SEC285 Final Course Project

Samuel Pearce

March 2025 DeVry University

Professor Jacob Mack

Introduction

- The point of this project is to be able to:
  - Encrypt/Decrypt files across various OS (Windows, Linux, Kali)
  - Conduct various security scans to help identify any kinds of threats
  - Survey network security devices and protocols
  - Implement MFA (Multi-Factor Authentication), Common-Authentication and other Authentication methods
  - Interpret security (application, device and physical)
  - Assess and develop risk management strategies.

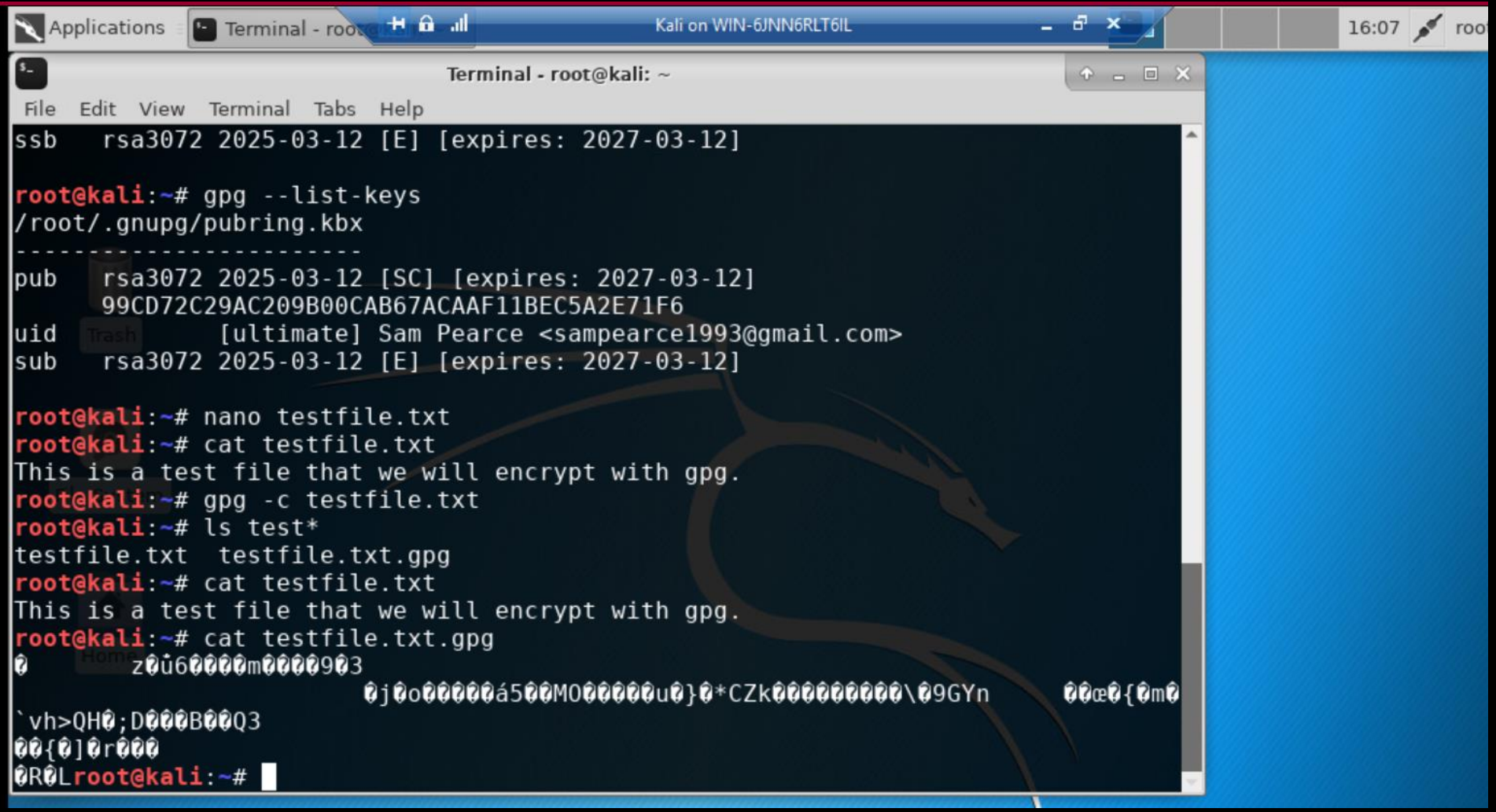
SEC285
Module 2
Asymmetric Key Encryption

By: Samuel Pearce
March 2025

Rubric

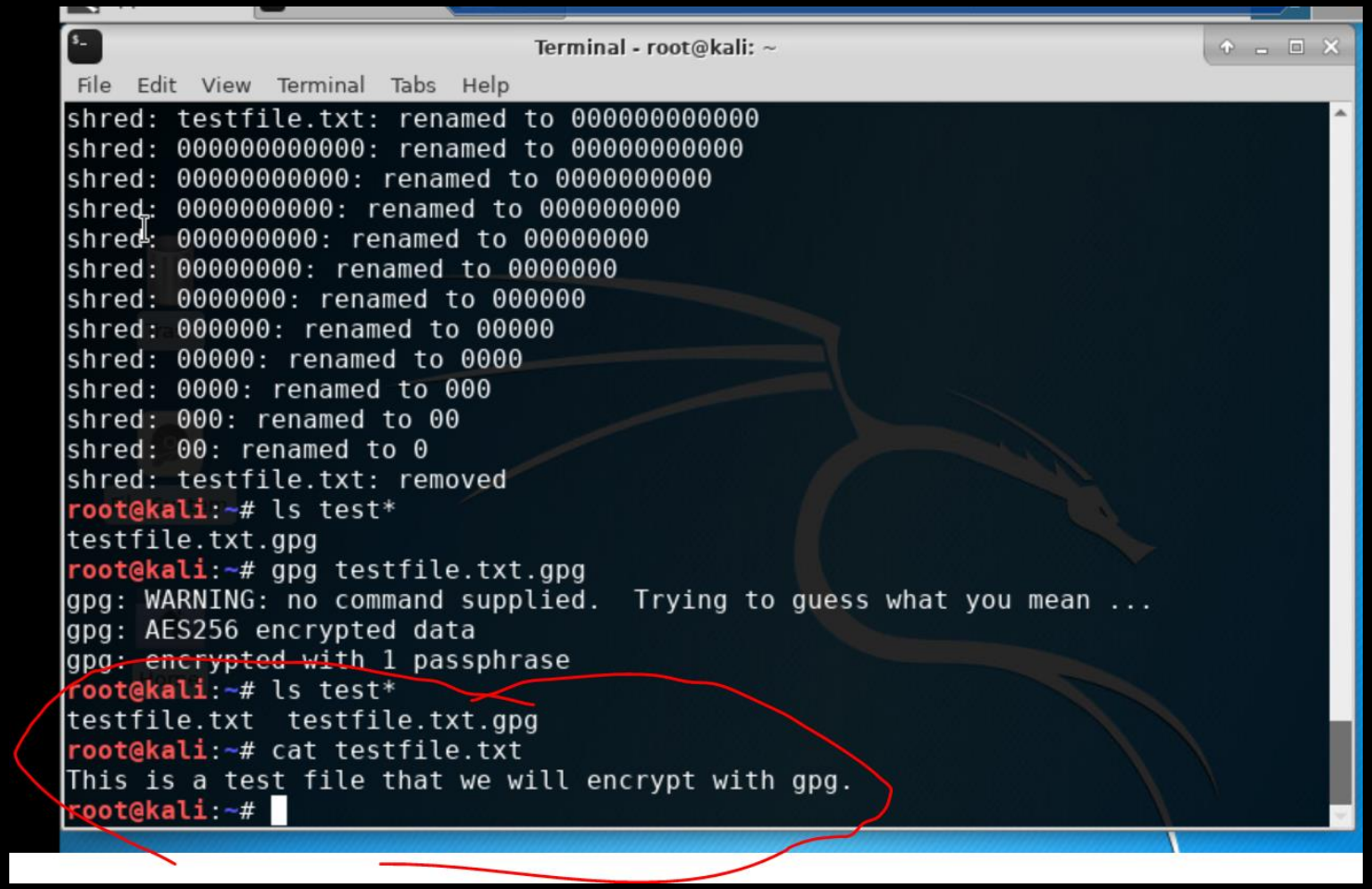
Activity	Requirement(s)	Points
File Encryption	Screenshot	15
File Decryption	Screenshot	15

This screenshot should show the following.

