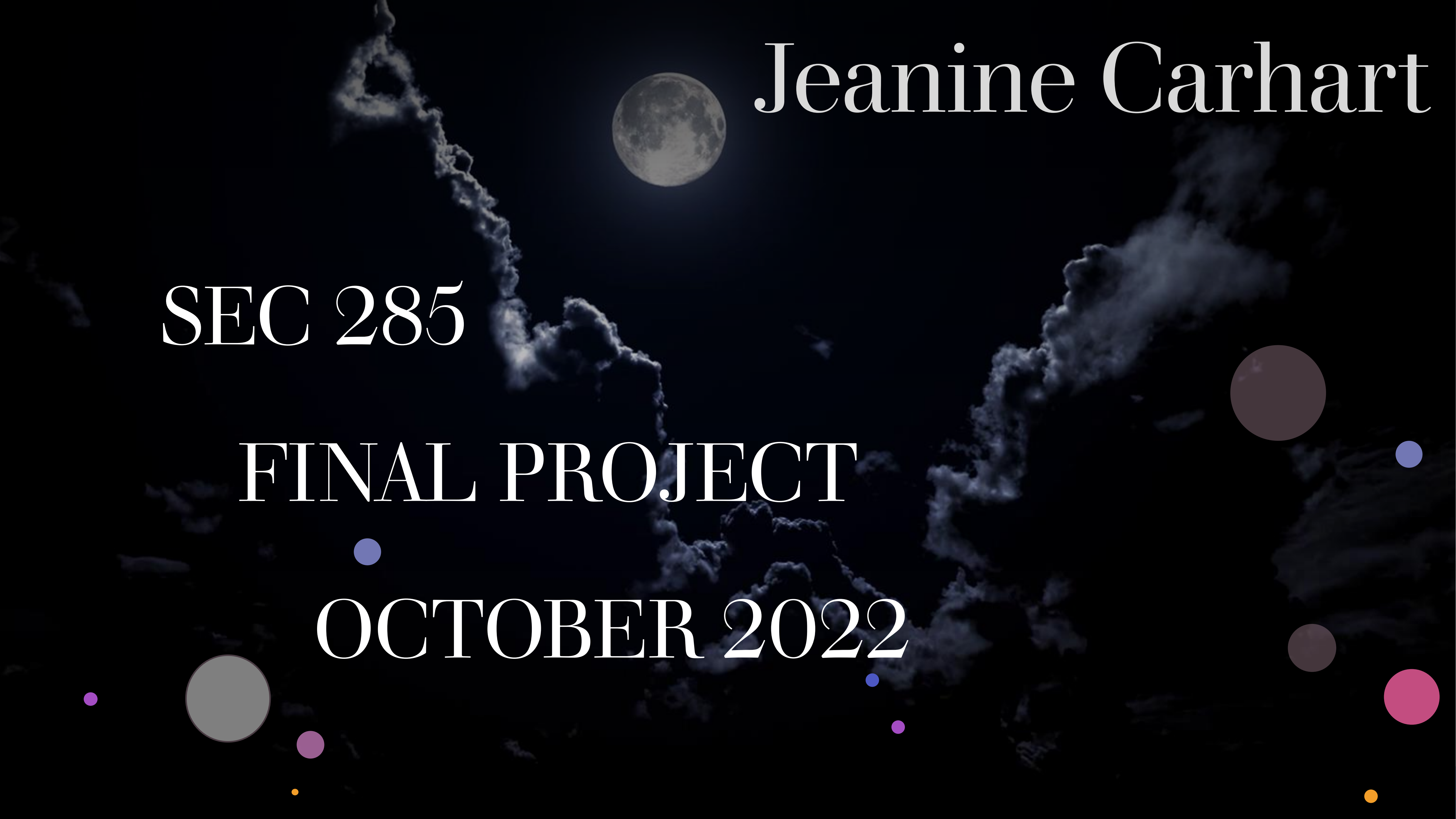


Jeanine Carhart

SEC 285

FINAL PROJECT

OCTOBER 2022

Content

Module 2

Asymmetric Key Encryption

Module 3

Stateful Firewall

Module 4

Bring Your Own Device (BYOD) Security Policy

Module 5

Multifactor Authentication (MFA)

Module 6

Vulnerability Assessment

Module 7

Share, Review, & Reflect

Resources

Virtual Machines (VM)

- Linux Server
- Kali
- Ubuntu

Introduction

The fundamentals needed to analyze internal and external security threats and implement security mechanisms were explored. Network and Internet security issues were evaluated to provide security solutions, design information systems security policy, network troubleshooting, and implement digital signatures

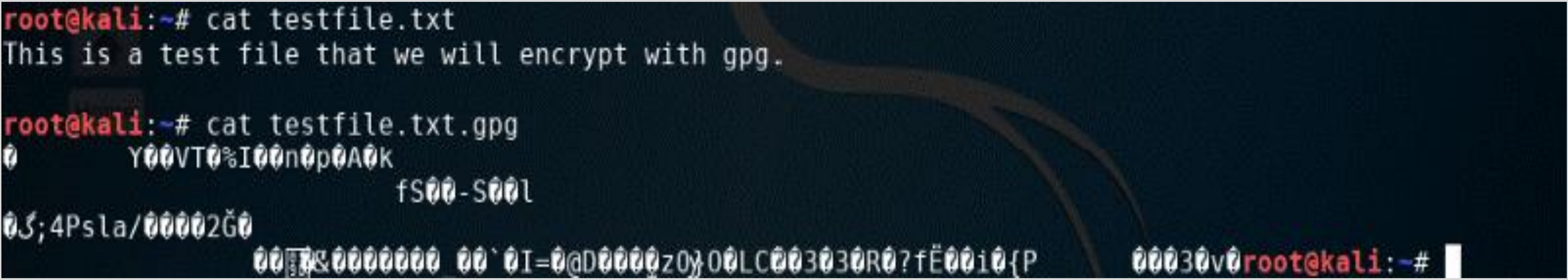
Module 2

Asymmetric Key Encryption

File Encryption

This screenshot shows the following:

