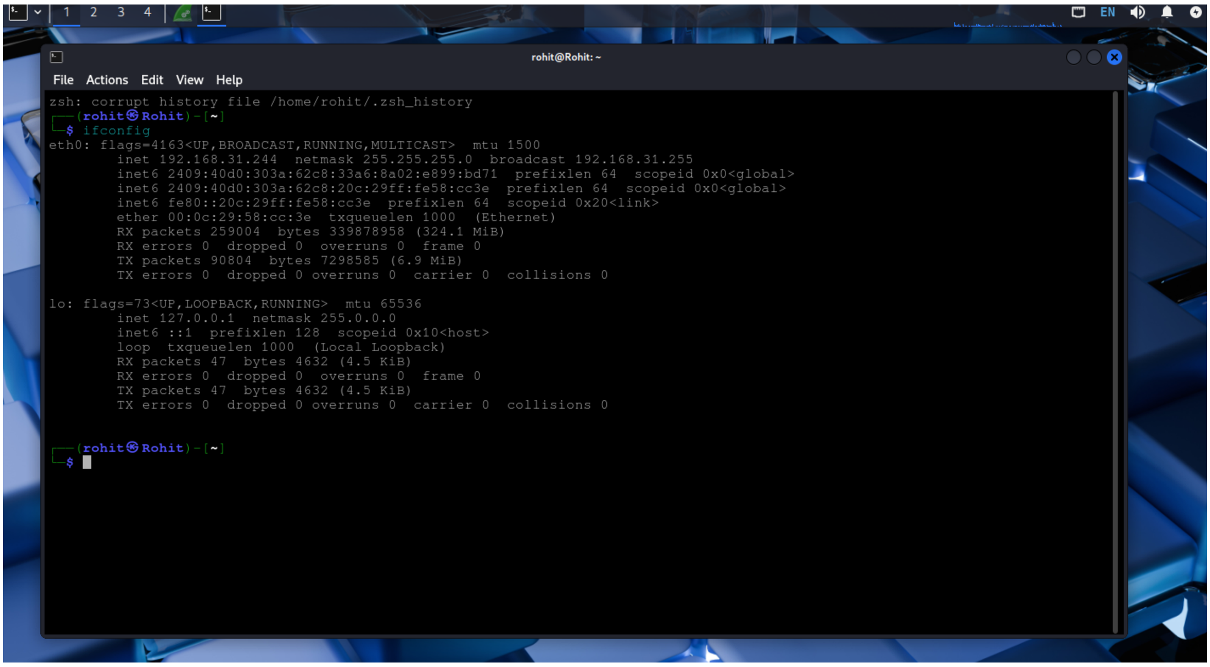
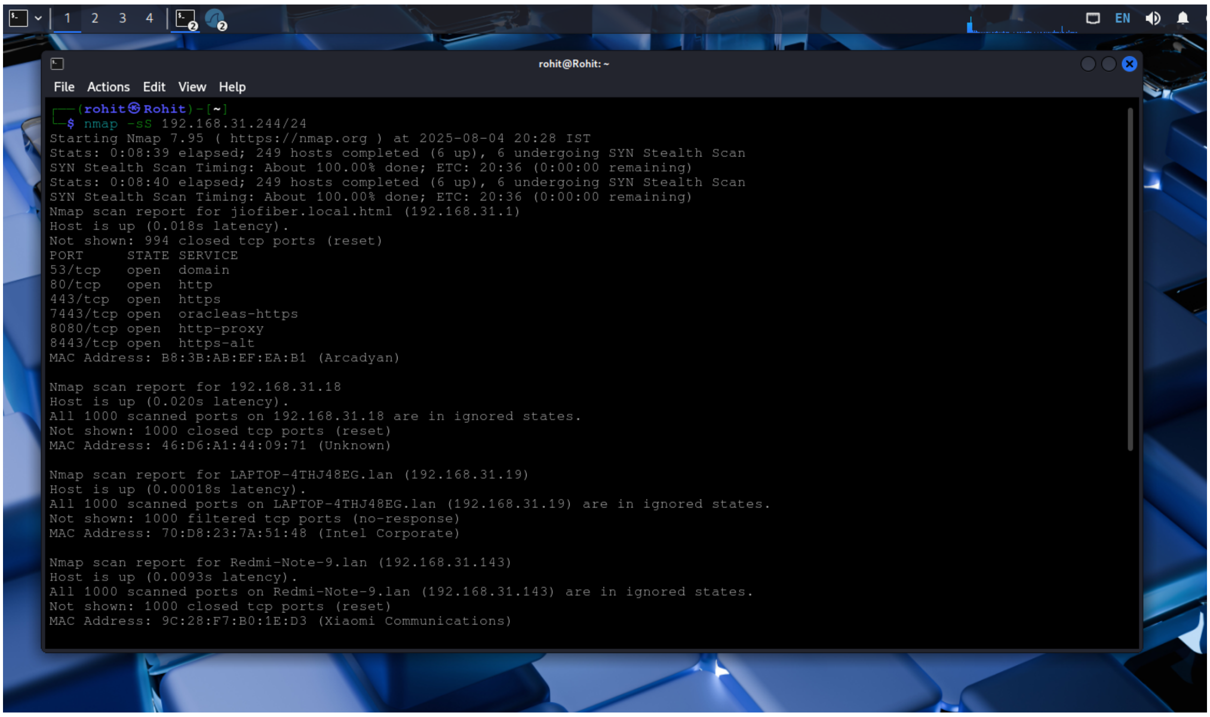
