

FUNDAMENTALS OF INFORMATION SECURITY



**SEC
285**

Louie Venegas

What This Project Covers

Module 2, Asymmetric key encryption: encrypting and decrypting files with GPG in a Kali terminal.

Module 3, Stateful firewall: changing iptables policy to drop inbound traffic, then scanning with Nmap.

Module 4, BYOD security policy: a written device policy for a fictional corporation.

Module 5, Multifactor authentication: adding Google Authenticator to Linux logon.

Module 6, Vulnerability assessment: Nmap, NetCat, Wireshark, and Nessus against lab targets.

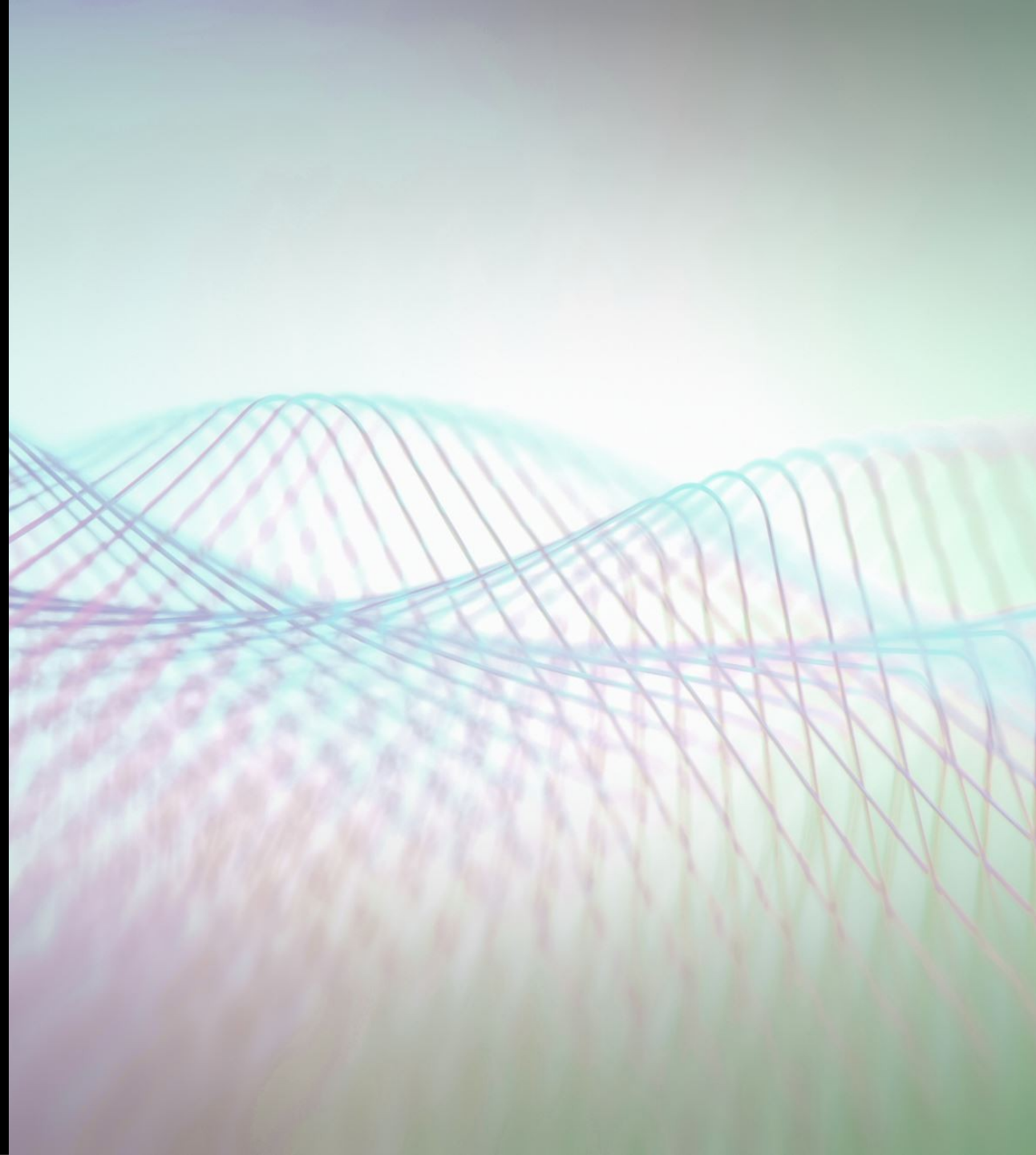
SEC285

MODULE 2

ASYMMETRIC KEY ENCRYPTION



Louie Santino Venegas



Asymmetric Key Encryption is used every time a https connection is established without most users even knowing it happens. It is also known as public key encryption. “is a type of cryptographic protocol that uses a public and private key to exchange encrypted data between two users or devices” (Ingles, 1997).

Another use for this type of technology is encrypting sensitive data before sending it to someone or storing it on a device. In the following two slides are screenshots of me using software called GPG also called GnuPg in a kali terminal. A brief explanation is provided to explain the contents of each.

