

# 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.

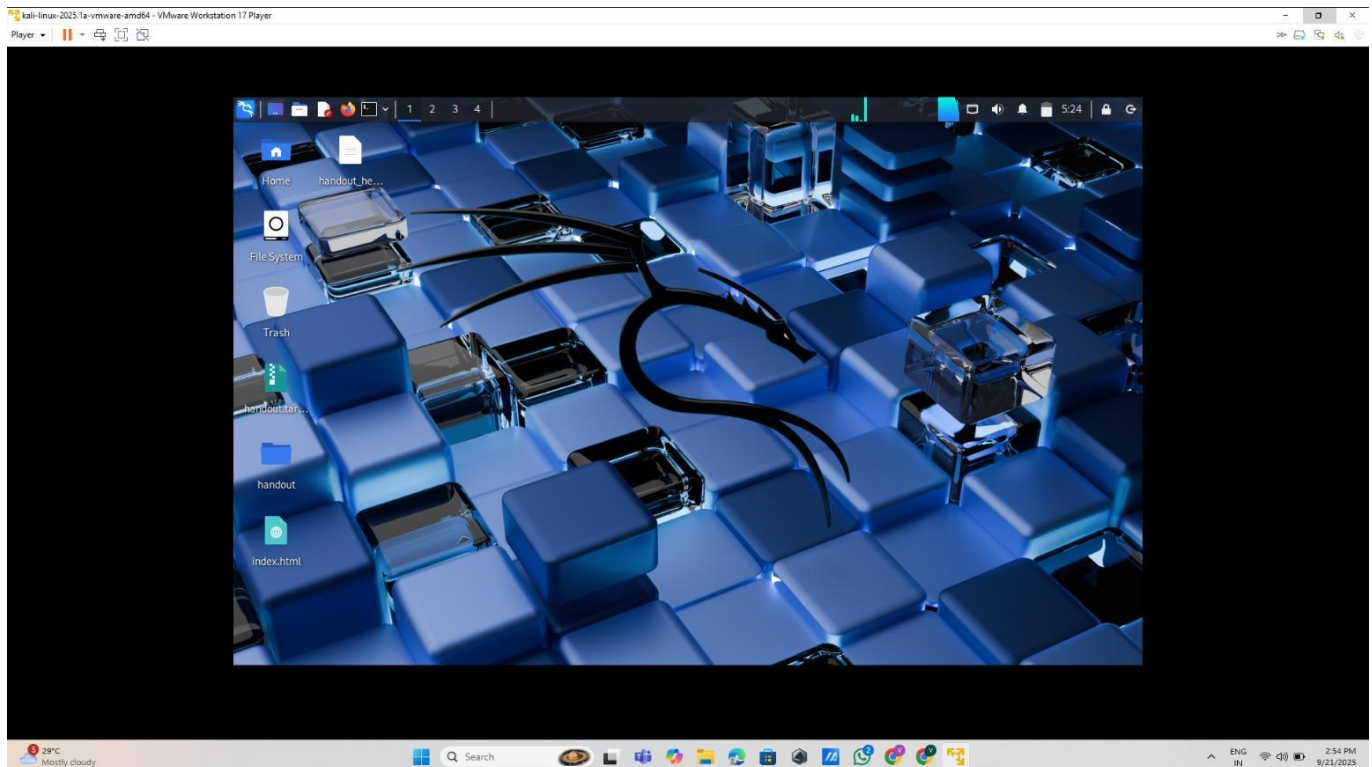
# TASK-1 FOUNDATIONS OF CYBERSECURITY

## 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.

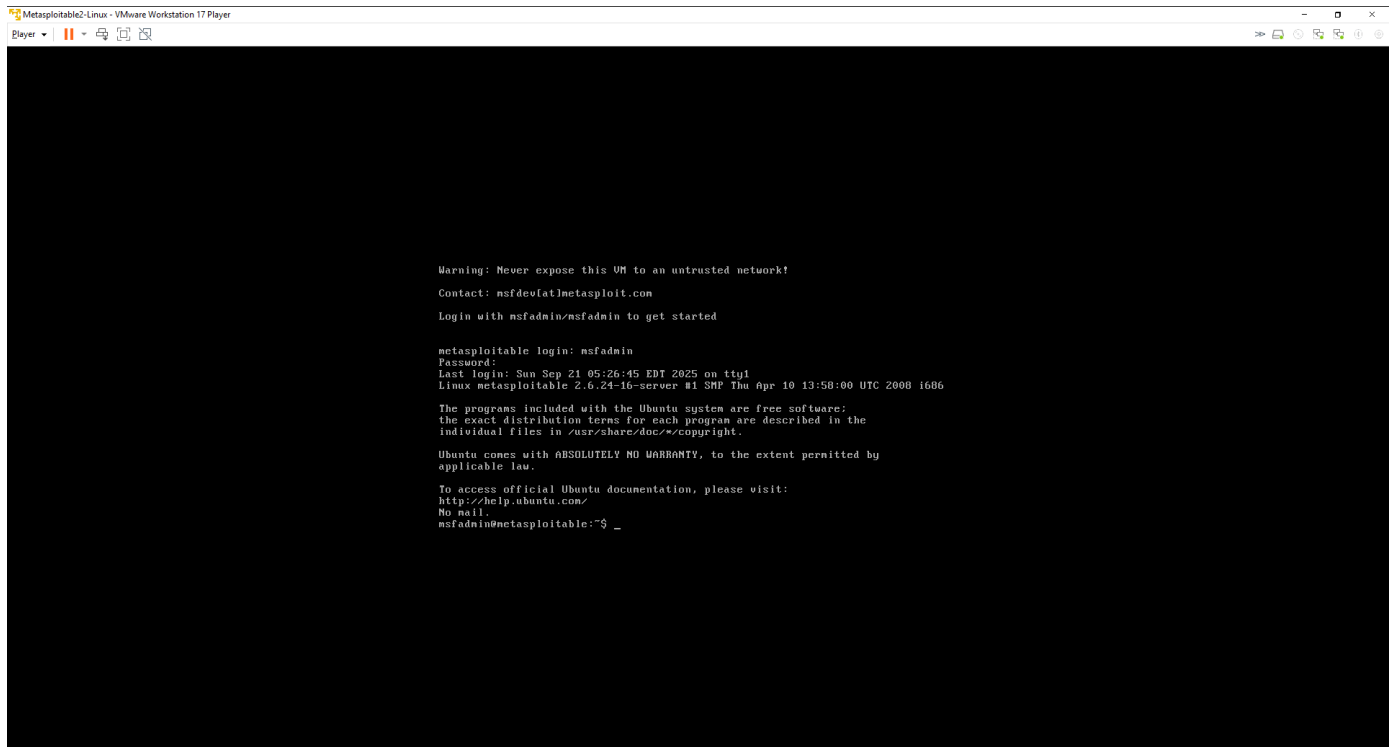
### Kali Linux desktop after login



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-Linux - VMware Workstation 17 Player
Player  ▾  ||  ▾  🔍  📄  🗑️

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Sun Sep 21 05:26:45 EDT 2025 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.

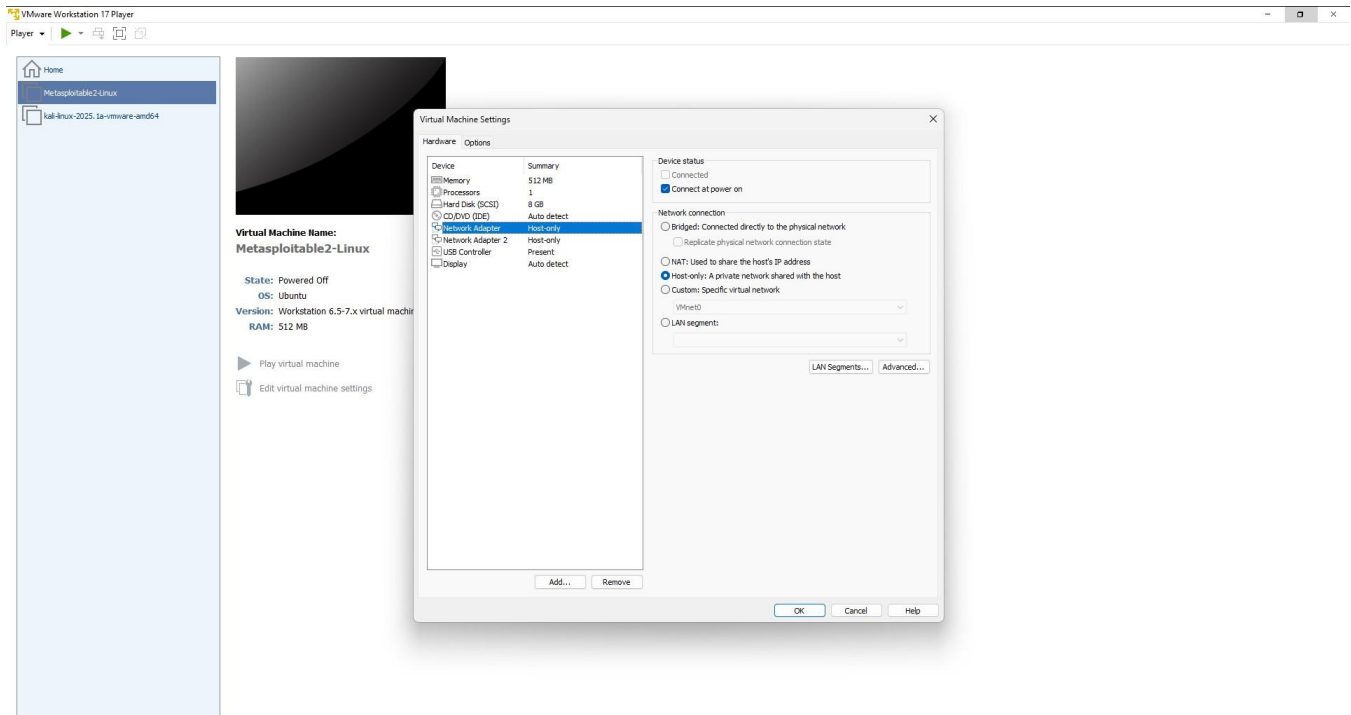
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ _
```

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.

## Ping test from Kali to Metasploitable2