✓ Content of the plaintext file	✓ Content of the encrypted file



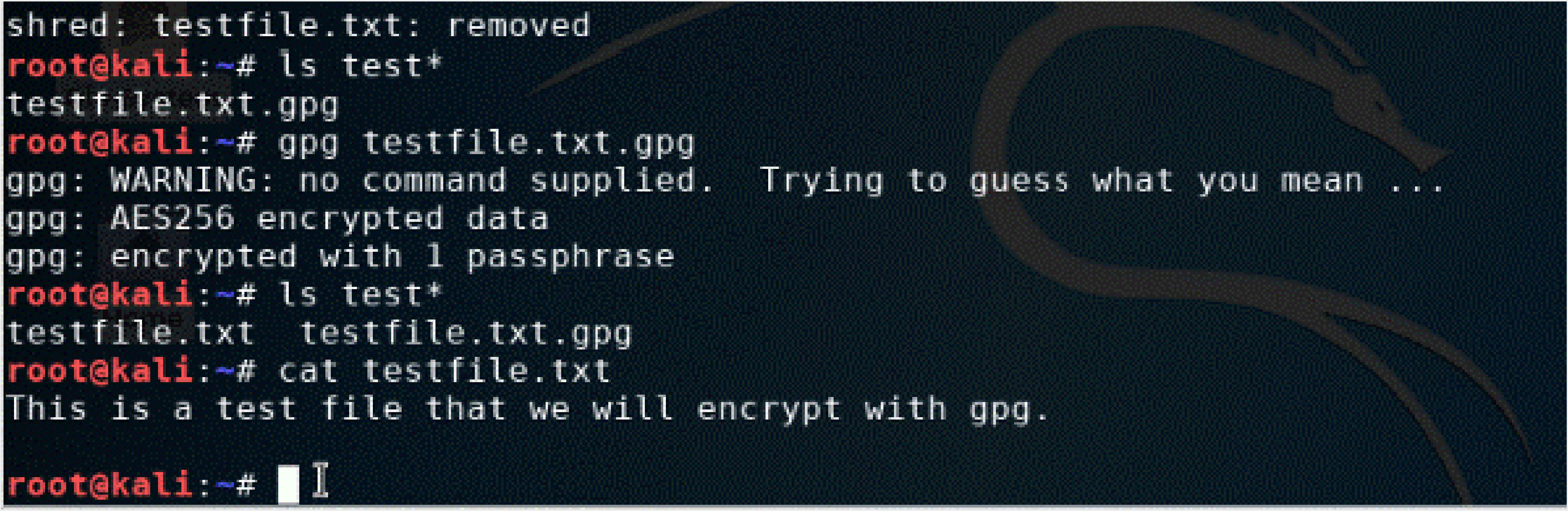
```
root@kali:~# cat testfile.txt
This is a test file that we will encrypt with gpg.

root@kali:~# cat testfile.txt.gpg
�       Y��VT�%I��n�p�A�k
                       fS��-S��l
�ڑ;4Psla/����2Ğ�
           ���&�������  ��`�I=�@D����z0}O�LC��3�3�R�?fË��i�{P      ���3�v�root@kali:~# 
```

Note: Encrypted information is unreadable

File Decryption

This screenshot shows the following:

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



```
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:~# 
```

Module **3**

Stateful Firewall

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

Answer:

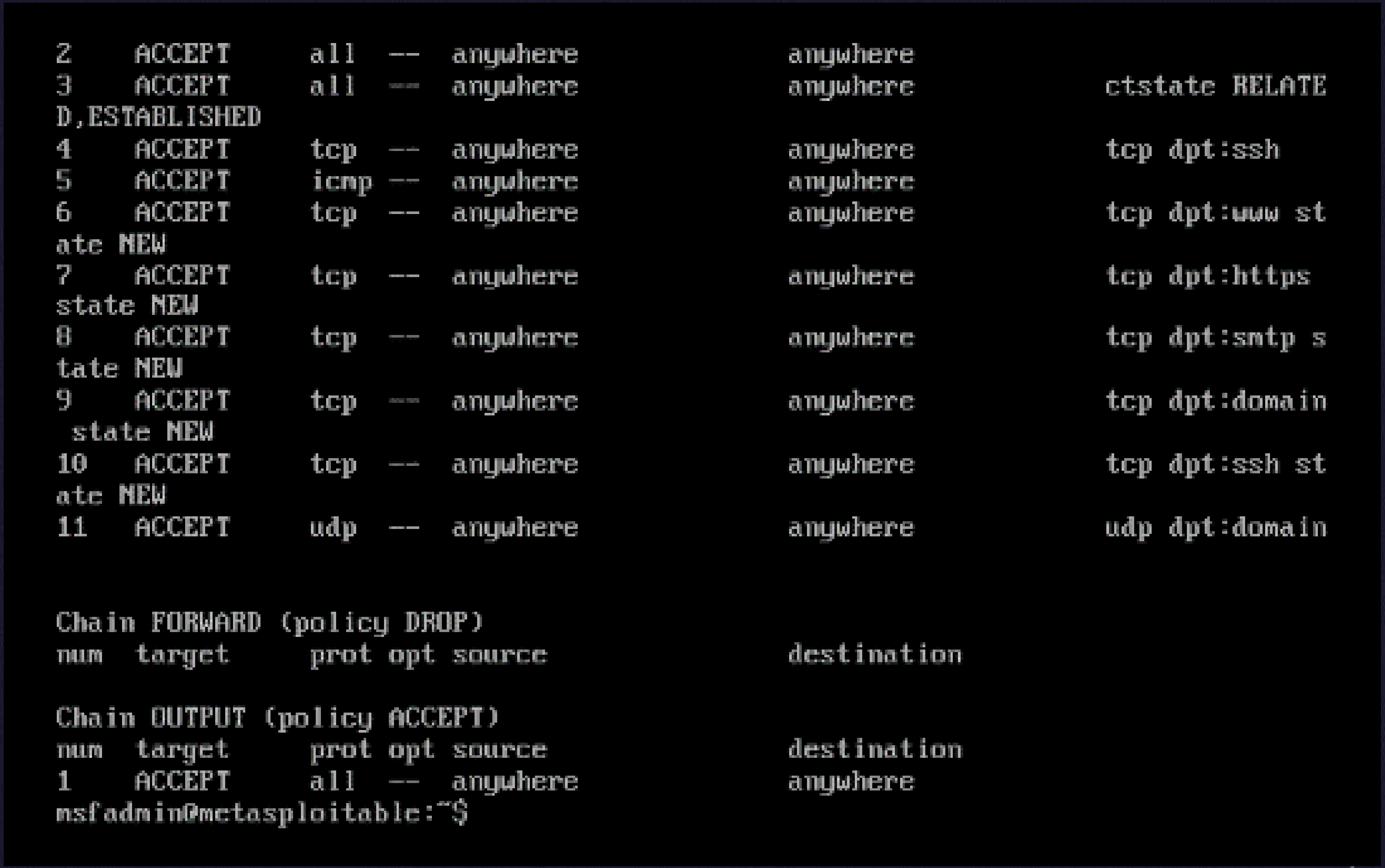
Using DROP makes the connection ‘disappear’. If outside sources try to find your systems it won’t show up

References:

Brown, K. (2020, August 27). The Beginner’s Guide to iptables, the Linux Firewall. How-To Geek. https://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall/

