TASK-1 FOUNDATIONS OF CYBERSECURITY

Cybersecurity Basics

1. CIA Triad

Confidentiality: Keeping information secret so that only the right people can see it. Example: WhatsApp uses end-to-end encryption to protect your chats.

Integrity: Making sure information stays correct and unchanged. Example: when downloading software, checksums are used to verify that the file hasn't been tampered with.

Availability: Ensuring systems and data are always accessible when needed. Example: banks use backup servers so online banking works even during failures.

2. Common Threats

Phishing: Fake emails, messages, or websites that trick people into sharing passwords or credit card details.

Malware: Harmful software like viruses, trojans, worms, and ransomware that can damage or steal data.

DDoS (Distributed Denial of Service): Attackers overload a server with traffic so it becomes unavailable.

SQL Injection: Attackers put malicious code in input fields to steal or change data from databases.

Brute Force Attacks: Continuously trying many password combinations until one works.

Ransomware: A type of malware that locks files and asks for payment to unlock them.

TASK-1 FOUNDATIONS OF CYBERSECURITY

3. Attack Vectors

Social Engineering: Tricking people into giving away sensitive info, like a call pretending to be from a bank.

Wireless Attacks: Hacking into WiFi networks that have weak passwords or poor encryption.

Insider Threats: Employees or trusted people misusing their access to steal or leak data.

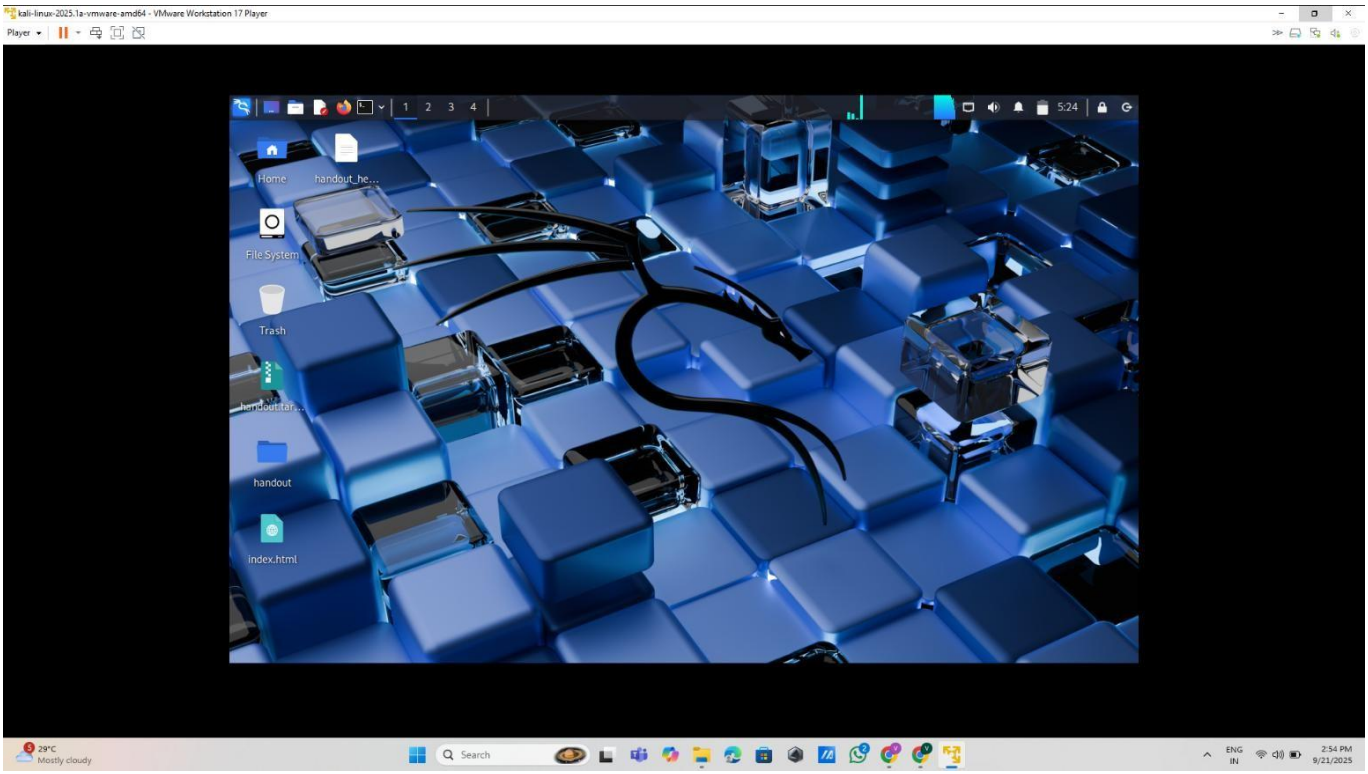
TASK-1 FOUNDATIONS OF CYBERSECURITY

Hacking Lab Setup — VMware with Kali Linux (Attacker) and Metasploitable2 (Target)

Introduction

This is my hacking lab setup using VMware with Kali Linux as the attacker machine and Metasploitable2 as the vulnerable target. Both virtual machines are configured on a Host-Only network to keep the environment isolated from the Internet and my physical LAN.

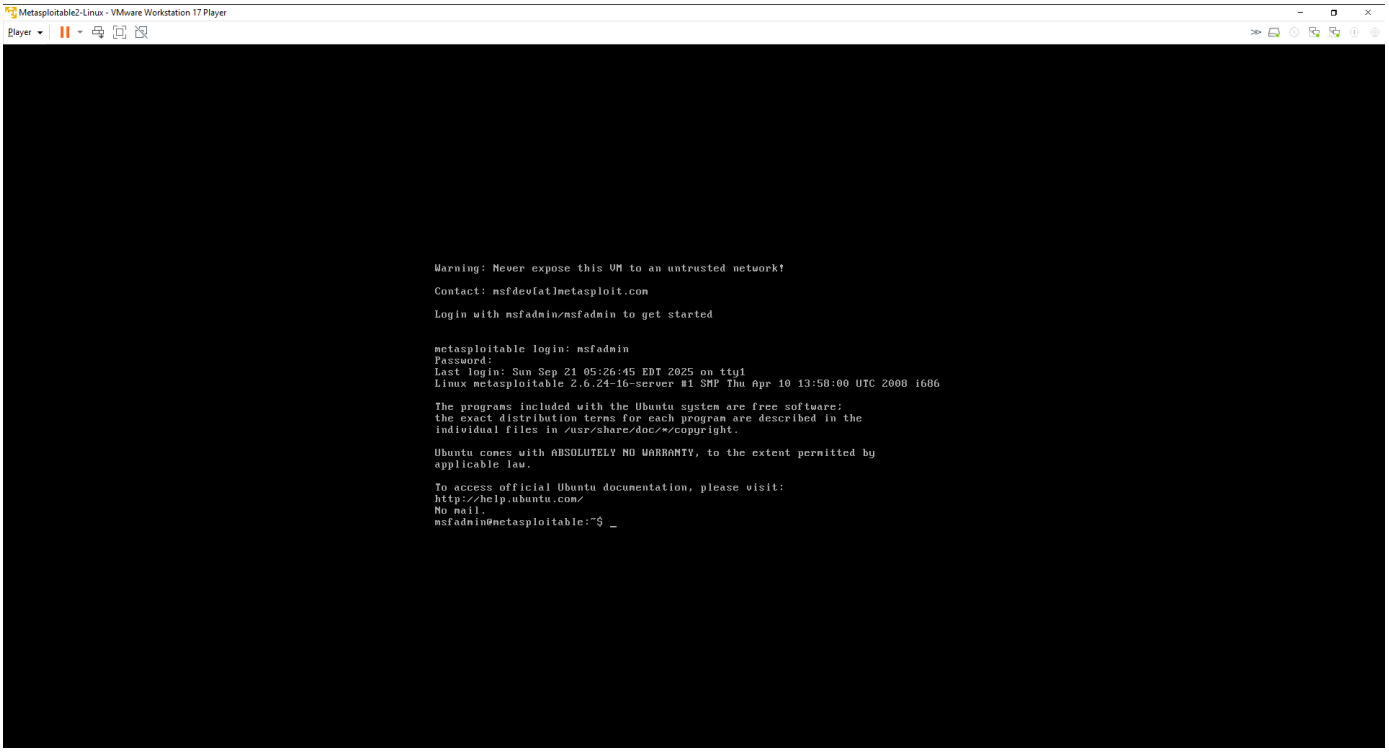
Kali Linux desktop after login



Kali Linux installed successfully and logged in. This VM will act as the attacker machine, with tools such as Nmap and Metasploit available for testing against the target.