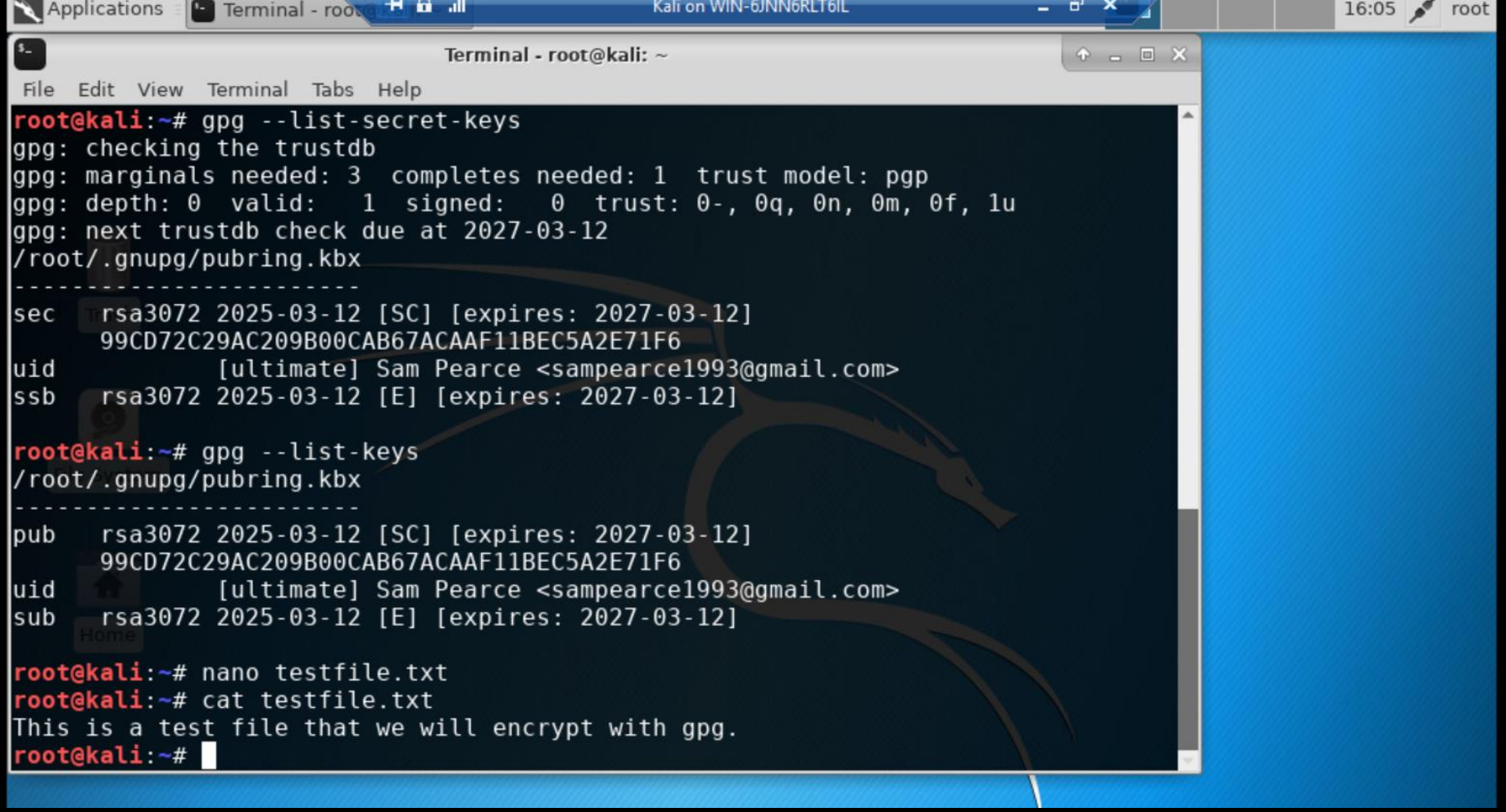


File Decryption

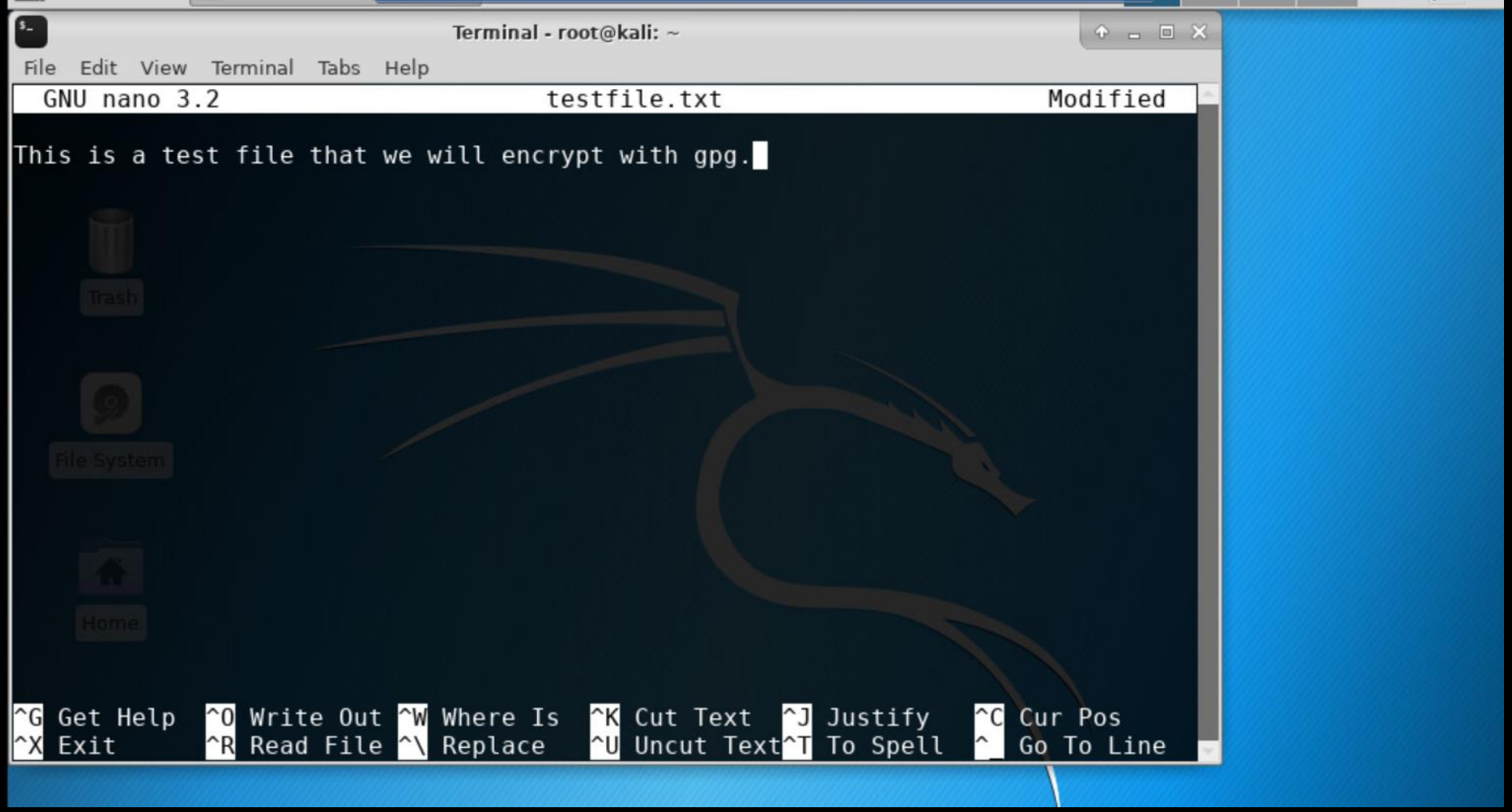
- being listed by itself
- The decrypting process
- Both the encrypted file and the original plaintext file being listed



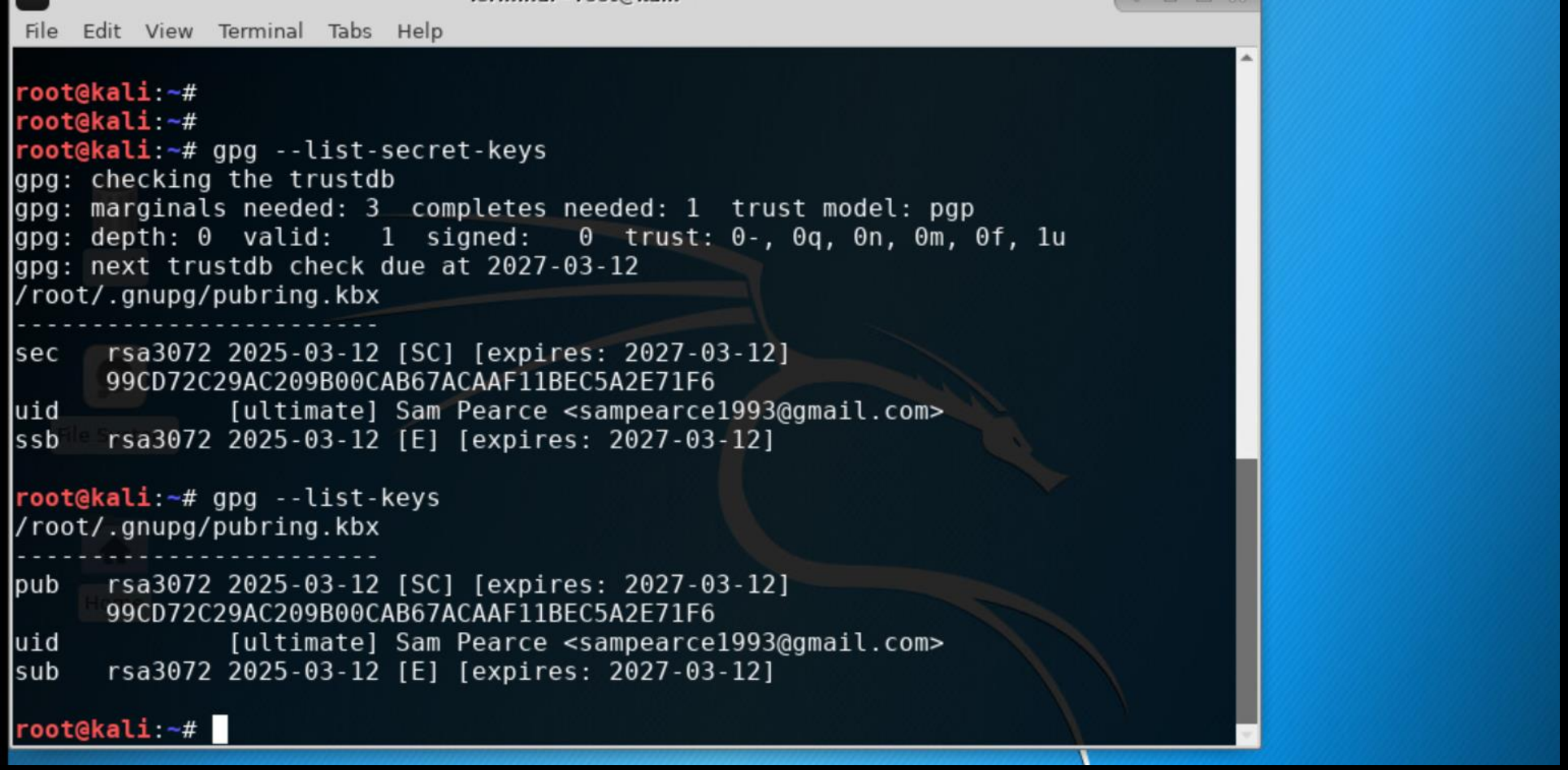
More


Applications
Terminal - root@kali: ~
Kali on WIN-6JNN6RLT6IL
16:05
root
Terminal - root@kali: ~
File Edit View Terminal Tabs Help
root@kali:~# gpg --list-secret-keys
gpg: checking the trustdb
gpg: marginals needed: 3 completes needed: 1 trust model: pgp
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2027-03-12
/root/.gnupg/pubring.kbx
sec rsa3072 2025-03-12 [SC] [expires: 2027-03-12]
99CD72C29AC209B00CAB67ACAAF11BEC5A2E71F6
uid [ultimate] Sam Pearce <sampearce1993@gmail.com>
ssb rsa3072 2025-03-12 [E] [expires: 2027-03-12]
root@kali:~# gpg --list-keys
/root/.gnupg/pubring.kbx
pub rsa3072 2025-03-12 [SC] [expires: 2027-03-12]
99CD72C29AC209B00CAB67ACAAF11BEC5A2E71F6
uid [ultimate] Sam Pearce <sampearce1993@gmail.com>
sub rsa3072 2025-03-12 [E] [expires: 2027-03-12]
root@kali:~# nano testfile.txt
root@kali:~# cat testfile.txt
This is a test file that we will encrypt with gpg.
root@kali:~#

