

# Fundamentals of Information System Security

❖ SEC285 Final Course  
Project

❖ April 2025

❖ Jonathan Waugh

❖ Professor Jacob Mack

# Introduction

- File Encryption/Decryption
- NMAP Scan
- BYOD Security Policy
- Common-auth Configuration File
- MFA Logon Screen
- Nmap
- NetCat
- Wireshark
- Nessus

# SEC285

## Module 2

Asymmetric Key Encryption

# File Encryption

```
Terminal - root@kali: ~  
File Edit View Terminal Tabs Help  
9B3688737E5DD2B3C18ACB8C48A7365CED6B5C90  
uid [ultimate] Jonathan Waugh <jwaugh4@my.devry.edu>  
ssb rsa3072 2025-03-15 [E] [expires: 2027-03-15]  
  
root@kali:~# gpg --list-keys  
/root/.gnupg/pubring.kbx  
-----  
pub rsa3072 2025-03-15 [SC] [expires: 2027-03-15]  
9B3688737E5DD2B3C18ACB8C48A7365CED6B5C90  
uid [ultimate] Jonathan Waugh <jwaugh4@my.devry.edu>  
sub rsa3072 2025-03-15 [E] [expires: 2027-03-15]  
  
root@kali:~# nano testfile.txt  
root@kali:~# cat testfile.txt  
This is a test file that we will encrypt with gpg.  
root@kali:~# gpg -c testfile.txt  
root@kali:~# ls test*  
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  
{0U000ie00mb00e||00~0_00?0Y-0000t000,^'00.0:m-0%0a0yZ_#Tx000000 c0S[0B00  
000  
0]0E000EjAK6@xkn 0000k000zroot@kali:~#
```

# File Decryption

```
Terminal - root@kali: ~
File Edit View Terminal Tabs Help
shred: testfile.txt: renamed to 000000000000
shred: 000000000000: renamed to 000000000000
shred: 000000000000: renamed to 000000000000
shred: 000000000000: renamed to 000000000000
shred: 0000000000: renamed to 0000000000
shred: 000000000: renamed to 00000000
shred: 00000000: renamed to 0000000
shred: 0000000: renamed to 000000
shred: 000000: renamed to 00000
shred: 00000: renamed to 0000
shred: 0000: renamed to 000
shred: 000: renamed to 00
shred: 00: renamed to 0
shred: testfile.txt: removed
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:~# ls test*
testfile.txt  testfile.txt.gpg
root@kali:~# cat testfile.txt
This is a test file that we will encrypt with gpg.
root@kali:~#
```

# SEC285

## Module 3

### Stateful Firewall

# Question

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

Answer here:

drops all incoming connections to the Linux Server VM

References:

Project Video

# Nmap Scan

```
Terminal - root@kali: ~
File Edit View Terminal Tabs Help
root@kali:~# nmap 192.168.105.55 | more
Starting Nmap 7.70 ( https://nmap.org ) at 2025-03-22 16:19 EDT
Nmap scan report for 192.168.105.55
Host is up (0.0028s 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 17.29 seconds
root@kali:~#
```



# SEC285

## Module 4

Bring Your Own Device (BYOD)  
Security Policy

## 1. Overview:

Tablets, cellphones, and laptops have become indispensable tools into today's enterprises. It has revolutionized productivity, collaboration, and communication. Tablets are widely used for things like presentations, meetings, and mobile workstations. While cellphones and laptops became essential parts of communication and productivity. Also allowing for remote work during and after a major pandemic. There are associated threats such as data breaches due to lost or stolen devices, malware and ransomware, and open wi-fi vulnerabilities.

## 2. Purpose:

Timely discovery of vulnerabilities within BYOD environments majorly reduce the attack vector on a company's computing resources by identifying and addressing insecure devices or outdated software early and eliminating potential entry points for attacks before they are exploited. This minimizes the risk of malware, phishing, and unauthorized access, making for better protection of data. Implementing regular vulnerability assessments strengthen security. Making for swift risk remediation and improving network resilience. This safeguards resources while having the flexibility of BYOD practices.