Nmap Scan

Nmap scan result of the Linux Server virtual machine



```
2     ACCEPT     all  --   anywhere               anywhere
3     ACCEPT     all  --   anywhere               anywhere             ctstate RELATE
D,ESTABLISHED
4     ACCEPT     tcp  --   anywhere               anywhere             tcp dpt:ssh
5     ACCEPT     icmp --   anywhere               anywhere
6     ACCEPT     tcp  --   anywhere               anywhere             tcp dpt:www st
ate NEW
7     ACCEPT     tcp  --   anywhere               anywhere             tcp dpt:https
state NEW
8     ACCEPT     tcp  --   anywhere               anywhere             tcp dpt:smtp s
tate NEW
9     ACCEPT     tcp  --   anywhere               anywhere             tcp dpt:domain
 state NEW
10    ACCEPT     tcp  --   anywhere               anywhere             tcp dpt:ssh st
ate NEW
11    ACCEPT     udp  --   anywhere               anywhere             udp dpt:domain


Chain FORWARD (policy DROP)
num   target     prot opt source                  destination

Chain OUTPUT (policy ACCEPT)
num   target     prot opt source                  destination
1     ACCEPT     all  --   anywhere               anywhere
msfadmin@metasploitable:~$
```

Module 4

Bring Your Own Device (BYOD) Security Policy

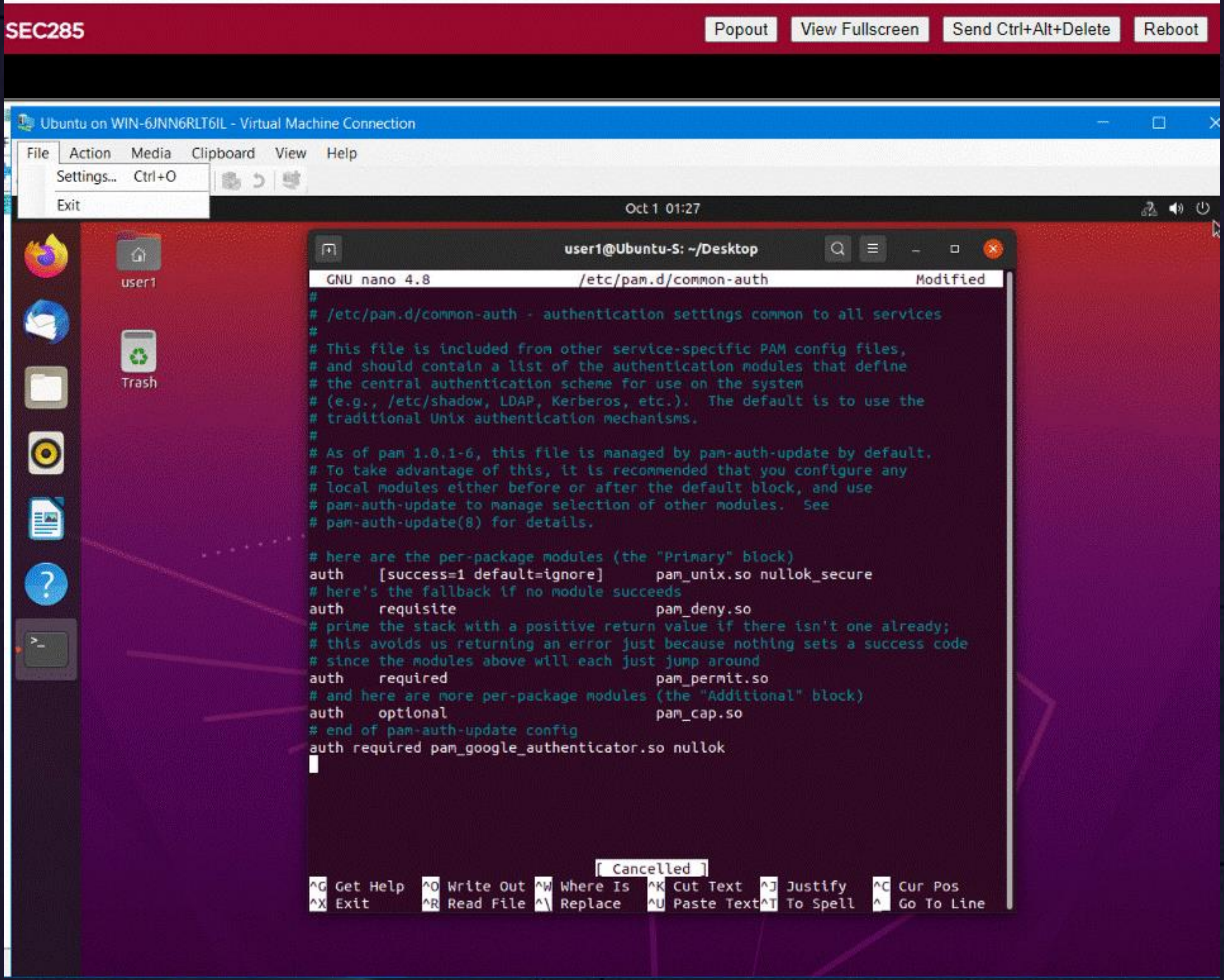
Bring Your Own Device (BYOD) Security Policy

(Double Click on Icon)

Module 5

Multifactor Authentication (MFA)

Common-auth Configuration File

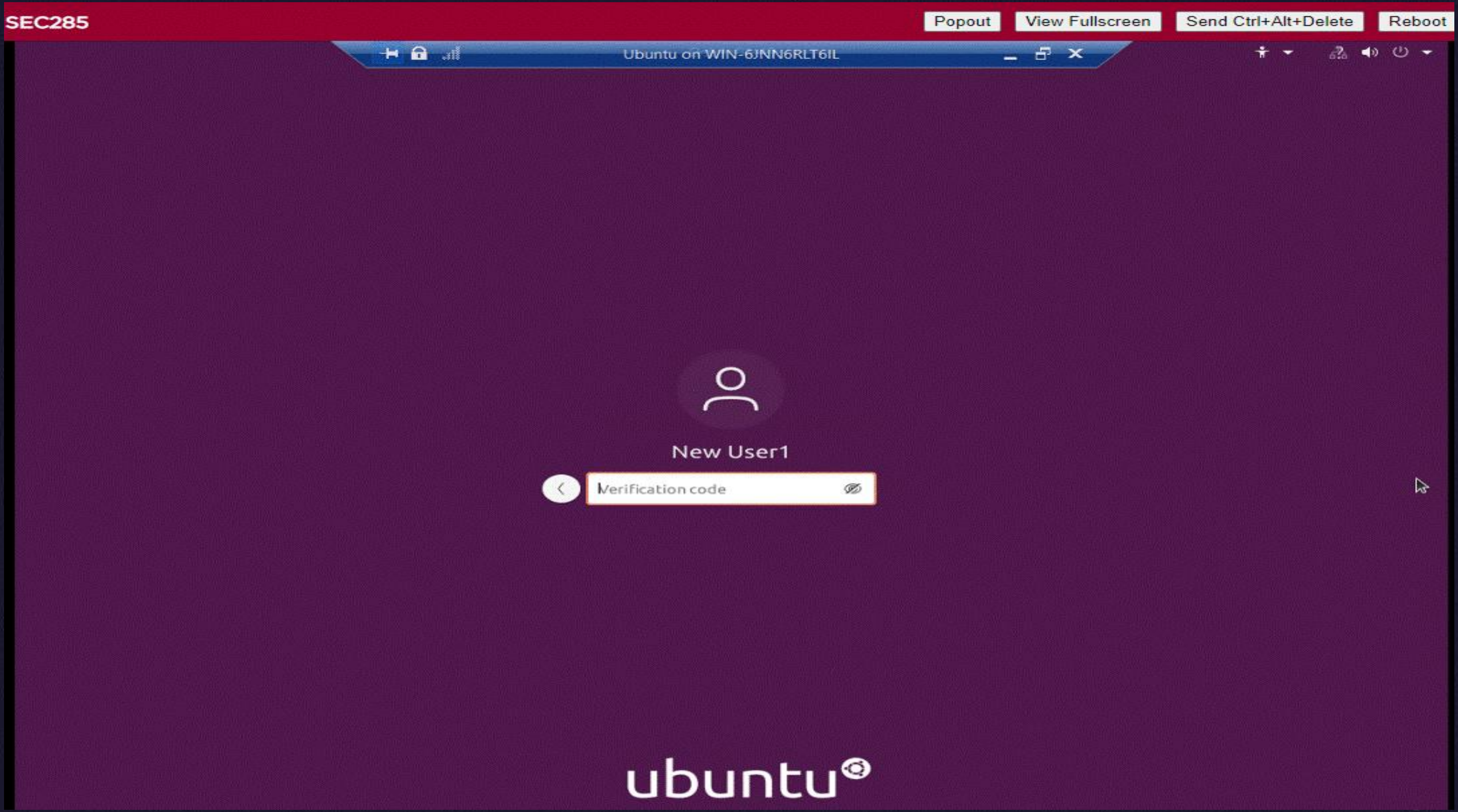


```
  GNU nano 4.8               /etc/pam.d/common-auth                 Modified
#
# /etc/pam.d/common-auth - authentication settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.).  The default is to use the
# traditional Unix authentication mechanisms.
#
# 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


                               [ Cancelled ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Paste Text^T To Spell  ^_ Go To Line
```