```

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:0c:29:fa:dd:2a
          inet addr:192.168.145.129  Bcast:192.168.145.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29fff:fefa:d42a:b4 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:39 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4272 (4.1 KB)  TX bytes:7112 (6.9 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:65536  Metric:1
          RX packets:100 errors:0 dropped:0 overruns:0 frame:0
          TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23401 (22.9 KB)  TX bytes:23401 (22.9 KB)

msfadmin@metasploitable:~$ _

```

The screenshot shows a Kali Linux terminal window with the following content:

```

kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.145.128 netmask 255.255.255.0 broadcast 192.168.145.255
    inet6 fe80::c13e:9812:7b71:8b6b prefixlen 64 scopeid 0<20<link>
    ether 00:0c:29:5c:84:1d txqueuelen 1000 (Ethernet)
    RX packets 492 bytes 193194 (188.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 420 bytes 50248 (49.0 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 0<1<host>
    loop txqueuelen 1000 (local loopback)
    RX packets 20008 bytes 8377533 (7.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20008 bytes 8377533 (7.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali@kali:~$ ping 192.168.145.129
PING 192.168.145.129 (192.168.145.129) 56(84) bytes of data:
64 bytes from 192.168.145.129: icmp_seq=1 ttl=64 time=0.257 ms
64 bytes from 192.168.145.129: icmp_seq=2 ttl=64 time=0.633 ms
64 bytes from 192.168.145.129: icmp_seq=3 ttl=64 time=0.422 ms
64 bytes from 192.168.145.129: icmp_seq=4 ttl=64 time=0.540 ms
64 bytes from 192.168.145.129: icmp_seq=5 ttl=64 time=0.645 ms
64 bytes from 192.168.145.129: icmp_seq=6 ttl=64 time=0.796 ms
64 bytes from 192.168.145.129: icmp_seq=7 ttl=64 time=0.628 ms
64 bytes from 192.168.145.129: icmp_seq=8 ttl=64 time=0.485 ms
64 bytes from 192.168.145.129: icmp_seq=9 ttl=64 time=0.414 ms
64 bytes from 192.168.145.129: icmp_seq=10 ttl=64 time=0.584 ms
64 bytes from 192.168.145.129: icmp_seq=11 ttl=64 time=0.601 ms
64 bytes from 192.168.145.129: icmp_seq=12 ttl=64 time=0.471 ms
64 bytes from 192.168.145.129: icmp_seq=13 ttl=64 time=0.544 ms
^C
--- 192.168.145.129 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12190ms
rtt min/avg/max/mdev = 0.257/0.540/0.796/0.128 ms

kali@kali:~$

```

# 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.

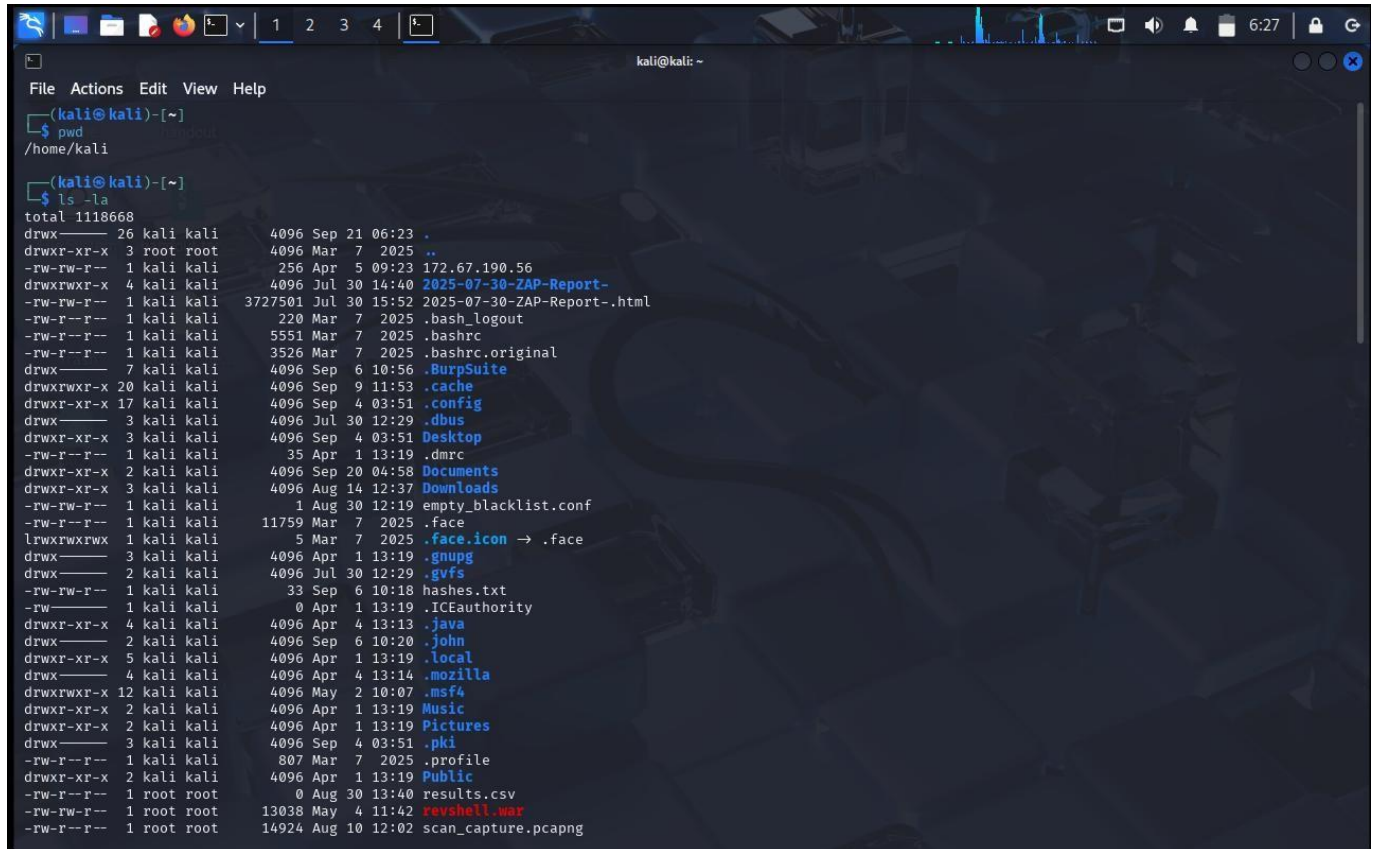
# TASK-1 FOUNDATIONS OF CYBERSECURITY

## Linux Fundamentals

### Introduction

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

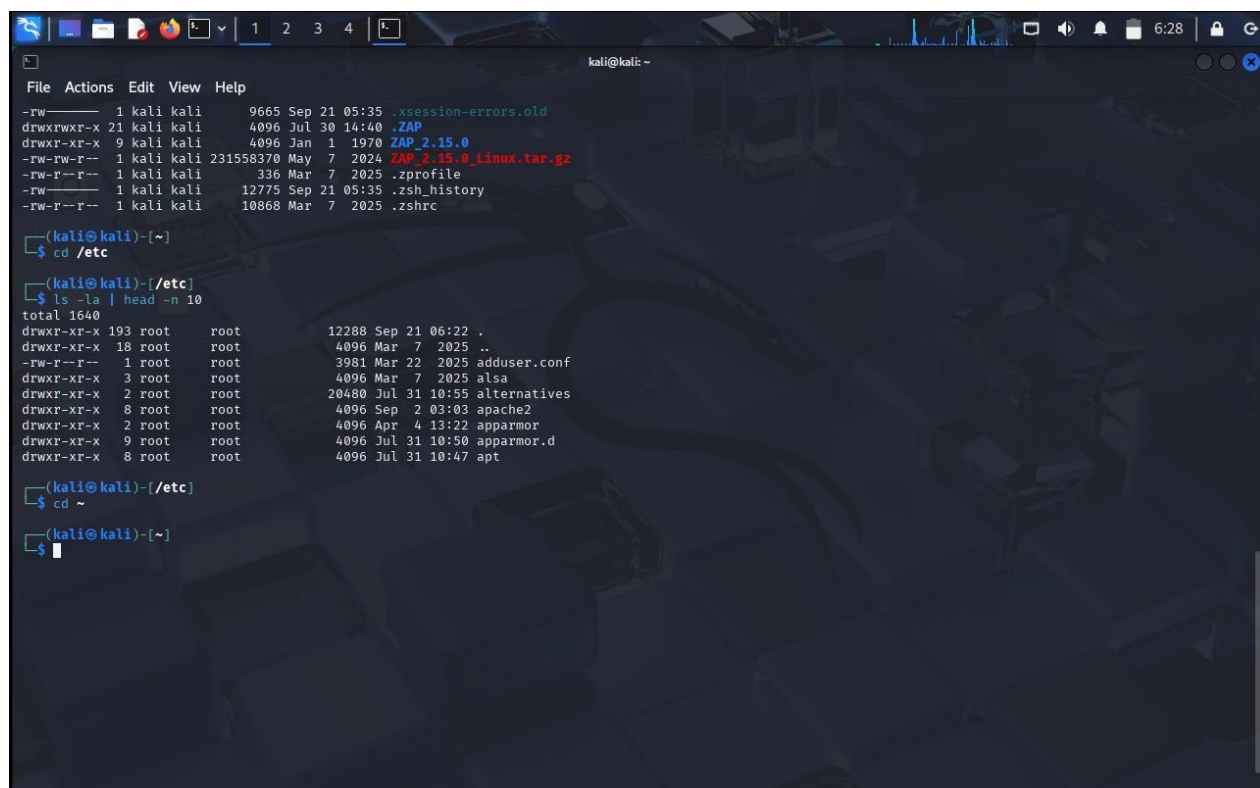
### File System Navigation



