



Information Security

Faith Burnett
DeVry University

Introduction

This presentation will go over technologies and best practices of information security

Overview

- Cryptography
- Network Attacks and Defenses
- Wireless Network and Device Security
- Identity and Access Management
- Risk Management

Cryptography

Decryption

- Content of the plaintext file
- Content of the encrypted file

```
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.
```

File Encryption

- Both the encrypted file and the

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

root@kali:~# cat testfile.txt.gpg
0          i"0u0000n0000{EY0007\26000[/G#J000BÜ00ž>`0C      I)X00_qH0000~0
                                                    /07l0u0T0b
0-000000H[z]
  00q
  04l0#{9s07root@kali:~#
```

Network Attacks and Defenses

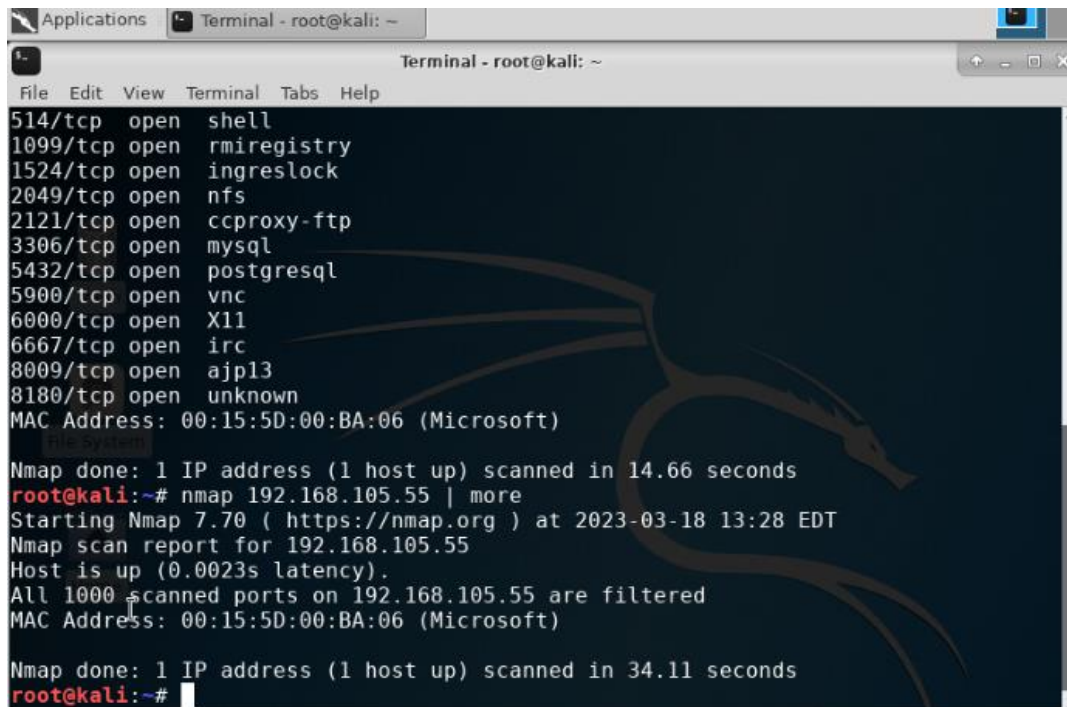
Knowledge Check

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

Answer: Ports are no longer visible, and the scan takes more time to complete.

Nmap Scan

Nmap scan result
of the Linux Server
VM.