The entry indicates the use of the Google Authenticator module

MFA Logon Screen

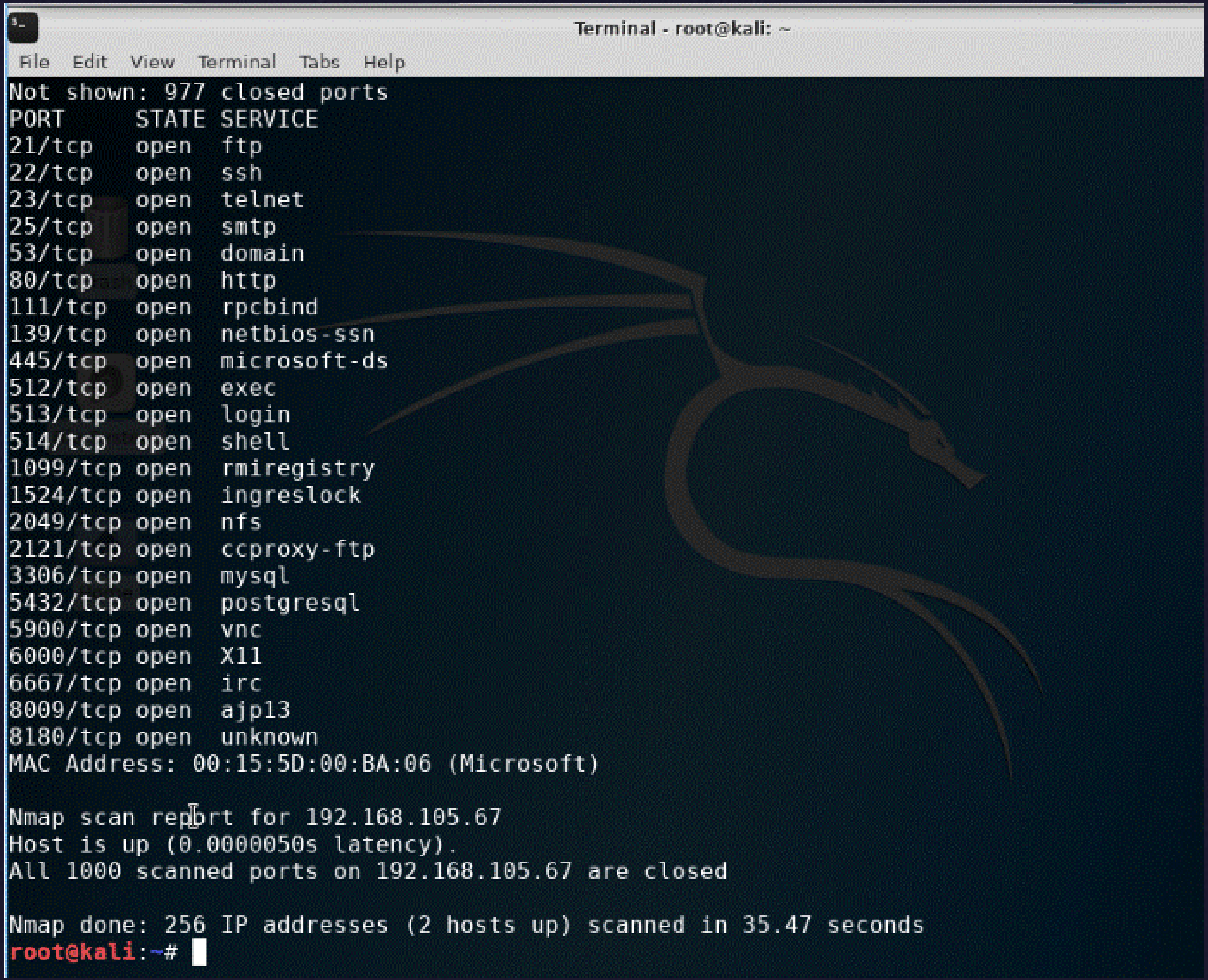
The logon screen shows a verification code is required