```
kali@kali: ~  
File Actions Edit View Help  
$ pwd  
/home/kali  
$ ls -la  
total 1118668  
drwxr-xr-x 26 kali kali 4096 Sep 21 06:23 .  
drwxr-xr-x 3 root root 4096 Mar 7 2025 ..  
-rw-rw-r-- 1 kali kali 256 Apr 5 09:23 172.67.190.56  
drwxrwxr-x 4 kali kali 4096 Jul 30 14:40 2025-07-30-ZAP-Report-  
-rw-rw-r-- 1 kali kali 3727501 Jul 30 15:52 2025-07-30-ZAP-Report-.html  
-rw-r--r-- 1 kali kali 220 Mar 7 2025 .bash_logout  
-rw-r--r-- 1 kali kali 5551 Mar 7 2025 .bashrc  
-rw-r--r-- 1 kali kali 3526 Mar 7 2025 .bashrc.original  
drwxr-xr-x 7 kali kali 4096 Sep 6 10:56 .BurpSuite  
drwxrwxr-x 20 kali kali 4096 Sep 9 11:53 .cache  
drwxr-xr-x 17 kali kali 4096 Sep 4 03:51 .config  
drwxr-xr-x 3 kali kali 4096 Jul 30 12:29 .dbus  
drwxr-xr-x 3 kali kali 4096 Sep 4 03:51 Desktop  
-rw-r--r-- 1 kali kali 35 Apr 1 13:19 .dmrc  
drwxr-xr-x 2 kali kali 4096 Sep 20 04:58 Documents  
drwxr-xr-x 3 kali kali 4096 Aug 14 12:37 Downloads  
-rw-rw-r-- 1 kali kali 1 Aug 30 12:19 empty_blacklist.conf  
-rw-r--r-- 1 kali kali 11759 Mar 7 2025 .face  
lrwxrwxrwx 1 kali kali 5 Mar 7 2025 .face.icon -> .face  
drwxr-xr-x 3 kali kali 4096 Apr 1 13:19 .gnupg  
drwxr-xr-x 2 kali kali 4096 Jul 30 12:29 .gvfs  
-rw-rw-r-- 1 kali kali 33 Sep 6 10:18 hashes.txt  
-rw-r--r-- 1 kali kali 0 Apr 1 13:19 .ICEauthority  
drwxr-xr-x 4 kali kali 4096 Apr 4 13:13 .java  
drwxr-xr-x 2 kali kali 4096 Sep 6 10:20 .john  
drwxr-xr-x 5 kali kali 4096 Apr 1 13:19 .local  
drwxr-xr-x 4 kali kali 4096 Apr 4 13:14 .mozilla  
drwxrwxr-x 12 kali kali 4096 May 2 10:07 .msf4  
drwxr-xr-x 2 kali kali 4096 Apr 1 13:19 Music  
drwxr-xr-x 2 kali kali 4096 Apr 1 13:19 Pictures  
drwxr-xr-x 3 kali kali 4096 Sep 4 03:51 .pki  
-rw-r--r-- 1 kali kali 807 Mar 7 2025 .profile  
drwxr-xr-x 2 kali kali 4096 Apr 1 13:19 Public  
-rw-r--r-- 1 root root 0 Aug 30 13:40 results.csv  
-rw-r--r-- 1 root root 13038 May 4 11:42 revshell.war  
-rw-r--r-- 1 root root 14924 Aug 10 12:02 scan_capture.pcapng
```



# TASK-1 FOUNDATIONS OF CYBERSECURITY



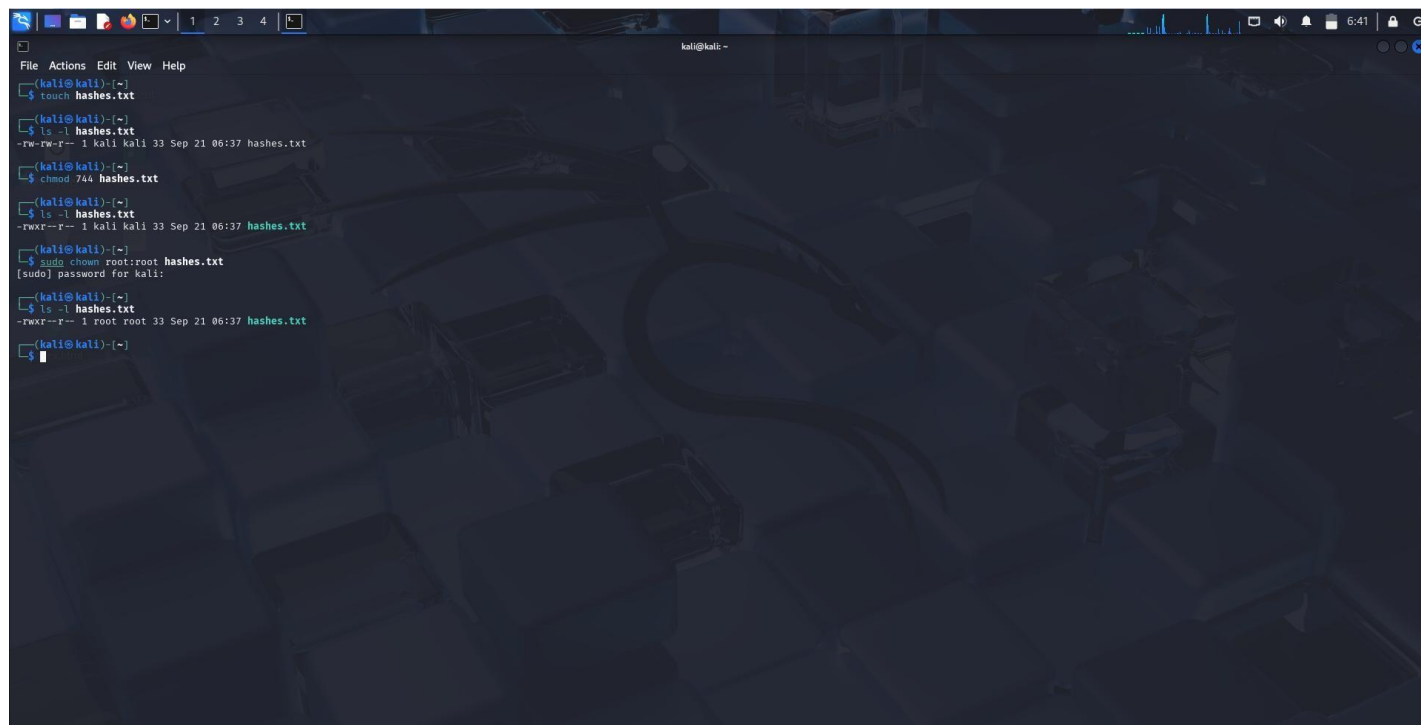
The screenshot shows a Kali Linux terminal window with a dark theme. The terminal displays the following commands and output:

```
kali@kali: ~  
File Actions Edit View Help  
-rw-rw-r-- 1 kali kali 9665 Sep 21 05:35 .xsession-errors.old  
drwxrwxr-x 21 kali kali 4096 Jul 30 14:40 .ZAP  
drwxr-xr-x 9 kali kali 4096 Jan 1 1970 ZAP_2.15.0  
-rw-rw-r-- 1 kali kali 231558370 May 7 2024 ZAP_2.15.0.Linux.tar.gz  
-rw-r--r-- 1 kali kali 336 Mar 7 2025 .zprofile  
-rw-rw-r-- 1 kali kali 12775 Sep 21 05:35 .zsh_history  
-rw-r--r-- 1 kali kali 10868 Mar 7 2025 .zshrc  
  
(kali@kali)-[~]  
$ cd /etc  
  
(kali@kali)-[/etc]  
$ ls -la | head -n 10  
total 1640  
drwxr-xr-x 193 root root 12288 Sep 21 06:22 .  
drwxr-xr-x 18 root root 4096 Mar 7 2025 ..  
-rw-r--r-- 1 root root 3981 Mar 22 2025 adduser.conf  
drwxr-xr-x 3 root root 4096 Mar 7 2025 alsa  
drwxr-xr-x 2 root root 20480 Jul 31 10:55 alternatives  
drwxr-xr-x 8 root root 4096 Sep 2 03:03 apache2  
drwxr-xr-x 2 root root 4096 Apr 4 13:22 apparmor  
drwxr-xr-x 9 root root 4096 Jul 31 10:50 apparmor.d  
drwxr-xr-x 8 root root 4096 Jul 31 10:47 apt  
  
(kali@kali)-[/etc]  
$ cd ~  
  
(kali@kali)-[~]  
$
```

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



```
File Actions Edit View Help
kali@kali: ~
$ touch hashes.txt
kali@kali: ~
$ ls -l hashes.txt
-rw-rw-r-- 1 kali kali 33 Sep 21 06:37 hashes.txt
kali@kali: ~
$ chmod 744 hashes.txt
kali@kali: ~
$ ls -l hashes.txt
-rwxr--r-- 1 kali kali 33 Sep 21 06:37 hashes.txt
kali@kali: ~
$ sudo chown root:root hashes.txt
[sudo] password for kali:
kali@kali: ~
$ ls -l hashes.txt
-rwxr--r-- 1 root root 33 Sep 21 06:37 hashes.txt
kali@kali: ~
$
```

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

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~$ sudo apt update  
[sudo] password for kali:  
Hit:1 https://artifacts.elastic.co/packages/7.x/apt stable InRelease  
Get:2 http://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling InRelease [41.5 kB]  
Get:3 http://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling/main amd64 Packages [21.2 MB]  
Get:4 http://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling/main amd64 Contents (deb) [51.8 MB]  
Get:5 http://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling/non-free amd64 Packages [200 kB]  
Get:6 http://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling/non-free amd64 Contents (deb) [911 kB]  
Get:7 http://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling/contrib amd64 Packages [120 kB]  
Get:8 http://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling/contrib amd64 Contents (deb) [326 kB]  
Fetched 74.6 MB in 60s (1,238 kB/s)  
1336 packages can be upgraded. Run 'apt list --upgradable' to see them.  
[kali@kali]~$ sudo apt install -y nmap  
Upgrading:  
ndiff nmap nmap-common zenmap  
Summary:  
Upgrading: 4, Installing: 0, Removing: 0, Not Upgrading: 1332  
Download size: 7,288 kB  
Space needed: 66.6 kB / 45.1 GB available  
Get:1 http://http.kali.org/kali kali-rolling/non-free amd64 nmap amd64 7.95+dfsg-3kali1 [1,940 kB]  
Get:2 http://http.kali.org/kali kali-rolling/non-free amd64 zenmap all 7.95+dfsg-3kali1 [636 kB]  
Get:3 http://http.kali.org/kali kali-rolling/non-free amd64 ndiff all 7.95+dfsg-3kali1 [314 kB]  
Get:4 http://http.kali.org/kali kali-rolling/non-free amd64 nmap-common all 7.95+dfsg-3kali1 [4,399 kB]  
Fetched 3,264 kB in 3s (1,260 kB/s)  
(Reading database ... 507941 files and directories currently installed.)  
Preparing to unpack .../nmap-7.95+dfsg-3kali1-amd64.deb ...  
Unpacking nmap (7.95+dfsg-3kali1) over (7.95+dfsg-1kali1) ...  
Preparing to unpack .../ndiff-7.95+dfsg-3kali1-all.deb ...  
Unpacking ndiff (7.95+dfsg-3kali1) over (7.95+dfsg-1kali1) ...  
Preparing to unpack .../nmap-common-7.95+dfsg-3kali1-all.deb ...  
Unpacking nmap-common (7.95+dfsg-3kali1) over (7.95+dfsg-1kali1) ...  
Preparing to unpack .../zenmap-7.95+dfsg-3kali1-all.deb ...  
Unpacking zenmap (7.95+dfsg-3kali1) over (7.95+dfsg-1kali1) ...  
Setting up nmap-common (7.95+dfsg-3kali1) ...  
Setting up ndiff (7.95+dfsg-3kali1) ...  
Setting up nmap (7.95+dfsg-3kali1) ...  
Setcap worked! Adding configuration to environment  
Setting up zenmap (7.95+dfsg-3kali1) ...  
Processing triggers for mailcap (3.74) ...  
Processing triggers for kali-menu (2025.1.1) ...  
Processing triggers for desktop-file-utils (0.28-1) ...  
Processing triggers for hicolor-icon-theme (0.18-2) ...  
Processing triggers for man-db (2.13.0-1) ...  
Processing triggers for wordlists (2023.2.0) ...  
Scanning processes ...  
Scanning linux images ...  
Running kernel seems to be up-to-date.
```

```
kali@kali: ~  
File Actions Edit View Help  
ndiff nmap nmap-common zenmap  
Summary:  
Upgrading: 4, Installing: 0, Removing: 0, Not Upgrading: 1332  
Download size: 7,288 kB  
Space needed: 66.6 kB / 45.1 GB available  
Get:1 http://http.kali.org/kali kali-rolling/non-free amd64 nmap amd64 7.95+dfsg-3kali1 [1,940 kB]  
Get:2 http://http.kali.org/kali kali-rolling/non-free amd64 zenmap all 7.95+dfsg-3kali1 [636 kB]  
Get:3 http://http.kali.org/kali kali-rolling/non-free amd64 ndiff all 7.95+dfsg-3kali1 [314 kB]  
Get:4 http://http.kali.org/kali kali-rolling/non-free amd64 nmap-common all 7.95+dfsg-3kali1 [4,399 kB]  
Fetched 3,264 kB in 3s (1,260 kB/s)  
(Reading database ... 507941 files and directories currently installed.)  
Preparing to unpack .../nmap-7.95+dfsg-3kali1-amd64.deb ...  
Unpacking nmap (7.95+dfsg-3kali1) over (7.95+dfsg-1kali1) ...  
Preparing to unpack .../ndiff-7.95+dfsg-3kali1-all.deb ...  
Unpacking ndiff (7.95+dfsg-3kali1) over (7.95+dfsg-1kali1) ...  
Preparing to unpack .../nmap-common-7.95+dfsg-3kali1-all.deb ...  
Unpacking nmap-common (7.95+dfsg-3kali1) over (7.95+dfsg-1kali1) ...  
Preparing to unpack .../zenmap-7.95+dfsg-3kali1-all.deb ...  
Unpacking zenmap (7.95+dfsg-3kali1) over (7.95+dfsg-1kali1) ...  
Setting up nmap-common (7.95+dfsg-3kali1) ...  
Setting up ndiff (7.95+dfsg-3kali1) ...  
Setting up nmap (7.95+dfsg-3kali1) ...  
Setcap worked! Adding configuration to environment  
Setting up zenmap (7.95+dfsg-3kali1) ...  
Processing triggers for mailcap (3.74) ...  
Processing triggers for kali-menu (2025.1.1) ...  
Processing triggers for desktop-file-utils (0.28-1) ...  
Processing triggers for hicolor-icon-theme (0.18-2) ...  
Processing triggers for man-db (2.13.0-1) ...  
Processing triggers for wordlists (2023.2.0) ...  
Scanning processes ...  
Scanning linux images ...  
Running kernel seems to be up-to-date.  
No services need to be restarted.  
No containers need to be restarted.  
No user sessions are running outdated binaries.  
No VM guests are running outdated hypervisor (qemu) binaries on this host.  
[kali@kali]~$ dpkg -l | grep nmap  
ii nmap 7.95+dfsg-3kali1 amd64 The Network Mapper  
ii nmap-common 7.95+dfsg-3kali1 all Architecture independent files for nmap  
ii python3-libnmap 0.7.3-1 all Python 3 NMAP library  
ii zenmap 7.95+dfsg-3kali1 all The Network Mapper Front End  
[kali@kali]~$
```