THIS SCREEN SHOT IS
AFTER THE INITIAL
PROCESS OF
ENCRYPTION.
THE ORIGINAL AND
ENCRYPTED FILE ARE
DISPLAYED IN THE
DIRECTORY, AND BOTH
ENCRYPTED AND
PLAINTEXT FORM.

```
root@kali:~# ls test*
testfile.txt  testfile.txt.gpg
root@kali:~# cat testfile.txt
This is a text file that we will encrypt with gpg my name is Louie Santino Venegas 1/12/2024
root@kali:~# cat testfile.txt.gpg
00000Y#o00510QM0
000J000
00C0$-0wc?0/Q0M00-0Froot@kali:~# 2R000-00n~8 i00\q0000q:0`000^x0!0J;J00000000D'd00+000
```

```
root@kali:~# cat testfile.txt
cat: testfile.txt: No such file or directory
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 text file that we will encrypt with gpg my name is Louie Santino Venegas 1/12/2024
root@kali:~#
```

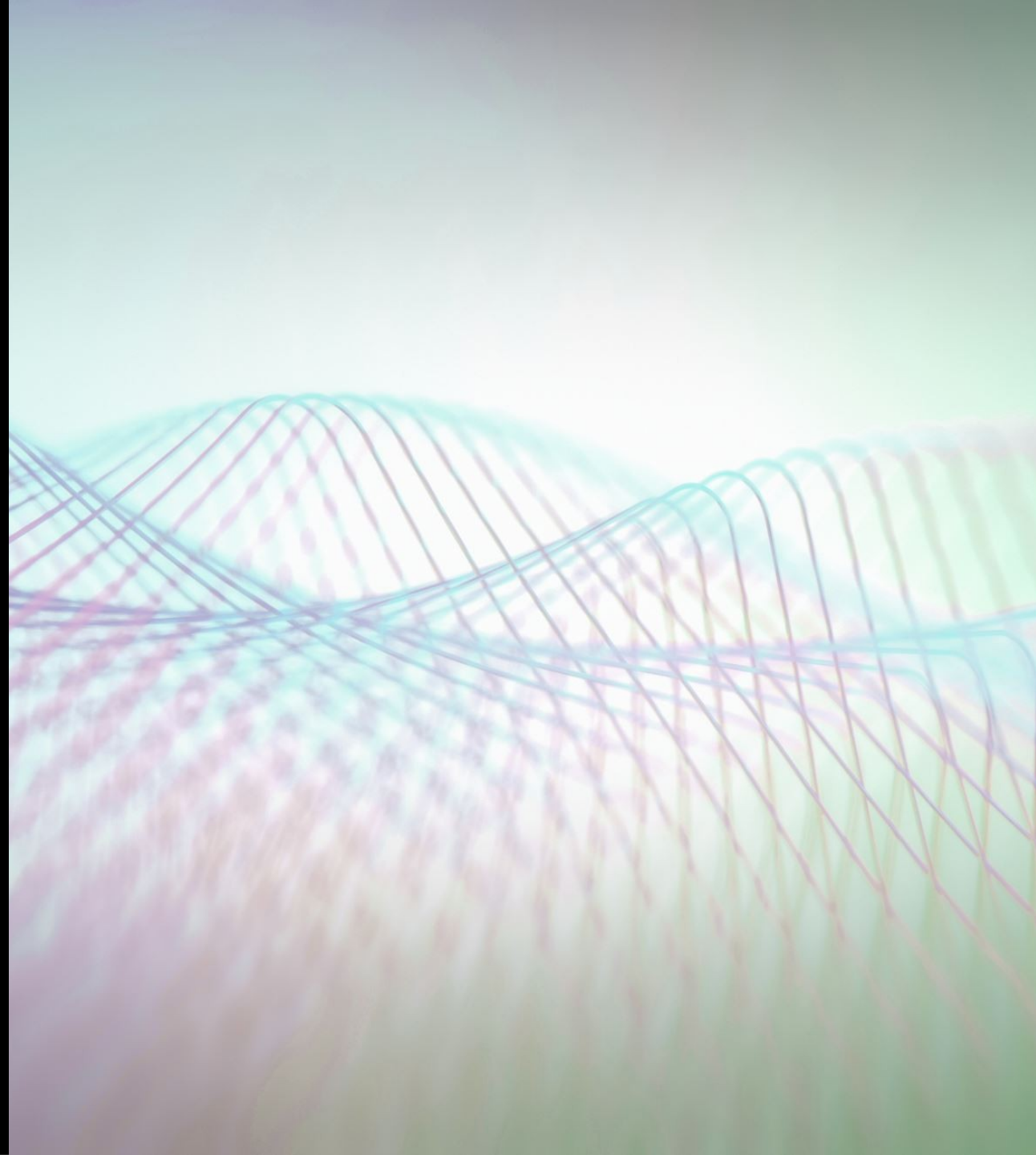
**FILE
DECRYPTION
INCLUDES THE
ENCRYPTED FILE,
THE DECRYPTING
PROCESS AND LIST
OF BOTH THE
ENCRYPTED AND
PLAINTEXT FILE.**

SEC285

MODULE 3
STATEFUL FIREWALL



Louie Santino Venegas



WHAT EFFECT DOES
THE SUDO IPTABLES
--POLICY INPUT
DROP COMMAND
HAVE ON THE ACCESS
TO COMPUTING
RESOURCES?

