SEC285
Module 2
Asymmetric Key Encryption

Andrew Newhart

Rubric

Activity	Requirement(s)	Points
File Encryption	Screenshot	15
File Decryption	Screenshot	15

File Encryption

```
Terminal - root@kali: ~
File  Edit  View  Terminal  Tabs  Help
ssb   rsa3072 2022-11-13 [E] [expires: 2024-11-12]

root@kali:~# gpg --list-keys
/root/.gnupg/pubring.kbx
------------------------
pub   rsa3072 2022-11-13 [SC] [expires: 2024-11-12]
      96DFDCA53B85B471A4A8749D59E40CE5BA20F8E3
uid           [ultimate] Andy Newhart <andy@newhart.com>
sub   rsa3072 2022-11-13 [E] [expires: 2024-11-12]

root@kali:~# nano testfile.txt
root@kali:~# ls testfile.txt
testfile.txt
root@kali:~# cat  testfile.txt
This is a test file that we will encrypt with gp.
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 gp.
root@kali:~# cat testfile.txt.gpg
[illegible]
[illegible]
[illegible]
root@kali:~#
```

File Decryption

This screenshot should show the following.

- The encrypted file being listed by itself
- The decrypting process
- Both the encrypted file and the original plaintext file being listed

```
root@kali:~# ls test*
testfile.txt.gpg
root@kali:~# gpg testfile.gpg
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
gpg: can't open 'testfile.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.
cat: testfile.txt.: No such file or directory
root@kali:~# cat testfile.txt
This is a test file that we will encrypt with gp.
root@kali:~# cat
^[[A
```

SEC285

Module 2 - Asymmetric Key Encryption

Conclusions and knowledge gained

This was a good look at Asymmetric Key Encryption.

The results clearly demonstrate the results of encrypting the files on the Linux cli.

The project lab taught the steps to generate an encryption key using the gpg utility.

I had a good understanding of the utility and the use of rewards of encrypting your data and rest and in motion and the encryption keys make that possible.

Andrew Newhart

SEC285
Module 3

Stateful Firewall

Andrew Newhart 12/11/22

Rubric

Activity	Requirement(s)	Points
Question	Answer	30
Nmap Scan	Screenshot	30

Question

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

Answer here: IPTABLES is just a resource for a CLI firewall utility in the Unix arena. If you would rather deny all connections and manually specify which ones you want to allow to connect, you should change the default policy of your chains to drop.

With your default chain policies configured, you can start adding rules to iptables so it knows what to do when it encounters a connection from or to a particular IP address or port.

CLI: iptables --policy INPUT DROP - Drop – Drop the connection, act like it never happened. This is best if you don't want the source to realize your system exists.

The example preformed in the mod 3 lab closed all connection to the server that used the INPUT DROP command

References: https://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall/

Kali on WIN-6JNN6RLT6IL - Virtual Machine Connection

File Action Media Clipboard View Help

Applications Terminal - root@kali: ~ 17:54 root

Terminal - root@kali: ~

File Edit View Terminal Tabs Help

```
Starting Nmap 7.70 ( https://nmap.org ) at 2022-12-11 17:11 EST
Nmap scan report for 192.168.105.55
Host is up (0.0022s 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 34.13 seconds
root@kali:~# nmap 192.168.105.55 | more
Starting Nmap 7.70 ( https://nmap.org ) at 2022-12-11 17:54 EST
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.105.55
Host is up (0.0024s 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 17.88 seconds
root@kali:~#
```

SEC285

Module 3 - Stateful Firewall

Conclusions and knowledge gained

The project as a valuable lab on working with the nmap command and iptables.

Iptables where not around when I was installing networks in the 80's and 90's so I can see where this function will help maintain the flow of secured data through your firewall and onto your network.

iptables is a user-space utility program that allows a system administrator to configure the IP packet filter rules of the Linux kernel firewall, implemented as different Netfilter modules.

The filters are organized in different tables, which contain chains of rules for how to treat network traffic packets. This is a good use of tech to resolve traffic direction and relieve other firewall operations by weeding out packets based on rules established by the iptables.

This was a great upload of knowledge into my skill-set and I am sure will be invaluable in my future dealings with firewalls.