### 3. Scope:

The BYOD policy would apply to all employees, contractors, and departments using personal devices at and for work. Approved devices would be cellphones, tablets, and laptops that are fully updated and have antivirus software installed. All devices need to be approved by IT and could access the network in designated segments only during work hours. While working there is no personal activities allowed. IT oversees all permissions in order to reduce risks and keep security

### 4. Policy:

All devices would undergo assessments before they could access ABC Corporation's network. They must have an approved operating system with up to date security patches, antivirus software, and have an active firewall. Any noncompliant device will undergo IT-supervised remediation in order to meet with compliance. In doing so ABC Corporation is able to ensure a secure network while supporting the use of BYOD practices.

## 5. Policy Compliance:

The InfoSec team verifies compliance with the BYOD security policy by implementing methods such as video monitoring, the use of intrusion detection tools, business tool reports, feedback and audits to the owner of the policy. Any employees who violated the policy could face disciplinary actions that could include termination in order to uphold the organizations security as well as accountability.

## 6. Related Standards, Policies, and Processes:

This policy aligns with key standards such as,

ISO/IEC 27001 This helps the establish an Information Security Management System (ISMS) in order for personal devices to be used.

GDPR Which safeguards personal data as well as privacy rights where applied. This helps meet compliance with data protection regulations.

NIST guidelines focuses on risk management and incident response for the mitigation of potential threats enhancing security measures.

# 7. Definitions and Terms:

CIA(Confidentiality, Integrity, Availability) The foundational principles of information security.

BYOD(Bring Your Own Device) A policy that allows employees the flexibility of using their personal devices for work intentions.

IT(Information Technology) is the use of computer systems, software, the networks and digitals tools that aid in storing, managing, and securing all data.

# 8. Revision History:

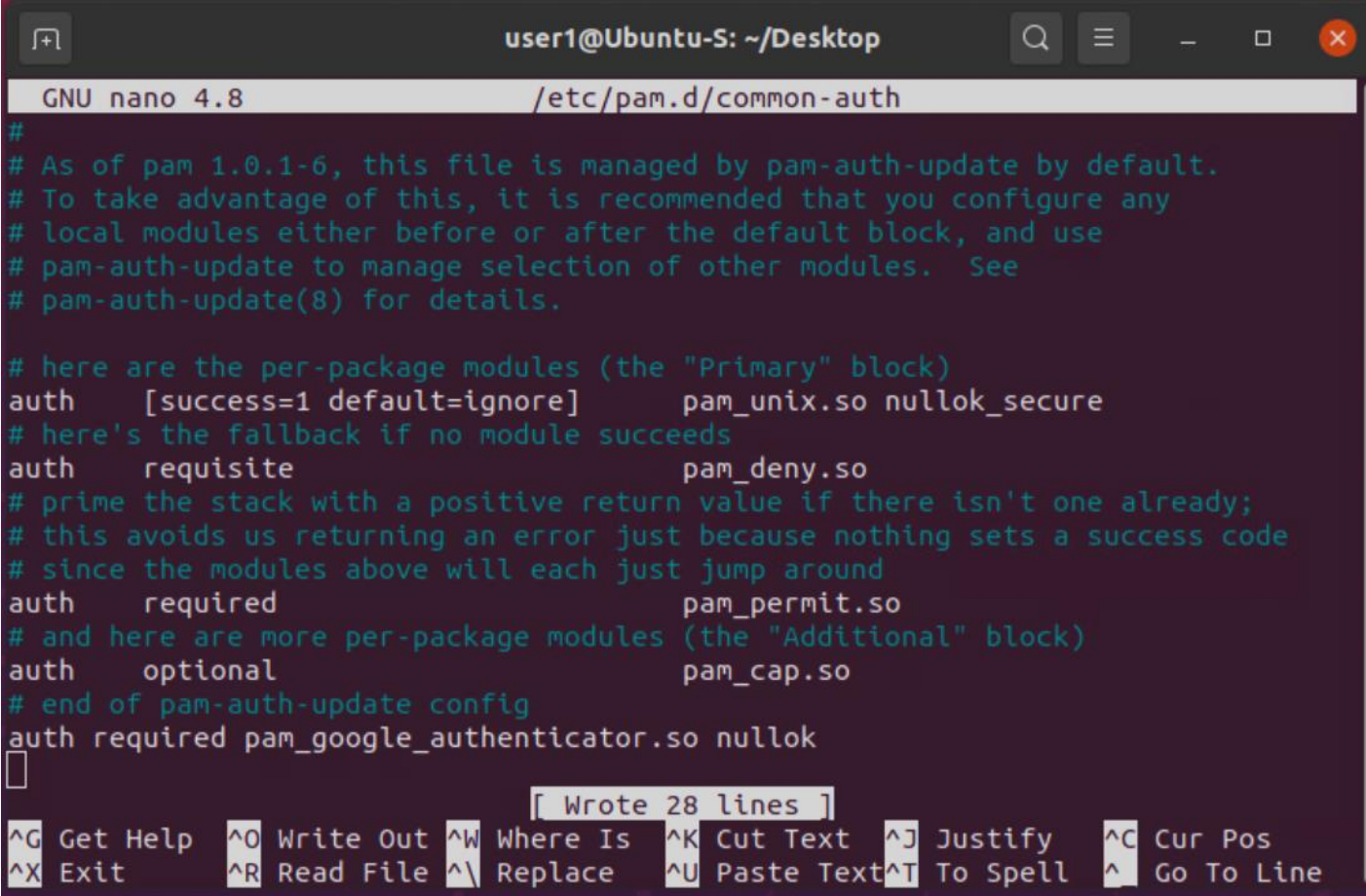
Date of change	Responsible	Summary of change
March 2025	Jonathan Waugh	Initial creation of the BYOD Security Policy based on SANS template