Module 6

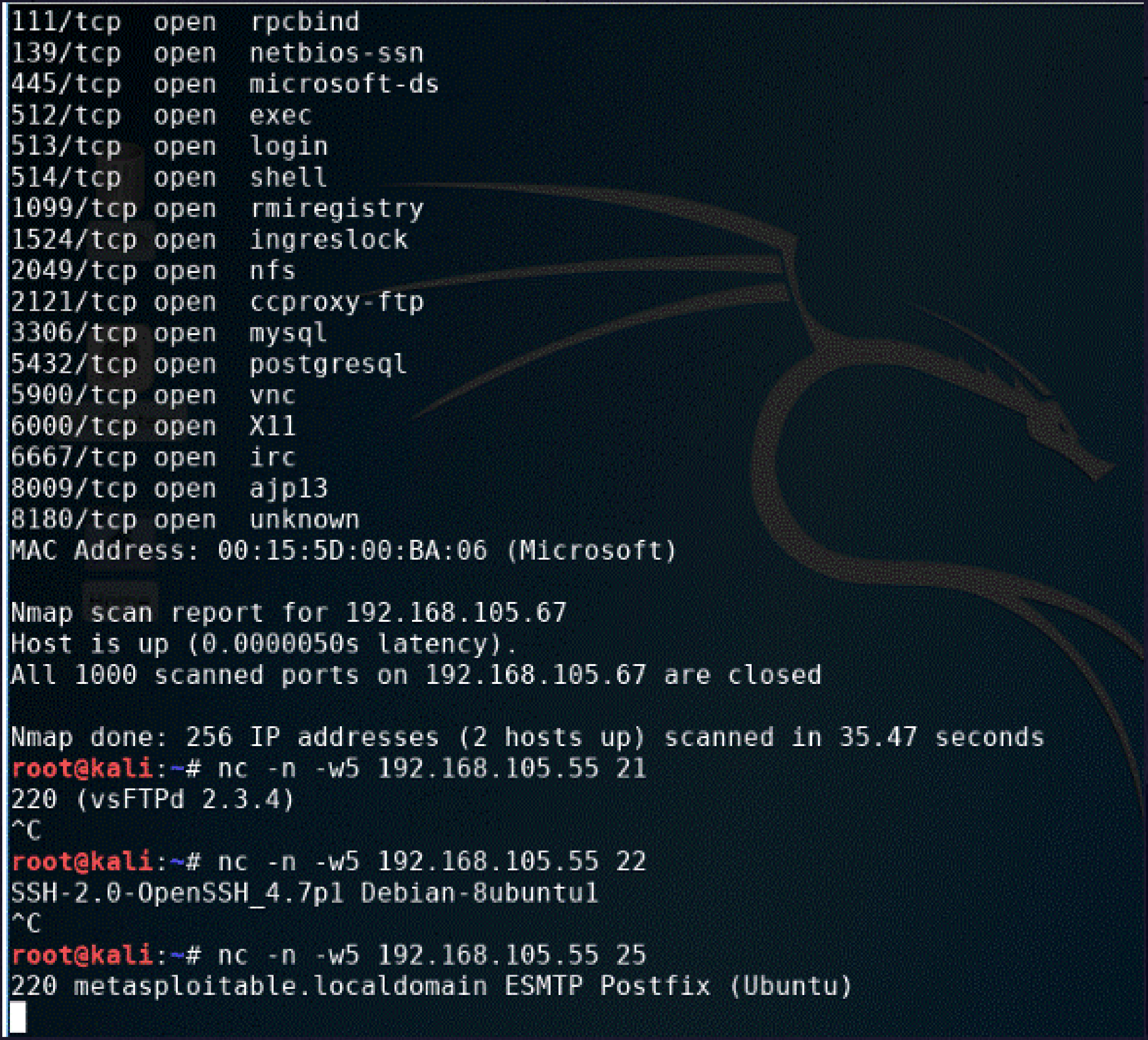
Vulnerability Assessment

Nmap



```
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 35.47 seconds
root@kali:~#
```

Scan result showing both the Kali and Linux Server virtual machines

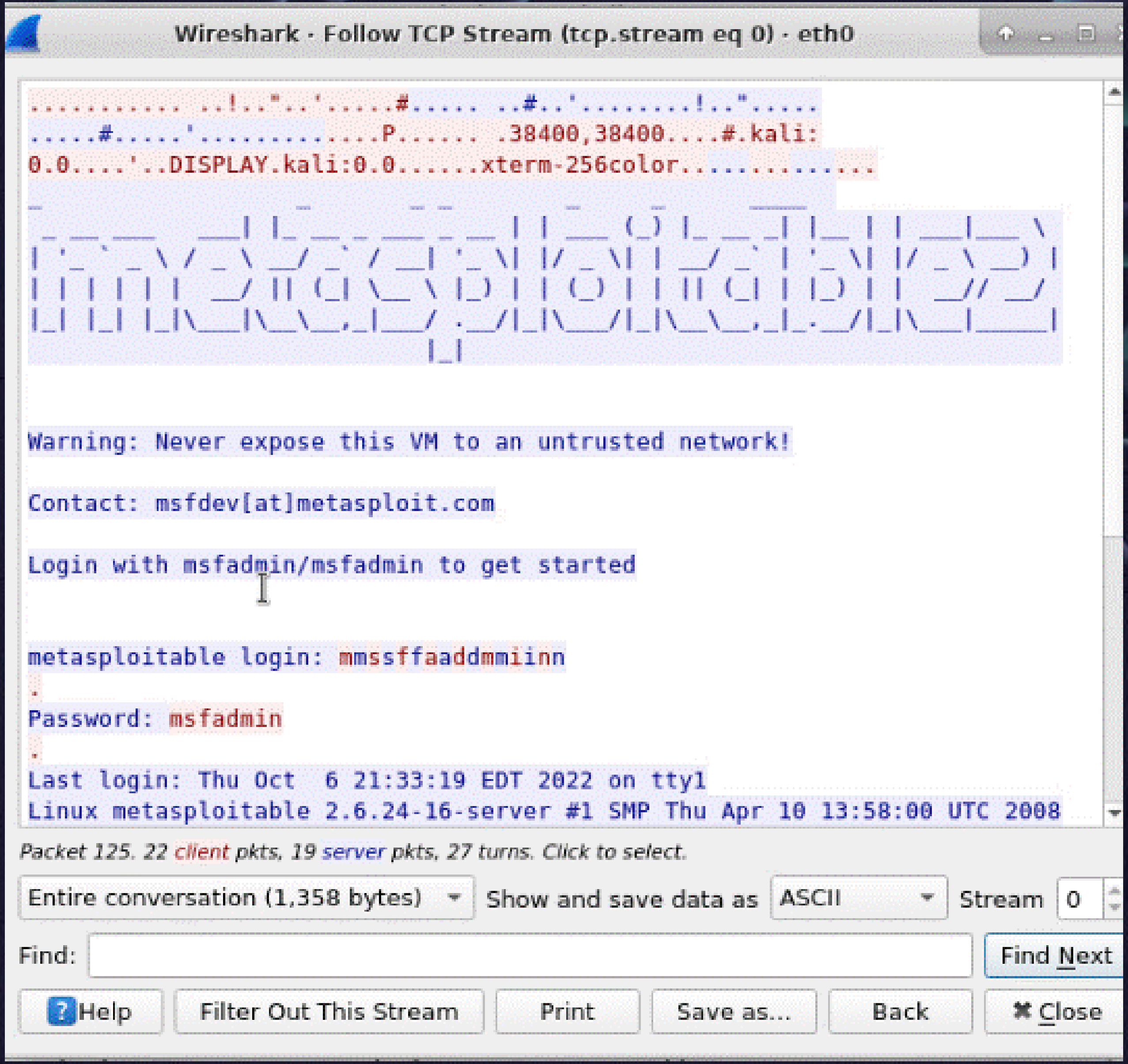


```
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  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 35.47 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)
```

NetCat

Scan result showing both the Kali and Linux Server virtual machines

Wireshark



```
........... ..!.."..'.....#..... ..#..'........!..".....
.....#.....'............P...... .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: mmssffaaddmmiinn
.
Password: msfadmin
.
Last login: Thu Oct  6 21:33:19 EDT 2022 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008
```

Packet 125. 22 client pkts, 19 server pkts, 27 turns. Click to select.