SEC285
Module 4

Bring Your Own Device (BYOD)
Security Policy

Andrew Newhart

Rubric

Activity	Requirement(s)	Points
BYOD Security Policy	The complete policy template	60

1. Overview: <u>BYOD as a SMB IT policy.</u>

Security has always been a multi-faceted issue for organizations that leverage mobile device strategies such as BYOD, choose-your-own-device (CYOD), corporate-owned, personally enabled (COPE) devices, and corporate-owned, business-only (COBO) devices.

However, the BYOD trend presents a more complex security environment than company-owned devices. For one, employee-owned endpoints usually contain employees' personal information in addition to corporate data. It can be much harder to mandate (through technical or policy controls) certain configurations, application use, or how much an employee can engage in "personal," i.e. non-work related, activities.

2. Purpose:

The main purpose of developing a BYOD device policy would be to set a clear set of parameters defining the AUP of personal devices and what access can be given to a users device. The goal is to keep any possible threat from an infected personal device to access your company secured network.

3. Scope:

It can be much harder to mandate (through technical or policy controls) certain configurations, application use, or how much an employee can engage in “personal,” i.e. non-work related, activities.

To help make clear definitions of expected use of company data and application on personal user devices a BYOB policy will set the terms and requirements as well as prerequisites required to allow a personal device to access the data or work network.

4. Policy:

The AUP of company applications and data access is clearly defined in this policy and will develop discovery techniques used on a regular basis to minimize threats from an infected or compromised security system on a personal use device.

Personal use devices used to access the company network or any of its resources has to comply with regular scheduled ad well as random threat assessment of the device and its security settings.

5. Policy Compliance:

Compliance to all security parameters defined here must be adhered to allow the users device access to company resources.

In the event a vulnerability or threat is discovered on a personal device trying to access or utilize company network resources or data the user must surrender to a devices analysis and security assessment and remain locked from the network by device MAC or user id until which time the threat can be neutralized and the device returned in a cleaned and secure condition.

An employee found to have violated this policy may be subject to disciplinary actions up to and including termination of employment.

6. Related Standards, Policies, and Processes:

The standards used to help define this policy are included in the NIST documents
NIST 800-171

7. Definitions and Terms:

BYOD – Bring Your Own Device
CYOD – Choose Your Own Device
COPE – Corporate Owned Personally Enabled Device
COBO – Corporate Owned Business Only Device
AUP – Acceptable Use Policy
MAC – Media Access Control Address

8. Revision History:

Date of change	Responsible	Summary of change
December 19 2022	Original Creation	New Policy

SEC285 Module 4 - The BYOD Security Policy

Conclusions and knowledge gained

This was the hardest module for me.
The context of the lesson was clear and I understand it but policy writing is not my greatest skill.

I do understand and can see the need to define and create policies to define the use and operation of any company resource as well as any device allowed to access company resources, data or networking.

As a previous small business owner in the IT industry I came to understand in the early stages of ramping up our firm from few contractors to a dozen tech vans and a twenty-six techs across 8 offices and 17 states, that a clear AUP had to be written to define the use or our data and the company resources.

AUP's for both IT, test and internal equipment had to be defined to keep a clear understating of expectation of security that was the responsibility of all employees and contractors.

Our policies where not as defined nor where that as much mobile access afforded users at that time but we still had to keep a vigil eye on the access to the network and all resources.