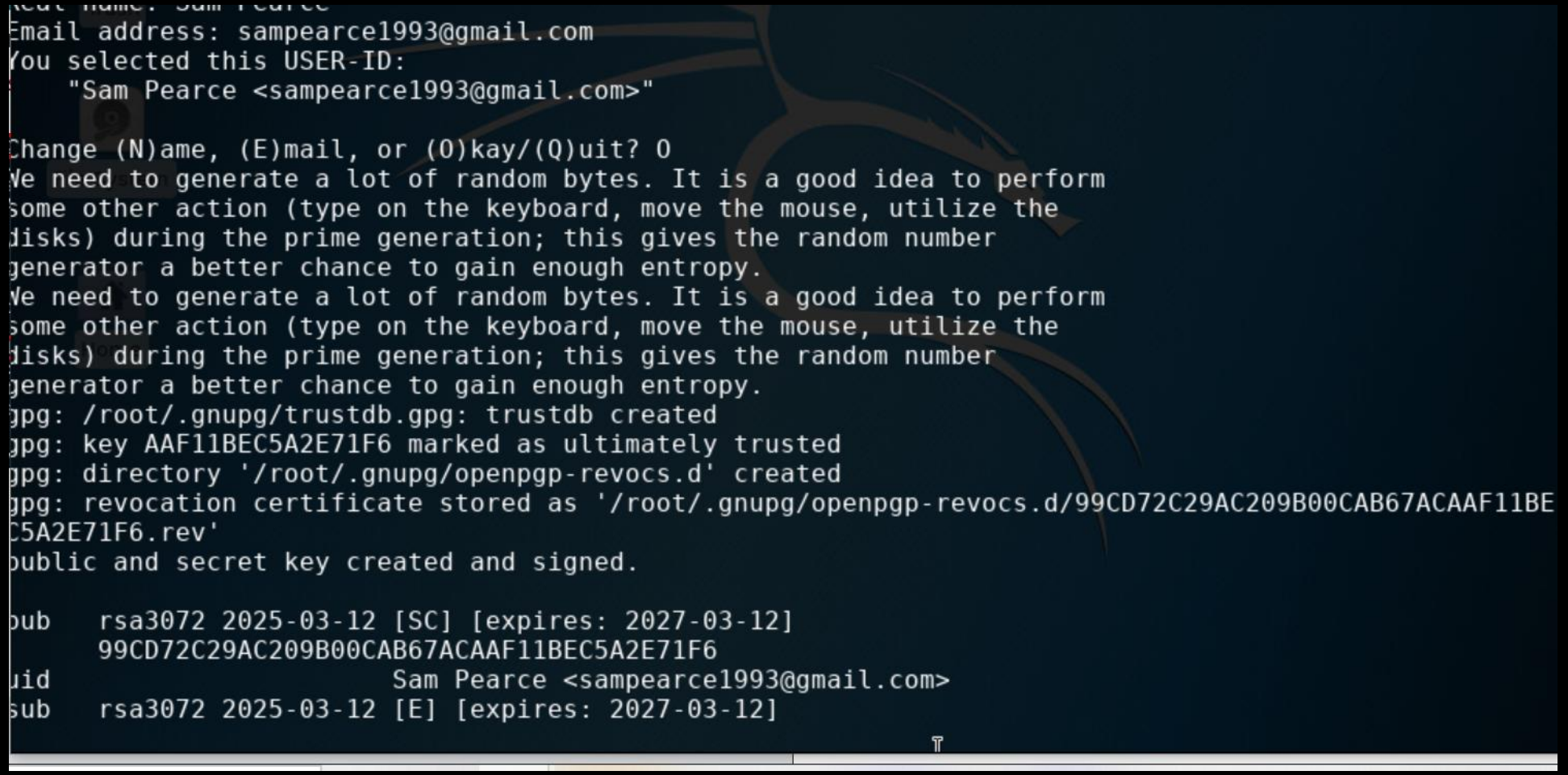
More


Terminal - root@kali: ~
File Edit View Terminal Tabs Help
GNU nano 3.2 testfile.txt Modified
This is a test file that we will encrypt with gpg.
Trash
File System
Home
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line

More


File Edit View Terminal Tabs Help
root@kali:~#
root@kali:~#
root@kali:~# gpg --list-secret-keys
gpg: checking the trustdb
gpg: marginals needed: 3 completes needed: 1 trust model: pgp
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2027-03-12
/root/.gnupg/pubring.kbx
---
sec rsa3072 2025-03-12 [SC] [expires: 2027-03-12]
99CD72C29AC209B00CAB67ACAAF11BEC5A2E71F6
uid [ultimate] Sam Pearce <sampearce1993@gmail.com>
ssb rsa3072 2025-03-12 [E] [expires: 2027-03-12]
root@kali:~# gpg --list-keys
/root/.gnupg/pubring.kbx
---
pub rsa3072 2025-03-12 [SC] [expires: 2027-03-12]
99CD72C29AC209B00CAB67ACAAF11BEC5A2E71F6
uid [ultimate] Sam Pearce <sampearce1993@gmail.com>
sub rsa3072 2025-03-12 [E] [expires: 2027-03-12]
root@kali:~#

More


Email address: sampearce1993@gmail.com
You selected this USER-ID:
"Sam Pearce <sampearce1993@gmail.com>"
Change (N)ame, (E)mail, or (O)kay/(Q)uit? O
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key AAF11BEC5A2E71F6 marked as ultimately trusted
gpg: directory '/root/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/root/.gnupg/openpgp-revocs.d/99CD72C29AC209B00CAB67ACAAF11BE
C5A2E71F6.rev'
public and secret key created and signed.
pub rsa3072 2025-03-12 [SC] [expires: 2027-03-12]
99CD72C29AC209B00CAB67ACAAF11BEC5A2E71F6
uid Sam Pearce <sampearce1993@gmail.com>
sub rsa3072 2025-03-12 [E] [expires: 2027-03-12]

SEC285
Module 3
Stateful Firewall
By: Samuel Pearce
March 2025
Professor Jacob Mack

Rubric

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

Question

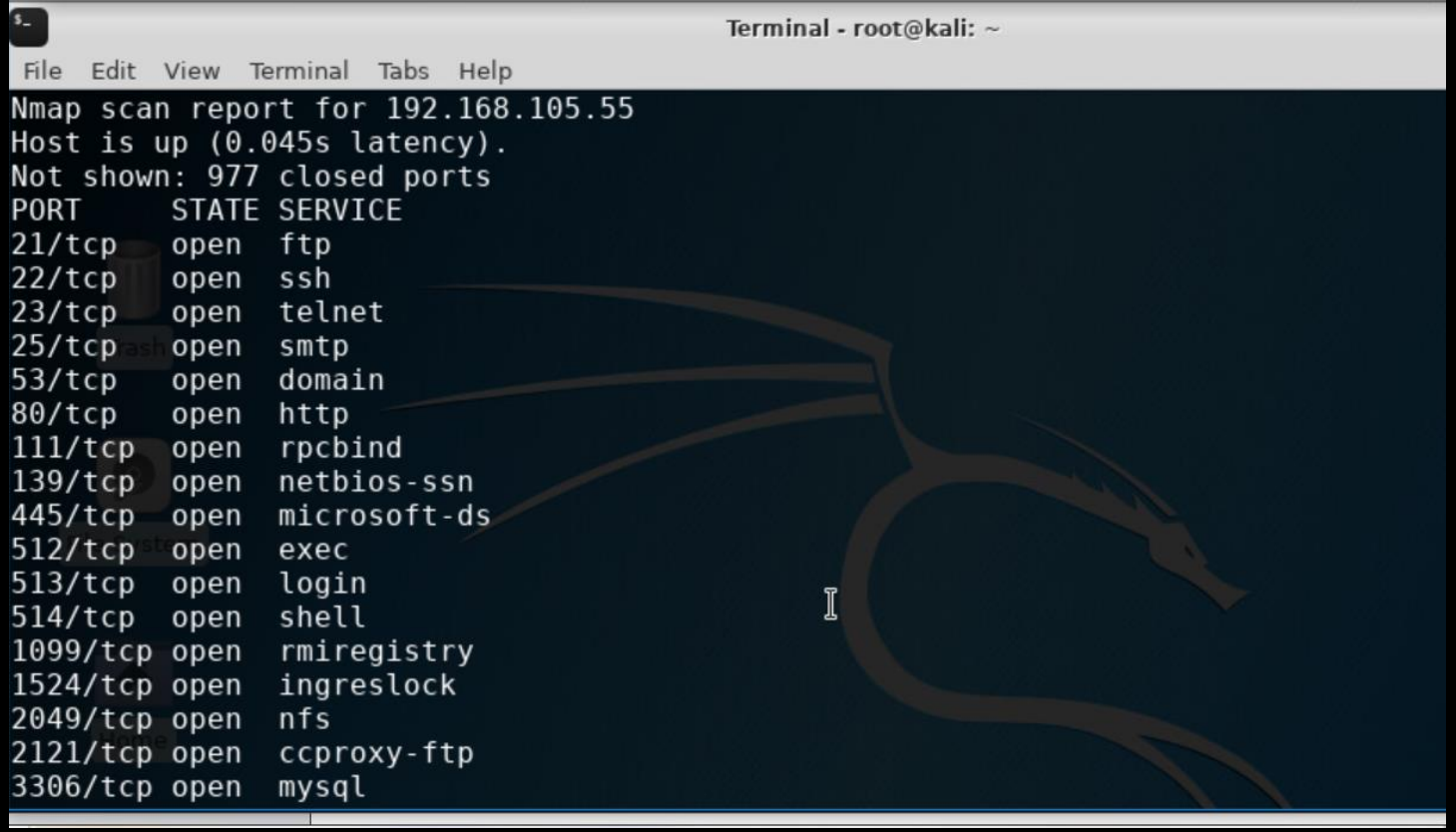
What effect does the sudo iptables --policy INPUT DROP command have on the access to computing resources?

Answer here: The command sudo iptables –policy INPUT DROP restricts access to computing resources; the command sets the default firewall policy to "drop" incoming internet traffic, meaning that it'll block all incoming connections unless said connections fit certain criteria. This improves security, but can also prevent access unless managed accordingly.