Answer

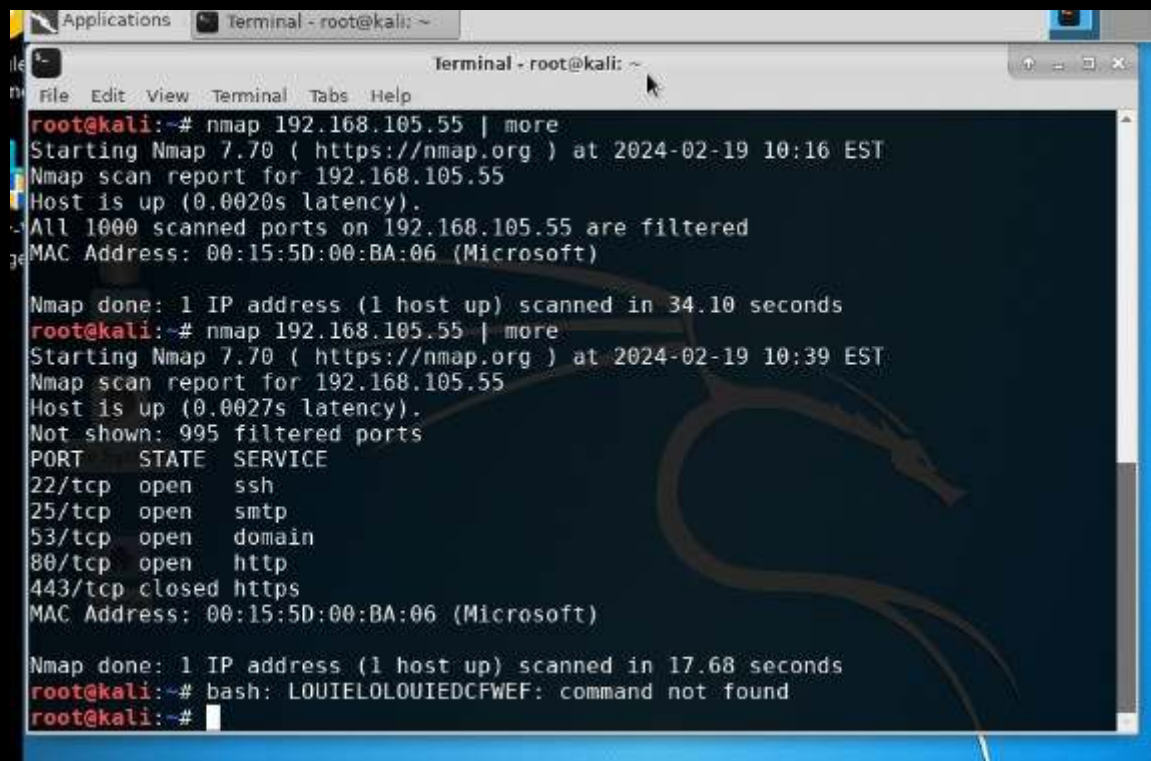
*Sudo iptables -policy INPUT
DROP*

Essentially this command changes the iptables firewall policy on a Linux system. The result of this is that all incoming packets are dropped until or unless otherwise specified.

References

Working with iptables. (n.d.). Network World.

<https://www.networkworld.com/article/930788/working-with-iptables.html>



```
root@kali:~# nmap 192.168.105.55 | more
Starting Nmap 7.70 ( https://nmap.org ) at 2024-02-19 10:16 EST
Nmap scan report for 192.168.105.55
Host is up (0.0020s 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 34.10 seconds
root@kali:~# nmap 192.168.105.55 | more
Starting Nmap 7.70 ( https://nmap.org ) at 2024-02-19 10:39 EST
Nmap scan report for 192.168.105.55
Host is up (0.0027s 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 17.68 seconds
root@kali:~# bash: LOUIELOLOUIEDCFWEF: command not found
root@kali:~#
```

