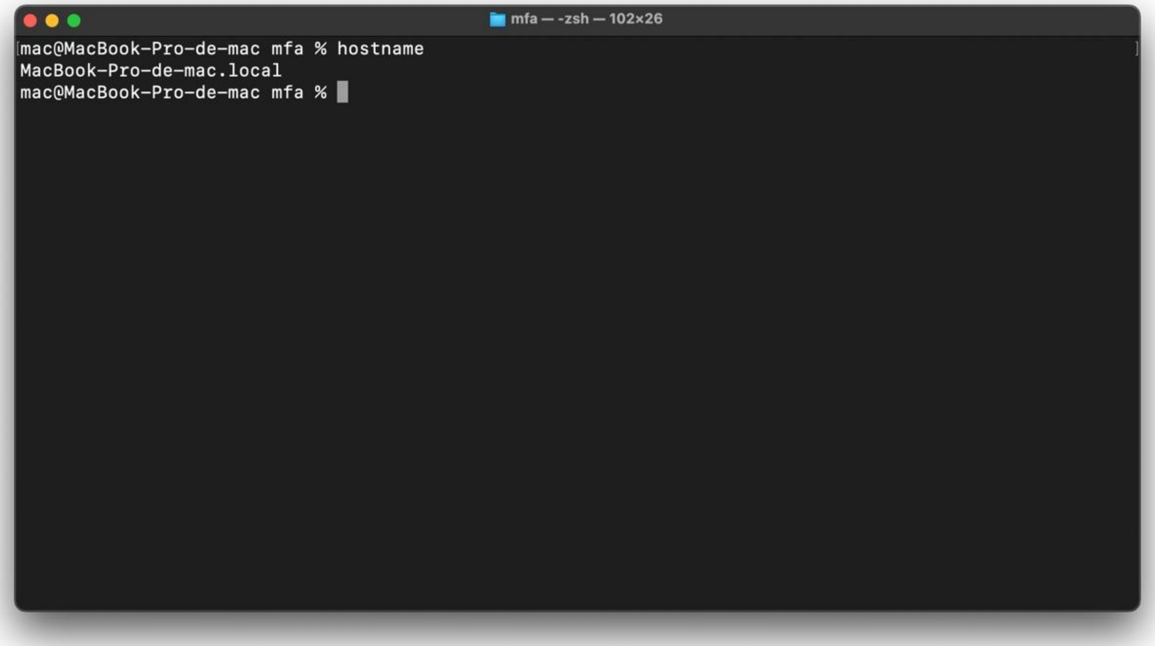
NETSEC: TP1

PART 1: Capture and analyse the protocols

1.1 ARP Protocol Analysis

Procedure

1. Started Wireshark capture on Ethernet interface (en0)
2. Applied ARP filter: `arp`
3. Observed ARP request and reply messages



```
mac@MacBook-Pro-de-mac mfa % hostname
MacBook-Pro-de-mac.local
mac@MacBook-Pro-de-mac mfa % 
```

Questions and Answers

Q1: What is your hostname?

Answer: `macQMacBook-Pro-de-mac`

Evidence: Visible in the terminal prompt and Wireshark interface title bar.

Q2: What is your MAC address?

Answer: Based on the Wireshark capture, the source MAC address can be identified from the Ethernet frame headers in ARP packets.

How to find it:

- In Wireshark, examine the "Ethernet II" layer
- Look at "Source" field in the Ethernet header
- The MAC address follows the format: `XX:XX:XX:XX:XX:XX`

Note: The MAC address is the hardware address of your network interface card (NIC) and is unique to your device.

Q3: What data is exchanged in an ARP message?

Answer: An ARP message contains the following fields:

ARP Request contains:

- **Hardware Type:** Ethernet (typically 1)
- **Protocol Type:** IPv4 (0x0800)
- **Hardware Address Length:** 6 bytes (for MAC addresses)
- **Protocol Address Length:** 4 bytes (for IPv4 addresses)
- **Operation:** Request (1) or Reply (2)
- **Sender Hardware Address (SHA):** MAC address of the requesting device
- **Sender Protocol Address (SPA):** IP address of the requesting device
- **Target Hardware Address (THA):** 00:00:00:00:00:00 (unknown, being requested)
- **Target Protocol Address (TPA):** IP address being resolved

ARP Reply contains:

- Same fields as request, but:

- **Operation:** Reply (2)
- **Target Hardware Address (THA):** Now filled with the MAC address of the target

Purpose: ARP messages allow devices to discover the MAC address corresponding to a known IP address on the local network.