TASK-1 FOUNDATIONS OF CYBERSECURITY

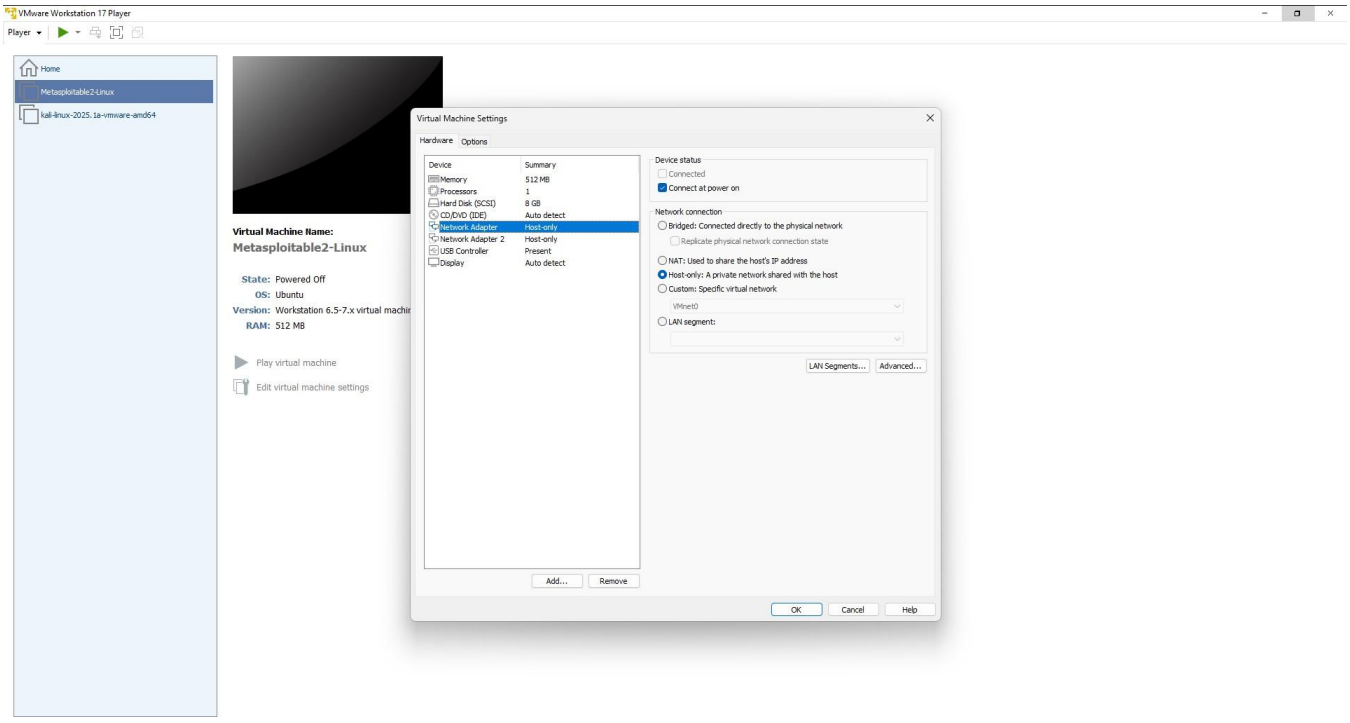
Metasploitable2 login screen



Metasploitable2 running and displaying the console login prompt. This intentionally vulnerable VM serves as the target for security testing and vulnerability scanning.

TASK-1 FOUNDATIONS OF CYBERSECURITY

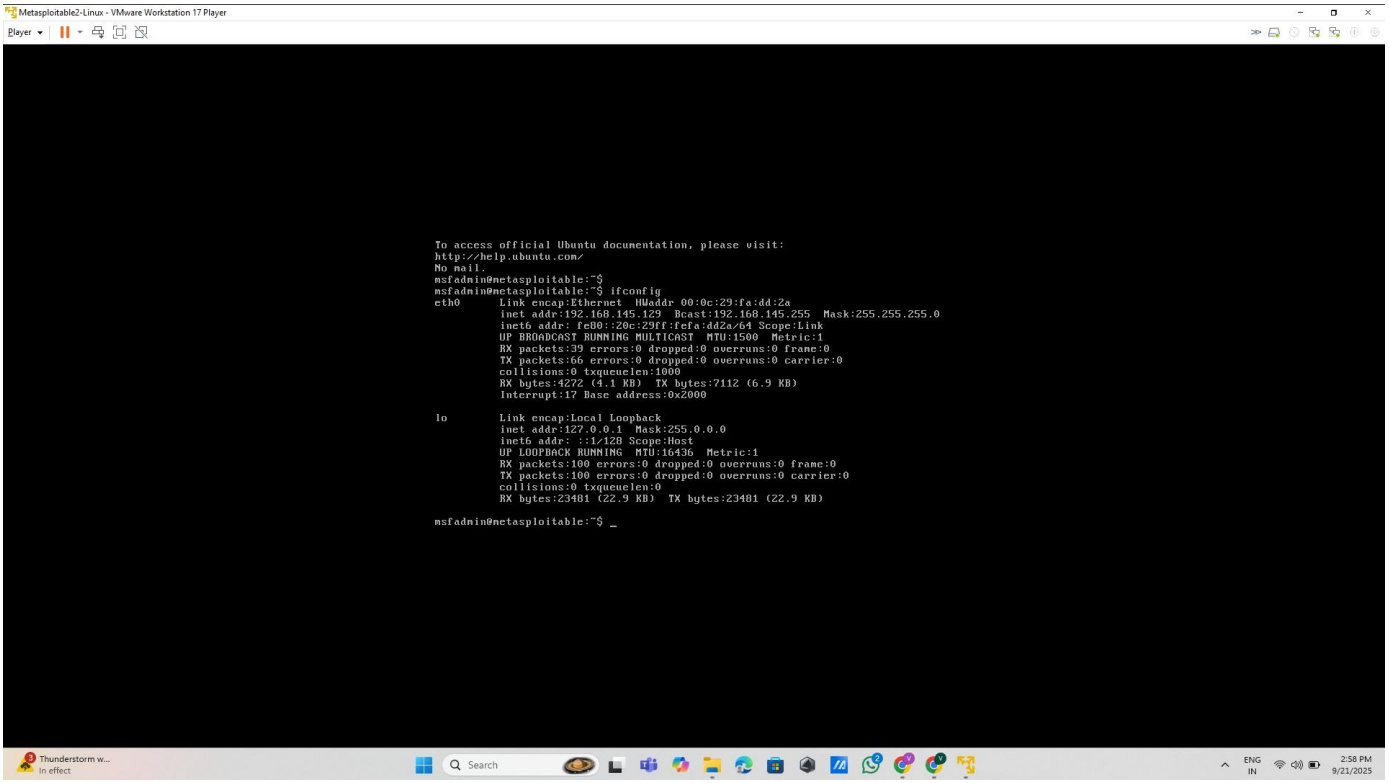
VMware network settings (Host-Only)

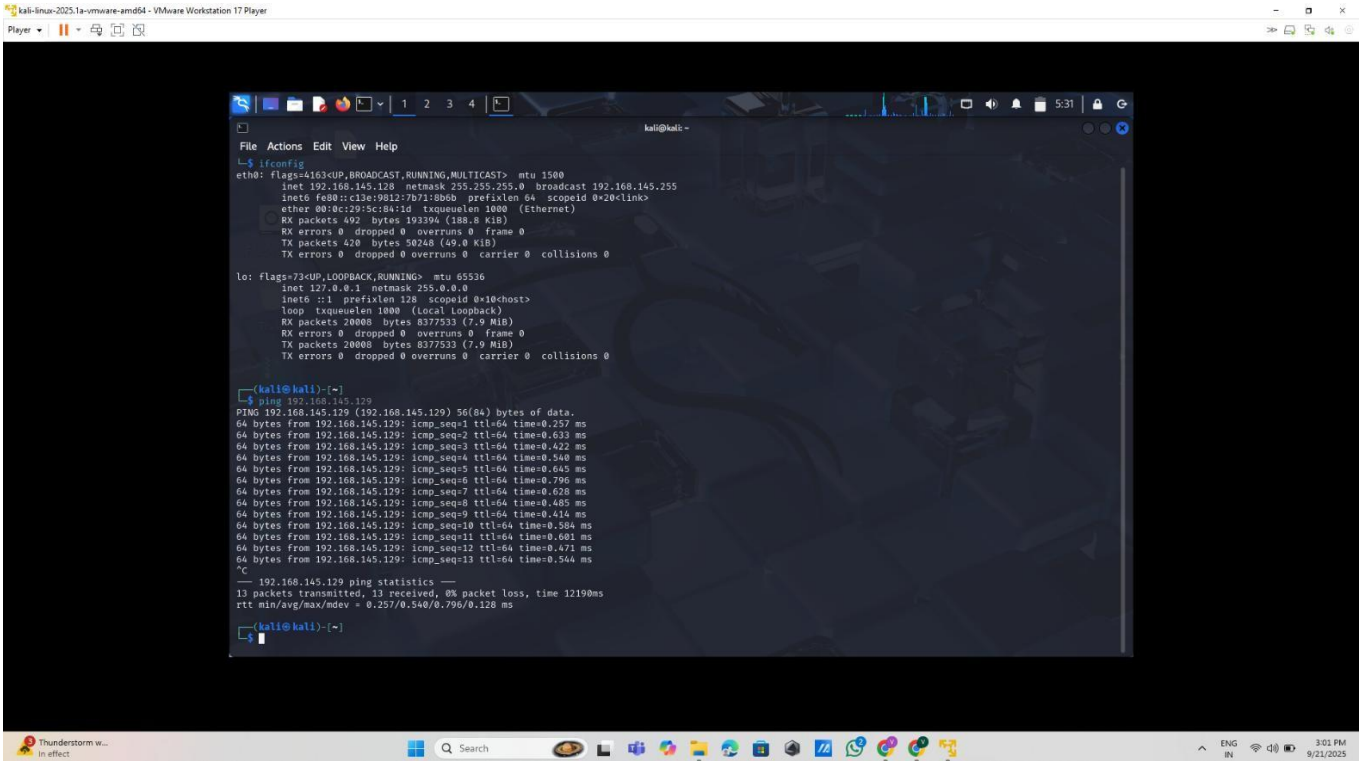


VMware virtual machine network adapter configured to Host-Only. Host-Only networking ensures communication is limited to the host and VMs (isolated lab), preventing exposure to the external network.