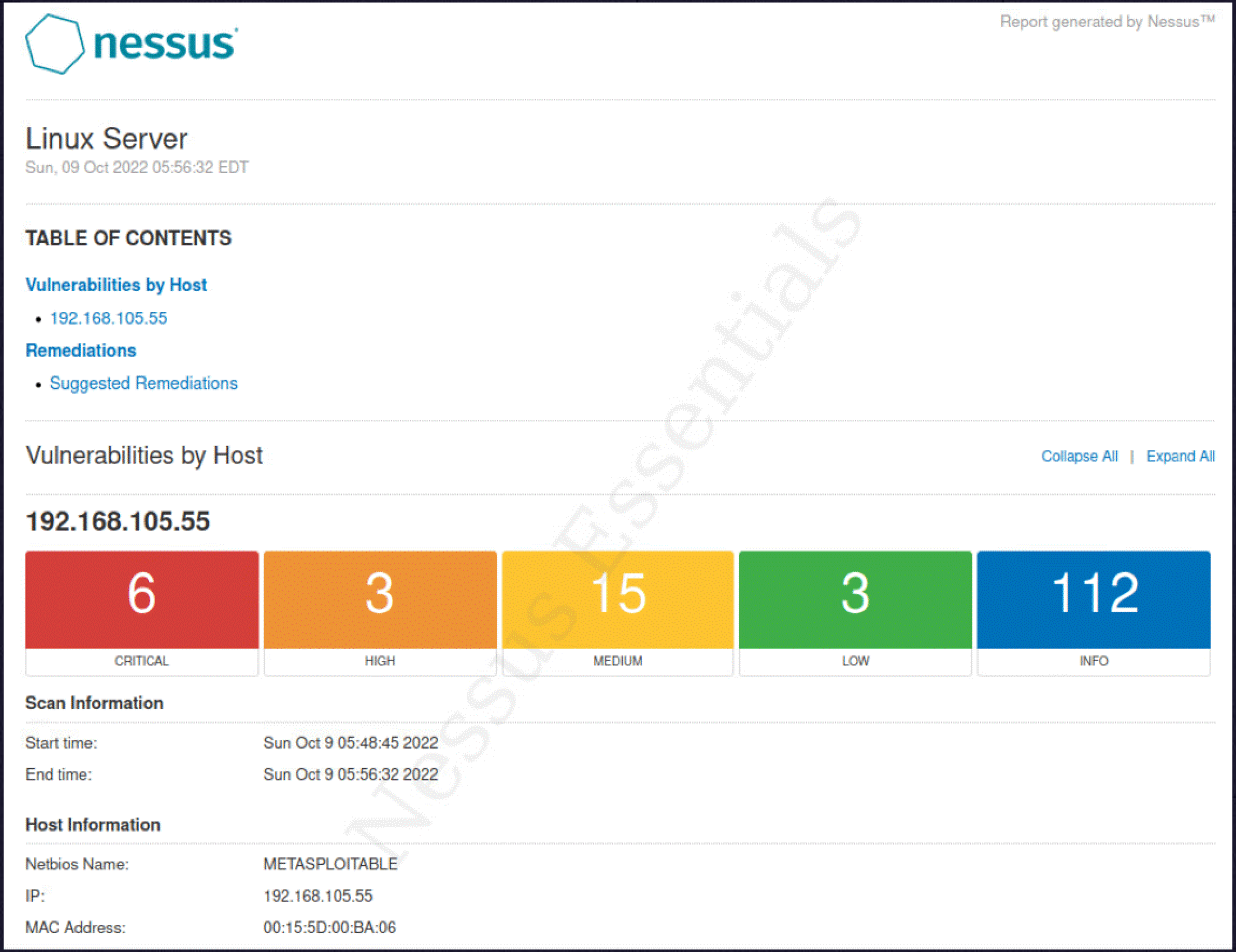
Entire conversation (1,358 bytes) Show and save data as ASCII Stream 0

Find:

Wireshark - Follow TCP Stream window showing the Telnet username and password

Nessus

High-level view of the Nessus vulnerability scan report (categories of vulnerability are in different colors)



Report generated by Nessus™

nessus

Linux Server

Sun, 09 Oct 2022 05:56:32 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

192.168.105.55

6	3	15	3	112
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Sun Oct 9 05:48:45 2022
End time:	Sun Oct 9 05:56:32 2022

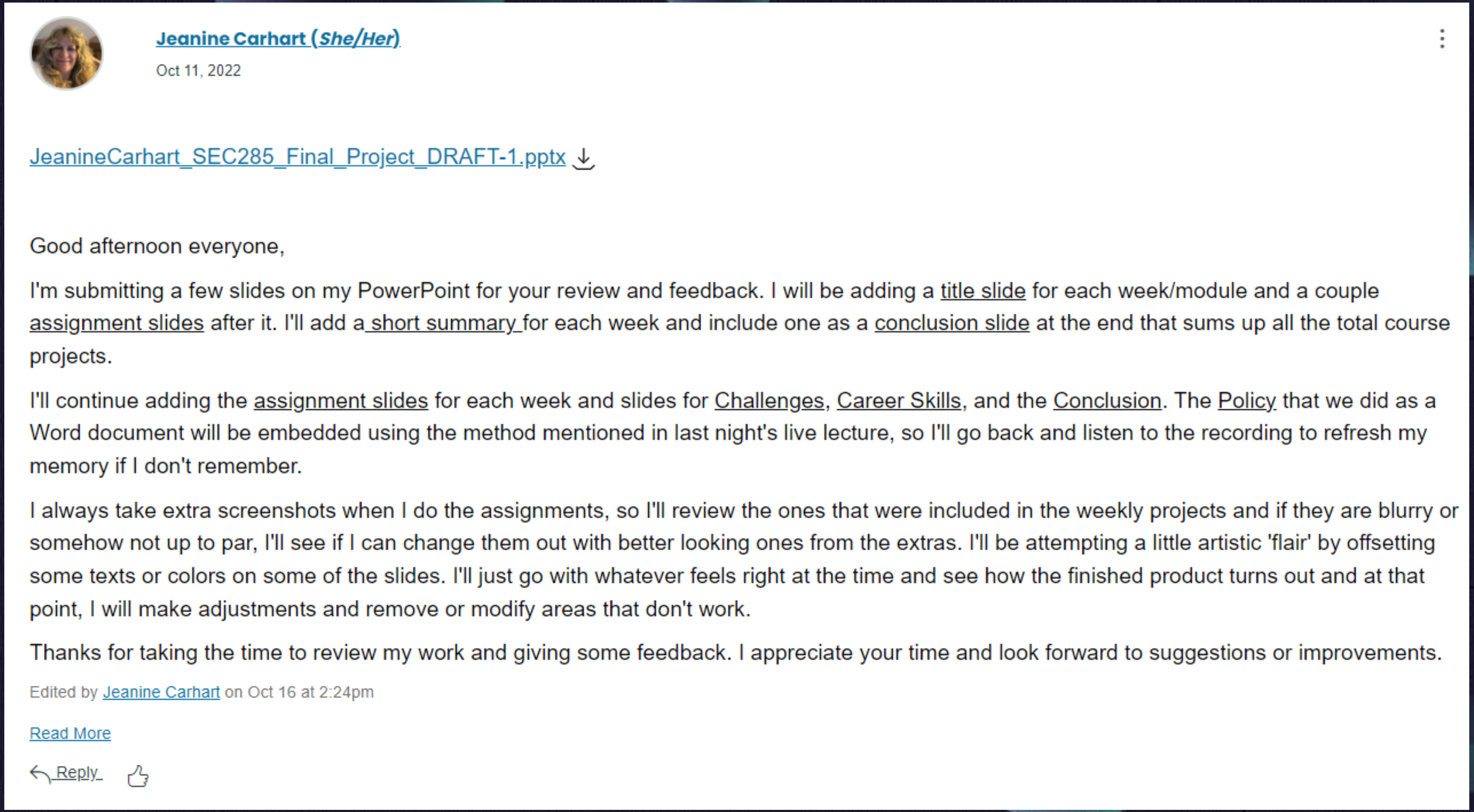
Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.105.55
MAC Address:	00:15:5D:00:BA:06