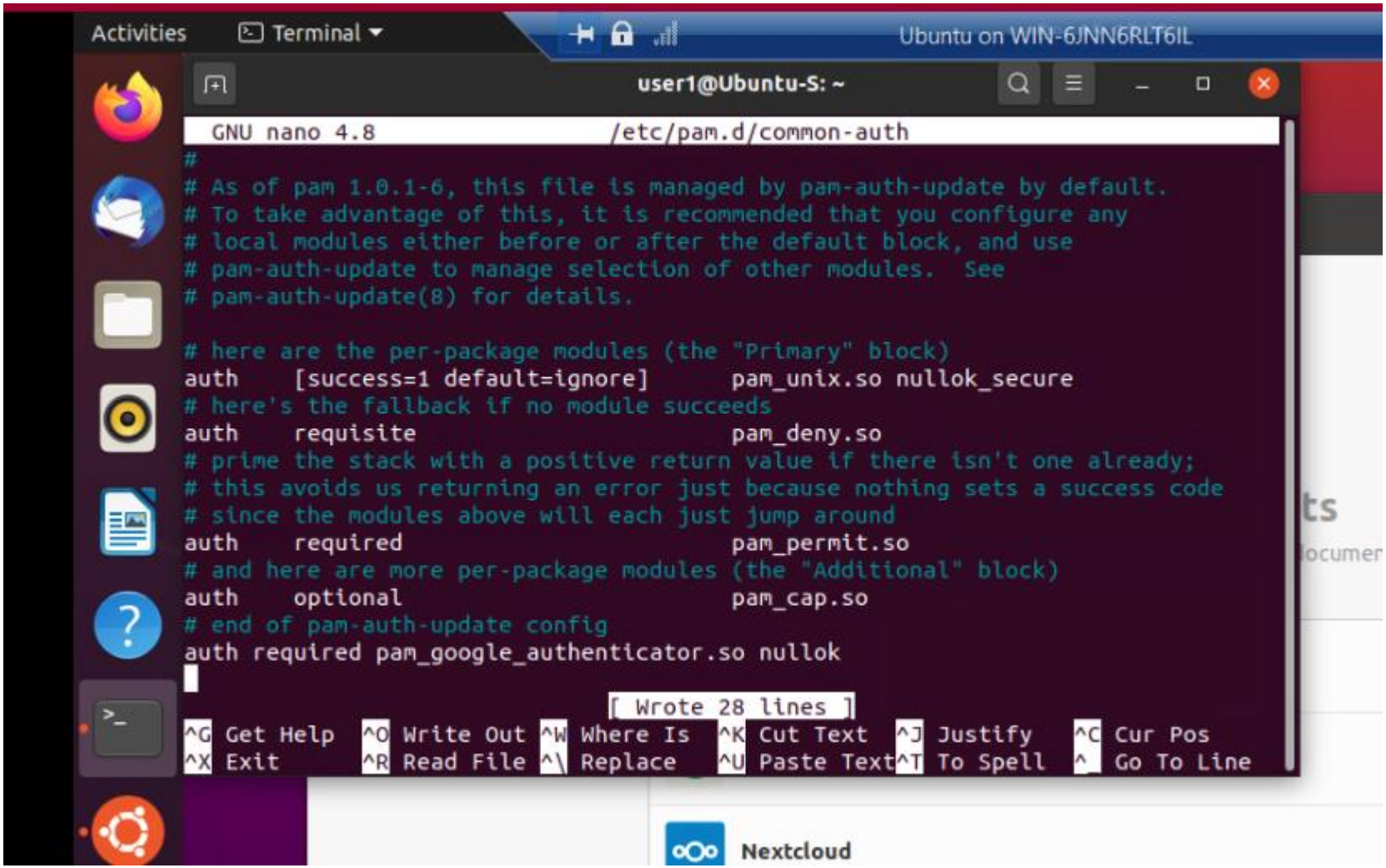
SEC285
Module 5
Multifactor Authentication (MFA)
Andrew Newhart

Rubric

Activity	Requirement(s)	Points
Common-auth Configuration File	Screenshot	30
MFA Logon Screen	Screenshot	30