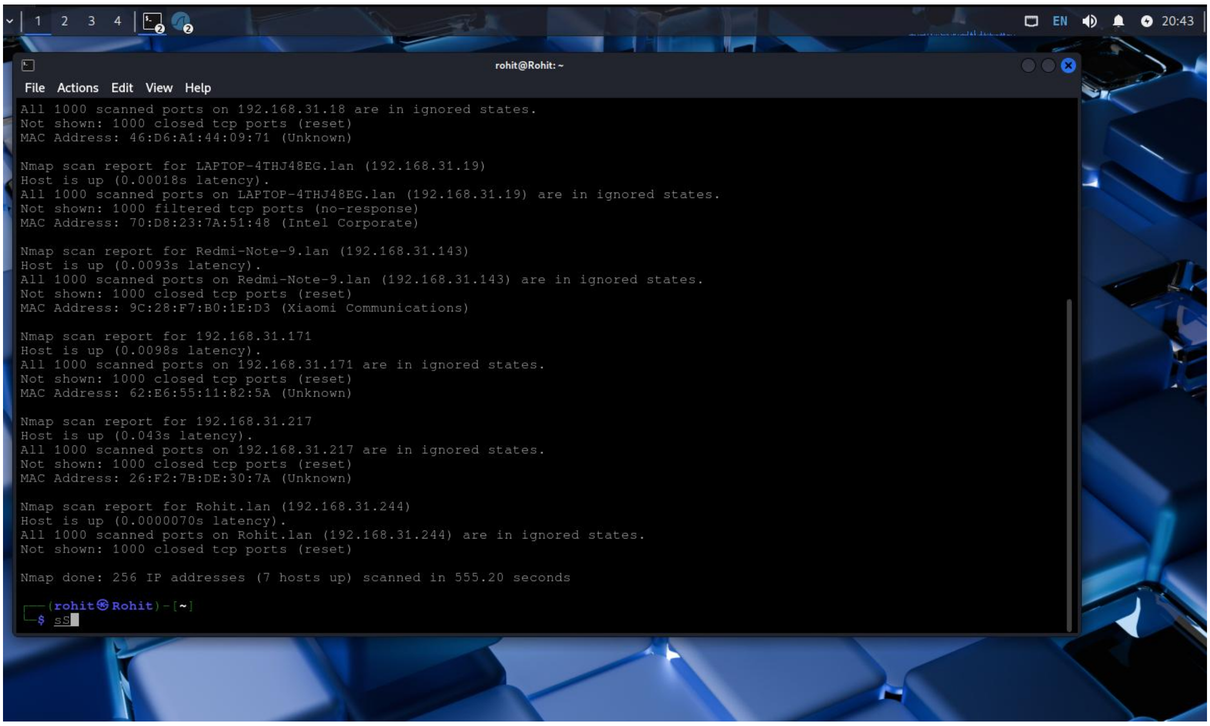
TASK 1