SEC285

Module 5

Multifactor Authentication (MFA)

# Common-auth Configuration File



The screenshot shows a terminal window titled "user1@Ubuntu-S: ~/Desktop" with a search icon, a menu icon, and window control buttons. The terminal displays the contents of the file `/etc/pam.d/common-auth` using GNU nano 4.8. The file contains configuration for PAM modules, including a primary block and an additional block. The primary block includes `auth [success=1 default=ignore] pam_unix.so nullok_secure` and `auth requisite pam_deny.so`. The additional block includes `auth required pam_permit.so` and `auth optional pam_cap.so`. The file ends with `auth required pam_google_authenticator.so nullok`. A status bar at the bottom indicates "Wrote 28 lines".

```
GNU nano 4.8 /etc/pam.d/common-auth
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

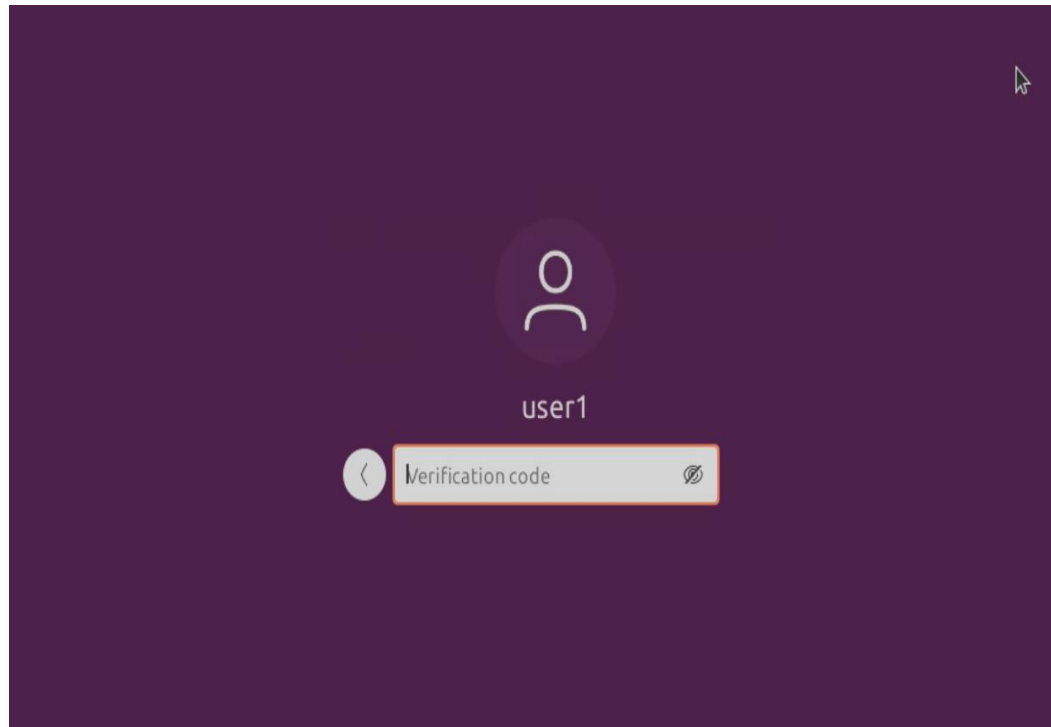
# here are the per-package modules (the "Primary" block)
auth      [success=1 default=ignore]      pam_unix.so nullok_secure
# here's the fallback if no module succeeds
auth      requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth      required                       pam_permit.so
# and here are more per-package modules (the "Additional" block)
auth      optional                       pam_cap.so
# end of pam-auth-update config
auth required pam_google_authenticator.so nullok