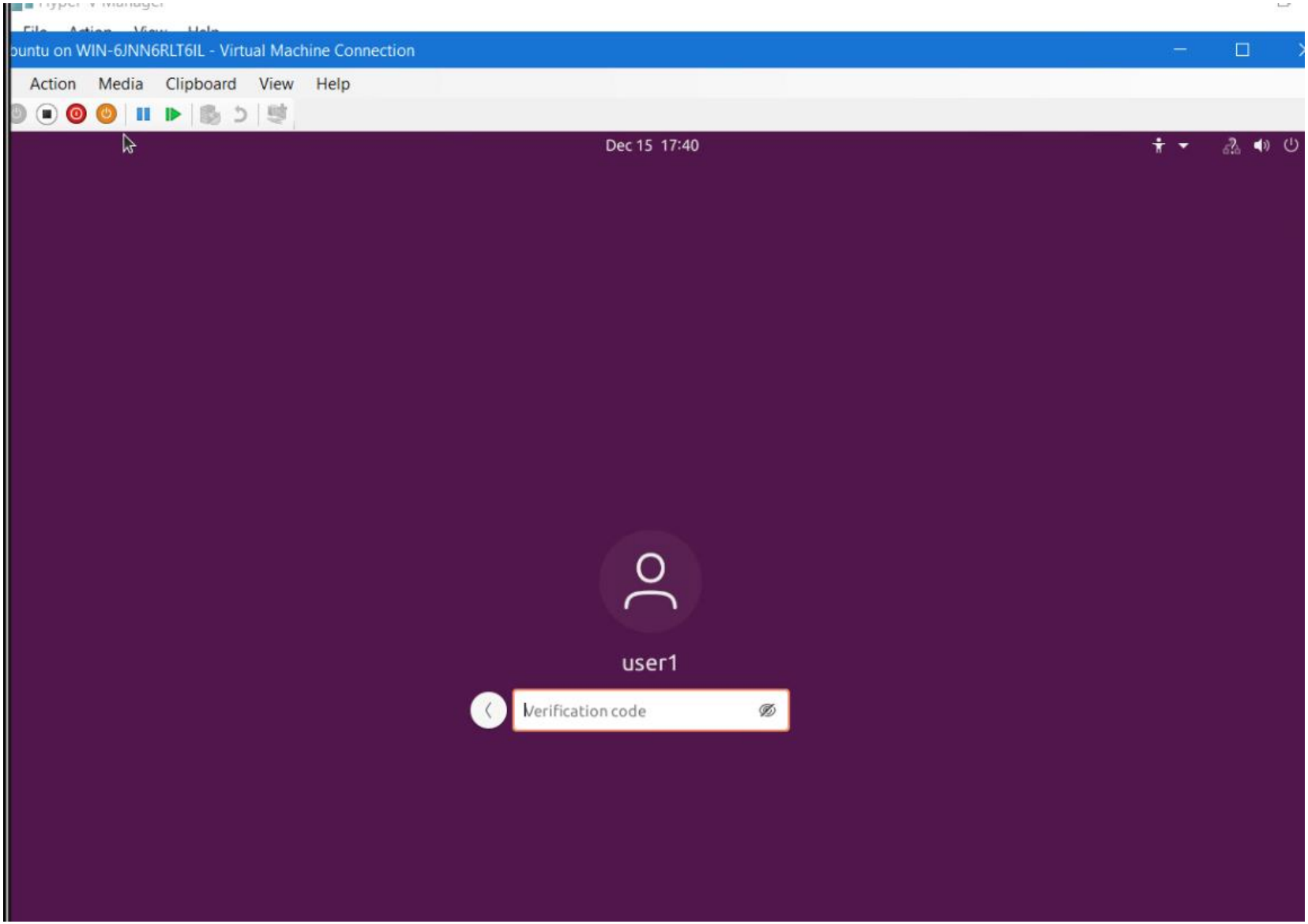
Common-auth Configuration File

This screenshot should show the entry that indicates the use of the Google Authenticator module.



MFA Logon Screen

This screenshot should show the logon screen where a verification code is required.



SEC285

Module 5 - Multifactor Authentication (MFA)

Conclusions and knowledge gained

This project was a great lesson on setting up MFA.

Using the google auth app was great to see and test. Most of my current MFA is biometric but I have set it up on all mobile apps and now have included in most of my internets sites that include any sensitive data or business operations such as; banking, insurance and other cloud apps.

MFA is a great option to help secure even your personal data and I recommend that everyone set it up on their banking connections at least.

Many sites will force you to set it up as Devry did and even prime now uses a MFA app that generates an approval page on a mobile app for access to your data.

MFA was a great and very useful addition to the authorization step of authenticating user access.