NMAP SCAN
THIS IS A SCREEN
SHOT OF A KALI
TERMINAL RUNNING
NMAP ON A LINUX
SERVER

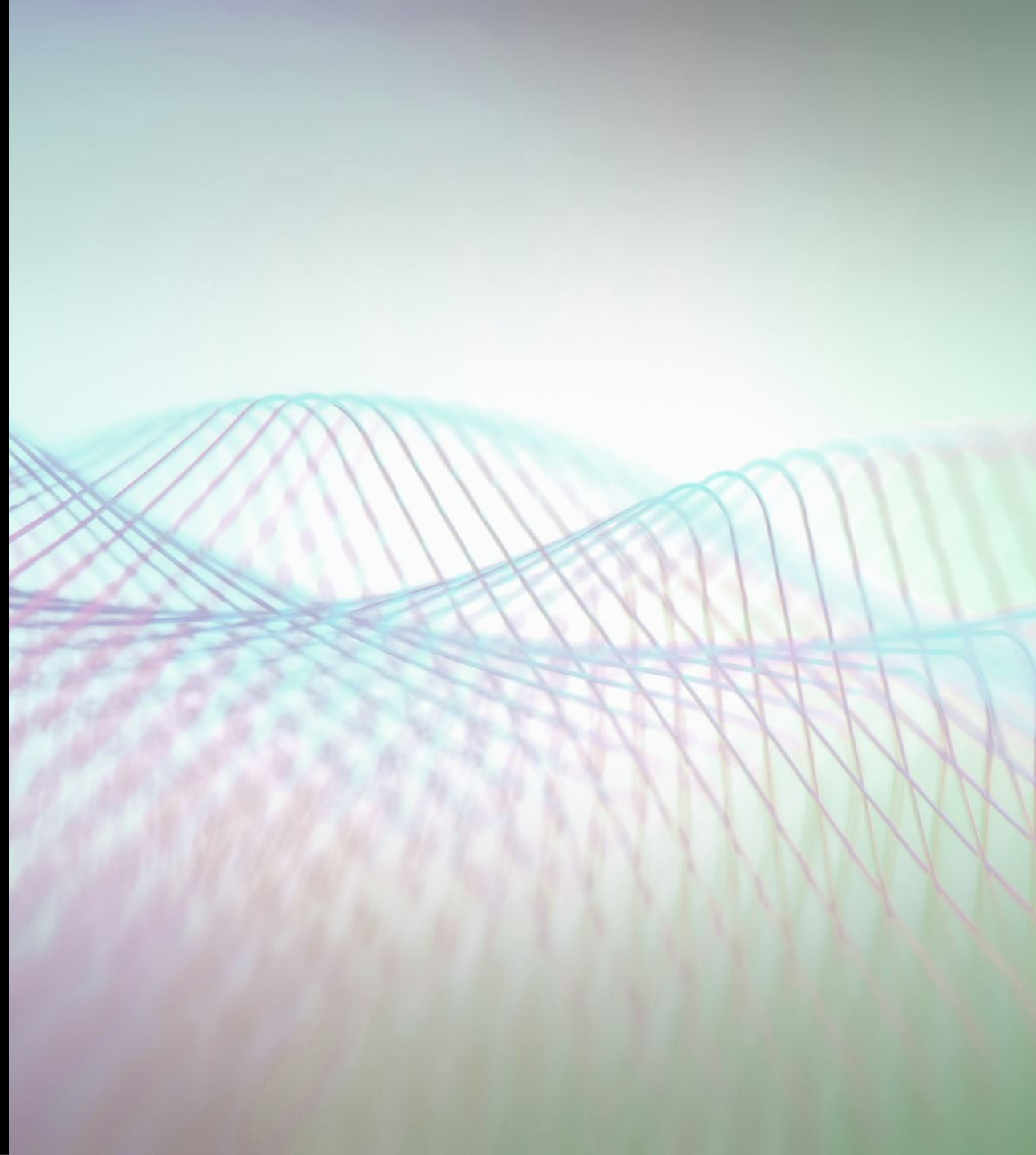
SEC285

MODULE 4

**BRING YOUR OWN
DEVICE (BYOD)**



Louie Santino Venegas



1. Overview:

ABC Fictional Corporation recognizes the productivity and flexibility of allowing employees to use personal devices for business purposes. Our BYOD security policy allows for employees to use personal devices such as smart phones, tablets, laptops and computers while addressing challenges like data security and device management. This policy's goal is to harness the economic, productivity and convenient benefits of allowing this while mitigating the risk involved.

2. Purpose:

Confidentiality, integrity, and availability (CIA) of data is the main purpose of this policy. Having the BYOD security policy helps to identify devices that introduce unnecessary vulnerabilities to the organization's computing resources and data. Another purpose is to address how timely discovery of such vulnerabilities will reduce the attack vector on our organization's computing resources and data. This policy aims to establish a process for regular security assessments and updates to ensure potential vulnerabilities are identified and addressed promptly

3. Scope

This policy will affect all personnel with reasons to use personal devices for work related reasons such as email and work related assignments. The devices that fall under this policy will be personal phones tablets and computers. If assigned technology related assignments but not issued a device to perform the duties on then it is assumed the personnel will be using personal devices. Assume all actions performed work related will be monitored but only to that extent. The exact type of devices will be outlined in the policy and the required security measures. Compliance and consequences will be outlined as well.

4. Policy

Security assessments prior to the acceptance to ABC Corporation's network. For a device to be compliant it must be password protected and up to date, maintain a firewall feature and anti virus software of some type. The operating system since so many exist is not restricted except that it is up to date with security patches and allows for updates automatically. Devices not in compliance will not be granted access to the network. The IT department will monitor for compliance as well as enforce it. All access to the network must be done through the designated applications and automatically logged out when no longer needed to prevent unauthorized access. Two step verification via company application will be required.

7. Definitions and Terms:

BYOD: (bring your own device) defined as any personal device used on our network, mobile devices are but not limited to cell phone tablets and laptops.

CIA(Confidentiality, Integrity and Availability) in regards to data stored for and used by people associated with our organization.

HIPAA(Health Insurance Portability and Accountability Act)

PCI-DSS (Payment Card Industry Data Security Standard)

8. I

Date of change	Responsible	Summary of change
February 2024	L. Venegas	Adapted from the SANS BYOD policy template