TASK-1 FOUNDATIONS OF CYBERSECURITY

Ping test from Kali to Metasploitable2





TASK-1 FOUNDATIONS OF CYBERSECURITY

Verified connectivity with ICMP: Kali successfully pings Metasploitable2 showing replies. This confirms the attacker and target are on the same host-only network and can communicate for testing.

Conclusion

The lab environment has been set up correctly: Kali (attacker) and Metasploitable2 (target) are online, isolated via Host-Only networking, and can communicate — ready for vulnerability scanning and exploitation exercises.

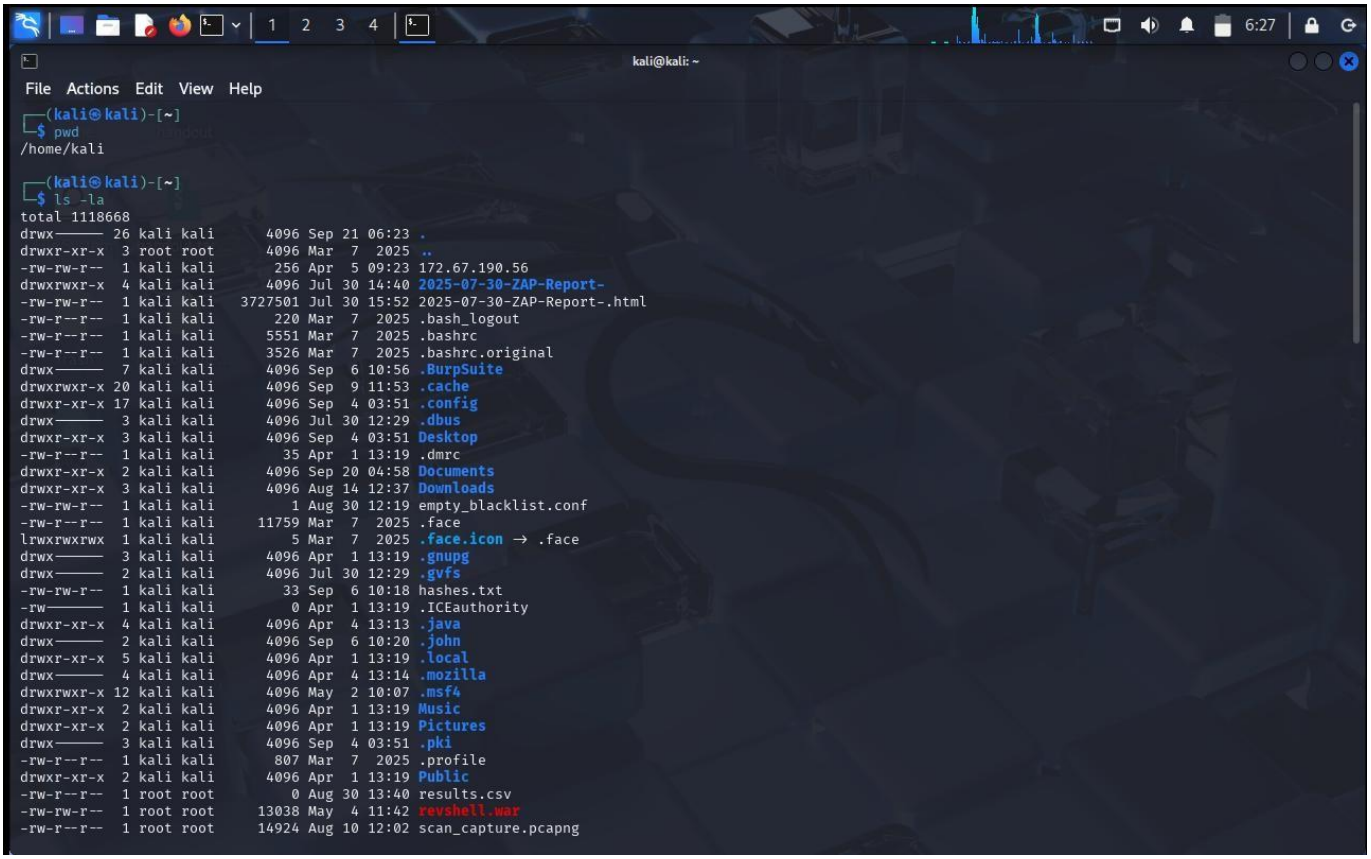
TASK-1 FOUNDATIONS OF CYBERSECURITY

Linux Fundamentals

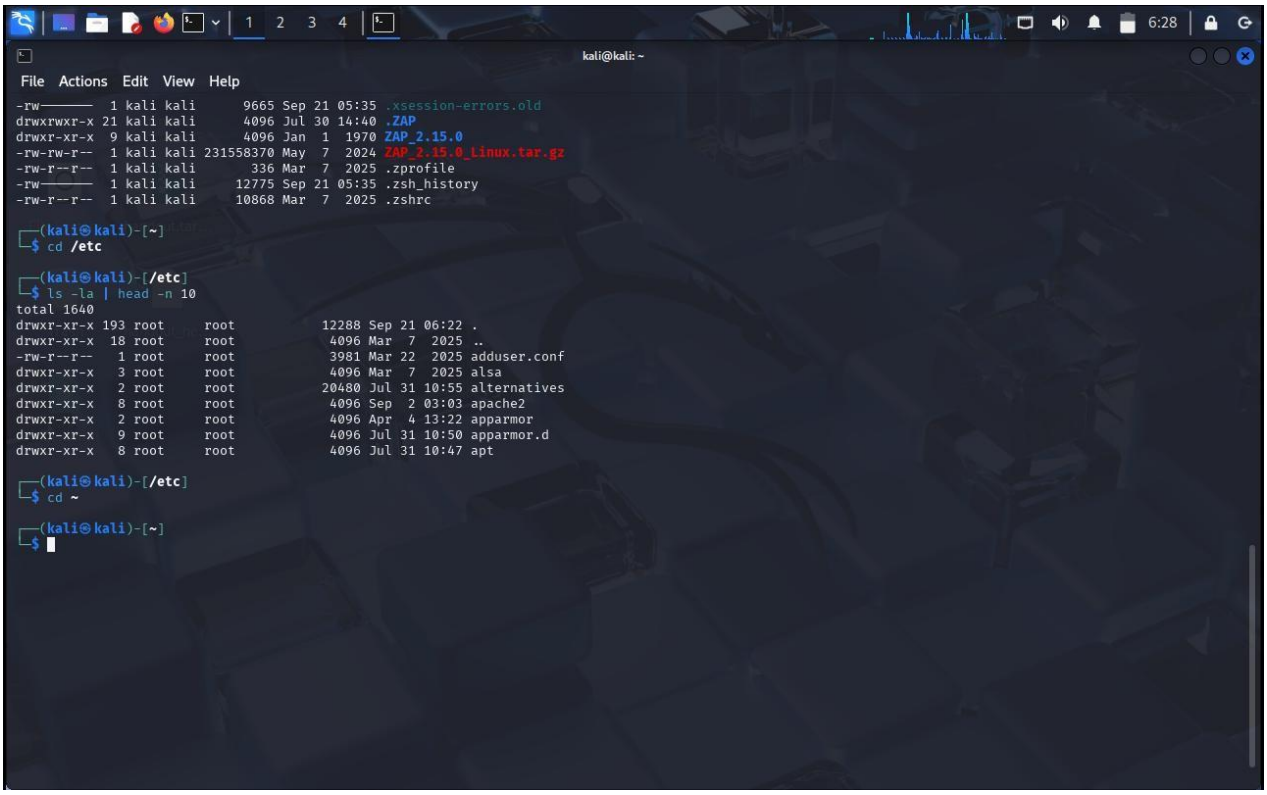
Introduction

This section demonstrates basic Linux fundamentals on the Kali Linux attacker VM: file system navigation, permissions, package management, and networking.