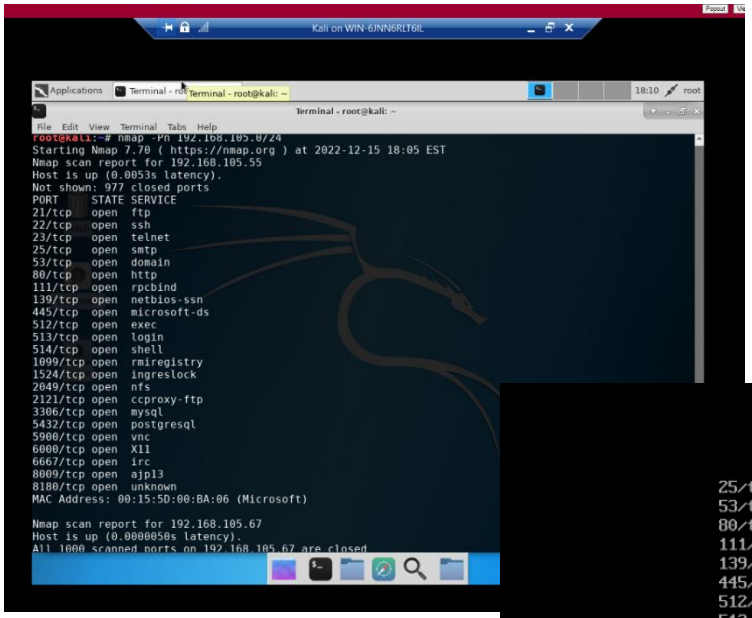
SEC285
Module 6
Vulnerability Assessment
Andrew Newhart

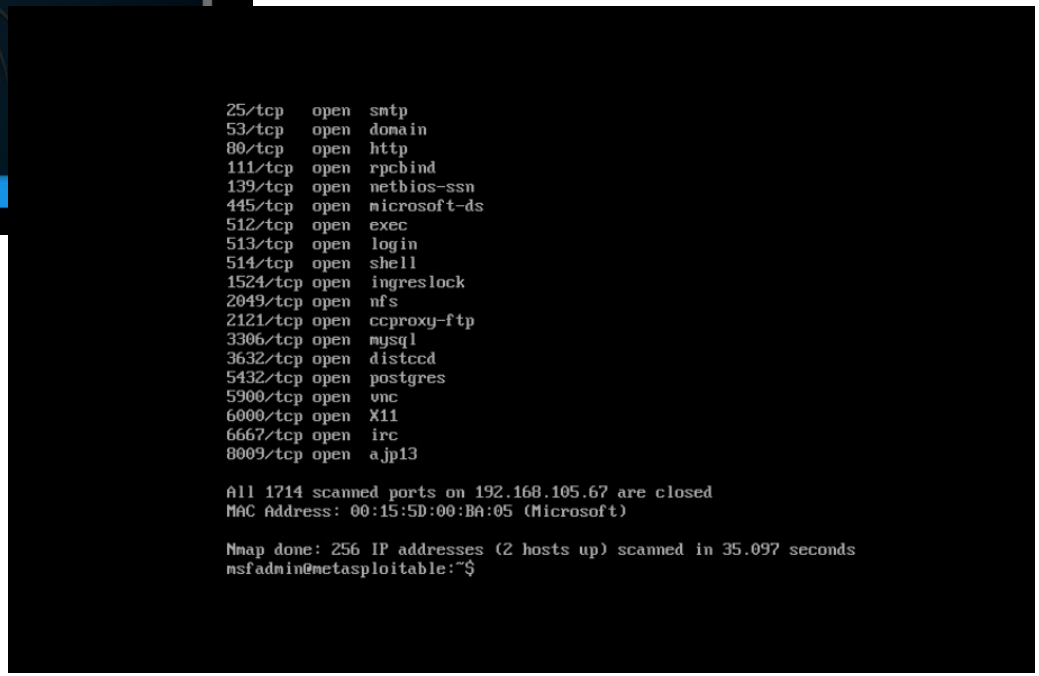
Rubric

Activity	Requirement(s)	Points
Nmap	Screenshot	15
NetCat	Screenshot	15
Wireshark	Screenshot	15
Nessus	Screenshot	15