Module 7

Share, Review, & Reflect

Share



Jeanine Carhart (*She/Her*)

Oct 11, 2022

JeanineCarhart_SEC285_Final_Project_DRAFT-1.pptx

Good afternoon everyone,

I'm submitting a few slides on my PowerPoint for your review and feedback. I will be adding a title slide for each week/module and a couple assignment slides after it. I'll add a short summary for each week and include one as a conclusion slide at the end that sums up all the total course projects.

I'll continue adding the assignment slides for each week and slides for Challenges, Career Skills, and the Conclusion. The Policy that we did as a Word document will be embedded using the method mentioned in last night's live lecture, so I'll go back and listen to the recording to refresh my memory if I don't remember.

I always take extra screenshots when I do the assignments, so I'll review the ones that were included in the weekly projects and if they are blurry or somehow not up to par, I'll see if I can change them out with better looking ones from the extras. I'll be attempting a little artistic 'flair' by offsetting some texts or colors on some of the slides. I'll just go with whatever feels right at the time and see how the finished product turns out and at that point, I will make adjustments and remove or modify areas that don't work.

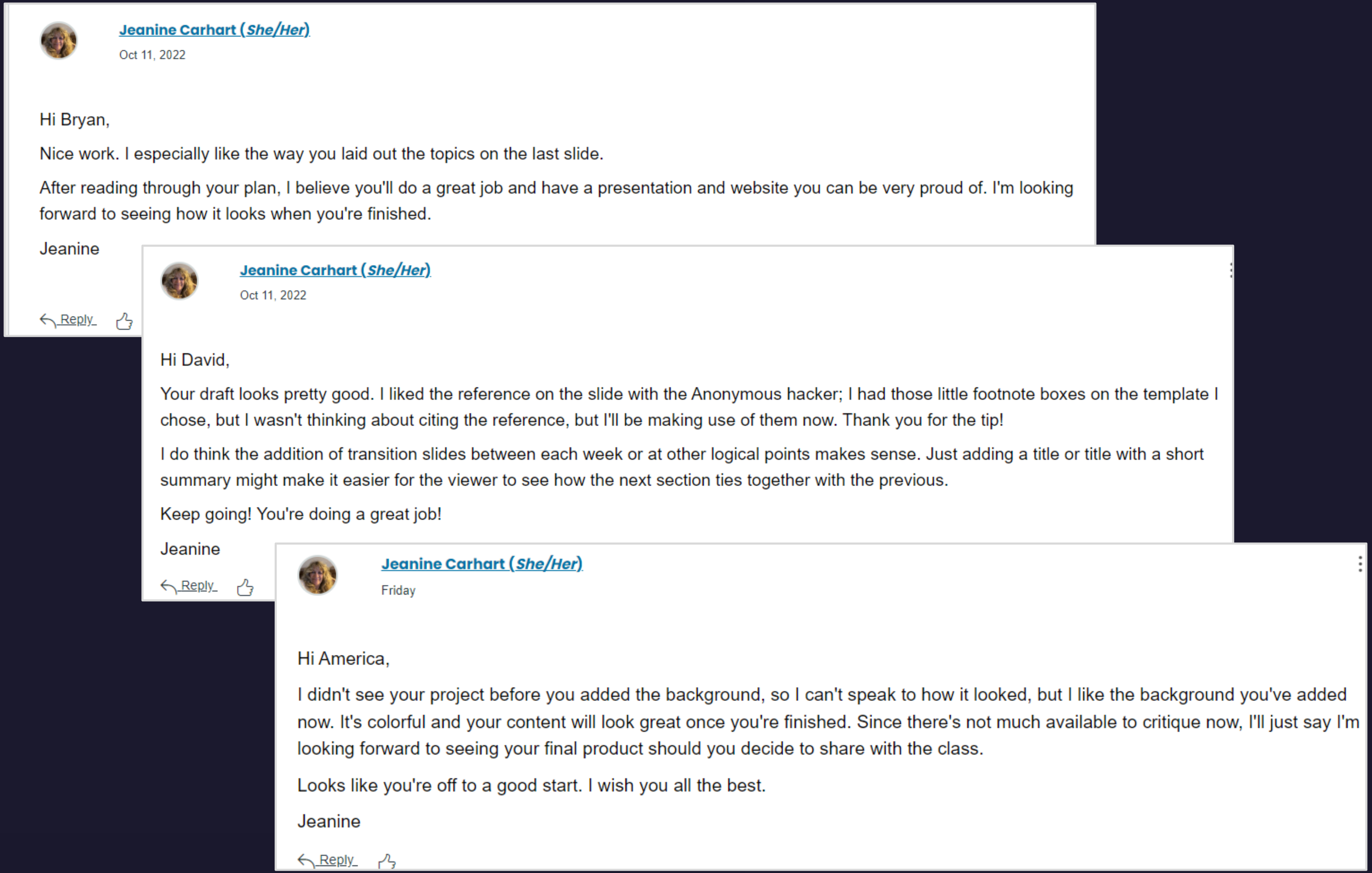
Thanks for taking the time to review my work and giving some feedback. I appreciate your time and look forward to suggestions or improvements.

Edited by Jeanine Carhart on Oct 16 at 2:24pm

Share a few slides from your final project. Briefly explain your plan on organizing and presenting the content. Seek suggestions if needed

Review

Review your peers' work in progress. Identify positive aspects of the work as well as areas for improvement. Give professional feedback.