```
Applications Terminal - root@kali: ~
Terminal - root@kali: ~
File Edit View Terminal Tabs Help
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 done: 1 IP address (1 host up) scanned in 14.66 seconds
root@kali:~# nmap 192.168.105.55 | more
Starting Nmap 7.70 ( https://nmap.org ) at 2023-03-18 13:28 EDT
Nmap scan report for 192.168.105.55
Host is up (0.0023s 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 34.11 seconds
root@kali:~#
```


Wireless Network and Device Security

BYOD Security Policy



Consensus Policy Resource Community

Bring Your Own Device (BYOD) Security Policy

Free Use Disclaimer: This policy was created by or for the SANS Institute for the internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required.

Last Update Status: Updated March 2023

1. Overview

Mobile devices are used by billions of people, and it has become more common to use them for business. Whether you use a tablet for design, your phone for in-person client meetings, or a laptop to have flexibility to work in the office or at home. The risks involved in having these devices include data breaches, malware and a lack of control on what that device is exposed to outside of the business.

2. Purpose

The aftermath of an attack is expensive and a detriment to your brand especially if it pertains to customer data. It is much more cost efficient to employ a team dedicated to monitoring the security of your network to find vulnerabilities before an attacker can strike.

3. Scope

This policy effects anyone who needs access to the company network this may include full and part-time employees, consultants, temp workers and contract workers. Devices include laptops, tablets, smartphones, external hard drives, thumb drives, portable music players and wearable devices. Employees will be granted access to the network through the network administrator.

4. Policy

As part of our companies dedication to the security of our network all devices are subject to evaluation. Employees must secure their devices with strong passwords, facial recognition and or fingerprint. They will be required to set a lock on all devices to ensure nobody else has access to the device if lost. Lastly each device should have the most recent software and antivirus update. InfoSec team will handle any remediation that may need to occur.



Consensus Policy Resource Community

5. Policy Compliance

To verify that employees are upholding our guidelines, walk throughs, inclusion detection tools and audits will be performed regularly. If they are not in compliance the employee will be subject to disciplinary action or termination.

6. Related Standards, Policies, and Processes

Depending on the business HIPAA is relevant when medical data is being stored, PCI-DSS is used for anyone accepting credit card payments. If these apply to the company, they will need to follow these guidelines as they are industry standards.

7. Definitions and Terms

BYOD is an acronym for bring your own device, a policy implemented by companies to control access to their network. This policy defines guidelines for employees bringing personal devices into their place of business. A mobile device is any device that requires a wireless connection. CIA is an acronym for confidentiality, integrity, and availability, these are foundational principles of information security.

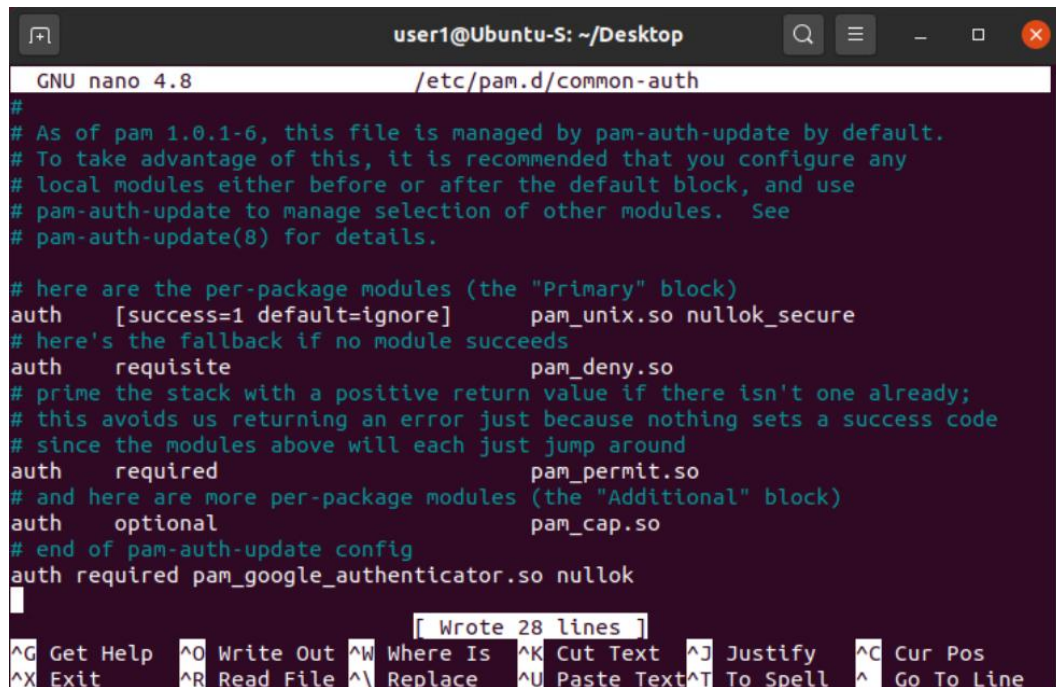
8. Revision History

Date of change	Responsible	Summary of change
March 2023	Faith Burnett policy team	Updated and converted to new format

Identity and Access Management

Common-auth Configuration File

entry that indicates the use of the Google Authenticator module.