Nmap

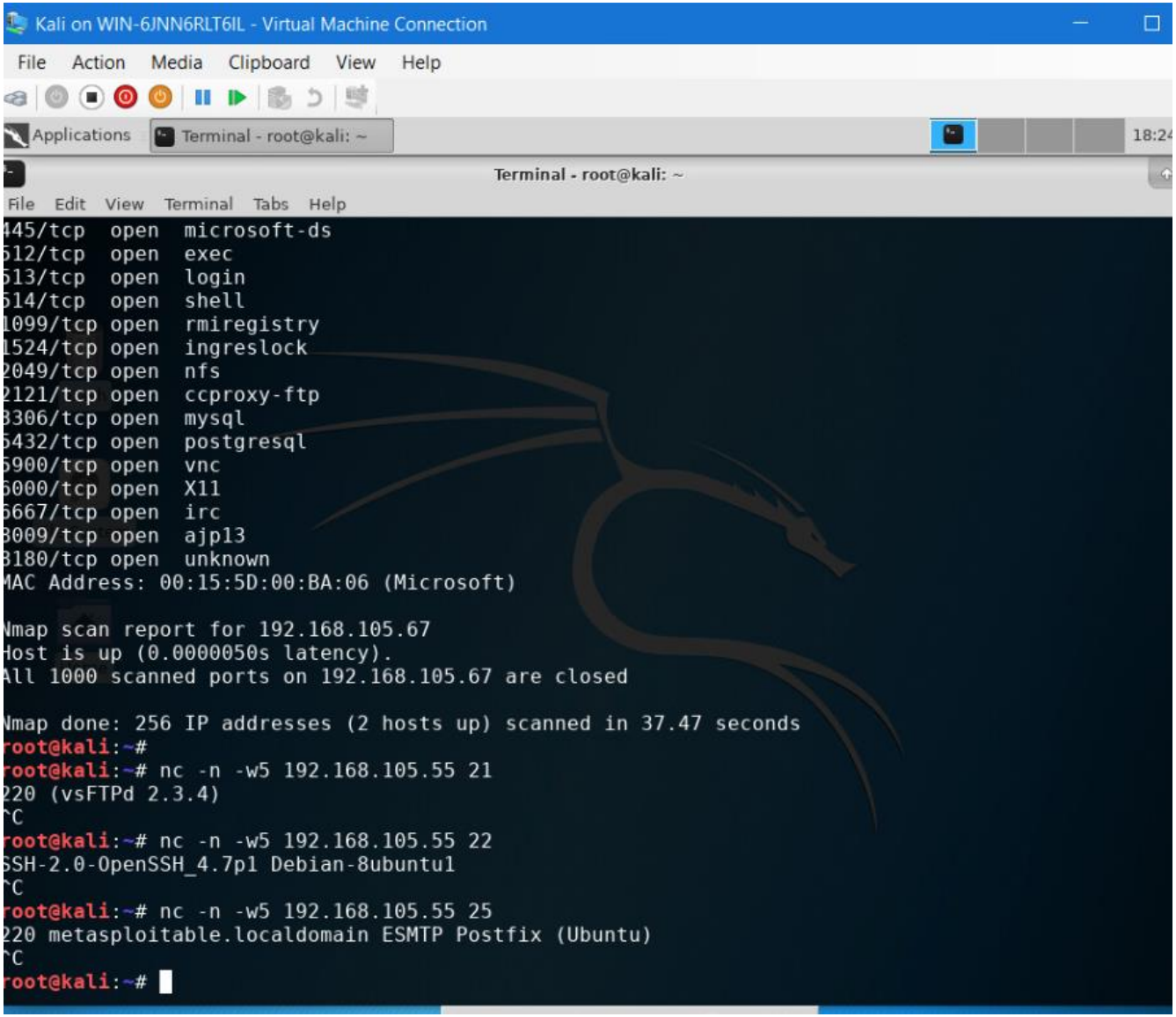
This screenshot should include the scan result showing both the Kali and Linux Server VMs.