Jeanine Carhart (*She/Her*)
Oct 11, 2022

Hi Bryan,

Nice work. I especially like the way you laid out the topics on the last slide.

After reading through your plan, I believe you'll do a great job and have a presentation and website you can be very proud of. I'm looking forward to seeing how it looks when you're finished.

Jeanine

Jeanine Carhart (*She/Her*)
Oct 11, 2022

Hi David,

Your draft looks pretty good. I liked the reference on the slide with the Anonymous hacker; I had those little footnote boxes on the template I chose, but I wasn't thinking about citing the reference, but I'll be making use of them now. Thank you for the tip!

I do think the addition of transition slides between each week or at other logical points makes sense. Just adding a title or title with a short summary might make it easier for the viewer to see how the next section ties together with the previous.

Keep going! You're doing a great job!

Jeanine

Jeanine Carhart (*She/Her*)
Friday

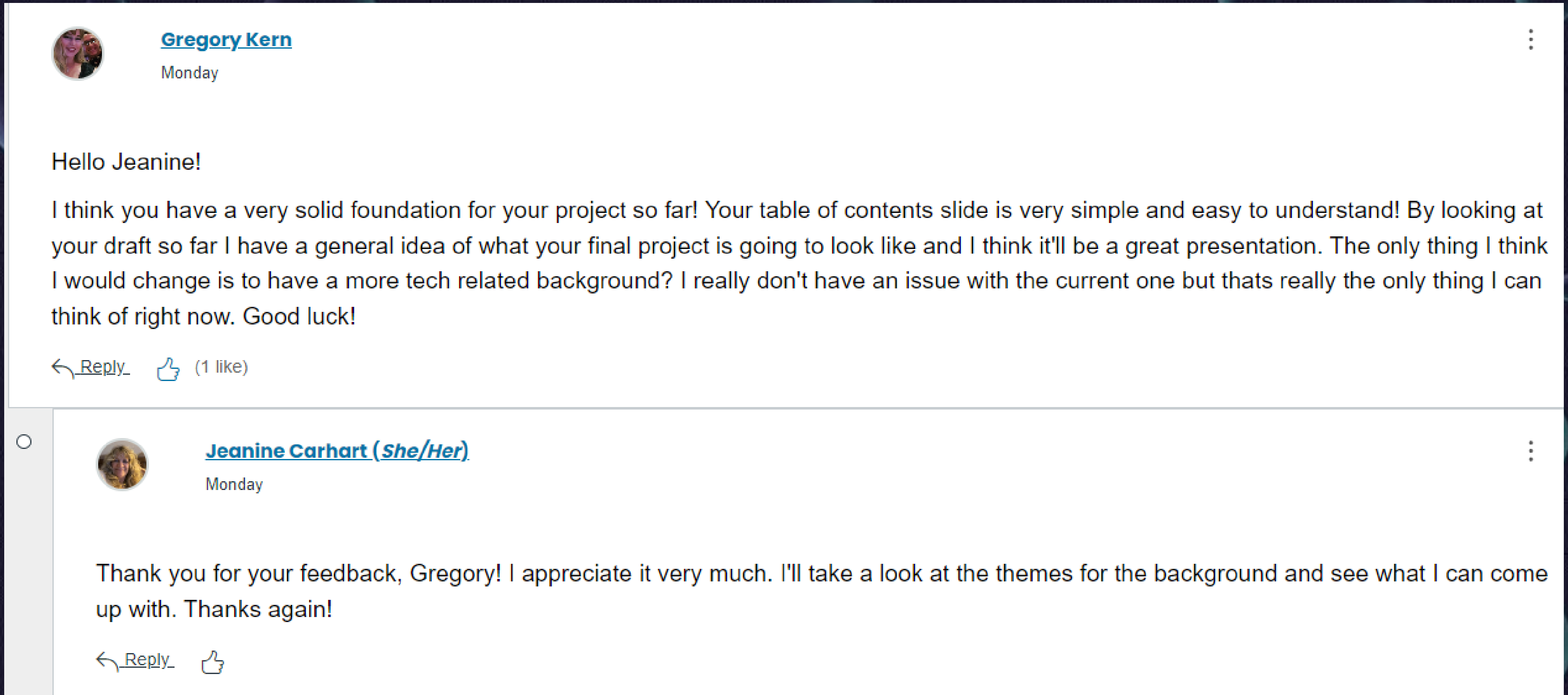
Hi America,

I didn't see your project before you added the background, so I can't speak to how it looked, but I like the background you've added now. It's colorful and your content will look great once you're finished. Since there's not much available to critique now, I'll just say I'm looking forward to seeing your final product should you decide to share with the class.

Looks like you're off to a good start. I wish you all the best.

Jeanine

Reflect



Gregory Kern

Monday

Hello Jeanine!

I think you have a very solid foundation for your project so far! Your table of contents slide is very simple and easy to understand! By looking at your draft so far I have a general idea of what your final project is going to look like and I think it'll be a great presentation. The only thing I think I would change is to have a more tech related background? I really don't have an issue with the current one but thats really the only thing I can think of right now. Good luck!

Jeanine Carhart (She/Her)

Monday

Thank you for your feedback, Gregory! I appreciate it very much. I'll take a look at the themes for the background and see what I can come up with. Thanks again!

Reflect on your peers' feedback and respond in an open and friendly manner. Describe how you plan to complete your final project deliverable.

Challenges

Challenges

<u>InfoSec had some issues on some assignments:</u>

- Mouse stopped working in black areas on VM
- Issues caused exercises to time out prematurely
- Password wasn’t working
- Help Desk wasn’t able to help

Career Skills

Career Skills

- ✓ Research
- ✓ Patience
- ✓ Problem Solving
- ✓ Overcoming Obstacles
- ✓ Flexibility
- ✓ Persistence
- ✓ Analytical Thinking
- ✓ Attention to Detail
- ✓ Resourcefulness

Conclusion

Conclusion

We learned about the challenges of securing information and why we need to protect it. We looked at different types of threat actors and how to defend against these types of attacks.

Cryptography was our next topic. We covered the basics and different types of cryptographic algorithms and attacks on cryptography, digital certificates, how to implement cryptography, and different transport encryption protocols, as well as public key infrastructure (PKI).

We reviewed different networking and server attacks and how to secure them. The internet has had a huge impact on our lives and through the Internet of Things (IoT), it’s a primary way for threat actors to launch attacks on any device connected to it.

continued...

Conclusion continued

We had the opportunity to explore securing wireless networks, clients and applications and mobile devices. We discussed wireless hacking and the vulnerabilities and techniques to enhance security on them and also wireless communication devices.

Authentication and secure management of user accounts was covered. We looked at best practice for access control and ways to implement it, as well as identity and access services.

Vulnerability assessment and data security was an interesting topic. We now understand how to create and maintain a business continuity plan and how to use the vulnerability data to mitigate the risk to a business.

Finally, we had practice exams to get us ready for our CompTIA certifications.