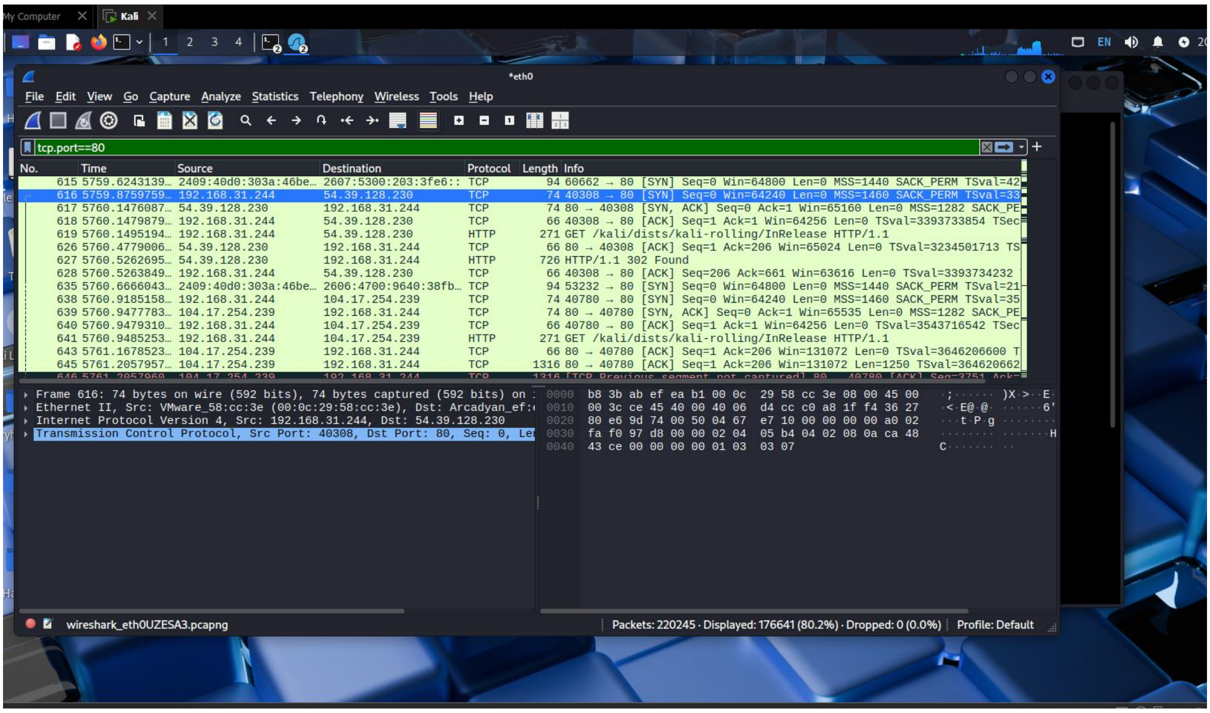
```
zsh: corrupt history file /home/rohit/.zsh_history
┌──(rohit㉿Rohit)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.31.244  netmask 255.255.255.0  broadcast 192.168.31.255
        inet6 2409:40d0:303a:62c8:33a6:8a02:e899:bd71  prefixlen 64  scopeid 0x0<global>
        inet6 2409:40d0:303a:62c8:20c:29ff:fe58:cc3e  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::20c:29ff:fe58:cc3e  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:58:cc:3e  txqueuelen 1000  (Ethernet)
        RX packets 259004  bytes 339878958 (324.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 90804  bytes 7298585 (6.9 MiB)
        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 47  bytes 4632 (4.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 47  bytes 4632 (4.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(rohit㉿Rohit)-[~]
└─$ 
```



```
┌──(rohit㉿Rohit)-[~]
└─$ nmap -sS 192.168.31.244/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 20:28 IST
Stats: 0:08:39 elapsed; 249 hosts completed (6 up), 6 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 100.00% done; ETC: 20:36 (0:00:00 remaining)
Stats: 0:08:40 elapsed; 249 hosts completed (6 up), 6 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 100.00% done; ETC: 20:36 (0:00:00 remaining)
Nmap scan report for jiofiber.local.html (192.168.31.1)
Host is up (0.018s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
7443/tcp open  oracleas-https
8080/tcp open  http-proxy
8443/tcp open  https-alt
MAC Address: B8:3B:AB:EF:EA:B1 (Arcadyan)

Nmap scan report for 192.168.31.18
Host is up (0.020s latency).
All 1000 scanned ports on 192.168.31.18 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 46:D6:A1:44:09:71 (Unknown)

Nmap scan report for LAPTOP-4THJ48EG.lan (192.168.31.19)
Host is up (0.00018s latency).
All 1000 scanned ports on LAPTOP-4THJ48EG.lan (192.168.31.19) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 70:D8:23:7A:51:48 (Intel Corporate)

Nmap scan report for Redmi-Note-9.lan (192.168.31.143)
Host is up (0.0093s latency).
All 1000 scanned ports on Redmi-Note-9.lan (192.168.31.143) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 9C:28:F7:B0:1E:D3 (Xiaomi Communications)
```



```
All 1000 scanned ports on 192.168.31.18 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 46:D6:A1:44:09:71 (Unknown)

Nmap scan report for LAPTOP-4THJ48EG.lan (192.168.31.19)
Host is up (0.00018s latency).
All 1000 scanned ports on LAPTOP-4THJ48EG.lan (192.168.31.19) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 70:D8:23:7A:51:48 (Intel Corporate)

Nmap scan report for Redmi-Note-9.lan (192.168.31.143)
Host is up (0.0093s latency).
All 1000 scanned ports on Redmi-Note-9.lan (192.168.31.143) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 9C:28:F7:B0:1E:D3 (Xiaomi Communications)

Nmap scan report for 192.168.31.171
Host is up (0.0098s latency).
All 1000 scanned ports on 192.168.31.171 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 62:E6:55:11:82:5A (Unknown)

Nmap scan report for 192.168.31.217
Host is up (0.043s latency).
All 1000 scanned ports on 192.168.31.217 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 26:F2:7B:DE:30:7A (Unknown)

Nmap scan report for Rohit.lan (192.168.31.244)