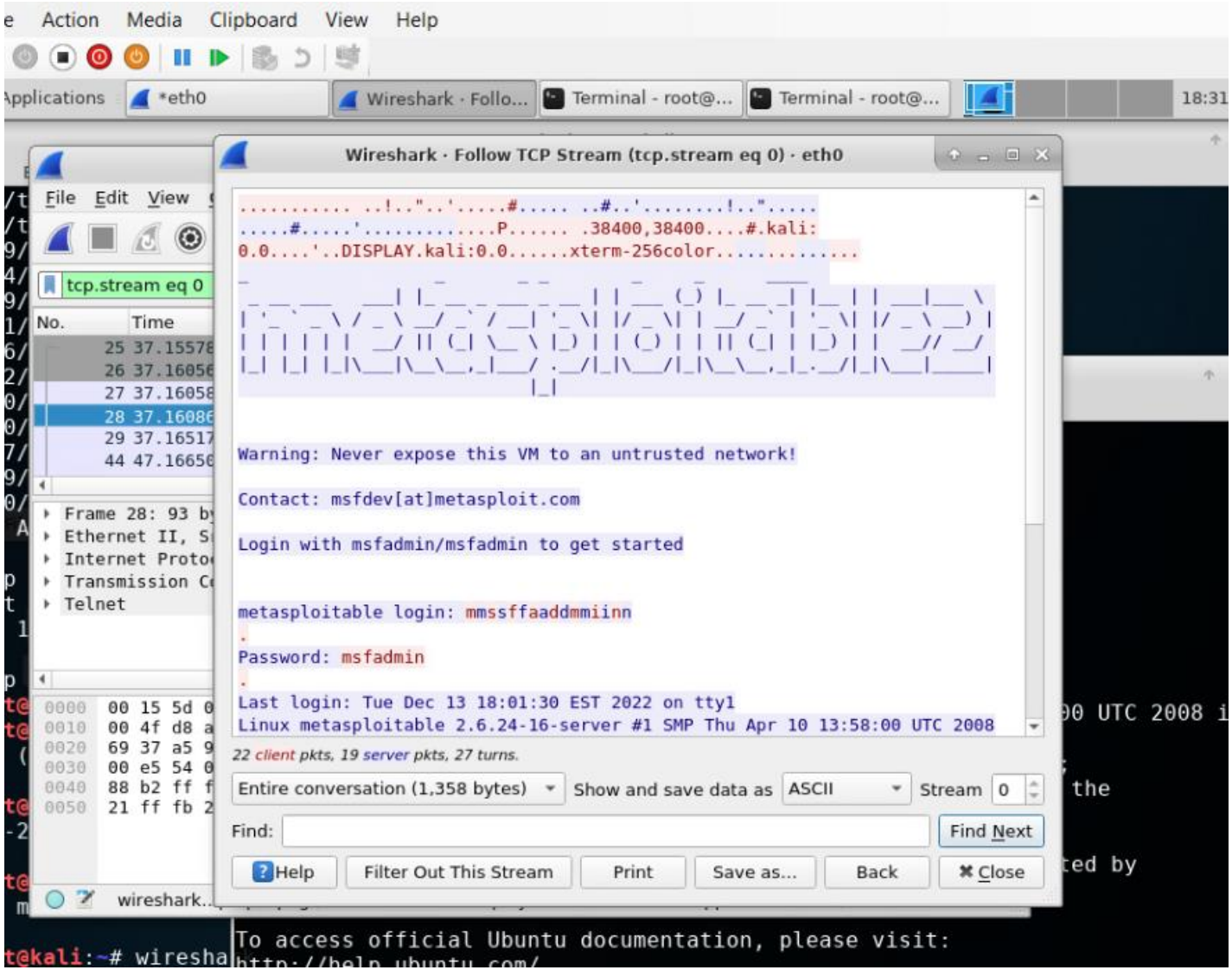
NetCat

This screenshot should include the scan result showing both the Kali and Linux Server VMs.