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

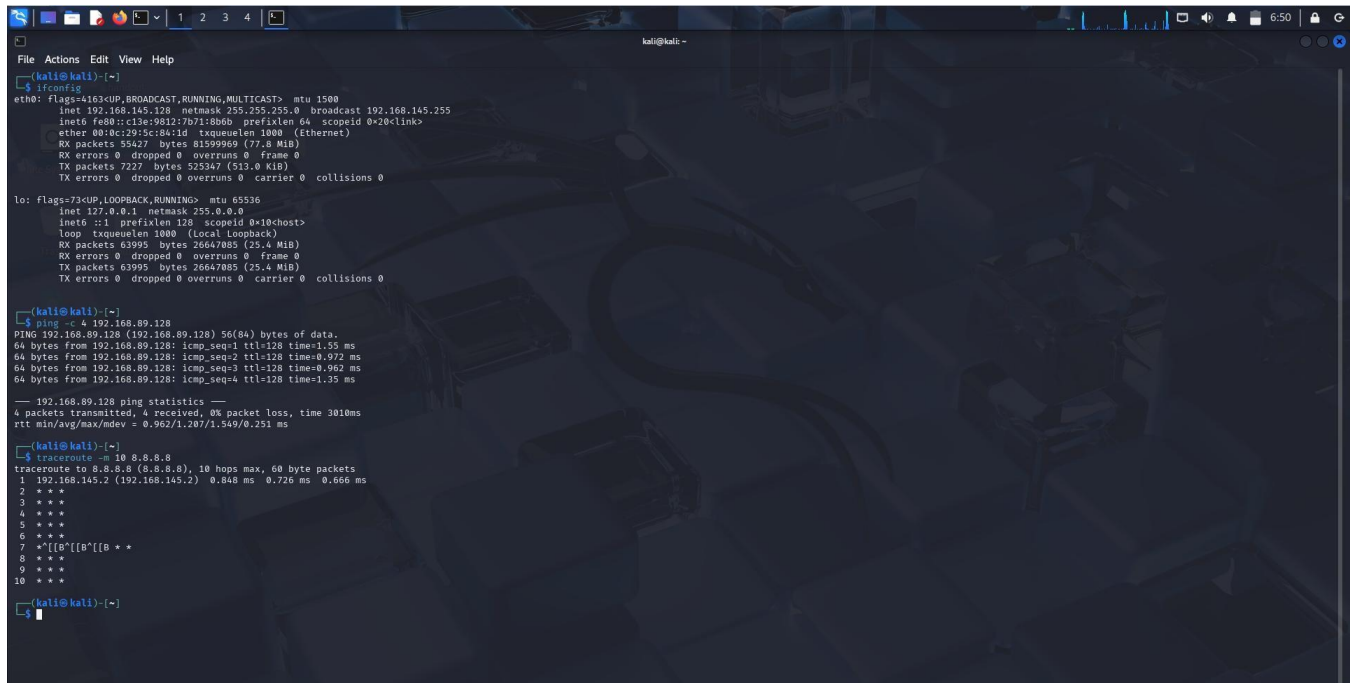
# TASK-1 FOUNDATIONS OF CYBERSECURITY

## 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:~$ _
```



```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.145.126 netmask 255.255.255.0 broadcast 192.168.145.255
    inet6 fe80::c13e:9812:7b71:8b0b prefixlen 64 scopeid 0<20<link>
    ether 00:0c:29:5c:84:1d txqueuelen 1000 (Ethernet)
    RX packets 55427 bytes 81599969 (77.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7227 bytes 525347 (513.0 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 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 63995 bytes 26647085 (25.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 63995 bytes 26647085 (25.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ ping -c 4 192.168.89.128
PING 192.168.89.128 (192.168.89.128) 56(84) bytes of data:
64 bytes from 192.168.89.128: icmp_seq=1 ttl=128 time=1.55 ms
64 bytes from 192.168.89.128: icmp_seq=2 ttl=128 time=0.972 ms
64 bytes from 192.168.89.128: icmp_seq=3 ttl=128 time=0.962 ms
64 bytes from 192.168.89.128: icmp_seq=4 ttl=128 time=1.35 ms
--- 192.168.89.128 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 0.962/1.207/1.549/0.251 ms

(kali@kali)-[~]
$ traceroute -m 10 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 10 hops max, 60 byte packets
 1 192.168.145.2 (192.168.145.2) 0.848 ms 0.726 ms 0.666 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 *[[B*[[B*[[B * *
 8 * * *
 9 * * *
10 * * *
```

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:

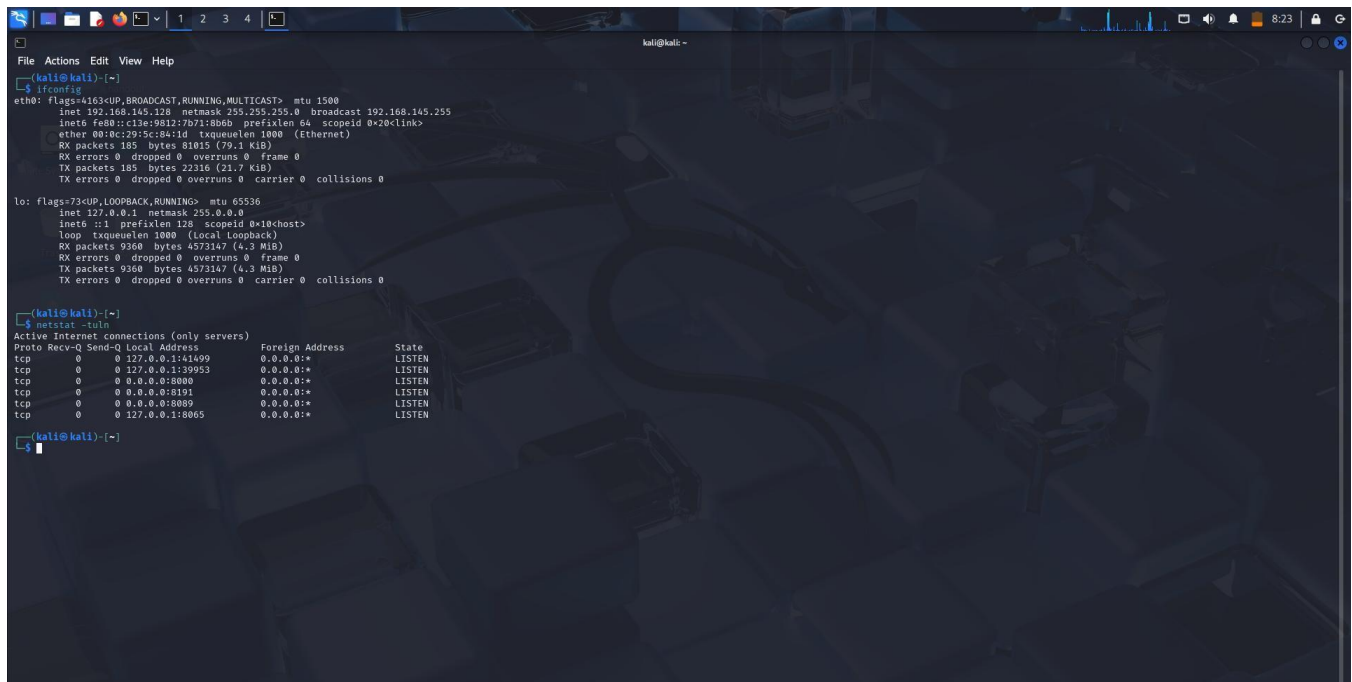
| Layer        | Function  |
|--------------|---|
| Application  | User interaction, applications like HTTP, FTP, DNS. |
| Presentation | Data translation, encryption, compression.          |
| Session      | Establish, manage and terminate sessions.           |
| Transport    | Reliable delivery using 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             |

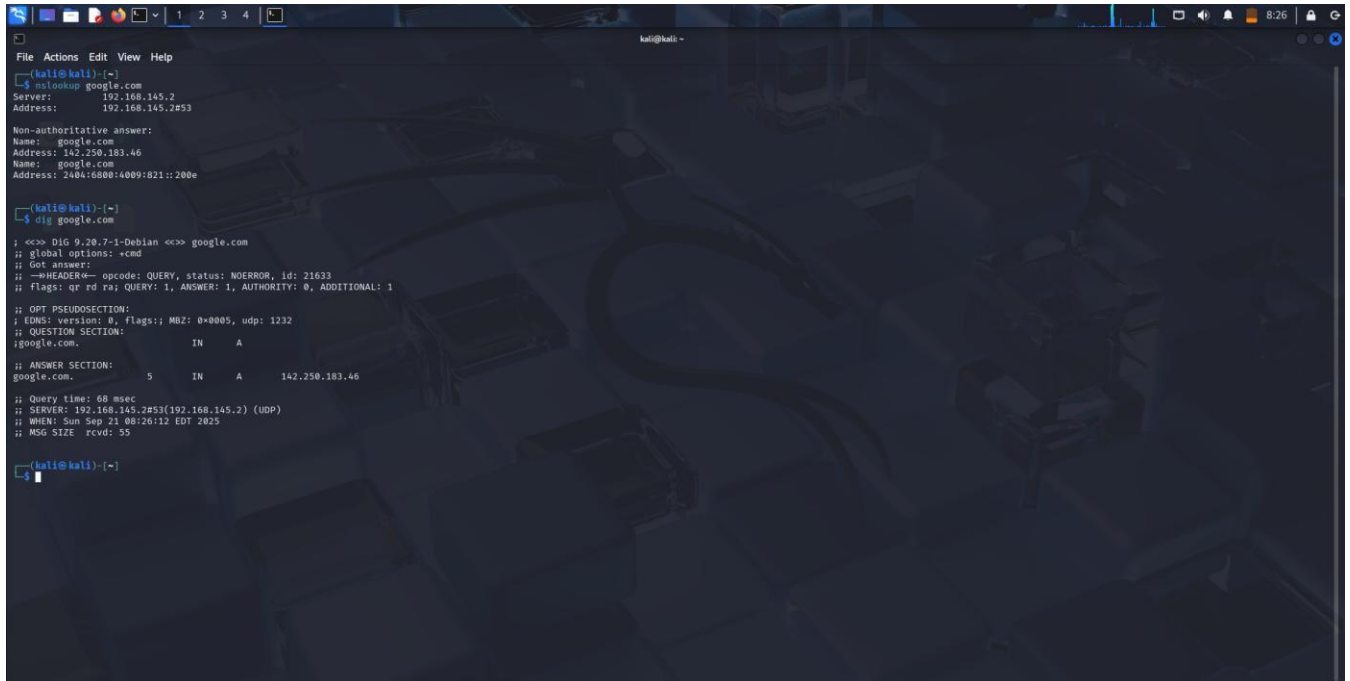