```
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

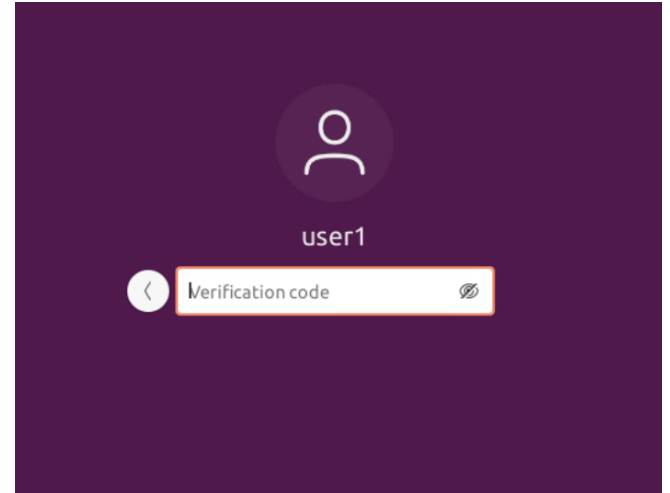
```

[Wrote 28 lines]

^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 Login Screen

the login screen where a verification code is required.



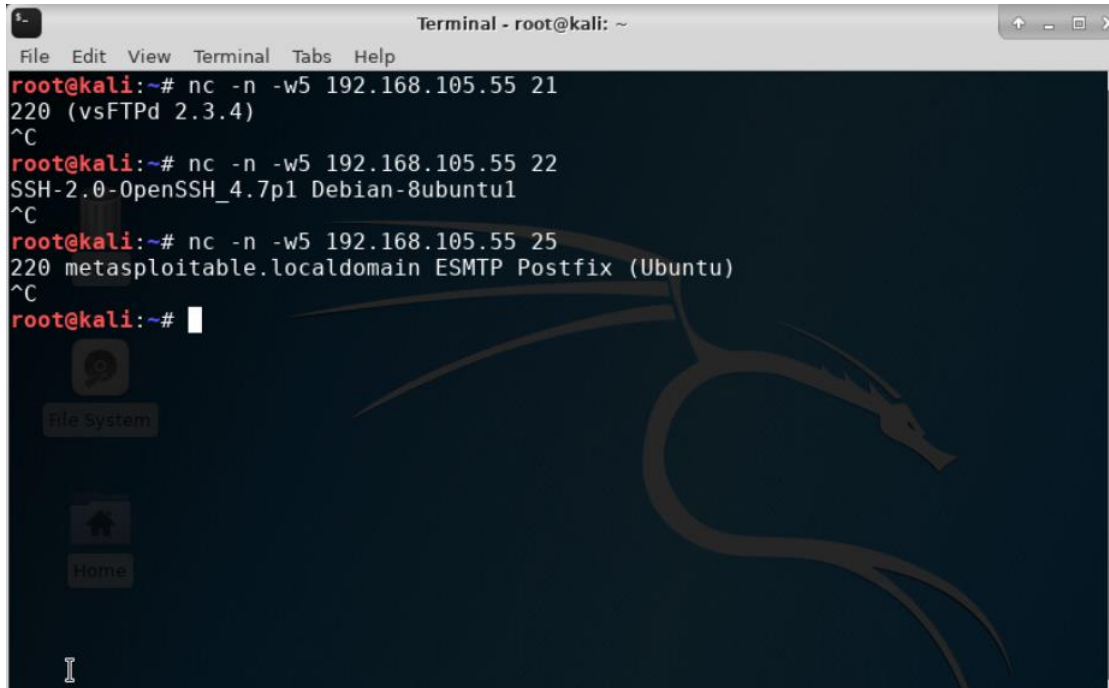
Risk Management

Nmap

scan result showing both the
Kali and Linux Server VMs.