```

[ Wrote 28 lines ]

<b>^G</b> Get Help	<b>^O</b> Write Out	<b>^W</b> Where Is	<b>^K</b> Cut Text	<b>^J</b> Justify	<b>^C</b> Cur Pos
<b>^X</b> Exit	<b>^R</b> Read File	<b>^I</b> Replace	<b>^U</b> Paste Text	<b>^T</b> To Spell	<b>^_</b> Go To Line

# MFA Logon Screen



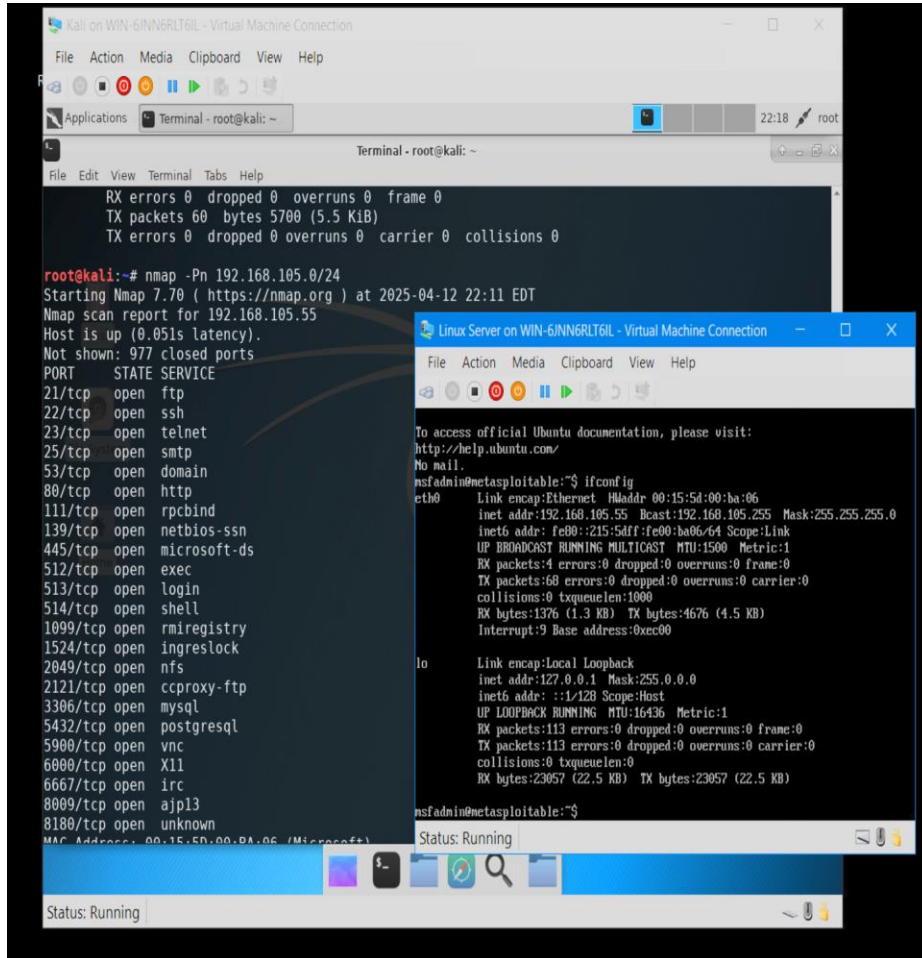


# SEC285

## Module 6

### Vulnerability Assessment

# Nmap



```
Kali on WIN-6/NN6RLT6IL - Virtual Machine Connection
File Action Media Clipboard View Help

Applications Terminal - root@kali: ~ 22:18 root

Terminal - root@kali: ~
File Edit View Terminal Tabs Help
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 60 bytes 5700 (5.5 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

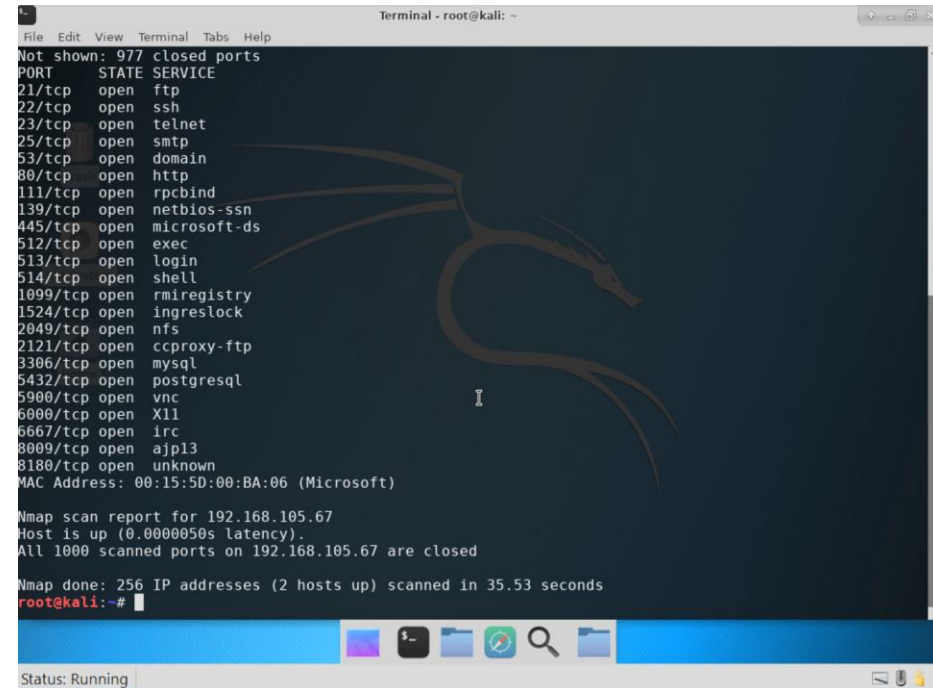
root@kali:~# nmap -Pn 192.168.105.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2025-04-12 22:11 EDT
Nmap scan report for 192.168.105.55
Host is up (0.051s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
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
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)

Linux Server on WIN-6/NN6RLT6IL - Virtual Machine Connection
File Action Media Clipboard View Help

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
nsfadmin@metasploitable:~$ ifconfig
eth0: Link encap:Ethernet HWaddr 00:15:5d:00:ba:06
      inet addr:192.168.105.55 Bcast:192.168.105.255 Mask:255.255.255.0
      inet6 addr: fe80::215:5dff:fe00:ba06:64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:4 errors:0 dropped:0 overruns:0 frame:0
      TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:1376 (1.3 KB) TX bytes:4676 (4.5 KB)
      Interrupt:9 Base address:0xec00

lo: Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:113 errors:0 dropped:0 overruns:0 frame:0
      TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:23057 (22.5 KB) TX bytes:23057 (22.5 KB)

nsfadmin@metasploitable:~$
Status: Running
```



```
Terminal - root@kali: ~
File Edit View Terminal Tabs Help

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
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 35.53 seconds
root@kali:~#
Status: Running
```