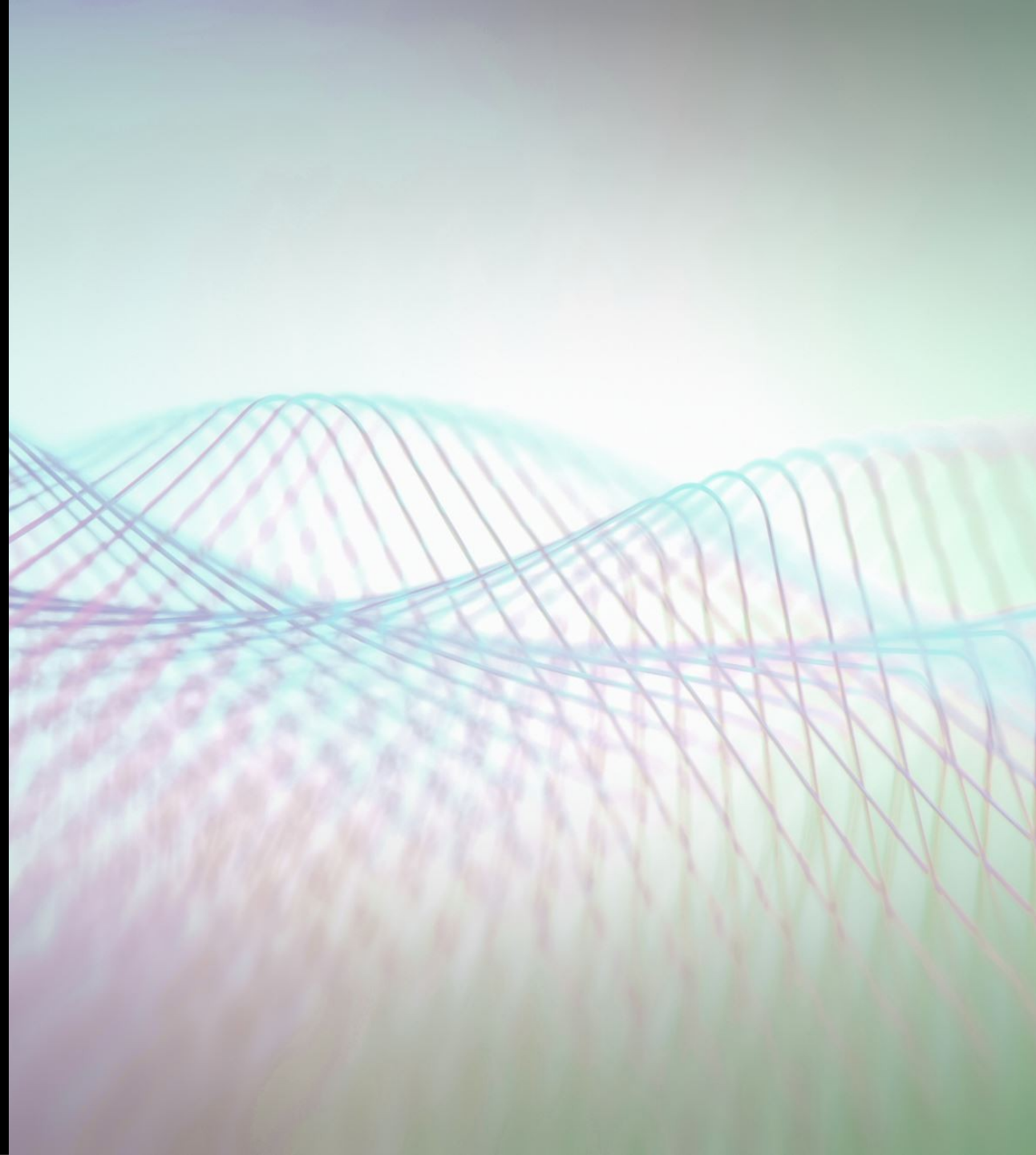
SEC285

MODULE 5

**MULTIFACTOR
AUTHENTICATION (MFA)**

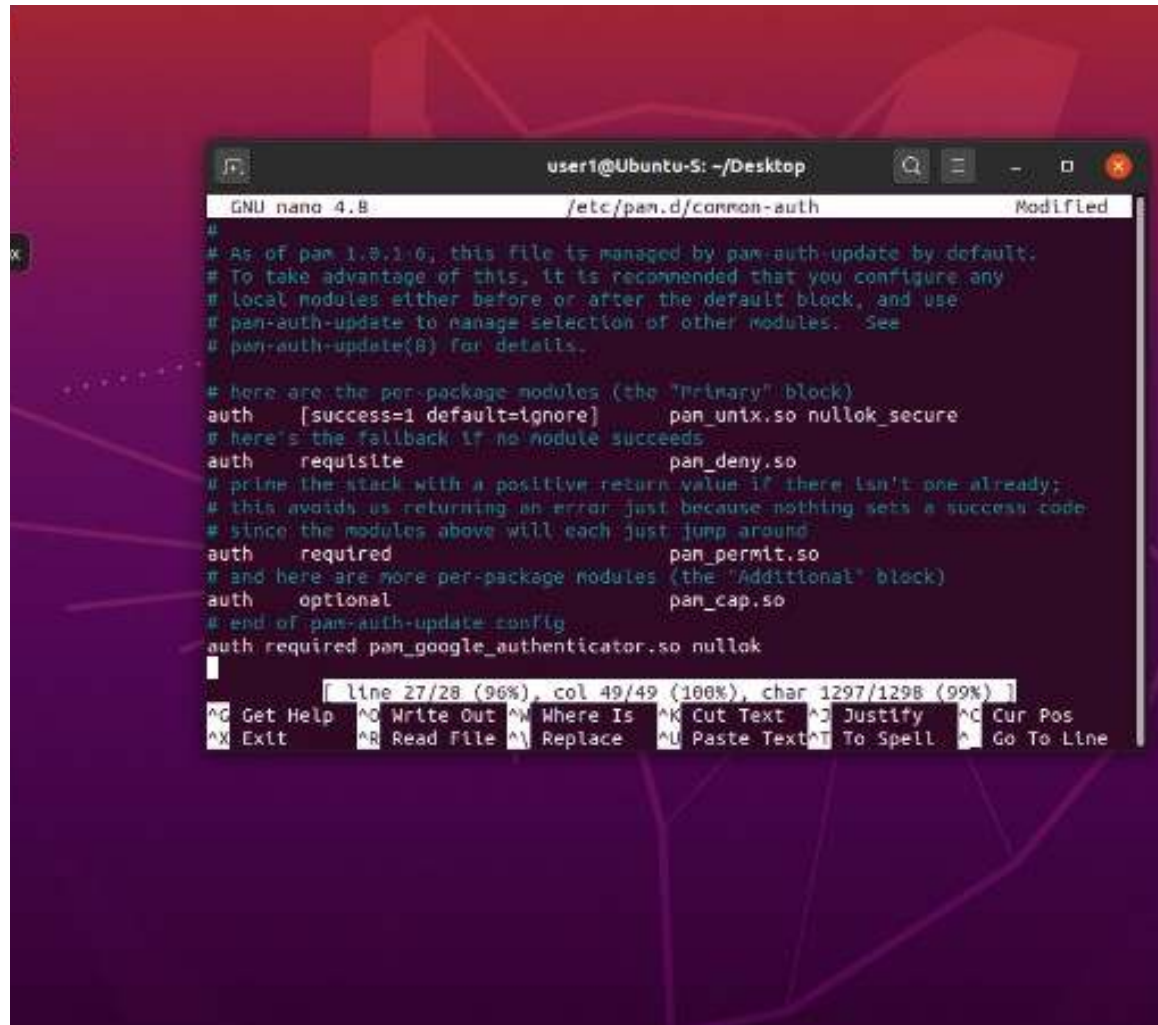


Louie Santino Venegas



Common-auth Configuration File

The common-auth configuration file, with the entry enabling the Google Authenticator module.



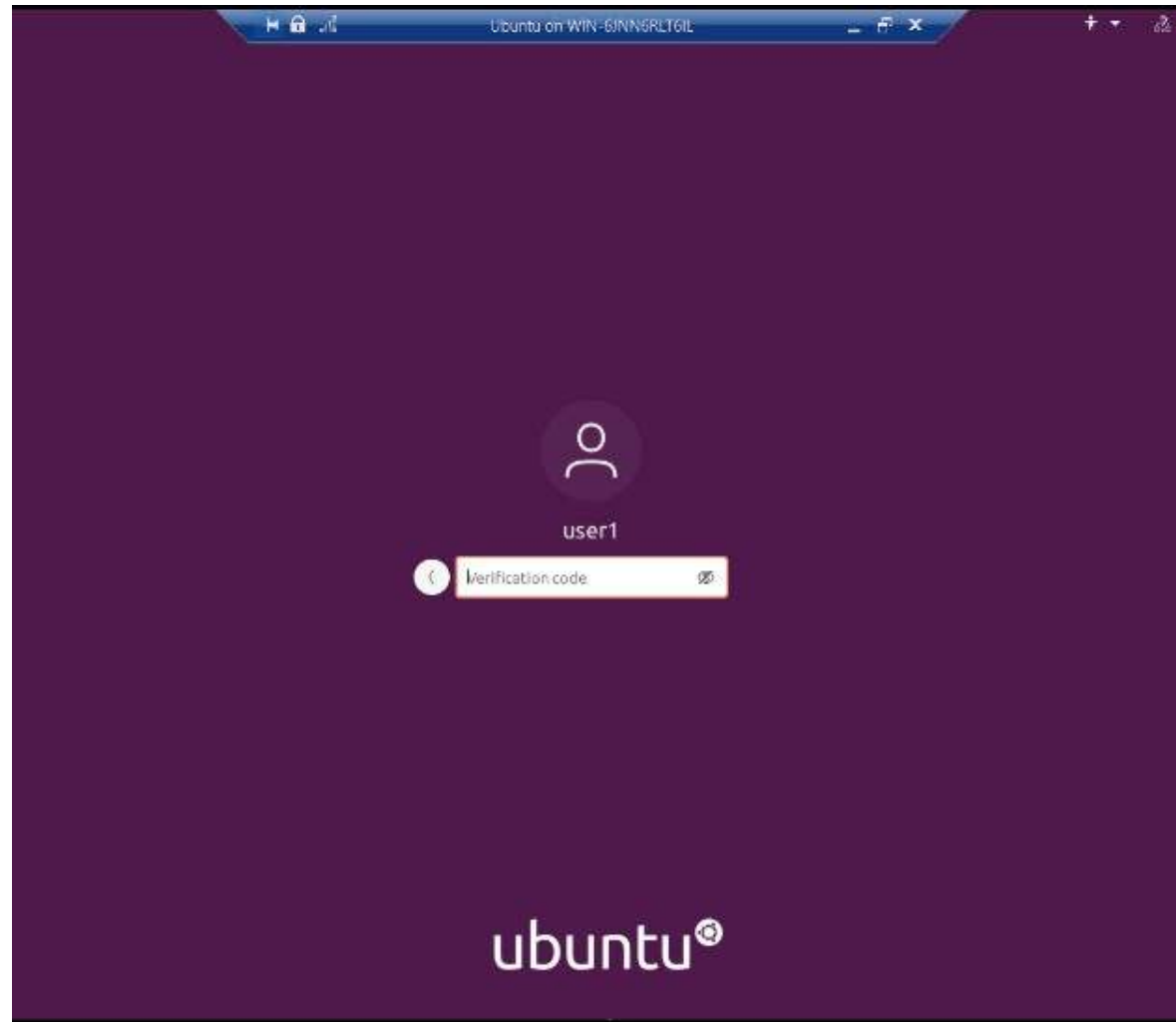
```
GNU nano 4.8 /etc/pam.d/common-auth Modified
#
# As of pam 1.5.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of 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

line 27/28 (96%), col 49/49 (100%), char 1297/1298 (99%)
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^I Replace  ^U Paste Text ^T To Spell  ^_ Go To Line
```