File System Navigation



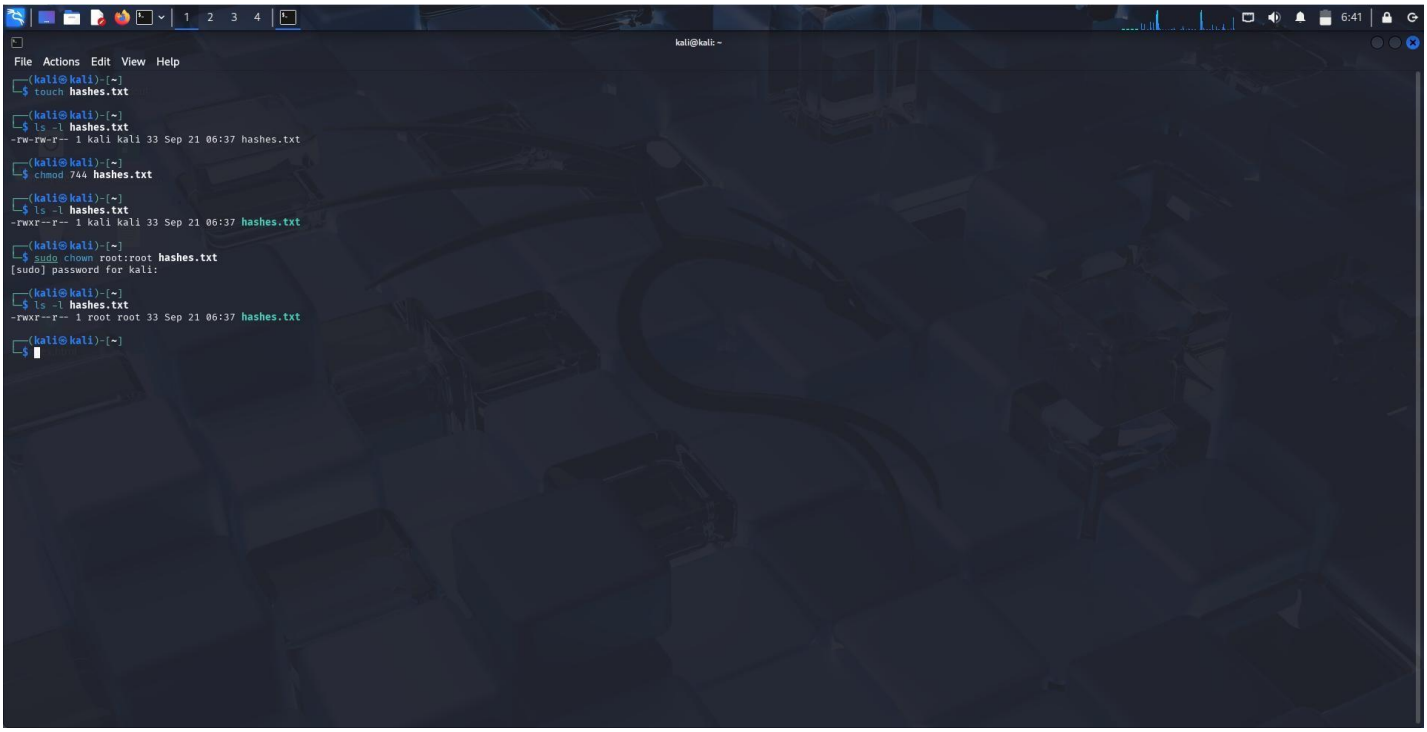
TASK-1 FOUNDATIONS OF CYBERSECURITY



Demonstrated navigation using pwd, ls, and cd. Verified the current working directory and listed contents of /etc and the home directory.

TASK-1 FOUNDATIONS OF CYBERSECURITY

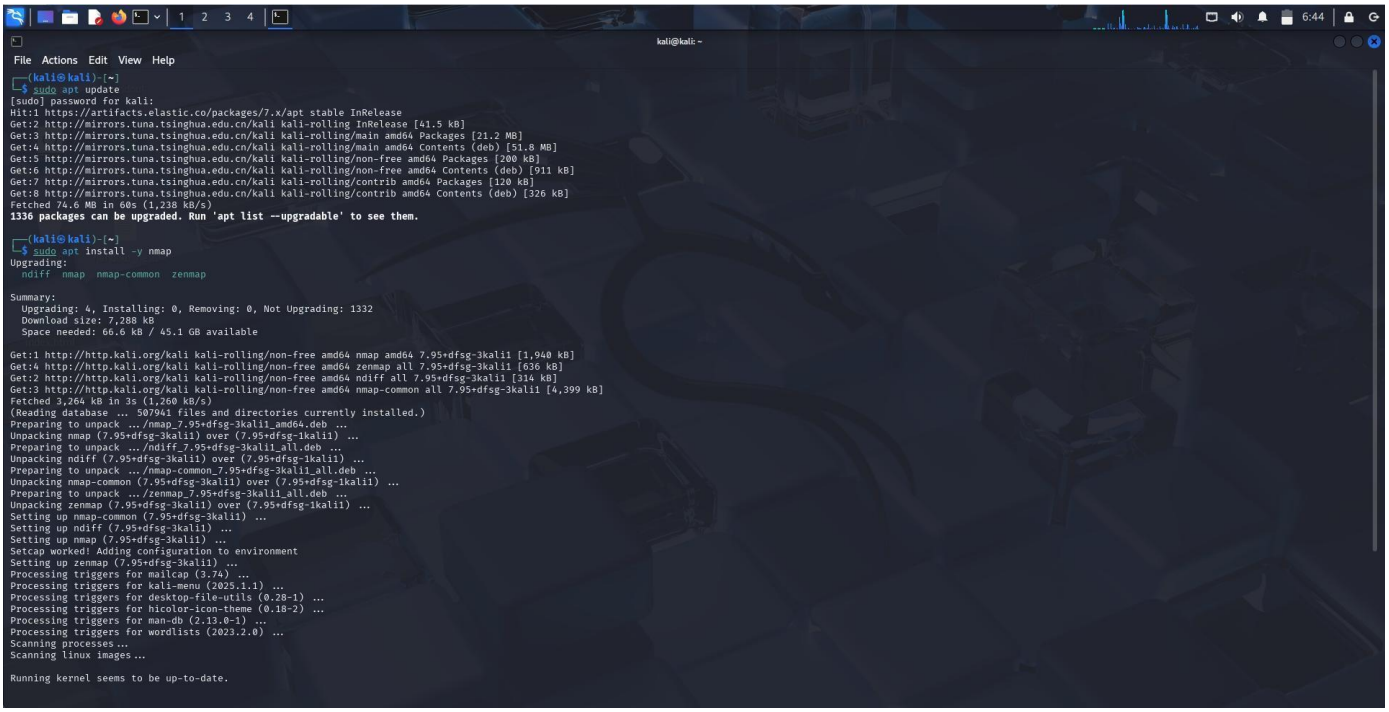
File s Directory Permissions

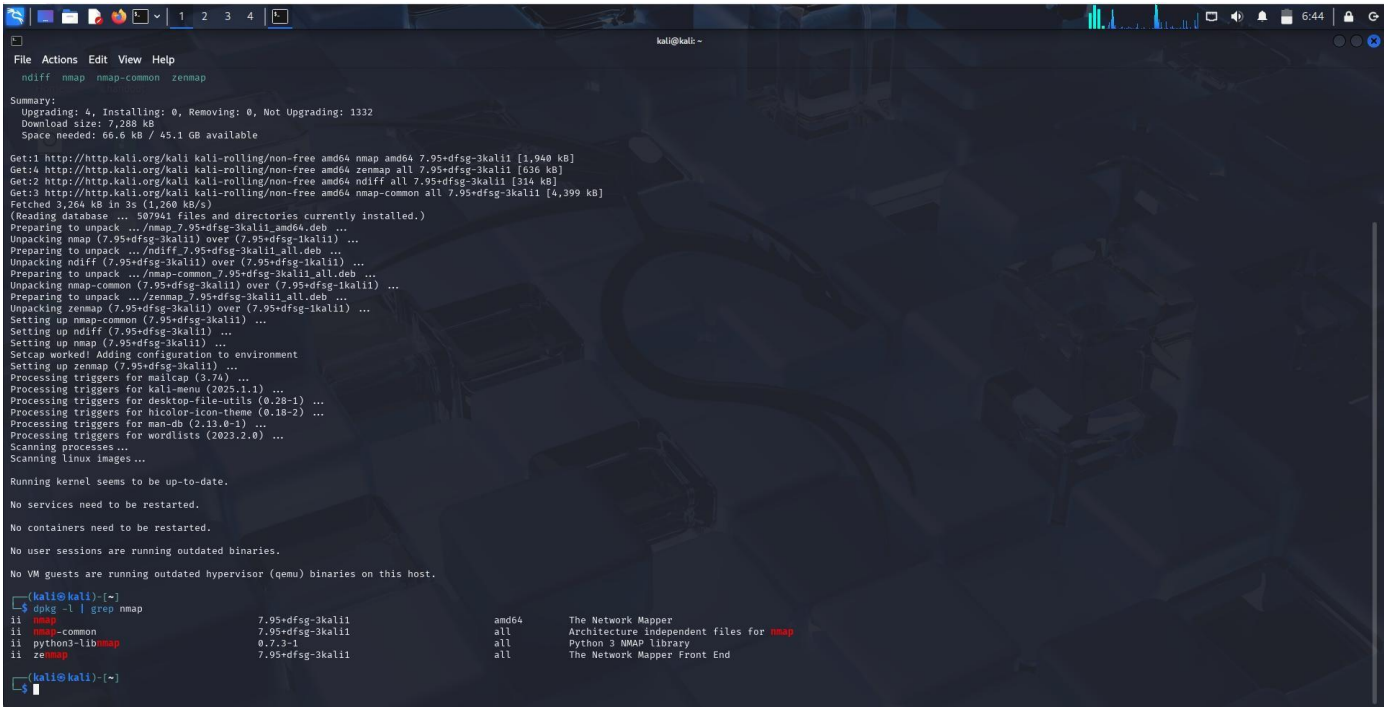


Changed permissions with chmod 744, and changed ownership to root:root with chown. ls -l output shows the permission and ownership changes.