```
kali@kali: ~  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.145.128 netmask 255.255.255.0 broadcast 192.168.145.255  
    inet6 fe80::c13e:9812:7b71:8bde prefixlen 64 scopeid 0<link>  
    ether 00:0c:29:5c:84:1d txqueuelen 1000 (Ethernet)  
    RX packets 185 bytes 81015 (79.1 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 185 bytes 22315 (21.7 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 0<host>  
    loop txqueuelen 1000 (local loopback)  
    RX packets 9360 bytes 4573147 (4.3 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 9360 bytes 4573147 (4.3 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
kali@kali: ~  
$ netstat -tuln  
Active Internet connections (only servers)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp        0      0 127.0.0.1:41499         0.0.0.0:*               LISTEN  
tcp        0      0 127.0.0.1:39953         0.0.0.0:*               LISTEN  
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN  
tcp        0      0 0.0.0.0:3191            0.0.0.0:*               LISTEN  
tcp        0      0 0.0.0.0:8089            0.0.0.0:*               LISTEN  
tcp        0      0 127.0.0.1:8065         0.0.0.0:*               LISTEN
```

# 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.

A screenshot of a Kali Linux terminal window. The terminal has a dark background with a faint, stylized cityscape pattern. The window title is 'kali@kali: ~'. The terminal shows the following commands and output:

```
(kali@kali)~$ nslookup google.com
Server:      192.168.145.2
Address:     192.168.145.2#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.183.46
Name:   google.com
Address: 2404:6808:6089:8211::200e

(kali@kali)~$ dig google.com

; eco: DIG 9.20.7-1-Debian eco> google.com
;; global options: +cmd
;; Got answer:
;; --HEADER-- opcode: QUERY, status: NOERROR, id: 21633
;; Flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: 0, MUZ: 0+000, udp: 1232
;; QUESTION SECTION:
;google.com.                IN      A
;; ANSWER SECTION:
google.com.                 5       IN      A      142.250.183.46

;; Query time: 68 msec
;; SERVER: 192.168.145.2#53(192.168.145.2) (UDP)
;; WHEN: Sun Sep 21 08:26:12 EDT 2025
;; MSG SIZE  rcvd: 55

(kali@kali)~$
```



# 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.

[illegible]



# 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

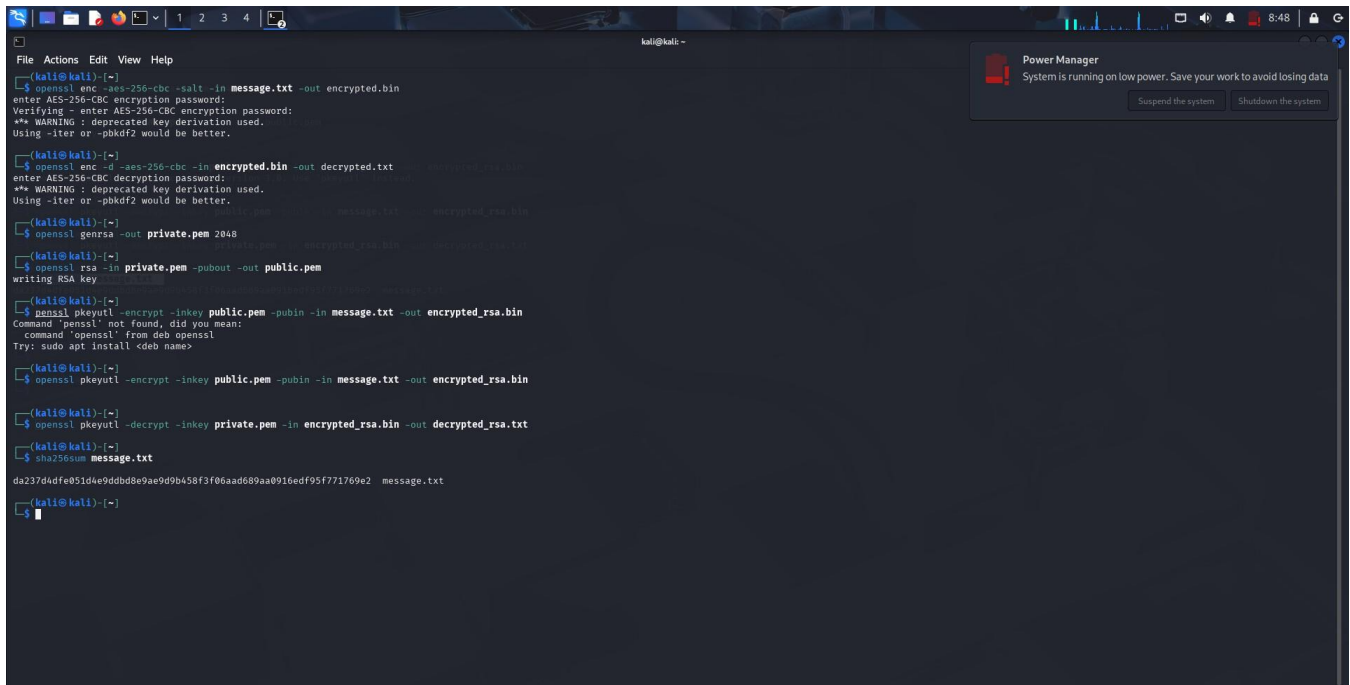
- Converts data into a fixed-length hash.
- One-way function (cannot retrieve original message).
- Examples: SHA-256, MD5.
- Used for password storage, integrity checks.

## 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.



