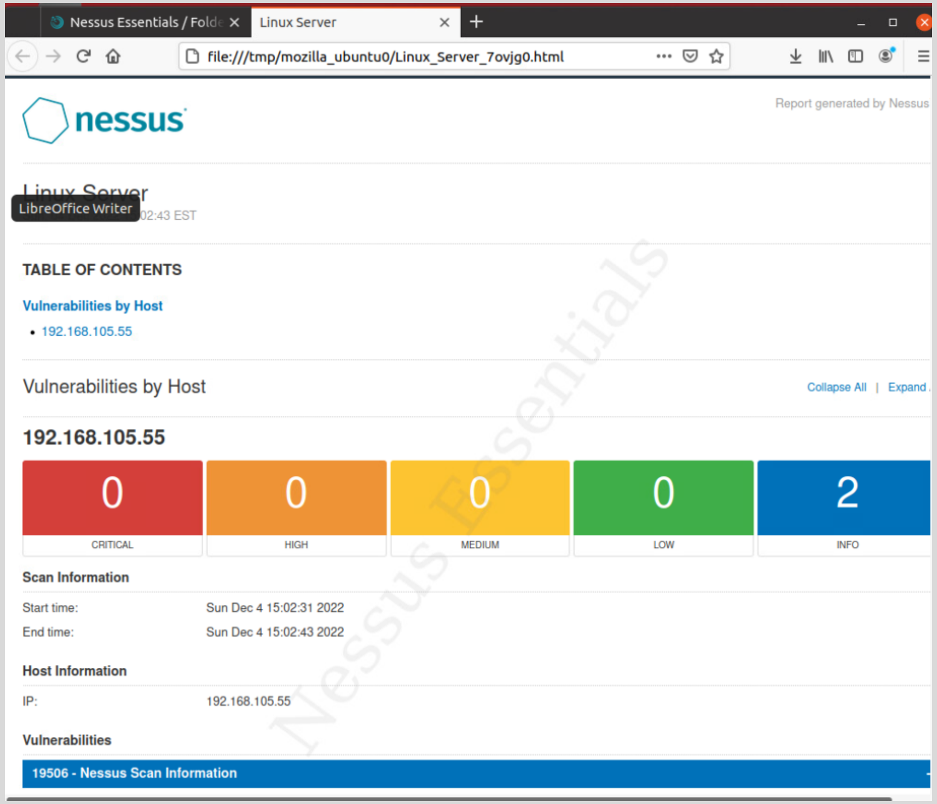
```
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:15:5D:00:BA:06 (Microsoft)

Nmap scan report for 192.168.105.67
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.105.67 are closed

Nmap done: 256 IP addresses (2 hosts up) scanned in 35.95 seconds
root@kali:~# 
```

Nessus

Is an open source network vulnerability scanner that uses the common vulnerabilities and exposures architecture for easy cross linking between compliant security tools.


Nessus Essentials / Folde
Linux Server
file:///tmp/mozilla_ubuntu0/Linux_Server_7ovjg0.html
nessus
Report generated by Nessus
LibreOffice Writer
Nessus Essentials

Linux Server

02:43 EST

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.105.55

Vulnerabilities by Host

Collapse All | Expand

192.168.105.55

0	0	0	0	2
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Sun Dec 4 15:02:31 2022
End time:	Sun Dec 4 15:02:43 2022

Host Information

IP:	192.168.105.55

Vulnerabilities

19506 - Nessus Scan Information

Challenges

- Figuring out work arounds to bad and outdated instructions
- Working with limited time

conclusion

- This project will me my future endeavors into this industry
- This was a sample of the vast industry that is system security

References

https://csrc.nist.gov/glossary?index=M

Past projects

Knowledge gained from course