TASK-1 FOUNDATIONS OF CYBERSECURITY

Package Management





Updated package lists and installed nmap using apt. Verified installation with dpkg -l, confirming package management works.

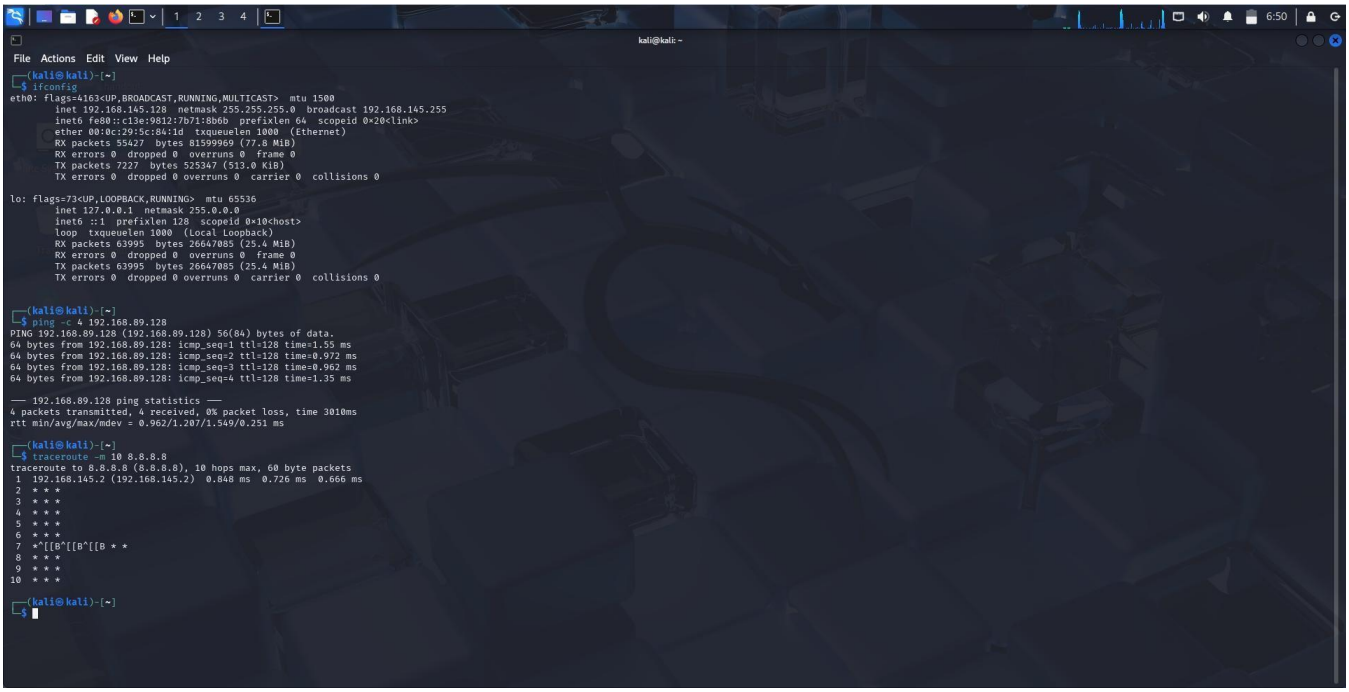
TASK-1 FOUNDATIONS OF CYBERSECURITY

Networking Commands

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:fa:dd:2a
          inet addr:192.168.89.128  Bcast:192.168.89.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fefa:dd2a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:44 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:806 (806.0 B)  TX bytes:4844 (4.7 KB)
          Interrupt:17 Base address:0x2000