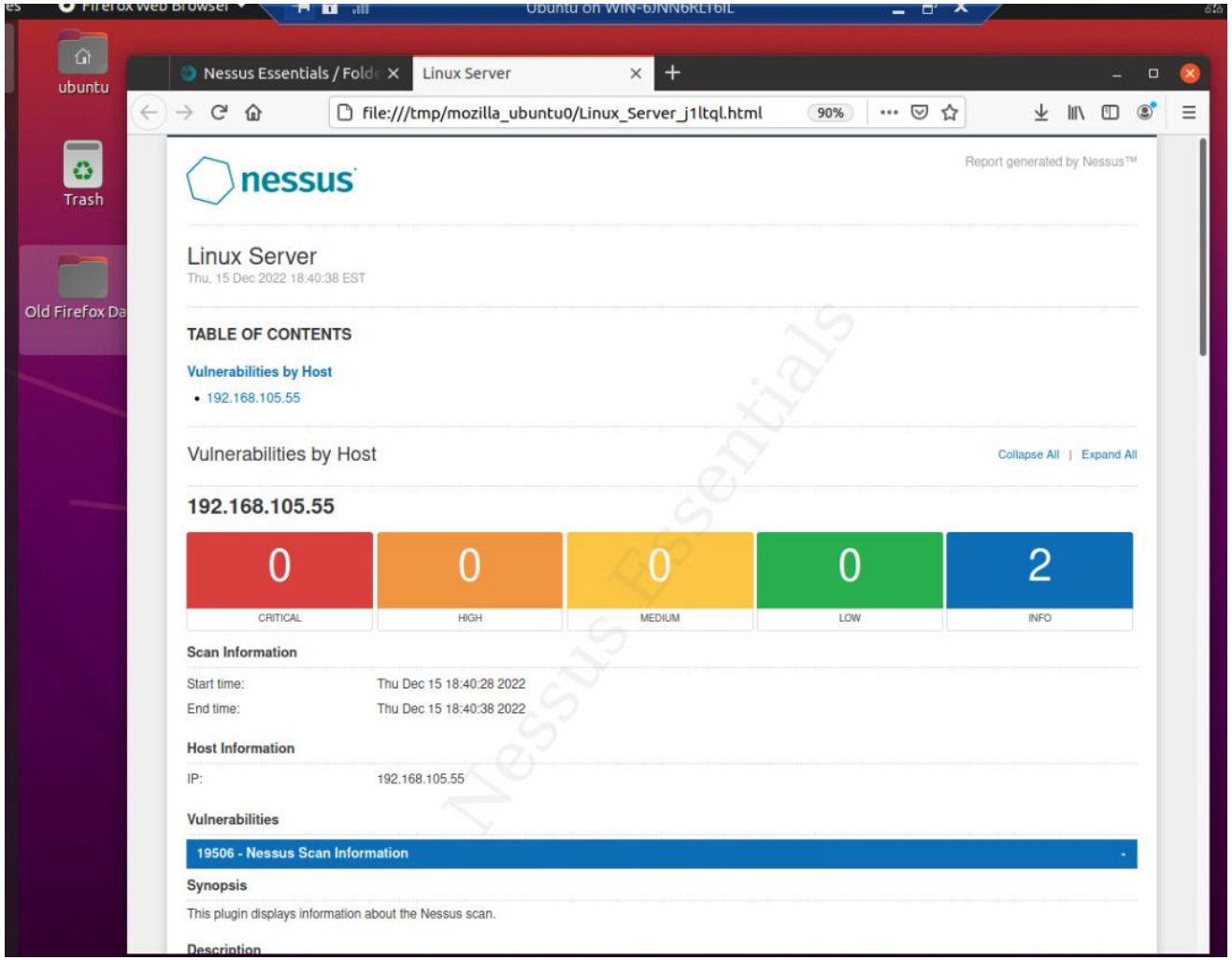
Wireshark

This screenshot should include the Wireshark—Follow TCP Steam window showing the Telnet username and password.



Nessus

This screenshot should include the high-level view of the Nessus vulnerability scan report (showing categories of vulnerability in different colors).



SEC285

Module 6 - Vulnerability Assessment

Conclusions and knowledge gained

This project helped me get as handle on one of the utilities that I used in a much older version ..we called LAN sniffers.
Working on a CNX certification in the mid 90's I was exposed to sniffing and disassembly of ethernet packets to help in locate LAN traffic issues.

NMAP and NCAT are surely useful commands but the wireshark and nessus utility surely make it a easier view of what's happening on your network.

The NESSUS utility is surely and easy way to look at your traffic and its impact on the lan.

I am nothing if not a layer 1 & 2 tech for over 30 years I have been developing and PM'ing infrastructure media and hardware included wireless bridging using Cisco 350 bridges to help connect data lans across local campus buildings.

I can remember in the days of the general network sniffers devices we used that helped us locate faulty ethernet interfaces on your lan.