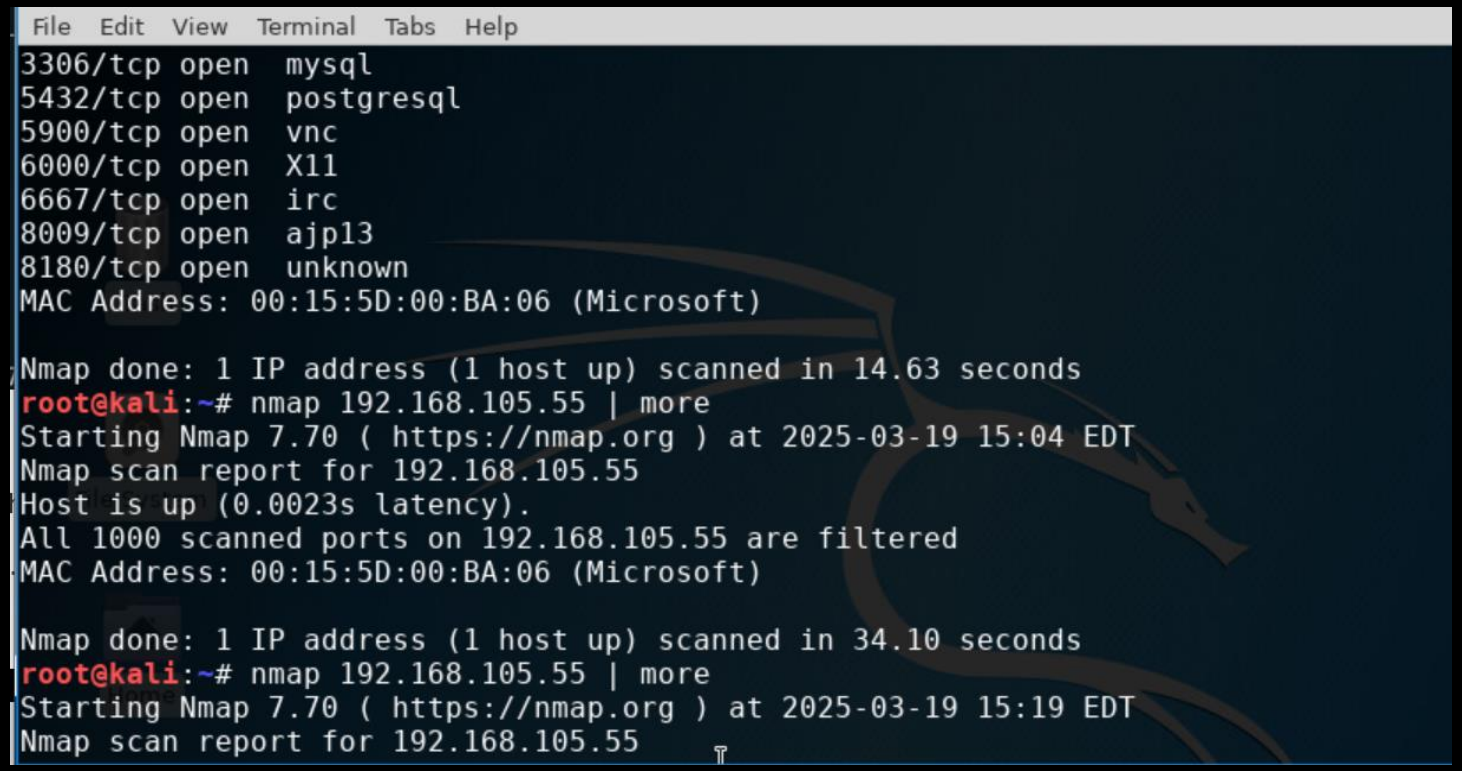
References:

Dancuk, Milica. "Iptables Tutorial: A beginners guide to the Linux Firewall". 30 May 2024. PhoenixNAP Global IT Services. https://phoenixnap.com/kb/iptables-linux#:~:text=iptables%20is%20a%20command%2Dline%20utility%20for%20configuring,pass%20through%20and%20which%20should%20be%20blocked

This screenshot should show the Nmap scan result of the Linux Server VM.



This screenshot should show the Nmap scan result of the Linux Server VM.