```
kali@kali:~$ openssl enc -aes-256-cbc -salt -in message.txt -out encrypted.bin
enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:
** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

kali@kali:~$ openssl enc -d -aes-256-cbc -in encrypted.bin -out decrypted.txt
enter AES-256-CBC decryption password:
** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

kali@kali:~$ openssl genrsa -out private.pem 2048
writing RSA key

kali@kali:~$ openssl rsa -in private.pem -pubout -out public.pem
writing RSA key

kali@kali:~$ openssl pkeyutl -encrypt -inkey public.pem -pubin -in message.txt -out encrypted_rsa.bin
Command 'pkeyutl' not found, did you mean:
Try: sudo apt install <deb name>

kali@kali:~$ openssl pkeyutl -encrypt -inkey public.pem -pubin -in message.txt -out encrypted_rsa.bin

kali@kali:~$ openssl pkeyutl -decrypt -inkey private.pem -in encrypted_rsa.bin -out decrypted_rsa.txt

kali@kali:~$ sha256sum message.txt
da237d4df051d4e9ddb0e9ae9d9b458f3f06aad689aa0916edf95f771769e2 message.txt

kali@kali:~$
```

# 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

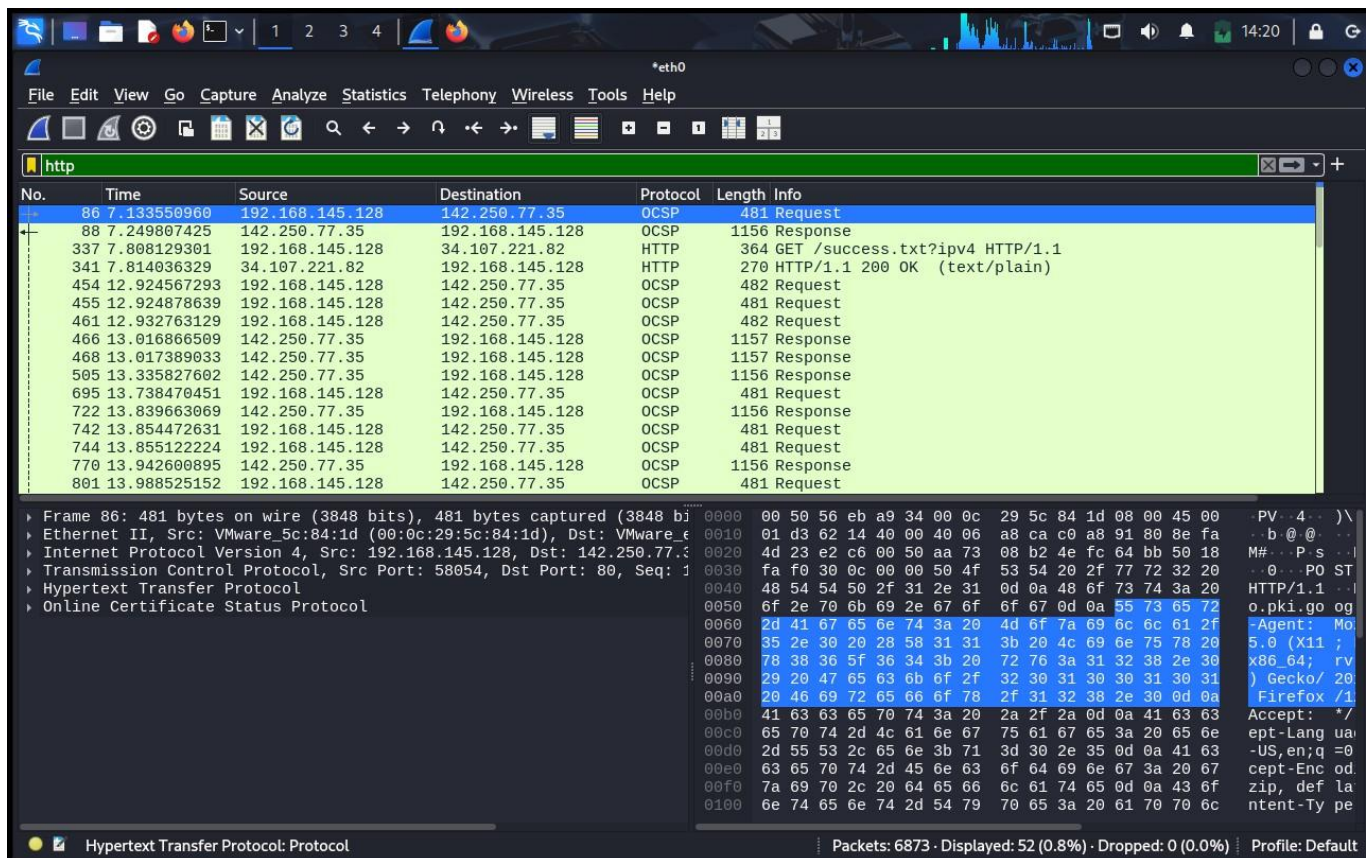
## Tool Familiarization

### 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)

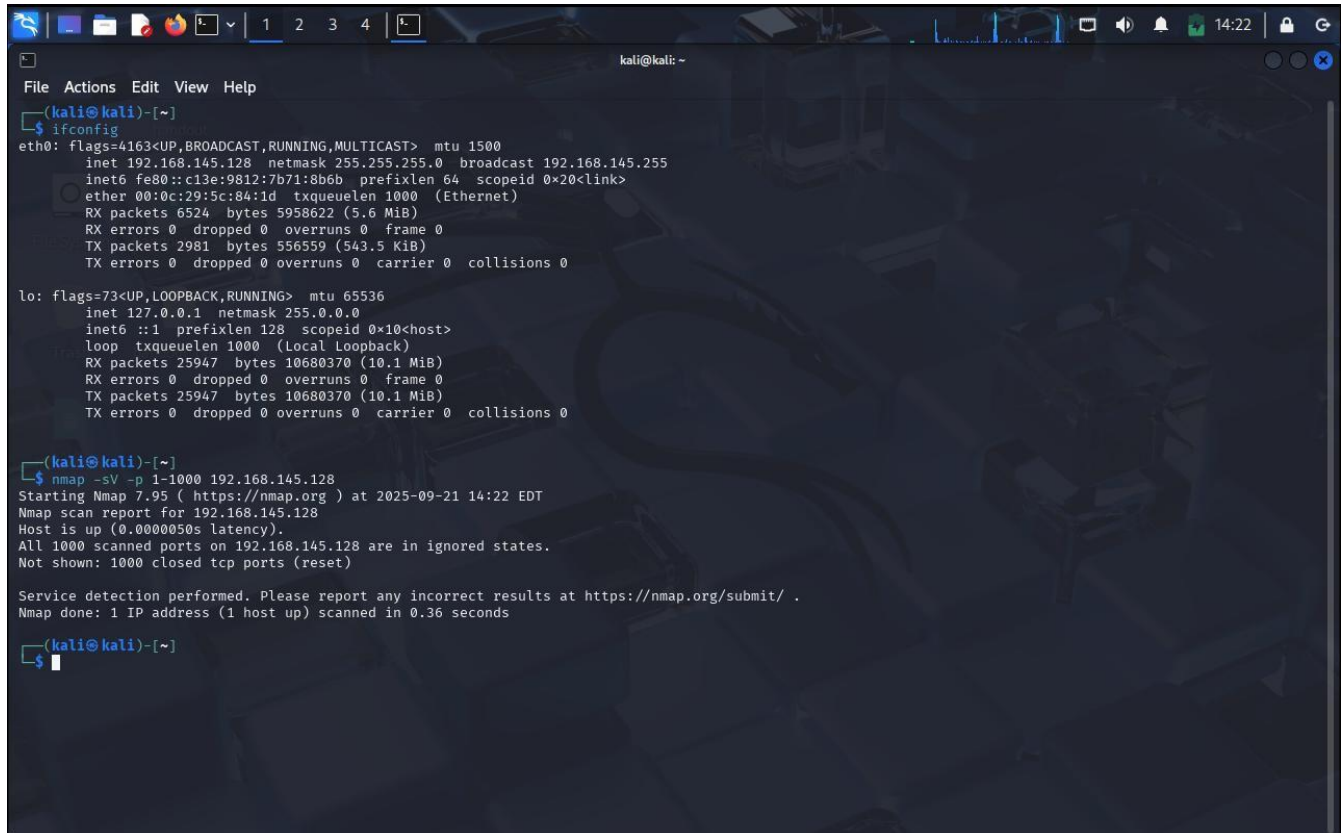
- A free, open-source packet analyzer.
- Used to capture and inspect network packets in real time.
- Helps in troubleshooting network issues and analyzing malicious traffic.



# 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.