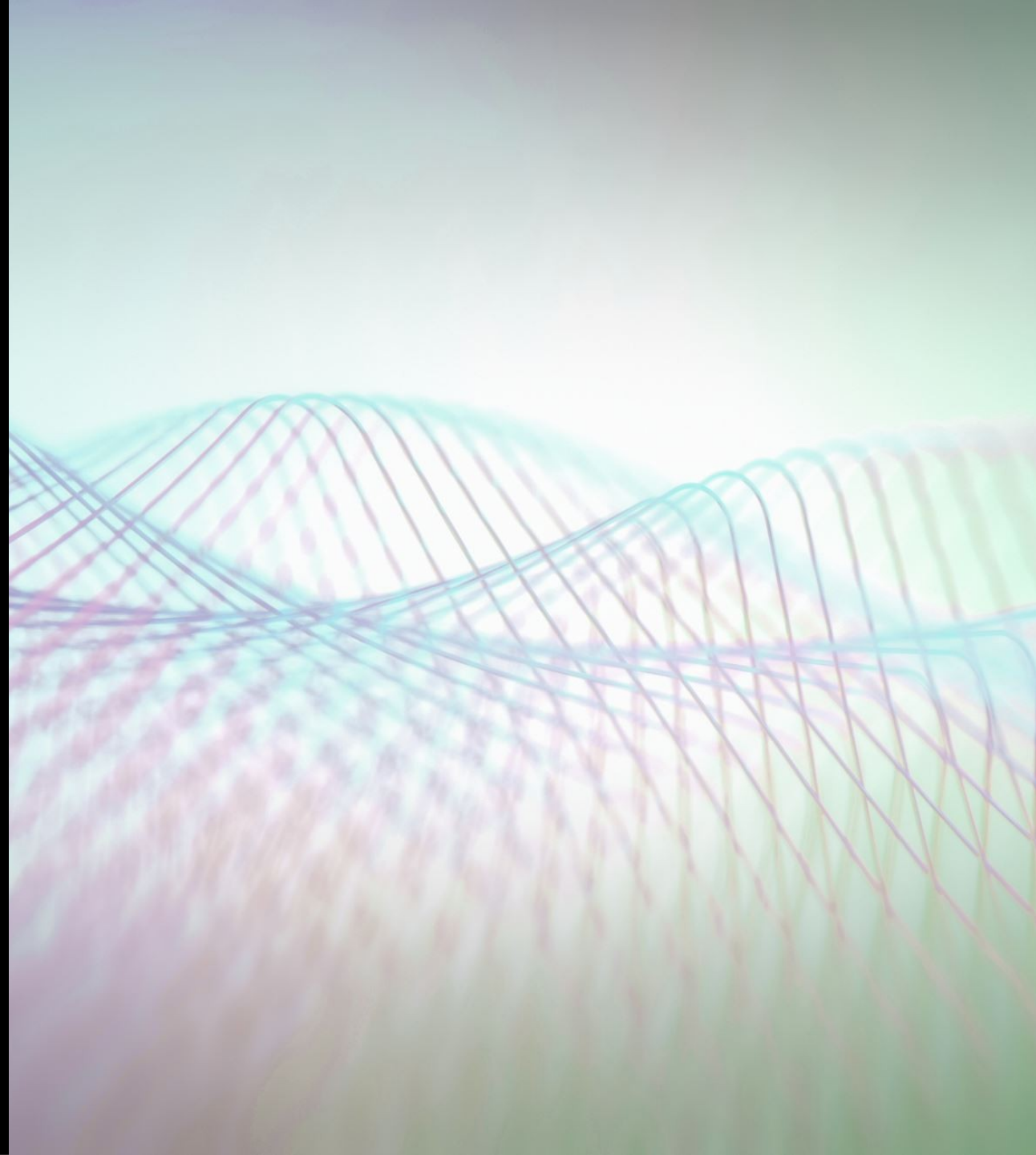
MFA Logon Screen

The logon screen prompting for a verification code.



SEC285
MODULE 6
**VULNERABILITY
ASSESSMENT**

Louie Santino Venegas



```
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
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgres
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
```

```
all 1714 scanned ports on 192.168.105.67 are closed
MAC Address: 00:15:5D:00:BA:05 (Microsoft)
```

```
Nmap done: 256 IP addresses (2 hosts up) scanned in 33.012 seconds
msfadmin@metasploitable:~$ nmap -PN 192.168.105.0/24 -oN /tmp/venegas_41112084.txt
284
```

Applications Terminal - root@kali: ~ 10:56 root

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)