Host is up (0.0000070s latency).
All 1000 scanned ports on Rohit.lan (192.168.31.244) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (7 hosts up) scanned in 555.20 seconds

┌──(rohit㉿Rohit)-[~]
└─$ sS
```



```
tcp.port==80
```

```
No.  Time            Source                Destination           Protocol Length Info
 615 5759.6243139…  2409:40d0:303a:46be…  2607:5300:203:3fe6::  TCP         94 60662 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=42
 616 5759.8759759…  192.168.31.244        54.39.128.230         TCP         74 40308 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=33
 617 5760.1476087…  54.39.128.230         192.168.31.244        TCP         74 80 → 40308 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1282 SACK_PE
 618 5760.1479879…  192.168.31.244        54.39.128.230         TCP         66 40308 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3393733854 TSec
 619 5760.1495194…  192.168.31.244        54.39.128.230         HTTP       271 GET /kali/dists/kali-rolling/InRelease HTTP/1.1
 626 5760.4779006…  54.39.128.230         192.168.31.244        TCP         66 80 → 40308 [ACK] Seq=1 Ack=206 Win=65024 Len=0 TSval=3234501713 TS
 627 5760.5262695…  54.39.128.230         192.168.31.244        HTTP       726 HTTP/1.1 302 Found
 628 5760.5263849…  192.168.31.244        54.39.128.230         TCP         66 40308 → 80 [ACK] Seq=206 Ack=661 Win=63616 Len=0 TSval=3393734232
 635 5760.6666043…  2409:40d0:303a:46be…  2606:4700:9640:38fb…  TCP         94 53232 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=21
 638 5760.9185158…  192.168.31.244        104.17.254.239        TCP         74 40780 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=35
 639 5760.9477783…  104.17.254.239        192.168.31.244        TCP         74 80 → 40780 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1282 SACK_PE
 640 5760.9479310…  192.168.31.244        104.17.254.239        TCP         66 40780 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3543716542 TSec
 641 5760.9485253…  192.168.31.244        104.17.254.239        HTTP       271 GET /kali/dists/kali-rolling/InRelease HTTP/1.1
 643 5761.1678523…  104.17.254.239        192.168.31.244        TCP         66 80 → 40780 [ACK] Seq=1 Ack=206 Win=131072 Len=0 TSval=3646206600 T
 645 5761.2057957…  104.17.254.239        192.168.31.244        TCP       1316 80 → 40780 [ACK] Seq=1 Ack=206 Win=131072 Len=1250 TSval=364620662
 646 5761.2057960   104.17.254.239        192.168.31.244        TCP       1316 [TCP Previous segment not captured] 80 → 40780 [ACK] Seq=3751 Ack=
```

```
› Frame 616: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on
› Ethernet II, Src: VMware_58:cc:3e (00:0c:29:58:cc:3e), Dst: Arcadyan_ef:
› Internet Protocol Version 4, Src: 192.168.31.244, Dst: 54.39.128.230
› Transmission Control Protocol, Src Port: 40308, Dst Port: 80, Seq: 0, Le
```

```
0000  b8 3b ab ef ea b1 00 0c  29 58 cc 3e 08 00 45 00   ·;······ )X·>··E·
0010  00 3c ce 45 40 00 40 06  d4 cc c0 a8 1f f4 36 27   ·<·E@·@· ······6'
0020  80 e6 9d 74 00 50 04 67  e7 10 00 00 00 00 a0 02   ···t·P·g ········
0030  fa f0 97 d8 00 00 02 04  05 b4 04 02 08 0a ca 48   ········ ·······H
0040  43 ce 00 00 00 00 01 03  03 07                     C······· ··
```