```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.145.128 netmask 255.255.255.0 broadcast 192.168.145.255
    inet6 fe80::c13e:9812:7b71:8b6b prefixlen 64 scopeid 0<link>
    ether 00:0c:29:5c:84:1d txqueuelen 1000 (Ethernet)
    RX packets 6524 bytes 5958622 (5.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2981 bytes 556559 (543.5 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 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 25947 bytes 10680370 (10.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 25947 bytes 10680370 (10.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ nmap -sV -p 1-1000 192.168.145.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 14:22 EDT
Nmap scan report for 192.168.145.128
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.145.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

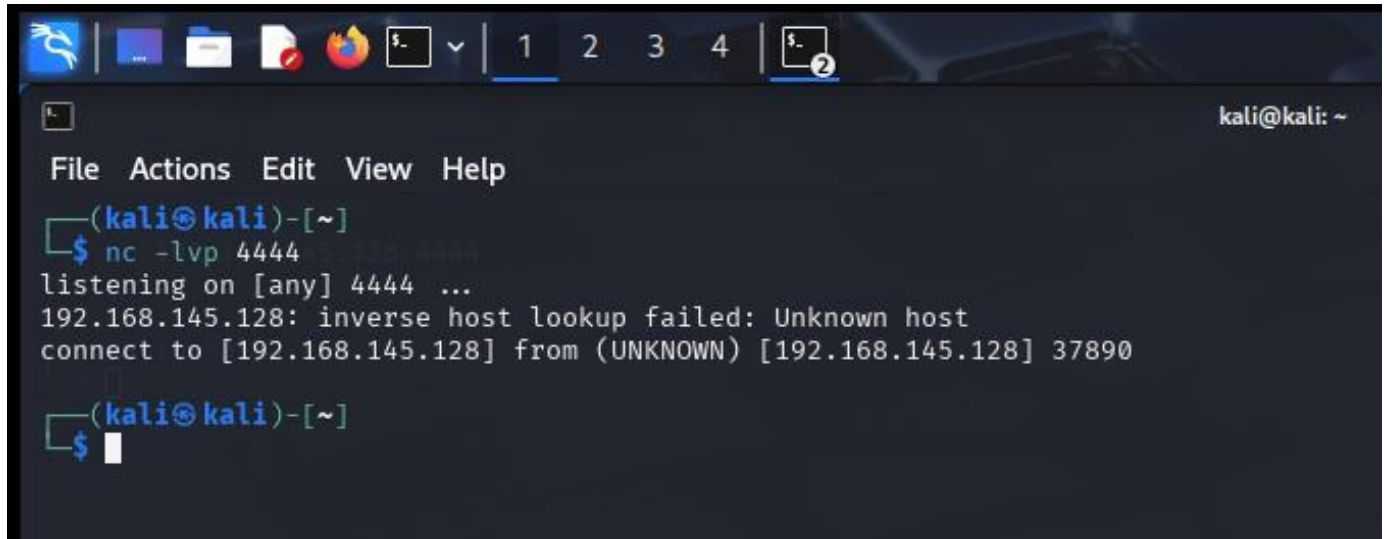
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds

(kali@kali)-[~]
```

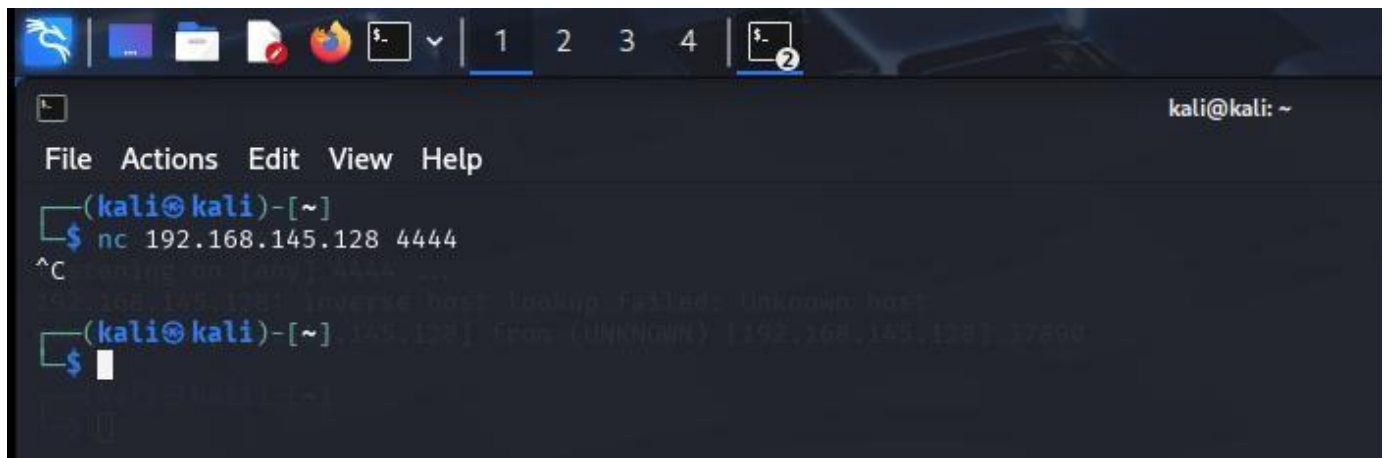
# TASK-1 FOUNDATIONS OF CYBERSECURITY

## 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.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nc -lvp 4444  
listening on [any] 4444 ...  
192.168.145.128: inverse host lookup failed: Unknown host  
connect to [192.168.145.128] from (UNKNOWN) [192.168.145.128] 37890  
(kali@kali)-[~]  
$
```

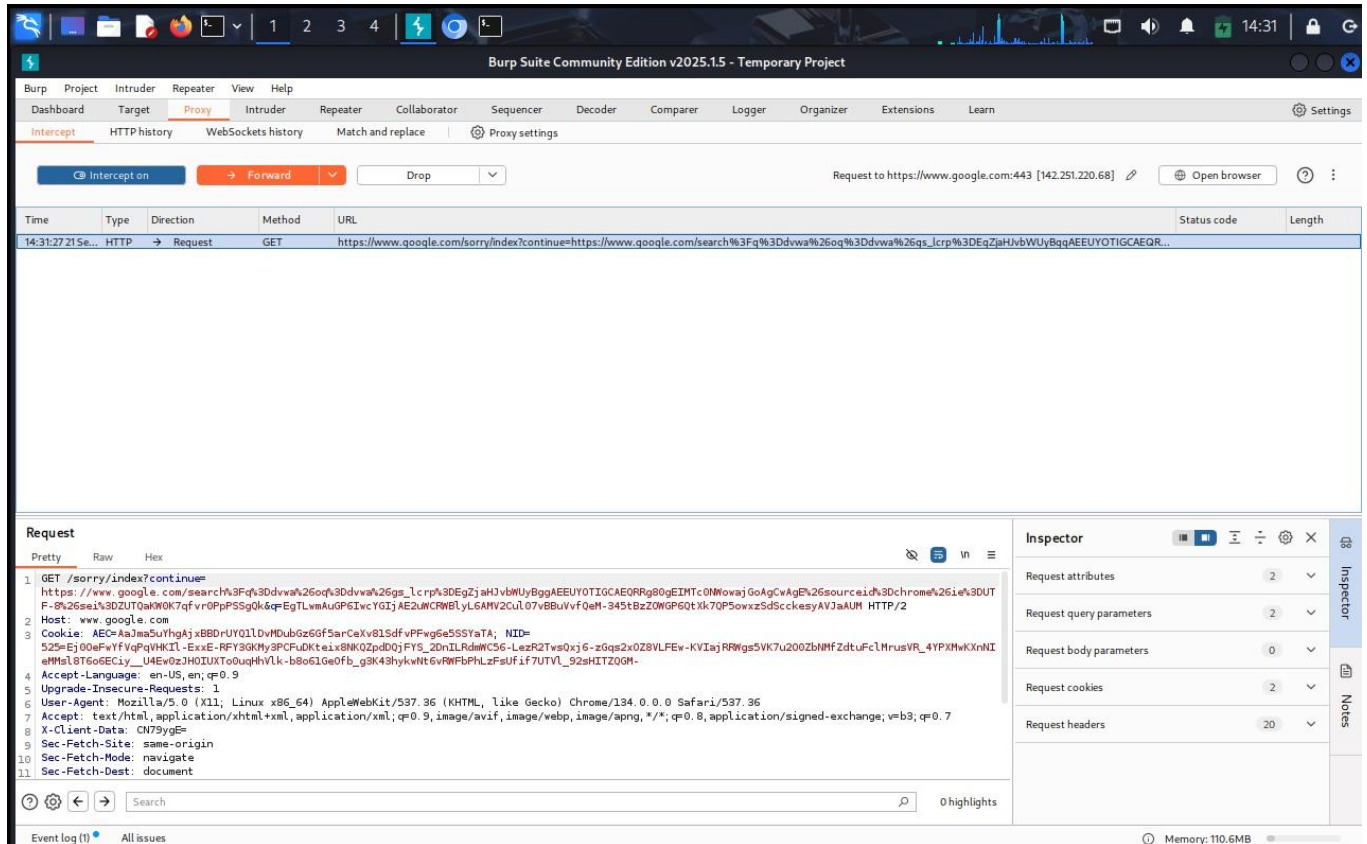


```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nc 192.168.145.128 4444  
^C  
(kali@kali)-[~]  
$
```

# 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.