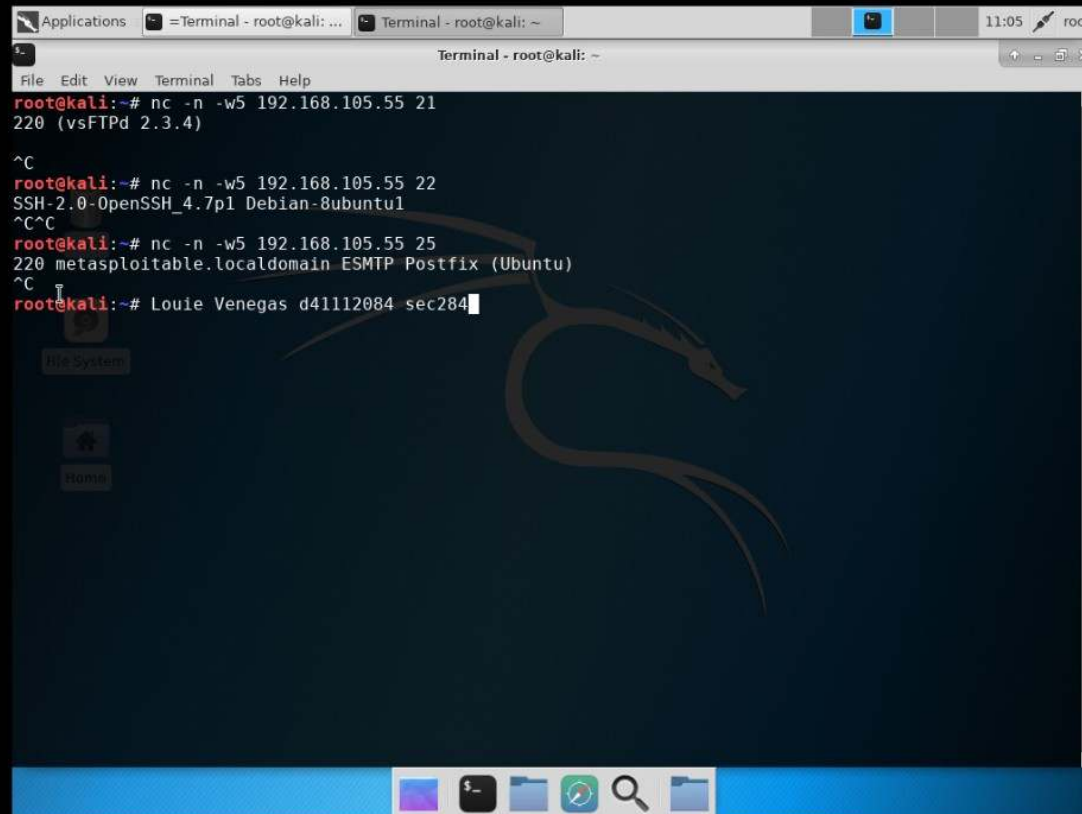
Nmap scan report for 192.168.105.67
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.105.67 are closed

Nmap done: 256 IP addresses (2 hosts up) scanned in 35.54 seconds

root@kali:~# Louie Venegas d41112084 SEC285

View Fullscreen

Send Ctrl+



The screenshot shows a Kali Linux desktop environment. A terminal window is open, displaying the following commands and output:

```
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^C
root@kali:~# nc -n -w5 192.168.105.55 25
220 metasploitable.localdomain ESMTD Postfix (Ubuntu)
^C
root@kali:~# Louie Venegas d41112084 sec284
```

The terminal window has a menu bar with 'File', 'Edit', 'View', 'Terminal', 'Tabs', and 'Help'. The desktop background is dark blue with a dragon logo. The taskbar at the bottom contains icons for various applications, including a file manager, terminal, and web browser.

Applications *eth0 Wireshark - ... =Terminal - ... Terminal - ro... Terminal - ro... 11:11 root

File Edit View Go

tcp.stream eq 0

Time
51 75.18710156
52 75.18925976
53 75.18927806
54 75.18944040
55 75.19127080
70 85.19360790
71 85.19363250
72 85.19550260

Frame 54: 93 bytes on wire (744 bits) captured (93 bytes) over Ethernet II, Src: ... Internet Protocol Version 4, Dst: ... Transmission Control Protocol, Seq: ... Telnet

000 00 15 5d 00 b
010 00 4f 7d df 4
020 69 37 95 b0 f
030 00 e5 54 0d 0
040 1c a8 ff fd 6
050 21 ff fb 22 f

Wireshark - Follow TCP Stream (tcp.stream eq 0) - eth0

```
.....!..".'.#.....#..'.!..".  
.....#.....'.P.....38400,38400....#.kali:0.0....'..DISPLAY.kali:  
0.0.....xterm-256color.....  
  
[ASCII Art]
```

Warning: Never expose this VM to an untrusted network!

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with msfadmin/msfadmin to get started

metasploitable login: **mmssffaaddmminn**

Password: **msfadmin**

Last login: Mon Feb 5 10:57:26 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by

Packet 80. 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: Louie Venegas d41112084 sec284 Find Next

Help Filter Out This Stream Print Save as... Back Close

wireshark_eth0 0 (0.0%) Profile: Default

Activities Firefox Web Browser Ubuntu on WIN-6JNN6RLT6IL

Nessus Essentials / Folder x Linus Server x Linus Server x

file:///tmp/mozilla_ubuntu0/Linus_Server_zf37hb.html

Report generated by Nessus™

nessus

Linus Server

Wed, 07 Feb 2024 11:24:21 EST

TABLE OF CONTENTS

- [Vulnerabilities by Host](#)
 - 192.168.105.55
- [Remediations](#)
 - [Suggested Remediations](#)

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: Wed Feb 7 11:16:40 2024
End time: Wed Feb 7 11:24:21 2024

Host Information

Netbios Name: METASPLOITABLE
IP: 192.168.105.55
MAC Address: 00:15:5D:00:BA:06
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

Ingles, S. (1997, October 17). *Asymmetric Encryption*.
<https://www.webopedia.com/definitions/asymmetric-encryption/>. Retrieved
February 15, 2024, from <https://www.webopedia.com/definitions/asymmetric-encryption/>