Extra

Included for

https://lab.infoseclearning.com/console/5474888/742

SEC285

Enforce US Keyboard Layout

Linux Server on WIN-6JNN6RLT6IL - Virtual Machine Connection

File Action Media Clipboard View Help

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 22 -m state --s
tate NEW -j ACCEPT
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p udp --dport 53 -j ACCEPT
msfadmin@metasploitable:~$ sudo iptables -P INPUT DROP
msfadmin@metasploitable:~$ sudo iptables -P FORWARD DROP
msfadmin@metasploitable:~$ sudo iptables -P OUTPUT ACCEPT
msfadmin@metasploitable:~$ sudo iptables-save
# Generated by iptables-save v1.3.8 on Mon Mar 17 15:16:51 2025
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -m state --state NEW -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -m state --state NEW -j ACCEPT
-A INPUT -p tcp -m tcp --dport 25 -m state --state NEW -j ACCEPT
-A INPUT -p tcp -m tcp --dport 53 -m state --state NEW -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
COMMIT
# Completed on Mon Mar 17 15:16:51 2025
msfadmin@metasploitable:~$
```

Uptime

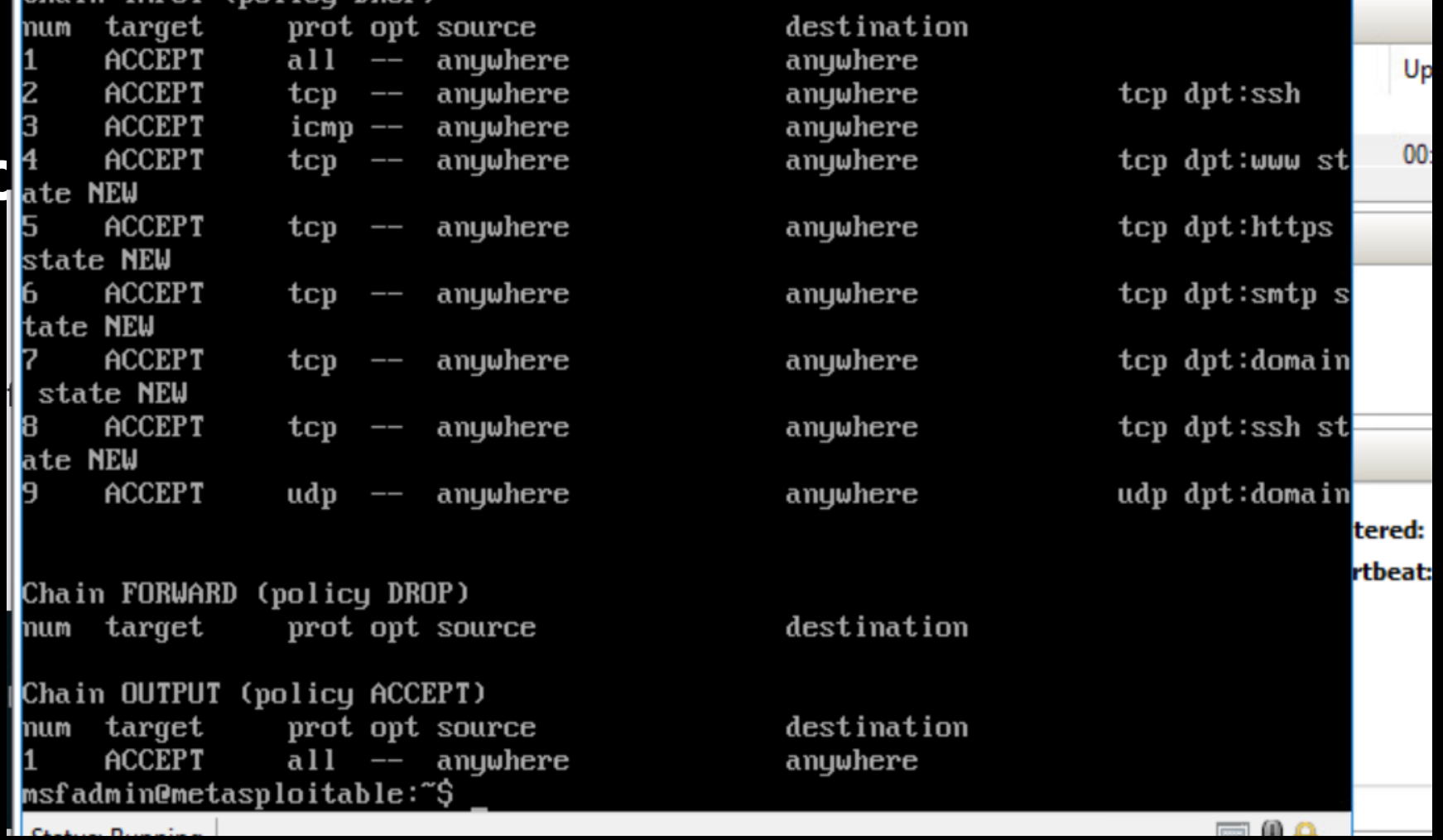
00:21:54

tered: No

rtbeat: No C

Extra sc

Included for fun



SEC285
Module 4
Bring Your Own Device (BYOD) Security Policy

By: Samuel Pearce

March 2025

Prof. Jacob Mack

Rubric

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

1. Overview:

Most modern enterprises (about 80% of them) use tablets, smartphones, and laptops in order to do their daily work-related tasks. Many employees at those organizations bring their own devices. However, this brings many security threats too, which are as listed:

-Data breaches: unauthorized access on devices and lost/stolen devices are the most common reasons. Can also lead to sensitive info leaking.

-Phishing attacks: usually done via SMS/Text, social media or email, phishing attacks are when hackers impersonate either a company, perosn or a website and trick the user into giving sensitive data (passwords, credit cards, etc.).

-Malware: all of these devices can be infected with malware, which can compromise company security and privacy of staff.

-Unsecured Networks: connecting these devices to public Wi-Fi networks can increase the frequency of man-in-the-middle attacks and device eavesdropping.

-Outdated software: older versions of software and apps on devices can lead to security risks.

-Data leakage: some websites and apps send personal data to a remote server, leading to data mining via advertisers and hackers.

2. Purpose:

Timely discovery of potential vulnerabilities via BYOD security policy reduces the attack vector allows for a company's IT security team to "get ahead of issues" before they happen. Taking a proactive mitigation approach by patching any software that needs it, or restricting access to sensitive data and enforcing specific security protocols. Addressing these vulnerabilities early can reduce the chances of cyberattacks and data breaches. A BYOD security policy helps to strengthen a company's cybersecurity framework by addressing a major issue for many IT security teams: personal devices accessing a company network. All of these steps ensure that a

3. Scope:

The hardware, applications, personnel, and departments that will be impacted by the security policy includes determining the types of personal devices allowed on the network and under what conditions. It is important to establish whether personnel must receive formal approval before using personal devices on the network. Additionally, the policy should outline the permitted activities on personal devices and specify who is responsible for granting permission to use a device on the network.

Criteria for making classifications in this area may include:

- Types of personal devices (e.g., smartphones, tablets, laptops)
- Conditions for allowing personal devices on the network (e.g., meeting certain security requirements, obtaining formal approval)
- Permitted activities on personal devices (e.g., accessing work-related applications, browsing the internet)
- Responsible personnel or department for granting permission to use a device on the network.

4. Policy:

Timely discovery of potential vulnerabilities via BYOD security policy reduces the attack vector allows for a company's IT security team to "get ahead of issues" before they happen. Taking a proactive mitigation approach by patching any software that needs it, or restricting access to sensitive data and enforcing specific security protocols. Addressing these vulnerabilities early can reduce the chances of cyberattacks and data breaches. A BYOD security policy helps to strengthen a company's cybersecurity framework by addressing a major issue for many IT security teams: personal devices accessing a company network. All of these steps ensure that a BYOD security policy protects the confidentiality, integrity and availability (CIA) of data.

5. Policy Compliance:

Employees who do not follow the security policy could face a wide range of disciplinary action, ranging up to termination of employment. Usually, an employee is given a warning to follow the security policy (verbal and/or written) and a notice to correct their behavior. They may need to undergo training to ensure an understanding of said policy. More serious disciplinary action may occur if the action(s) are severe enough, ranging from reprimand to suspension. If the violations still persist, then the employee may be terminated of their position if everything else fails.

6. Related Standards, Policies, and Processes:

Other documents that can be linked to this policy (and their reasons) are listed:

-GDPR (General Data Protection Regulation): It's a regulation in Europe on data protection and privacy. It's relevancy lies in the fact that it governs how personal data should be handled, which in turn aligns wth many privacy and security policies of HIPAA and PCI-DSS.

-SOX (Sarbanes-Oxley Act): A law in the U.S. that requires certain practices when it comes to financial record keeping and reporting. It's relevancy lies in the fact that it is linked to data integrity and security policies, similar to PCI-DSS.

-FISMA (Federal Information Security Management Act): FISMA requires federal agencies to develop, keep track of, and implement

7. Definitions and Terms:

BYOD: Means "Bring Your Own Device"; the practice of people using their personal devices (laptops, tablets, etc.) for work or educational purposes.

Mobile Devices: Portable electronic devices that are designed to be used when on the move. These include: smartphones, tablets, smartwatches, laptops, handheld gaming devices, and others.

CIA: In the context of information security, it means Confidentiality, Integrity, and Availability. These are the key principles that guide the protection of information and c
Integrity ensures the information is

8. Revision History:

Date of change	Responsible	Summary of change
August 2019	SANS policy team	Updated and converted to new format
March 2025	Samuel Pearce	Updated and converted to new format

SEC285
Module 5
Multifactor Authentication (MFA)

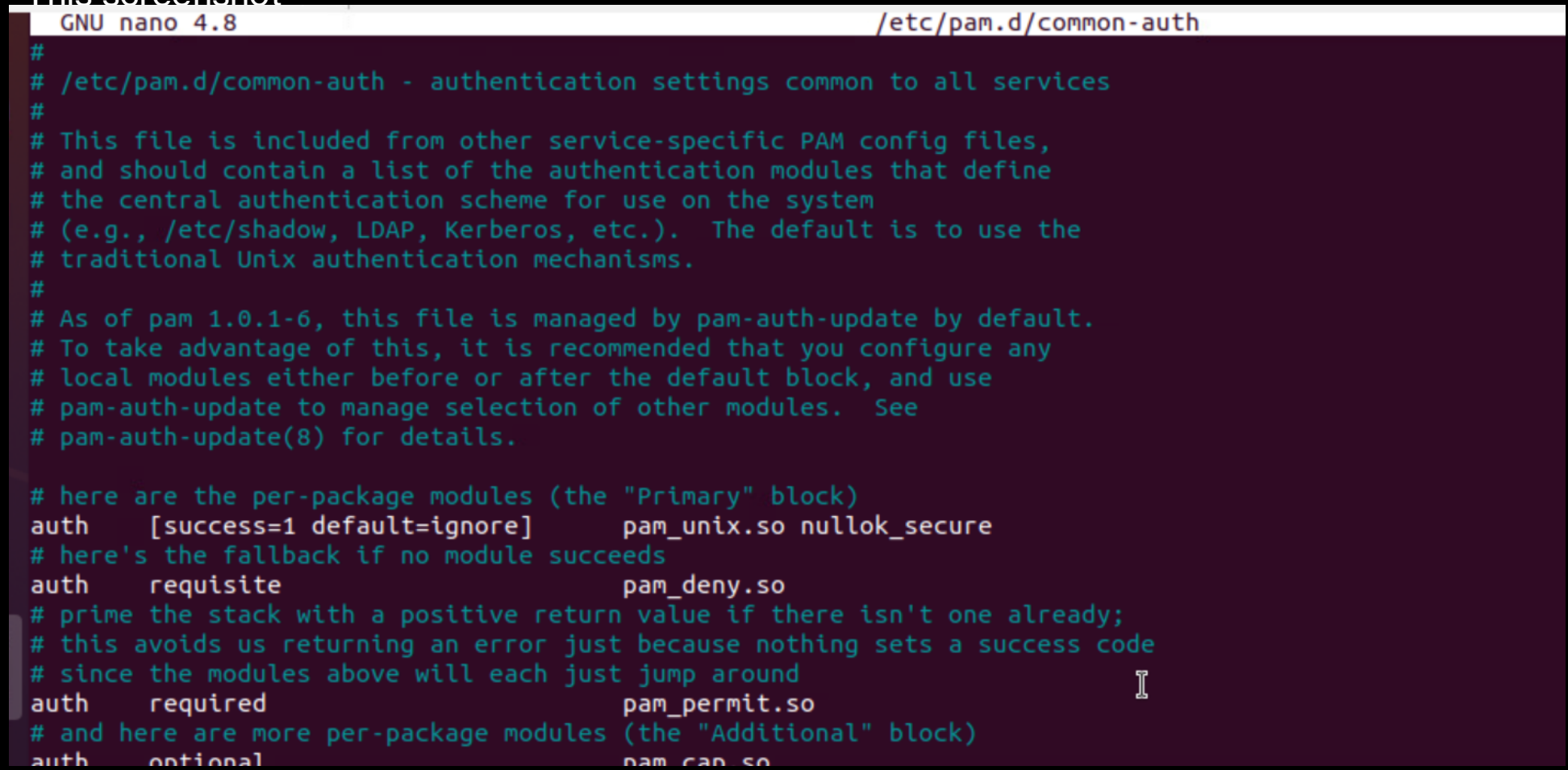
By: Samuel Pearce
March 2025

Rubric

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

File

This screenshot

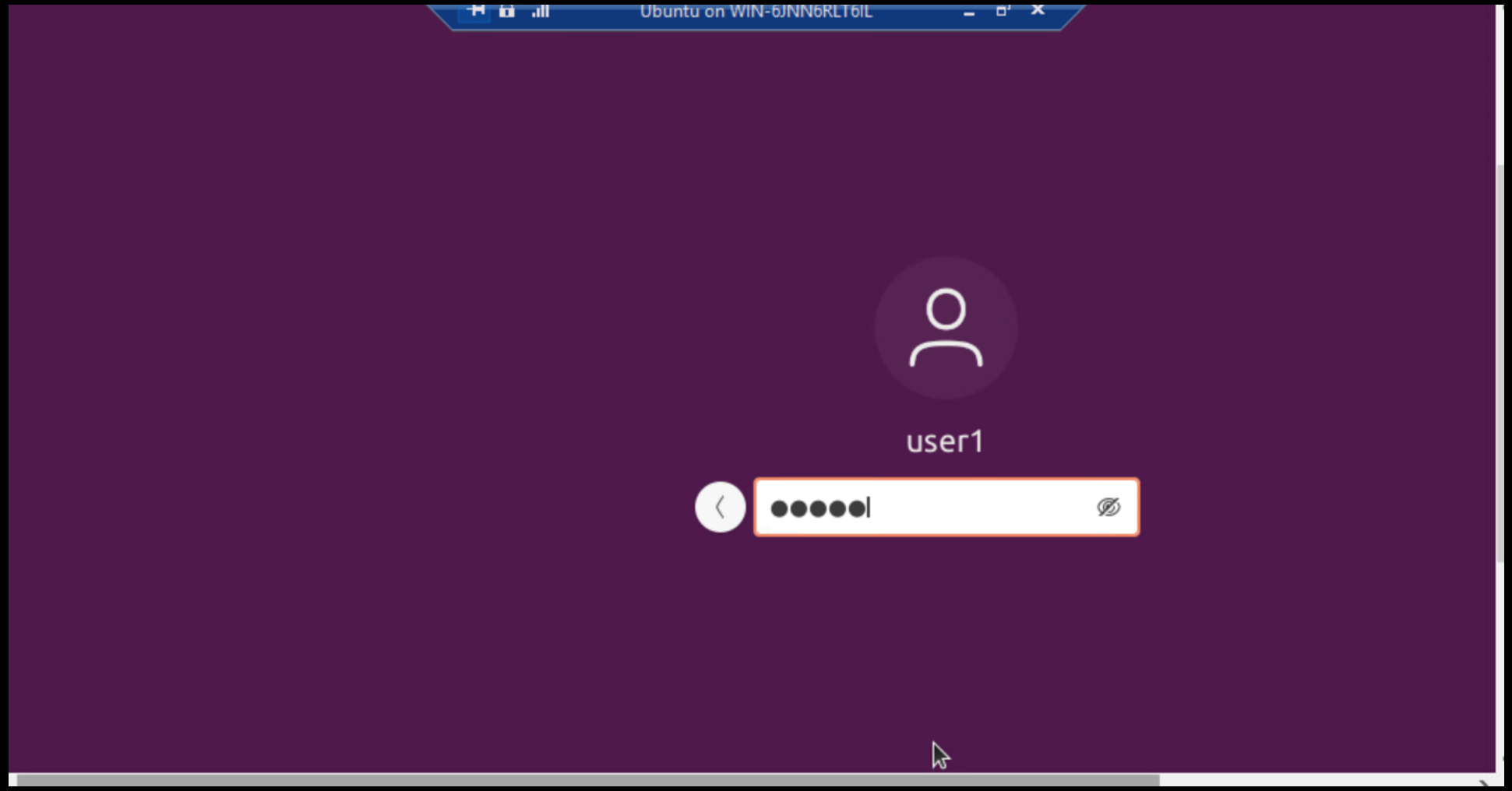


File

This screenshot should show the

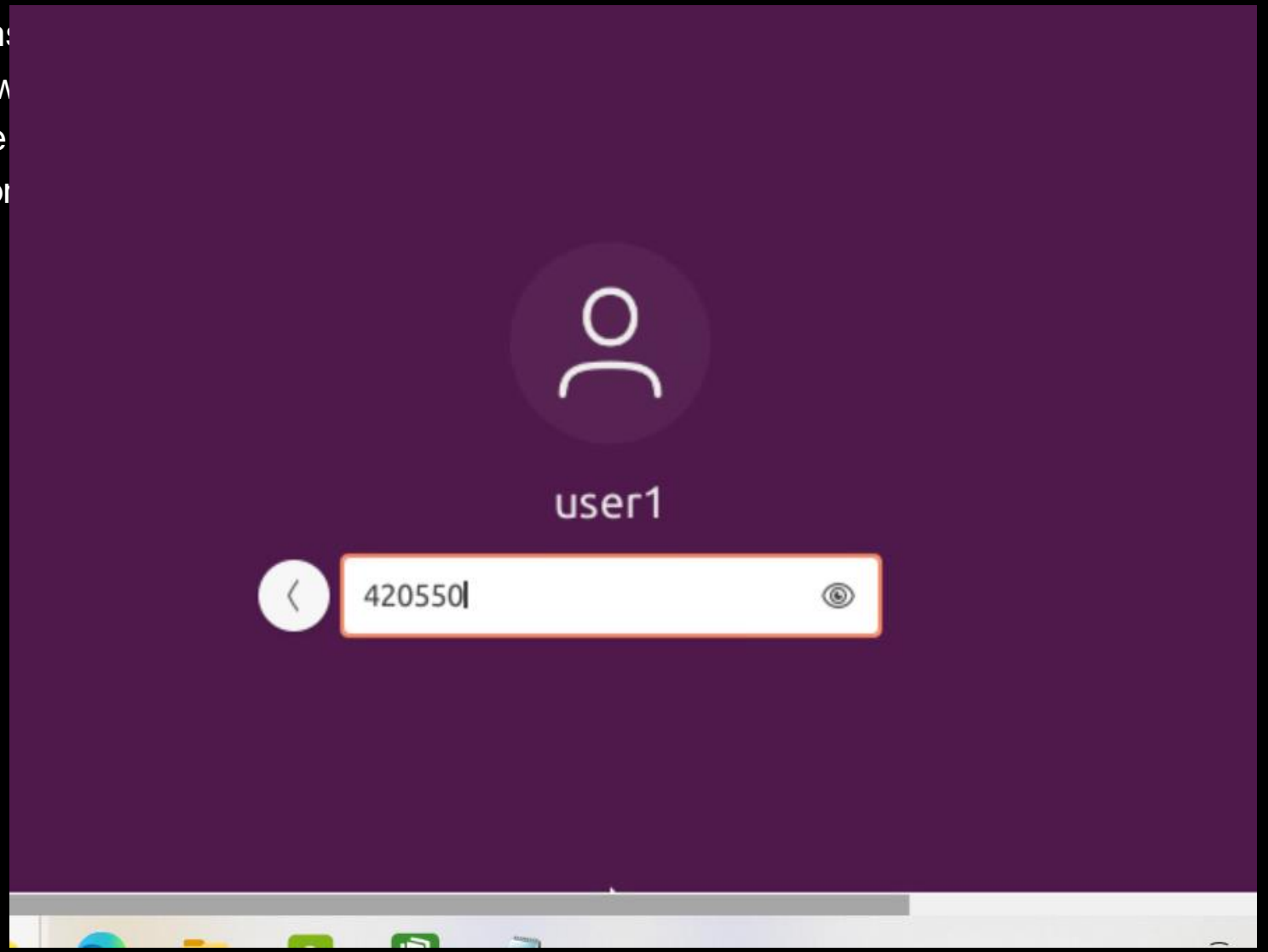
MFA Logon Screen

MFA Logon Screen



MFA Logon Screen

This screens
should show
logon scree
a verificatio
required.



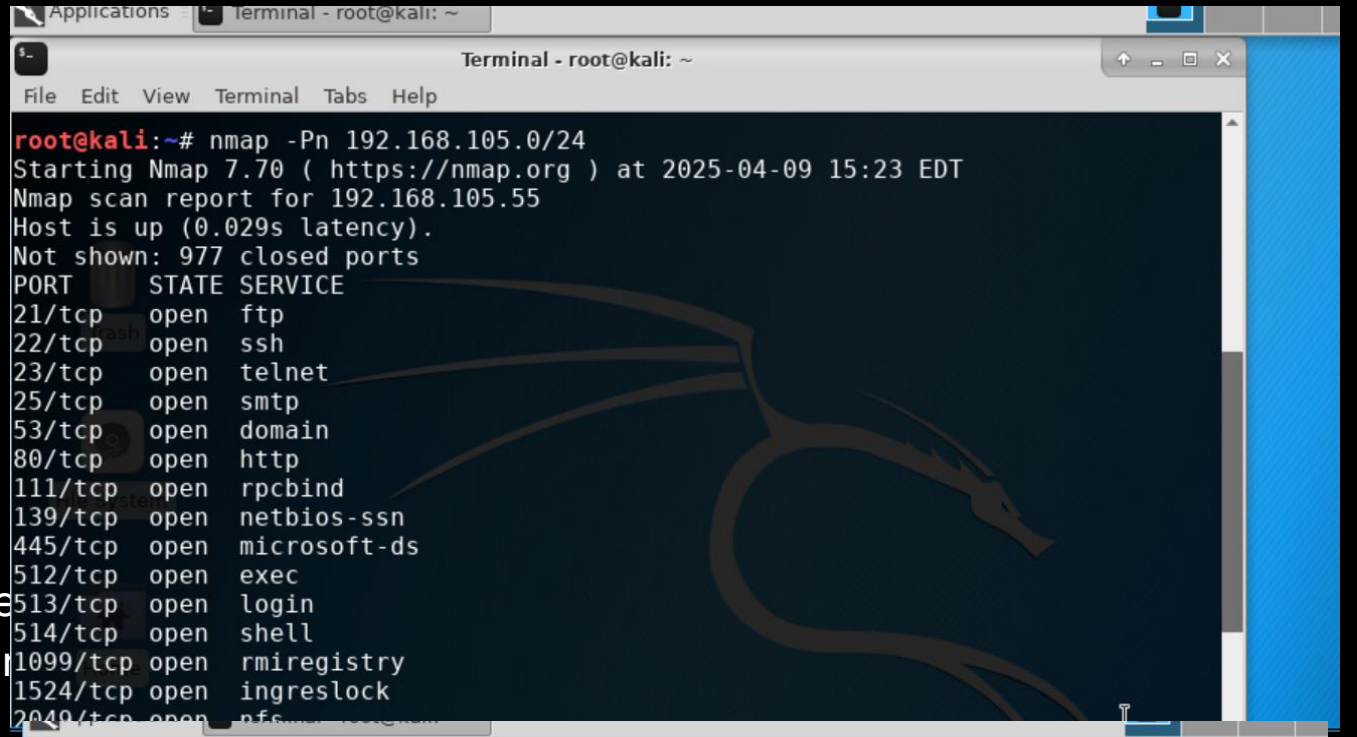
SEC285
Module 6
Vulnerability Assessment

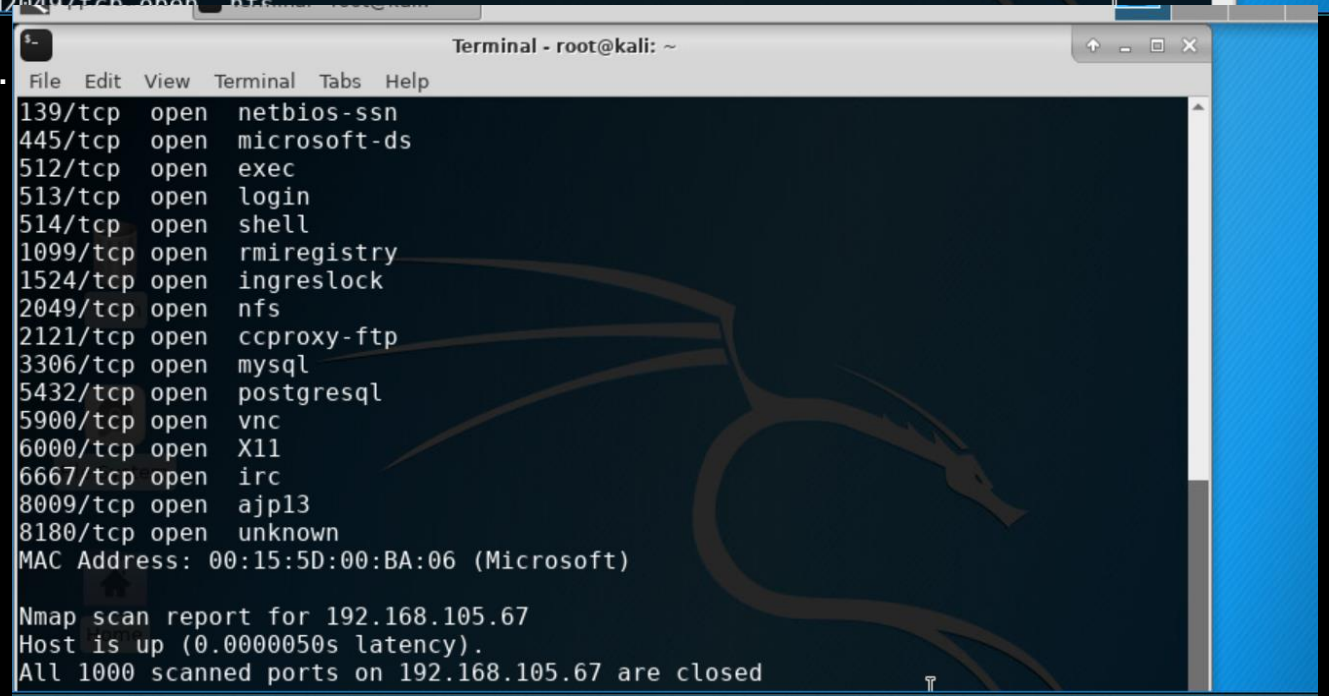
By: Samuel Pearce
March 2025
Jacob Mack

Rubric

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

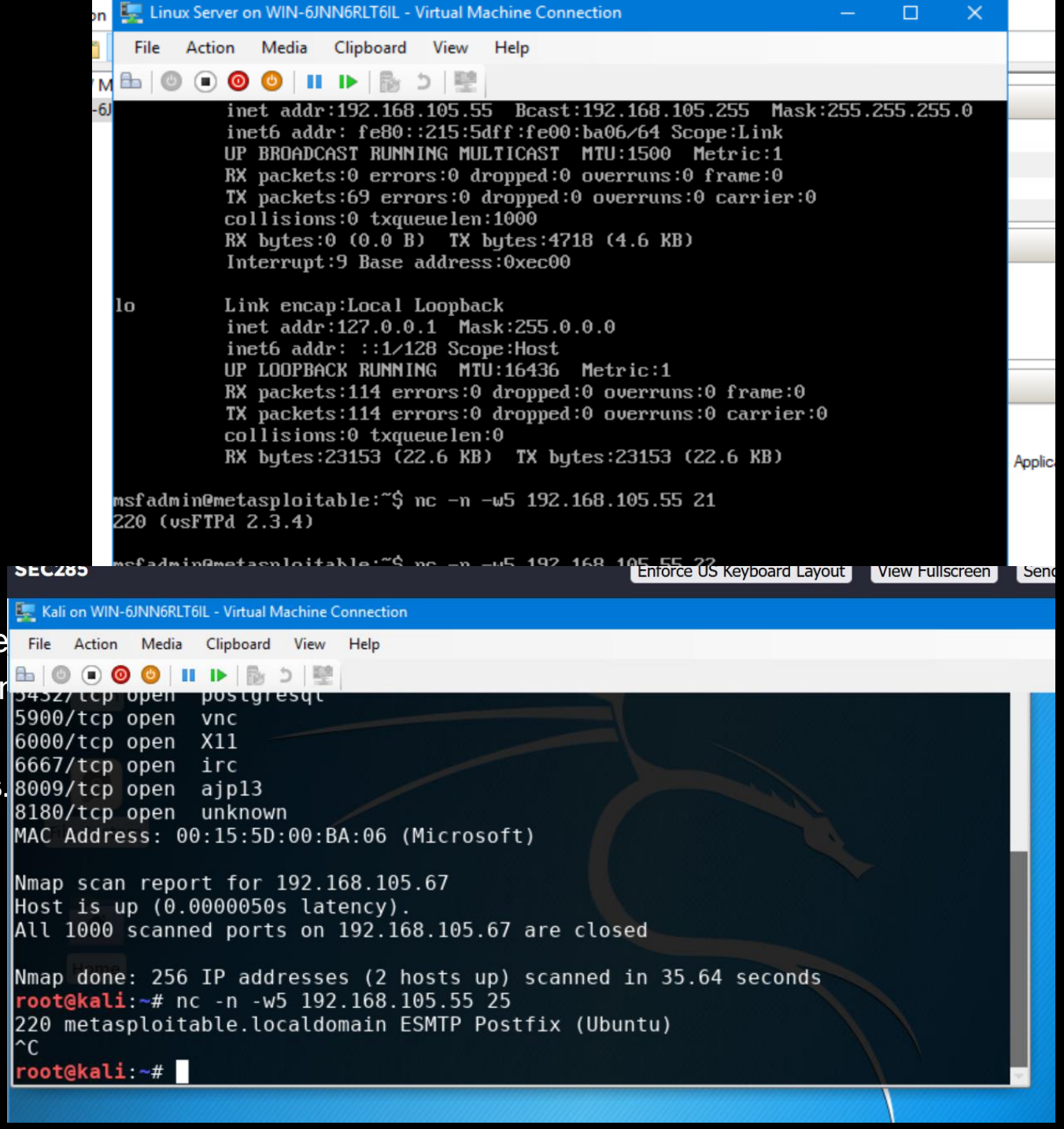
This screenshot should include the scan result showing both the Kali and Linux Server VMs.





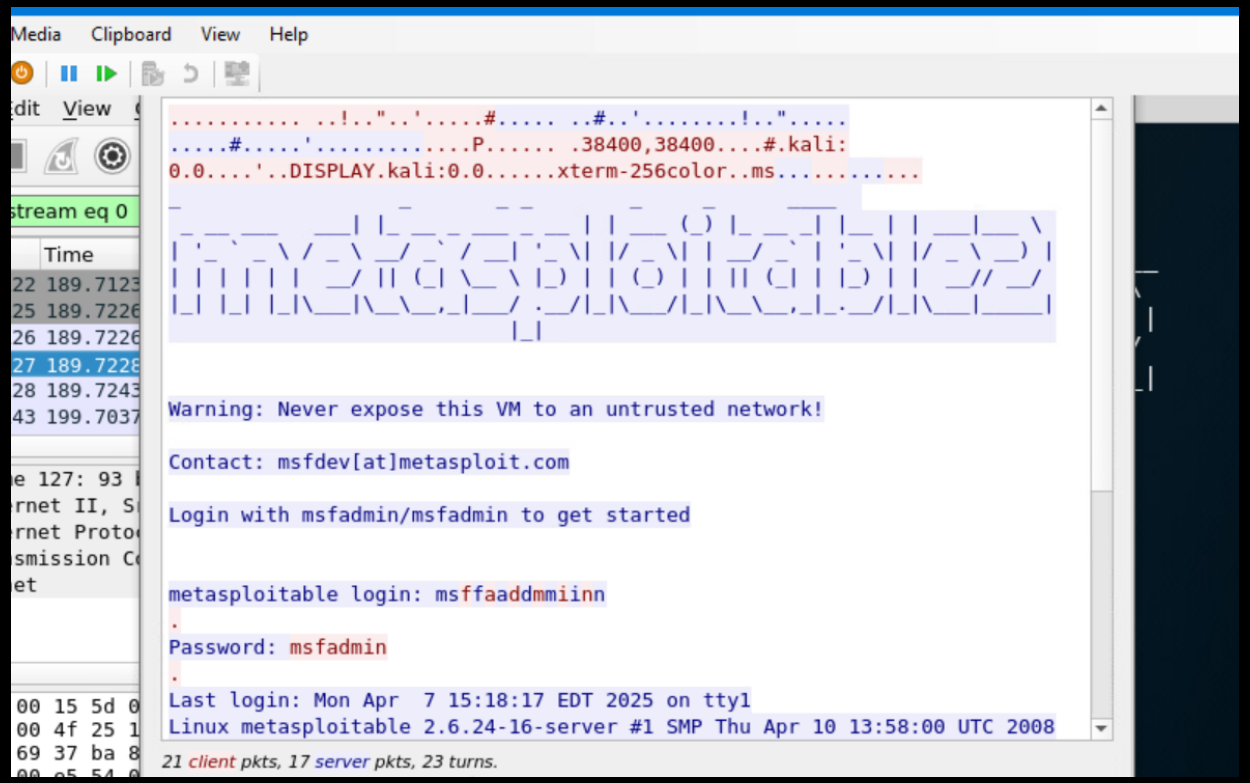
NetCat

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



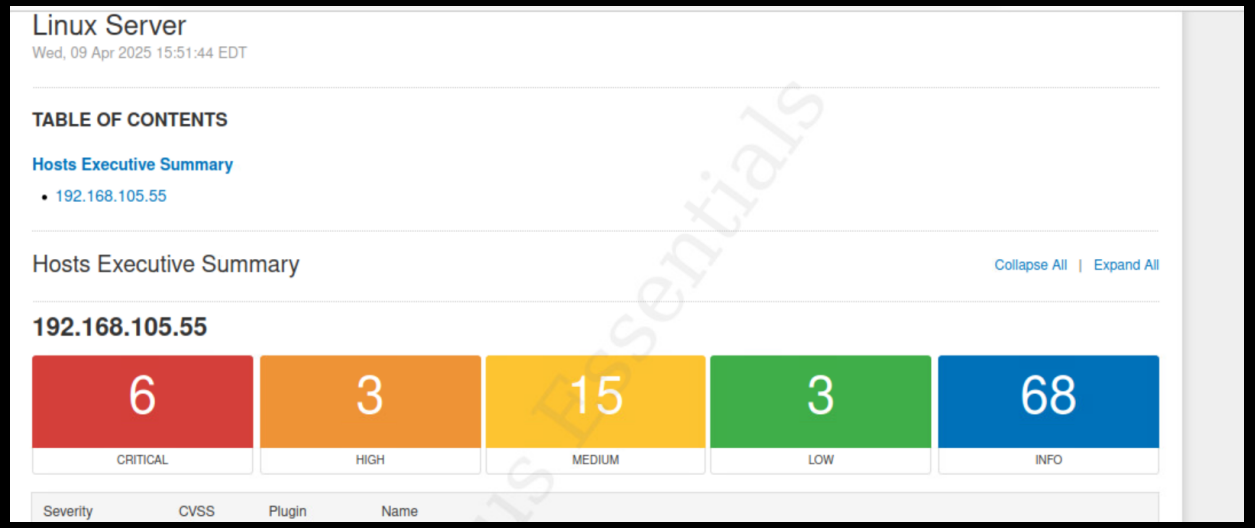
Wireshark

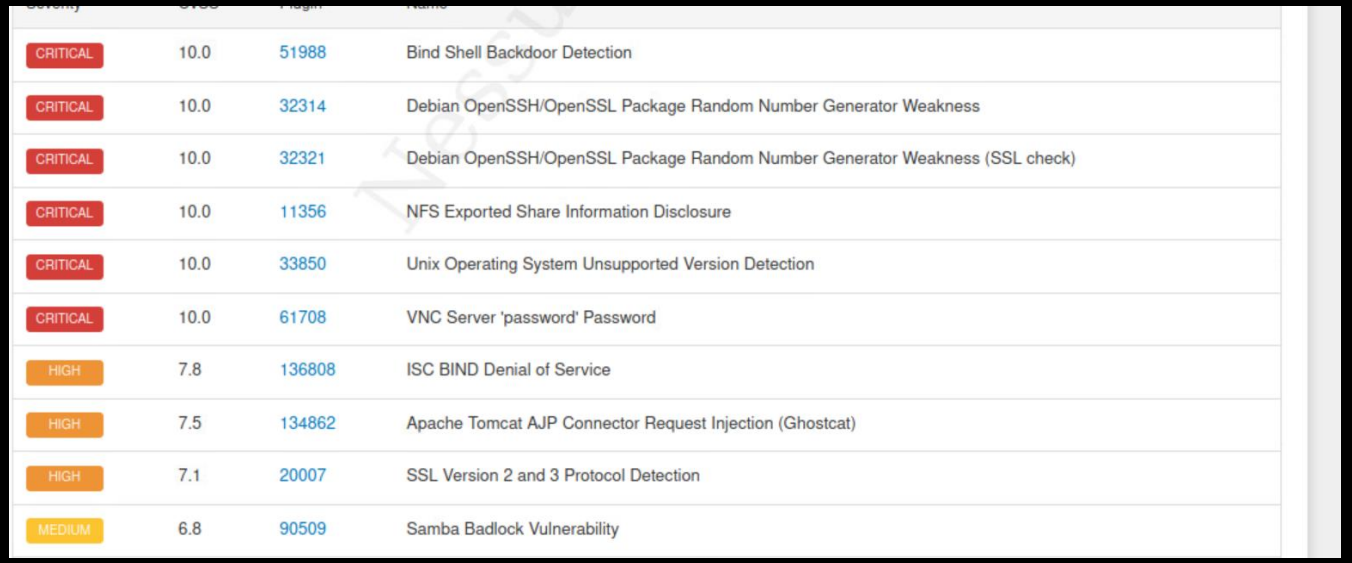
This screenshot should include the Wireshark—Follow TCP Steam window showing the Telnet username and password.



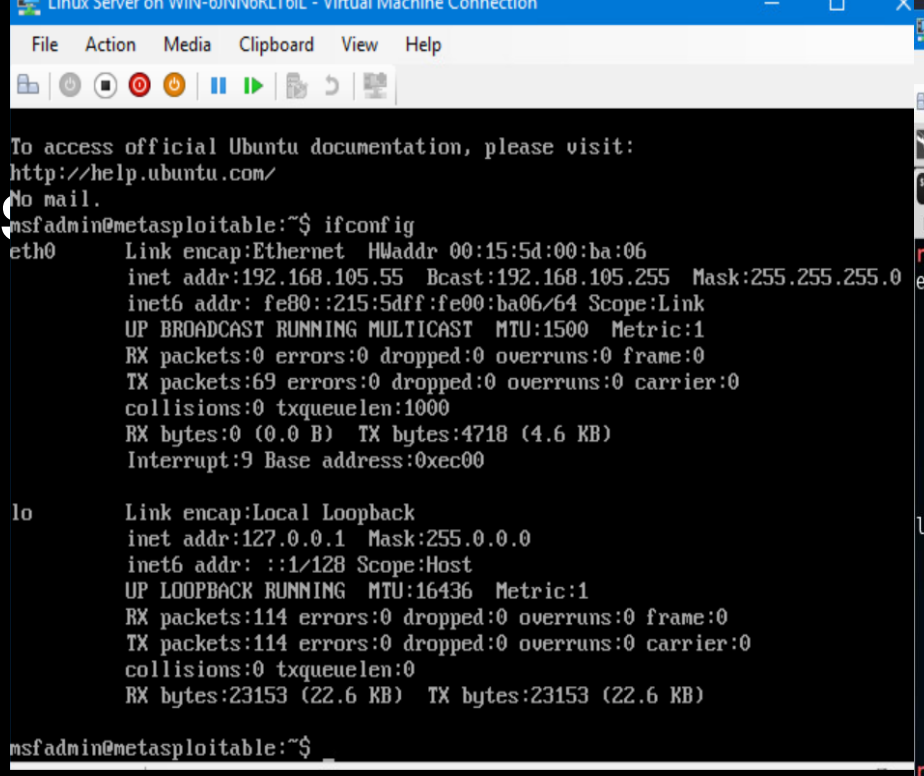
Nessus

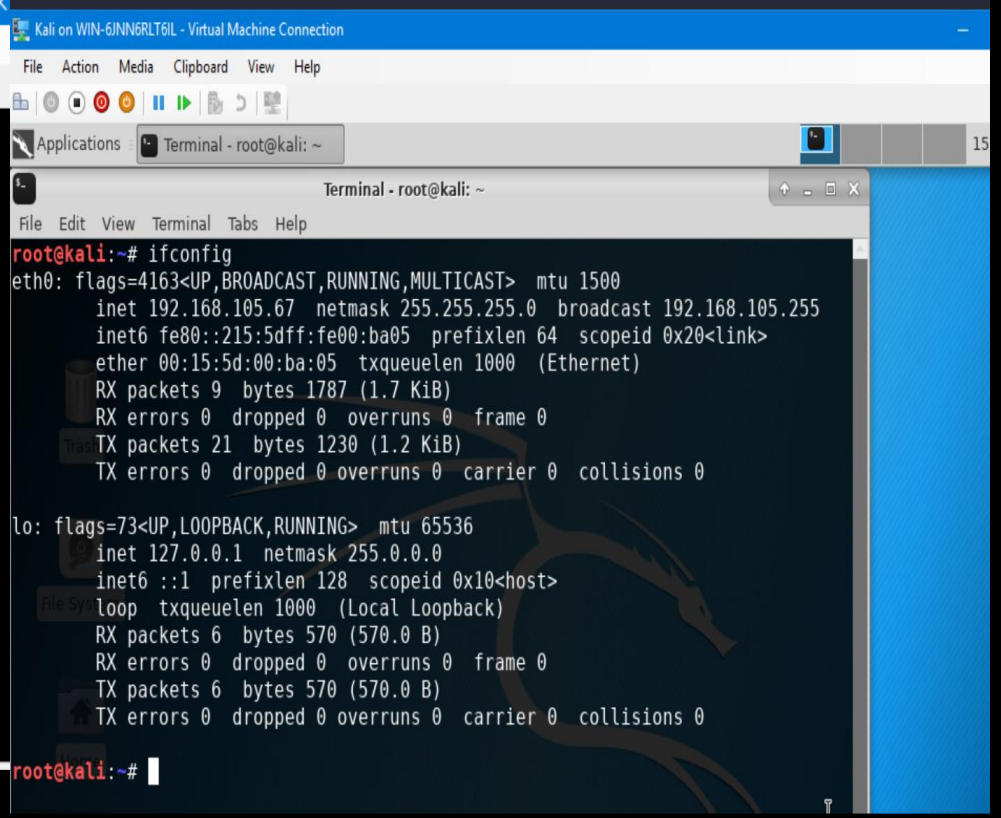
This screenshot should include the high-level view of the Nessus vulnerability scan report (showing categories of vulnerability in different colors).





Extras


Linux Server on WIN-6JNN6RLT6IL - Virtual Machine Connection
File Action Media Clipboard View Help
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@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:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:4718 (4.6 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:114 errors:0 dropped:0 overruns:0 frame:0
TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:23153 (22.6 KB) TX bytes:23153 (22.6 KB)
msfadmin@metasploitable:~$


Kali on WIN-6JNN6RLT6IL - Virtual Machine Connection
File Action Media Clipboard View Help
Applications
Terminal - root@kali: ~
Terminal - root@kali: ~
File Edit View Terminal Tabs Help
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.105.67 netmask 255.255.255.0 broadcast 192.168.105.255
inet6 fe80::215:5dff:fe00:ba05 prefixlen 64 scopeid 0x20<link>
ether 00:15:5d:00:ba:05 txqueuelen 1000 (Ethernet)
RX packets 9 bytes 1787 (1.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 21 bytes 1230 (1.2 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 6 bytes 570 (570.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 6 bytes 570 (570.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~#