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:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ _
```



Displayed network interfaces to find the VM IP, verified connectivity with ping to the target, listed listening services with netstat, and ran traceroute to show the packet path.

TASK-1 FOUNDATIONS OF CYBERSECURITY

Networking Basics

Objective:

To understand the fundamental concepts of computer networking (OSI Model, TCP/IP Suite, DNS, HTTP/HTTPS, IP Addressing, Subnetting, and NAT) and to perform basic networking commands on Kali Linux for practical learning.

OSI Model Layers s Functions

The OSI (Open Systems Interconnection) Model has 7 layers that define how data travels over a network:

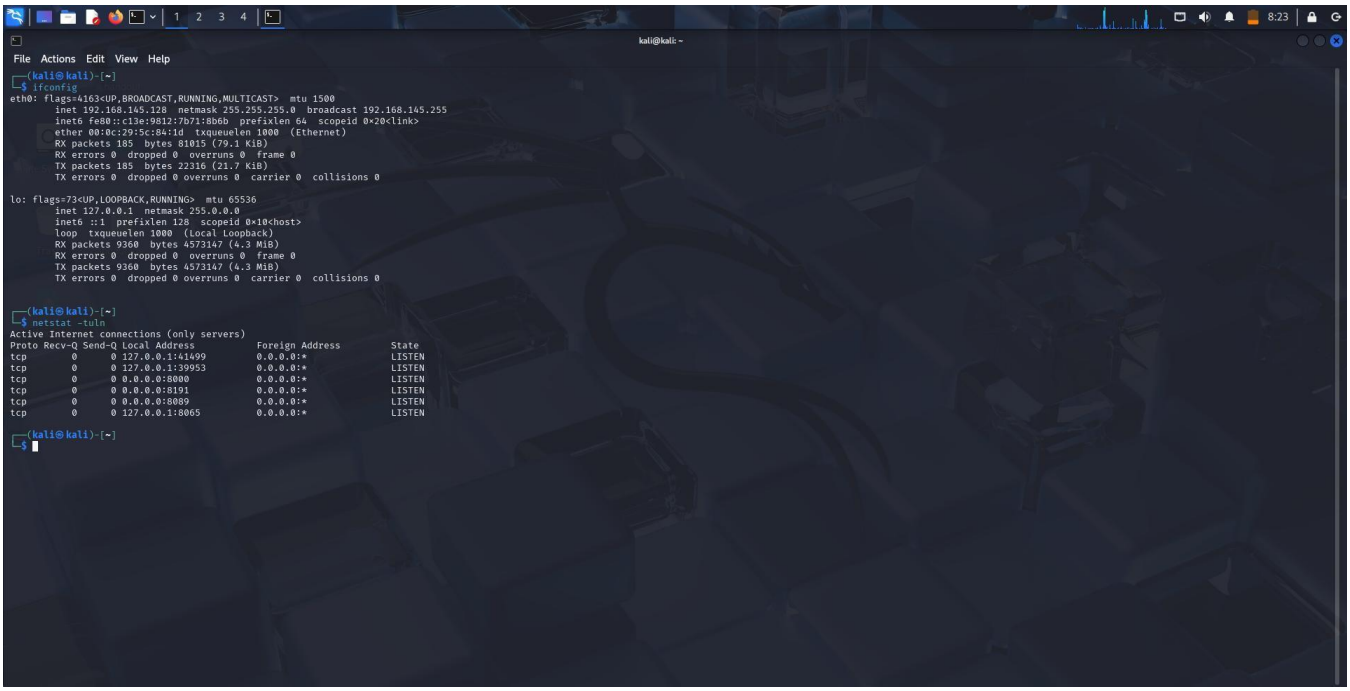
Layer	Function
Application	User interaction, applications like HTTP, FTP, DNS.
Presentation	Data translation, encryption, compression.
Session	Establish, manage and terminate sessions.
Transport	Reliable delivery using TCP/UDP, segmentation.
Network	Logical addressing (IP), routing packets.
Data Link	Physical addressing (MAC), error detection.
Physical	Transmission of bits over cables/wireless.

TASK-1 FOUNDATIONS OF CYBERSECURITY

TCP/IP Protocol Suite

TCP/IP has 4 layers mapping to OSI layers:

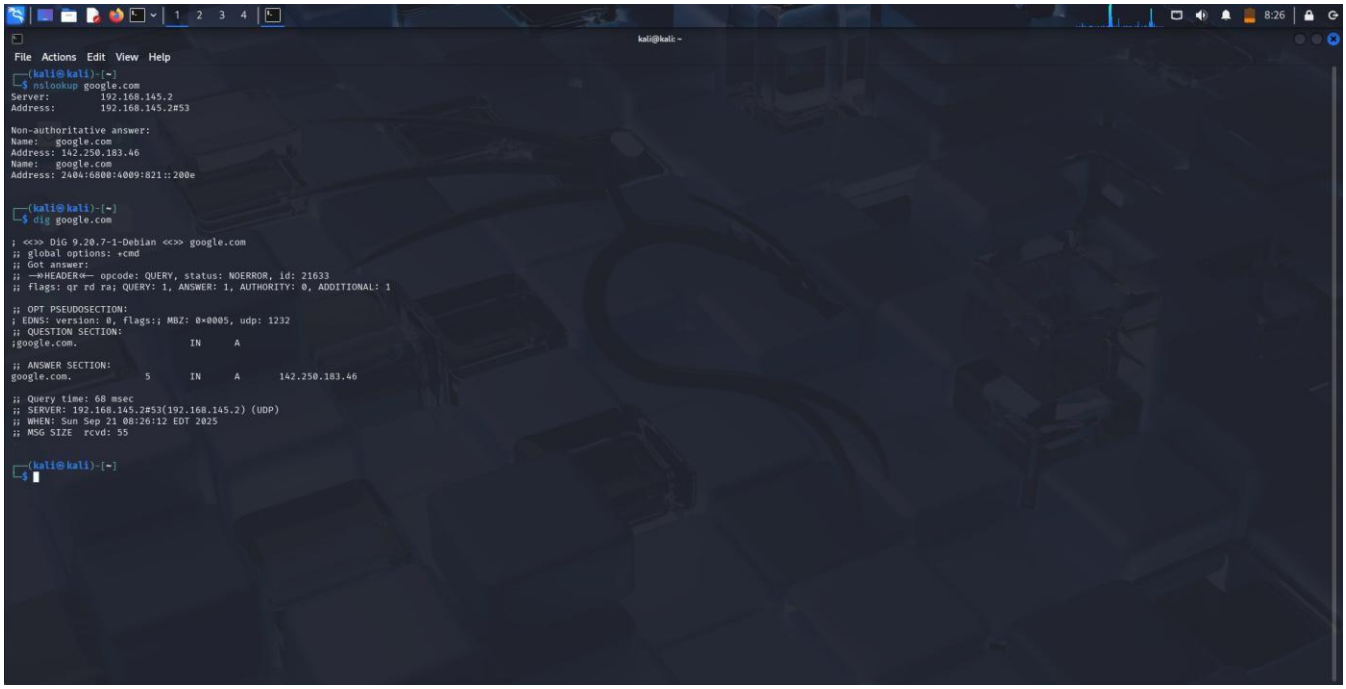
TCP/IP Layer	Example Protocols
Application Layer	HTTP, HTTPS, DNS, FTP, SMTP
Transport Layer	TCP, UDP
Internet Layer	IP, ICMP
Link Layer	Ethernet, Wi-Fi



TASK-1 FOUNDATIONS OF CYBERSECURITY

DNS and HTTP/HTTPS Deep Dive

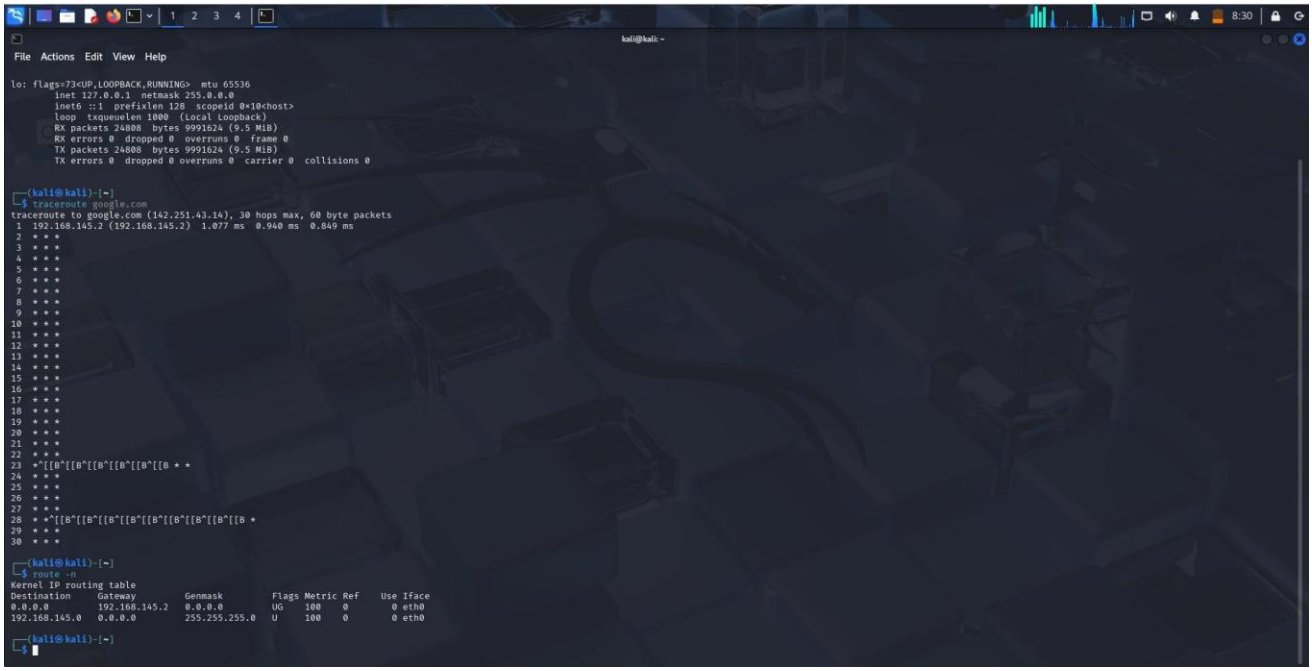
- **DNS** converts domain names (like google.com) into IP addresses.
- **HTTP** is the protocol for transferring web pages; **HTTPS** is HTTP secured with SSL/TLS encryption.



TASK-1 FOUNDATIONS OF CYBERSECURITY

IP Addressing, Subnetting, and NAT

- **IP Address**: Unique address assigned to each device.
- **Subnetting**: Dividing a network into smaller sub-networks; e.g., 192.168.1.0/24.
- **NAT (Network Address Translation)**: Converts private IP addresses to public IP addresses for Internet access.



TASK-1 FOUNDATIONS OF CYBERSECURITY

Cryptography Basics

Objective:

To understand the fundamental concepts of cryptography (symmetric and asymmetric encryption, hashing, and digital signatures) and perform basic encryption/decryption operations using Linux tools.

1. Introduction to Cryptography

Cryptography is the practice of securing information by converting it into a form unreadable to unauthorized users. It ensures:

- Confidentiality (data hidden from unauthorized users),
- Integrity (data not modified),
- Authentication (verify identity),
- Non-repudiation (actions cannot be denied later).

2. Symmetric Encryption

- Uses a single secret key for both encryption and decryption.
- Examples: AES, DES, 3DES, Blowfish.
- Fast but key distribution is harder.

3. Asymmetric Encryption

- Uses two keys: public (for encryption) and private (for decryption).
- Examples: RSA, ECC.
- Slower but solves key distribution problem.

TASK-1 FOUNDATIONS OF CYBERSECURITY

4. Hashing

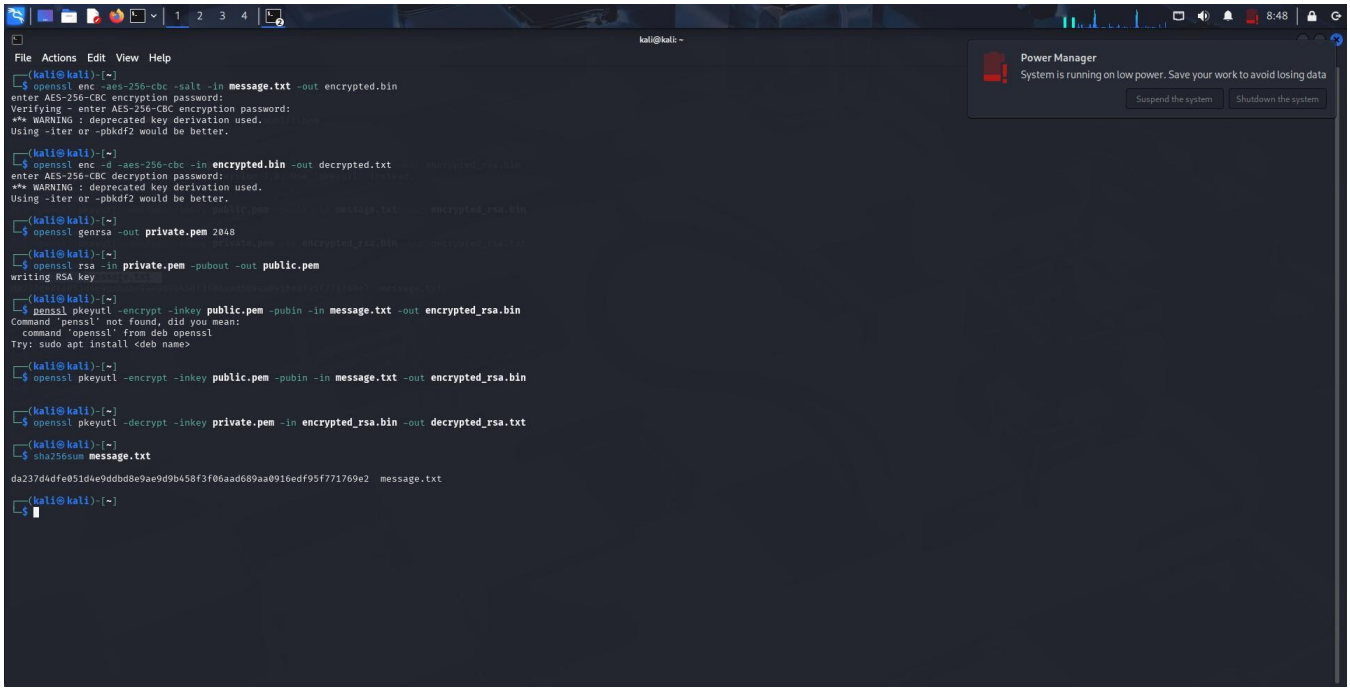
- Converts data into a fixed-length hash.
- One-way function (cannot retrieve original message).
- Examples: SHA-256, MD5.
- Used for password storage, integrity checks.

5. Digital Signatures

- Combine hashing and asymmetric encryption.
- Verify sender authenticity and message integrity.

Observations:

- Encrypted and decrypted files using AES symmetric encryption.
- Generated RSA key pairs and performed public/private key encryption/decryption.
- Created SHA256 hash of a file to verify integrity.



TASK-1 FOUNDATIONS OF CYBERSECURITY

Conclusion:

By performing this task, I learned the basics of cryptography, including symmetric and asymmetric encryption, and hashing. I successfully used OpenSSL commands to encrypt, decrypt, generate keys, and hash files.

TASK-1 FOUNDATIONS OF CYBERSECURITY

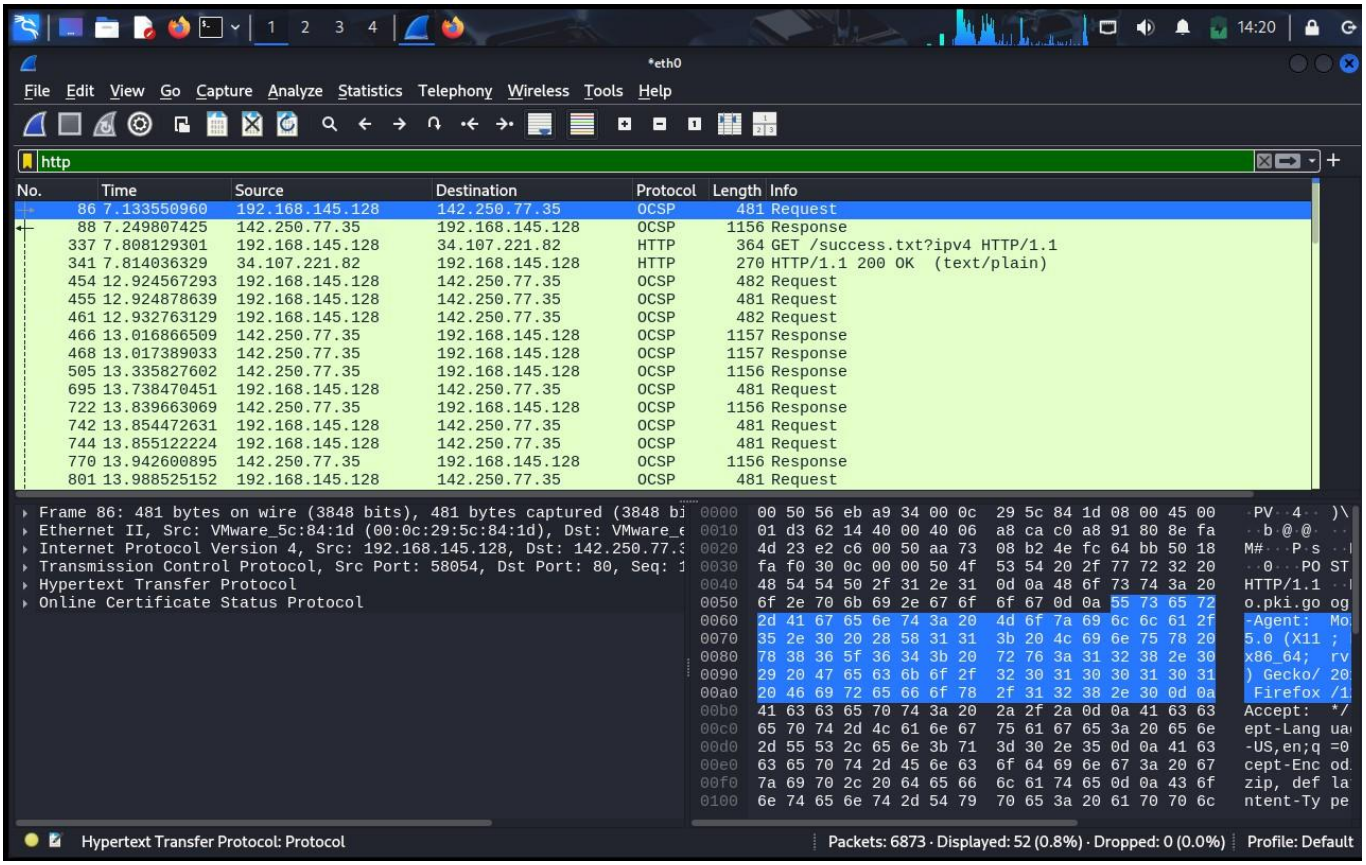
Tool Familiarization

Objective:

To understand the purpose and usage of essential cybersecurity tools and perform basic practical exercises using Wireshark, Nmap, Netcat, and Burp Suite.

1. Wireshark (Packet Capture Tool)

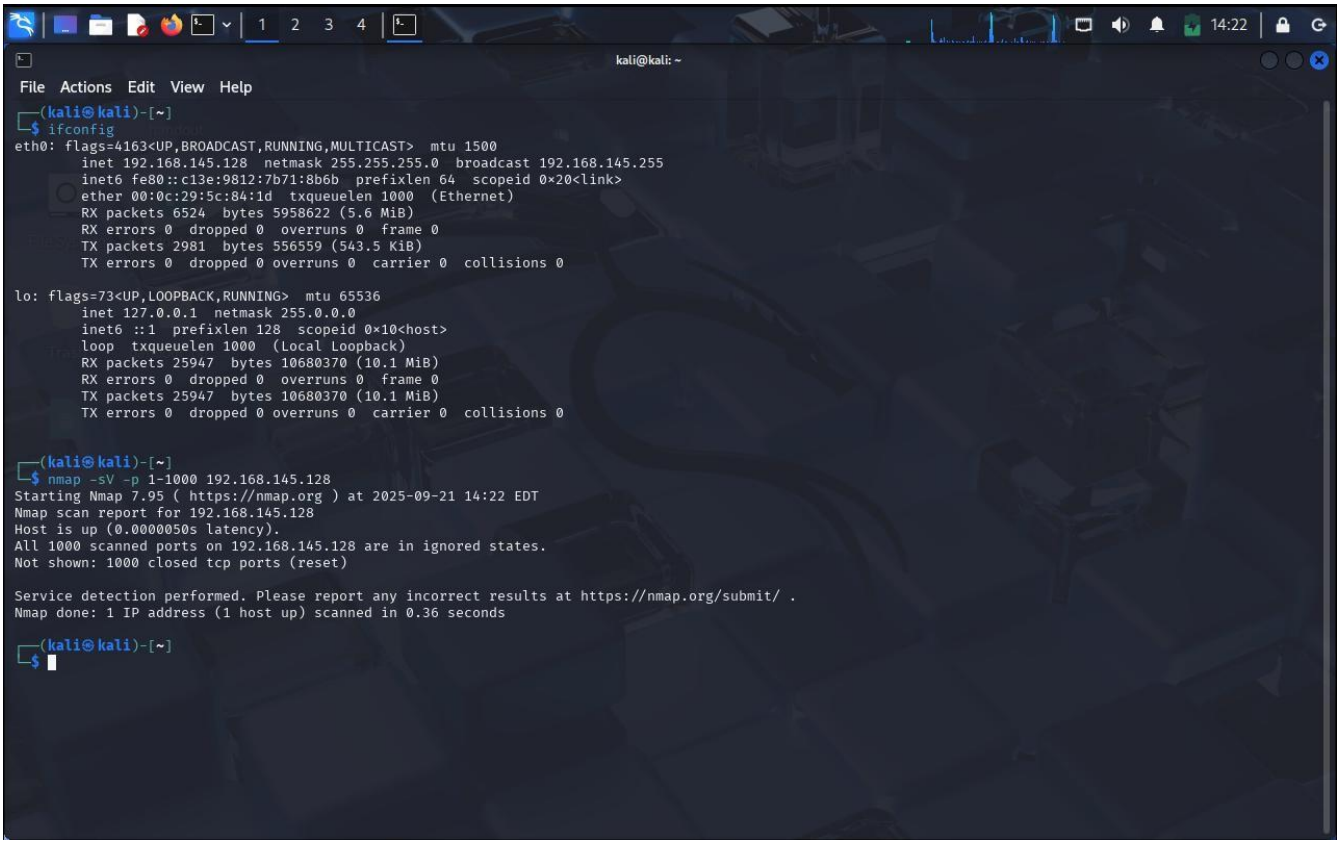
- A free, open-source packet analyzer.
- Used to capture and inspect network packets in real time.
- Helps in troubleshooting network issues and analyzing malicious traffic.