wireshark_eth0UZESA3.pcapng | Packets: 220245 · Displayed: 176641 (80.2%) · Dropped: 0 (0.0%) | Profile: Default

Analysis of Each Port

Port 53 (TCP) – Domain Name System (DNS)

Service: DNS

Common Use: Resolving domain names to IPs; TCP is used for large queries or zone transfers.

Security Risks:

- **DNS Zone Transfer**: If misconfigured, attackers can download entire DNS records.
- **DNS Tunneling**: Used to exfiltrate data.
- **Amplification Attacks**: Can be used in DDoS attacks if open resolvers exist.

Port 80 – HTTP

Service: Web server

Common Use: Hosting websites

Security Risks:

- **Unencrypted Traffic**: Can leak sensitive data (login credentials, cookies).
- **Outdated Web Apps**: Vulnerable to XSS, SQL Injection, RCE.
- **Directory Traversal** or **Misconfigured File Permissions**

Port 443 – HTTPS (Encrypted Web Traffic)

Service: Secure HTTP

Common Use: Secure communication with SSL/TLS

Security Risks:

- **Weak SSL/TLS Versions**: Support for SSLv2/SSLv3 or TLS 1.0 is insecure.
- **Self-signed Certificates**: May allow MITM attacks.

- **Vulnerable Web App Behind HTTPS**: Still attackable despite encryption.

Port 7443 – Oracle Application Server HTTPS

Service: Often used for web-based management portals

Common Use: Admin panels or dashboards

Security Risks:

- **Weak authentication**: Admin access exposed
- **Known CVEs** in Oracle WebLogic (like RCE vulnerabilities)
- **Unpatched CMS or dashboard**

Port 8080 – HTTP Proxy / Alternate HTTP

Service: Proxy servers, Tomcat, Jenkins, or custom web servers

Common Use: Dev/test servers, admin panels

Security Risks:

- **Default credentials** in admin apps (like Jenkins, Tomcat)
- **Outdated Dev Servers** with known bugs
- **Proxy Abuse** for bypassing firewalls

Port 8443 – HTTPS Alternate (Common for APIs & Admin Portals)

Service: HTTPS for custom apps (like Spring Boot, Palo Alto, VMware)

Common Use: Encrypted admin interfaces or APIs

Security Risks:

Exposed Admin Panels (often default on 8443)

Weak TLS or Default Credentials

API Abuse if input validation is weak