```
Terminal - root@kali: ~
File Edit View Terminal Tabs Help
root@kali:~# nmap -Pn 192.168.105.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2023-04-08 18:14 EDT
Nmap scan report for 192.168.105.55
Host is up (0.0031s 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
```

NetCat

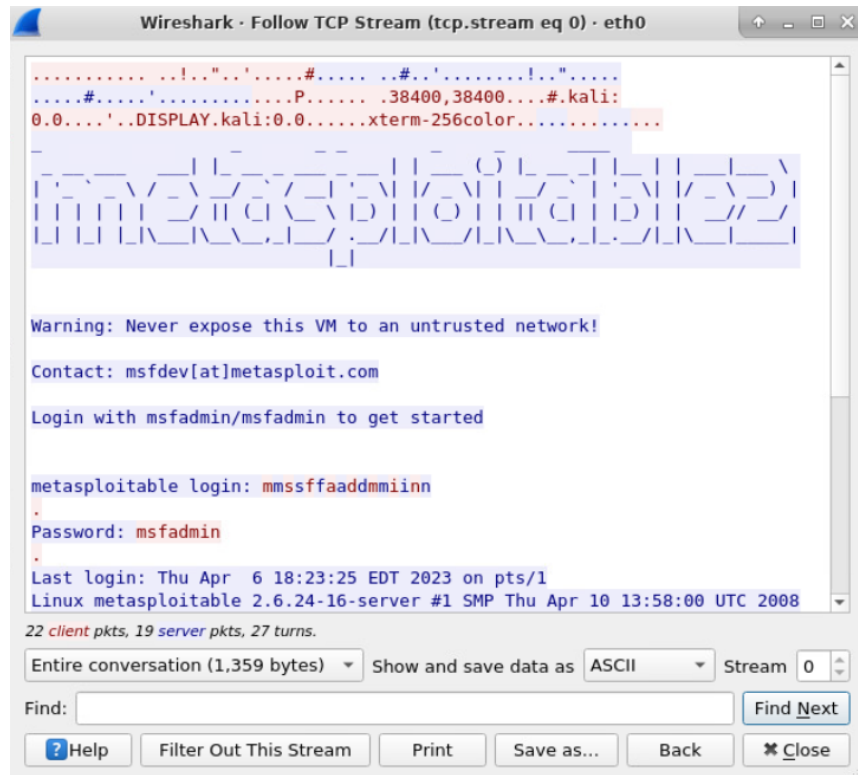
A terminal window titled "Terminal - root@kali: ~" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal shows three NetCat scan commands and their results. The first command connects to 192.168.105.55 port 21, returning "220 (vsFTPD 2.3.4)". The second command connects to 192.168.105.55 port 22, returning "SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1". The third command connects to 192.168.105.55 port 25, returning "220 metasploitable.localdomain ESMTF Postfix (Ubuntu)". The terminal background features a large, faint dragon logo. On the left side, there are icons for "File System" and "Home".

```
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 ESMTF Postfix (Ubuntu)
^C
root@kali:~#
```

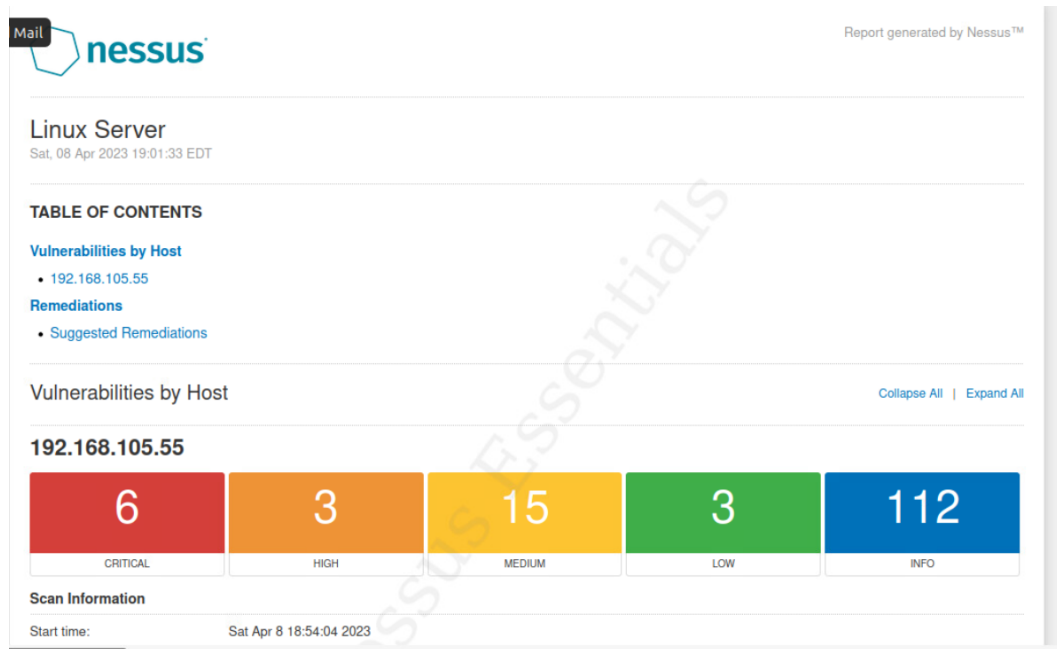
scan result showing both
the Kali and Linux Server
VMs.

Wireshark

Wireshark—Follow TCP Stream window showing the Telnet username and password.



Nessus



high-level view of
the Nessus
vulnerability scan
report

• Challenges

- When having 3 VM's open it was difficult to keep track of where my commands needed entered
- Using the VM's was time consuming as things often took awhile to load

• Skills Learned

- Identify social engineering attacks
- Identify different types of malware
- Differentiate cryptographic algorithms and their applications
- Survey network security devices and protocols
- Examine authentication and access control techniques

THANKS!

Do you have any questions?
faithburnett@outlook.com

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, infographics & images by **Freepik** and illustrations by Stories