TASK-1 FOUNDATIONS OF CYBERSECURITY

2. Nmap (Network Mapper)

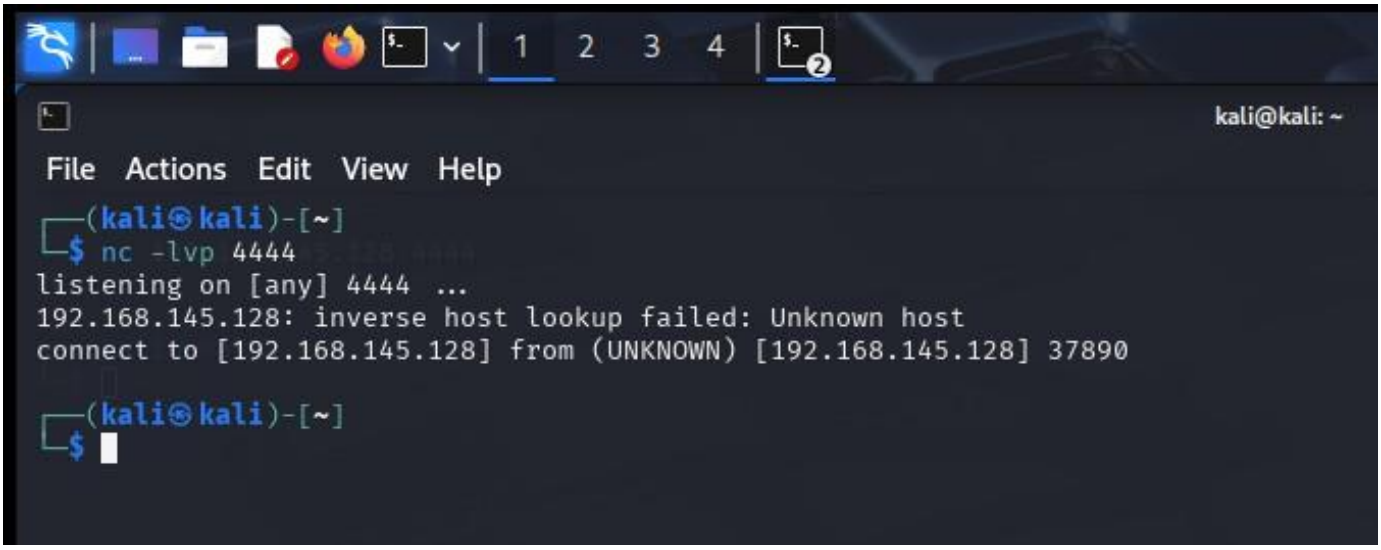
- A network scanning tool used to discover hosts, services, and open ports on a network.
- Can detect operating systems and service versions.



TASK-1 FOUNDATIONS OF CYBERSECURITY

3. Netcat (Swiss Army Knife)

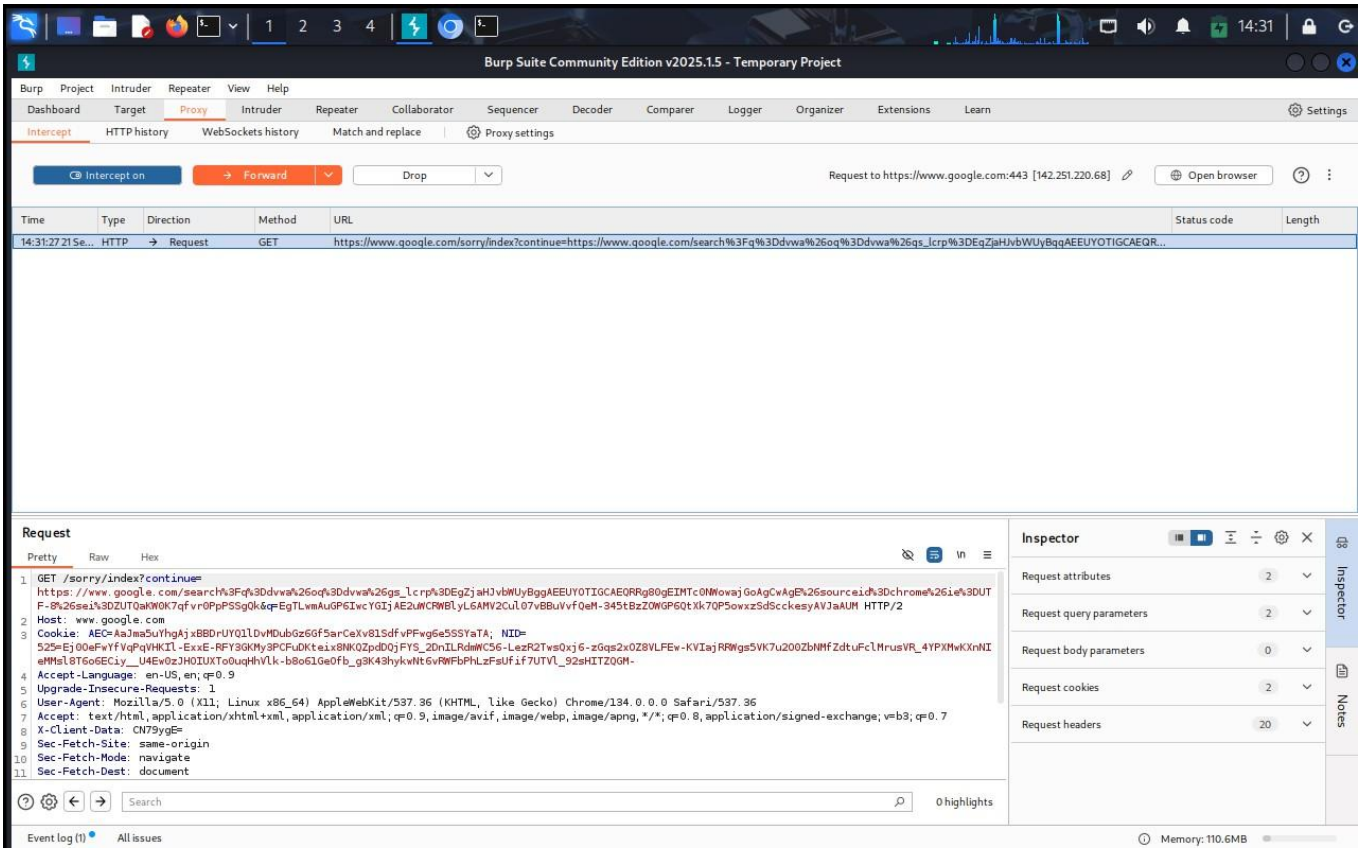
- A utility to read and write data across network connections using TCP/UDP.
- Used for port scanning, file transfer, and simple chat between hosts.



TASK-1 FOUNDATIONS OF CYBERSECURITY

4. Burp Suite (Web Proxy/Testing Tool)

- Intercepts web traffic between browser and server.
- Allows security testing of web applications (analyzing requests, performing injections, scanning vulnerabilities).



TASK-1 FOUNDATIONS OF CYBERSECURITY

Observations:

- Captured live network packets in Wireshark and filtered HTTP traffic.
- Scanned a host using Nmap and identified open ports and services.
- Used Netcat to create a simple listener and connected to it to transfer data.
- Intercepted HTTP requests using Burp Suite.

Conclusion:

By performing these tasks, I learned the practical usage of key cybersecurity tools:

- **Wireshark** for packet capture and analysis.
- **Nmap** for scanning networks and services.
- **Netcat** for creating network connections and testing ports.
- **Burp Suite** for intercepting and analyzing web traffic.
  This gave me a strong foundation for future vulnerability assessment and penetration testing activities.

TASK-1 FOUNDATIONS OF CYBERSECURITY

Conclusion

By completing Task 1 – Foundation & Environment Setup, I successfully built and configured a safe cybersecurity lab environment using Kali Linux, Metasploitable, and Wireshark. Each section strengthened my understanding of Linux basics, networking concepts, and security fundamentals. I practiced using essential tools, captured live network traffic, and documented my work with theory and screenshots.

This lab setup now serves as a secure environment for performing penetration testing and practicing cybersecurity skills. It provides a strong foundation for upcoming tasks in the internship and has improved my hands-on experience with real-world cybersecurity tools.