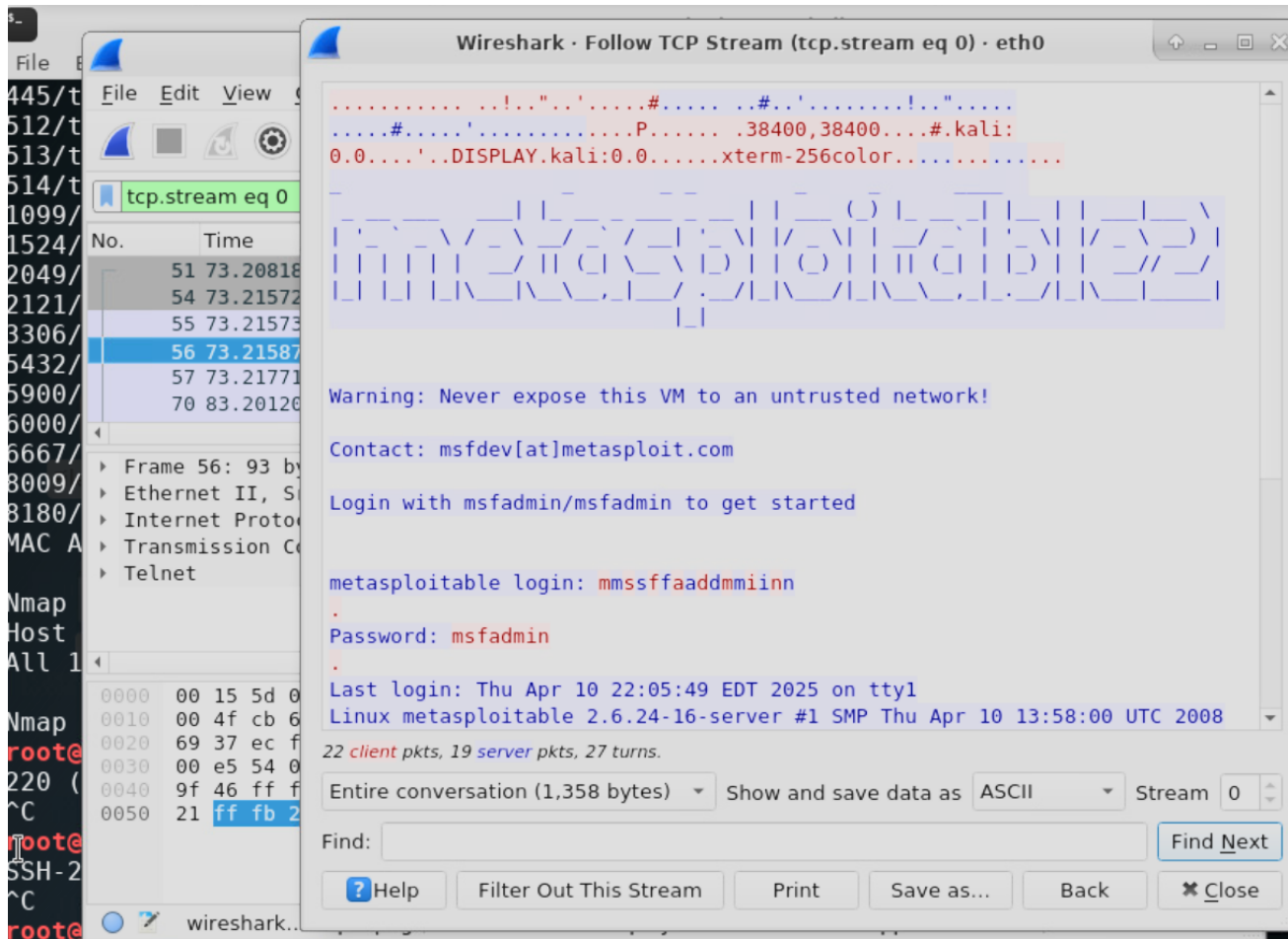
# NetCat

```
Terminal - root@kali: ~
File Edit View Terminal Tabs Help
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
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)

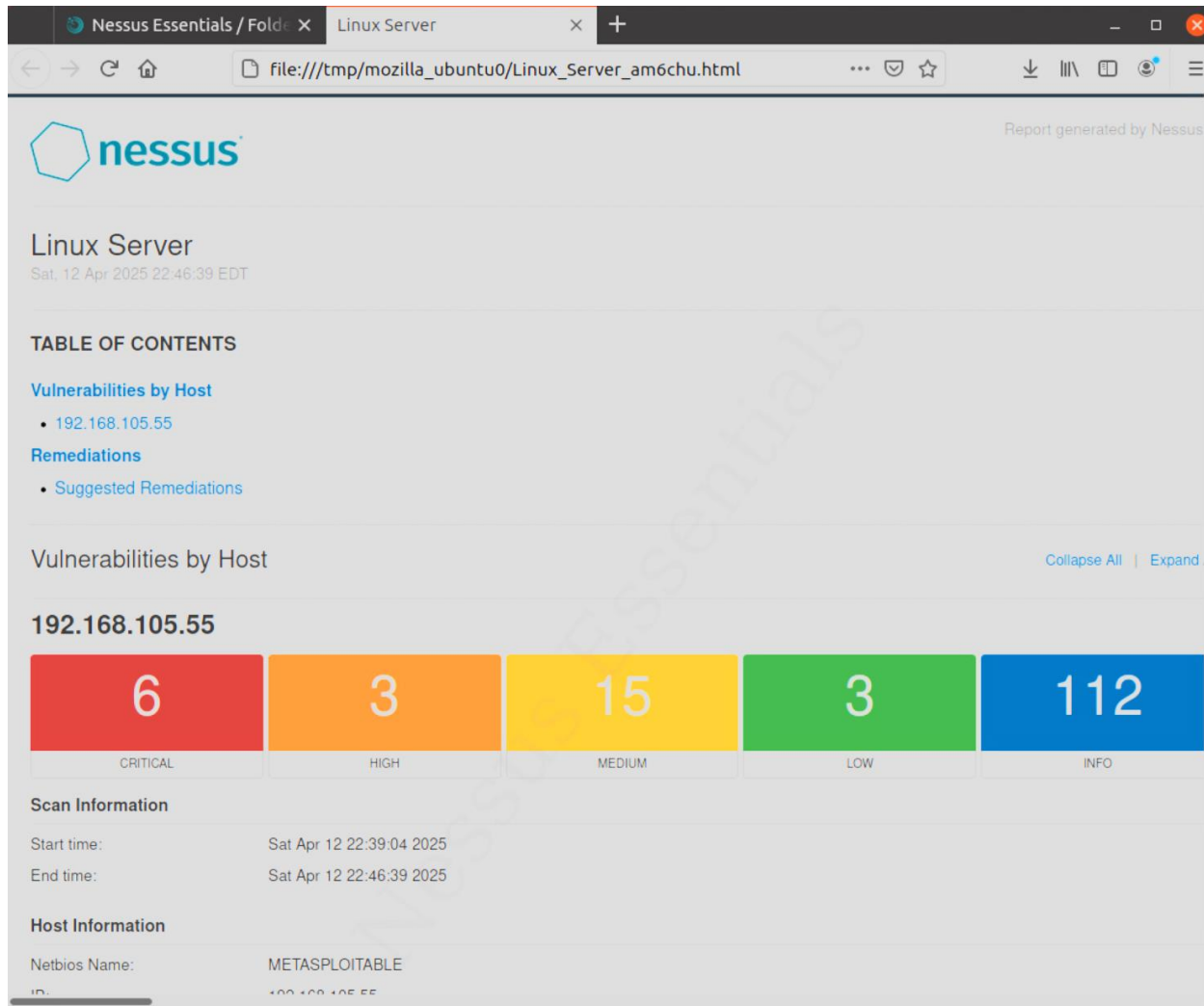
Nmap scan report for 192.168.105.67
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.105.67 are closed

Nmap done: 256 IP addresses (2 hosts up) scanned in 35.53 seconds
root@kali:~# nc -n -w5 192.168.105.55 21
220 (vsFTPd 2.3.4)
^C
root@kali:~# nc -n -w5 192.168.105.55 22
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
^C
root@kali:~# nc -n -w5 192.168.105.55 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
^C
root@kali:~#
```

# Wireshark



# Nessus



# Challenges

Challenges I faced during this course was time. I did not manage my time well due to things in my life being uncontrollable and another class that I felt was a waste of time taking from my ability to focus on this class.

I didn't overcome any of these challenges, because I was too focused on the other class. Yes I got a good grade in this class and that was thankful to prior knowledge, but I felt I could of learned more had I had more time.

# Career Skills

- Security Policy Development
- Vulnerability assessment
- Firewall Implementation
- Business Continuity Planning
- Compliance and Auditing
- Secure System Design

# Conclusion

In this project I developed a security policy, used encryption techniques, configured firewalls, assessed vulnerabilities, and planned for system recovery and continuity during disruptions.



# References

- Instructional Videos
- Project Guides