Challenges

- Severe lag on my computer when running the VM's, more notably the Linux VM than the others. Also severe lag with Microsoft 365 when trying to create project deliverables.
- Terminal window in Linux kept lagging when typing, even when it wasn't a username/password being typed.
- Having to constantly reboot the VM's made projects drag on longer than needed.

Career Skills

- Being able to identify social engineering attacks
- Encrypting and Decrypting files
- Creating MFA and Common-auth Configuration files for added security methods.
- Conduct various vulnerability scans for security reasons
  - Nmap, NetCat, Wireshark and Nessus
- Knowledge of BYOD security policies
- Being able to utilize terminal windows to conduct various functions needed to complete tasks.

References

- Dancuk, Milica. "Iptables Tutorial: A beginners guide to the Linux Firewall". 30 May 2024. PhoenixNAP Global IT Services. https://phoenixnap.com/kb/iptables-linux#:~:text=iptables%20is%20a%20command%2Dline%20utility%20for%20configuring,pass%20through%20and%20which%20should%20be%20blocked
- "Basic and most common iptables rules." 14 November 2022. Hostens. https://www.hostens.com/knowledgebase/basic-and-most-common-iptables-rules/#:~:text=INPUT%20%E2%80%93%20All%20packets%20destined%20for,your%20computer%20as%20a%20router.
- Cooper, Naomi. (2023, February 8). *NIST to standardize 'lightweight cryptography' algorithms to secure IOT devices.* ExecutiveGov. **https://executivegov.com/2023/02/nist-to-standardize-lightweight-cryptography-algorithms-to-secure-iot-devices/**
- (2023, February 7th). *NIST Selects "Lightweight Cryptography" Algorithms to Protect Small Devices*. NIST. https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices
- Close, David. (2025 January). *How Will Lightweight Cryptography Impact You?* Futurex. https://www.futurex.com/blog/how-will-lightweight-cryptography-impact-you
- Rosencrance, Linda. What is software defined networking? TechTarget Search Networking. 11 May 2022. https://www.techtarget.com/searchnetworking/definition/software-defined-networking-SDN#:~:text=Software%2Ddefined%20networking%20(SDN)%20is%20an%20architecture%20that,to%20respond

References

- What is Jailbreaking, Cracking, or Rooting a Mobile Device? Pearl Hawaii Federal Credit Union. 10 March 2025. https://pearlhawaii.com/blog/what-is-_jailbreaking-cracking-or-rooting-a-mobile-device/
- Malenkovich, Serge. Rooting and Jailbreaking: What Can They Do, and How Do They Affect Security? Kapersky Daily English Global. 31 May 2013. https://usa.kaspersky.com/blog/rooting-and-jailbreaking/1979/?srsltid=AfmBOooPiJ0xQtMfo3zvWu6DUfoZmd4tPj-UqVT1aFVQ6-__BpzgXeF5
- Korkuzaite, Ausra. "LastPass vs Dashlane comparison in 2025". Cybernews. 10 March 2025. https://cybernews.com/best-password-managers/dashlane-vs-lastpass/
- Sheldon, Robert (23 April 2024). *What is a business impact analysis (BIA)?* Search Storage. TechTarget. https://www.techtarget.com/searchstorage/definition/business-impact-analysis
- (26 December 2023). Business Impact Analysis | Ready.gov. Ready. https://www.ready.gov/business/planning/impact-analysis