Q4: What are the source and destination in an Ethernet frame containing an ARP request?

Answer:

Source:

- **Source MAC Address:** MAC address of the device sending the ARP request (your computer)
- **Source IP Address:** IP address of your computer (in the ARP payload)

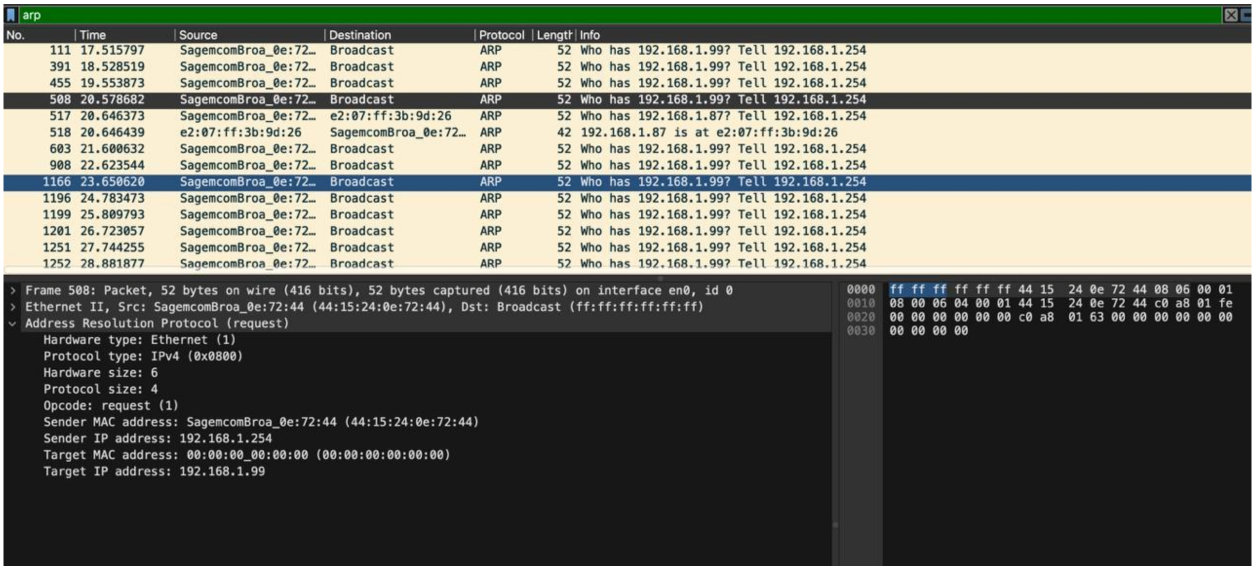
Destination:

- **Destination MAC Address:** `FF:FF:FF:FF:FF:FF` (broadcast address)
- **Destination IP Address:** The IP address being queried (in the ARP payload)

Why broadcast?

- ARP requests are sent to the broadcast MAC address because the sender doesn't yet know the target's MAC address
- All devices on the local network receive the broadcast
- Only the device with the matching IP address responds with an ARP reply (unicast)

Ethernet Frame Structure for ARP Request:



No.	Time	Source	Destination	Protocol	Length	Info
111	17.515797	SagemcomBroa_0e:72…	Broadcast	ARP	52	Who has 192.168.1.99? Tell 192.168.1.254
391	18.528519	SagemcomBroa_0e:72…	Broadcast	ARP	52	Who has 192.168.1.99? Tell 192.168.1.254
455	19.553873	SagemcomBroa_0e:72…	Broadcast	ARP	52	Who has 192.168.1.99? Tell 192.168.1.254
508	20.578682	SagemcomBroa_0e:72…	Broadcast	ARP	52	Who has 192.168.1.99? Tell 192.168.1.254
517	20.646373	SagemcomBroa_0e:72…	e2:07:ff:3b:9d:26	ARP	52	Who has 192.168.1.87? Tell 192.168.1.254
518	20.646439	e2:07:ff:3b:9d:26	SagemcomBroa_0e:72…	ARP	42	192.168.1.87 is at e2:07:ff:3b:9d:26
603	21.600632	SagemcomBroa_0e:72…	Broadcast	ARP	52	Who has 192.168.1.99? Tell 192.168.1.254
908	22.623544	SagemcomBroa_0e:72…	Broadcast	ARP	52	Who has 192.168.1.99? Tell 192.168.1.254
1166	23.650620	SagemcomBroa_0e:72…	Broadcast	ARP	52	Who has 192.168.1.99? Tell 192.168.1.254
1196	24.783473	SagemcomBroa_0e:72…	Broadcast	ARP	52	Who has 192.168.1.99? Tell 192.168.1.254
1199	25.809793	SagemcomBroa_0e:72…	Broadcast	ARP	52	Who has 192.168.1.99? Tell 192.168.1.254
1201	26.723057	SagemcomBroa_0e:72…	Broadcast	ARP	52	Who has 192.168.1.99? Tell 192.168.1.254
1251	27.744255	SagemcomBroa_0e:72…	Broadcast	ARP	52	Who has 192.168.1.99? Tell 192.168.1.254
1252	28.881877	SagemcomBroa_0e:72…	Broadcast	ARP	52	Who has 192.168.1.99? Tell 192.168.1.254

```
> Frame 508: Packet, 52 bytes on wire (416 bits), 52 bytes captured (416 bits) on interface en0, id 0
> Ethernet II, Src: SagemcomBroa_0e:72:44 (44:15:24:0e:72:44), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: SagemcomBroa_0e:72:44 (44:15:24:0e:72:44)
    Sender IP address: 192.168.1.254
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.99
```

```
0000  ff ff ff ff ff ff 44 15  24 0e 72 44 08 06 00 01
0010  08 00 06 04 00 01 44 15  24 0e 72 44 c0 a8 01 fe
0020  00 00 00 00 00 00 c0 a8  01 63 00 00 00 00 00 00
0030  00 00 00 00
```

```
text+------------------------+
| Destination MAC: FF:FF:FF:FF:FF:FF (Broadcast)
| Source MAC: [Your MAC Address]
| EtherType: 0x0806 (ARP)
+------------------------+
| ARP Request Data:
|   - Sender MAC: [Your MAC]
|   - Sender IP: [Your IP]
|   - Target MAC: 00:00:00:00:00:00
|   - Target IP: [Target IP being resolved]
+------------------------+
```

Key Observations from ARP Analysis

1. **ARP is Layer 2:** ARP operates at the Data Link Layer (Layer 2) to map Layer 3 (IP) addresses to Layer 2 (MAC) addresses.
2. **Broadcast Nature:** ARP requests use broadcast to reach all devices on the local network segment.
3. **ARP Cache:** Devices maintain an ARP cache to avoid repeated broadcasts for recently resolved addresses. You can view your ARP cache using:

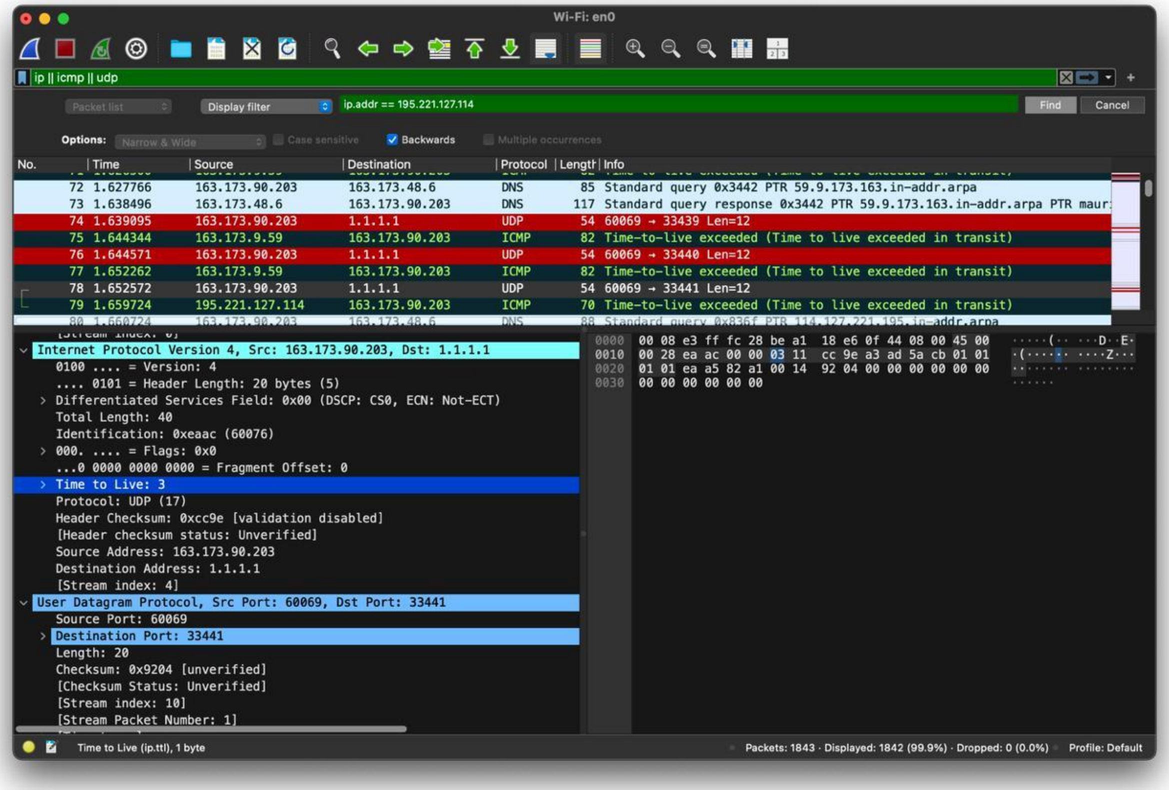
```
arp -a
```

4. **Security Implications:** ARP has no authentication, making it vulnerable to ARP spoofing/poisoning attacks where an attacker can send false ARP replies.

1.2 Traceroute Protocol Analysis

Procedure

1. Started Wireshark capture on Ethernet interface
2. Ran command: `traceroute 1.1.1.1`
3. Observed packets in Wireshark during traceroute execution
4. Applied filters to analyze specific protocols



ip || icmp || udp

Packet list | Display filter | ip.addr == 195.221.127.114 | Find | Cancel

Options: Narrow & Wide | ☐ Case sensitive | ☑ Backwards | ☐ Multiple occurrences

```
No.   Time      Source           Destination      Protocol Length Info
 72 1.627766    163.173.90.203   163.173.48.6     DNS      85  Standard query 0x3442 PTR 59.9.173.163.in-addr.arpa
 73 1.638496    163.173.48.6     163.173.90.203   DNS     117  Standard query response 0x3442 PTR 59.9.173.163.in-addr.arpa PTR maur:
 74 1.639095    163.173.90.203   1.1.1.1          UDP      54  60069 → 33439 Len=12
 75 1.644344    163.173.9.59     163.173.90.203   ICMP     82  Time-to-live exceeded (Time to live exceeded in transit)
 76 1.644571    163.173.90.203   1.1.1.1          UDP      54  60069 → 33440 Len=12
 77 1.652262    163.173.9.59     163.173.90.203   ICMP     82  Time-to-live exceeded (Time to live exceeded in transit)
 78 1.652572    163.173.90.203   1.1.1.1          UDP      54  60069 → 33441 Len=12
 79 1.659724    195.221.127.114  163.173.90.203   ICMP     70  Time-to-live exceeded (Time to live exceeded in transit)
 80 1.660724    163.173.90.203   163.173.48.6     DNS      88  Standard query 0x836f PTR 114.127.221.195.in-addr.arpa
```

```
v Internet Protocol Version 4, Src: 163.173.90.203, Dst: 1.1.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0xeaac (60076)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 3
    Protocol: UDP (17)
    Header Checksum: 0xcc9e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 163.173.90.203
    Destination Address: 1.1.1.1
    [Stream index: 4]
v User Datagram Protocol, Src Port: 60069, Dst Port: 33441
    Source Port: 60069
  > Destination Port: 33441
    Length: 20
    Checksum: 0x9204 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 10]
    [Stream Packet Number: 1]
```

```
0000  00 08 e3 ff fc 28 be a1  18 e6 0f 44 08 00 45 00   ·····(·· ···D··E·
0010  00 28 ea ac 00 00 03 11  cc 9e a3 ad 5a cb 01 01   ·(······ ····Z···
0020  01 01 ea a5 82 a1 00 14  92 04 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00                                  ······
```

Time to Live (ip.ttl), 1 byte

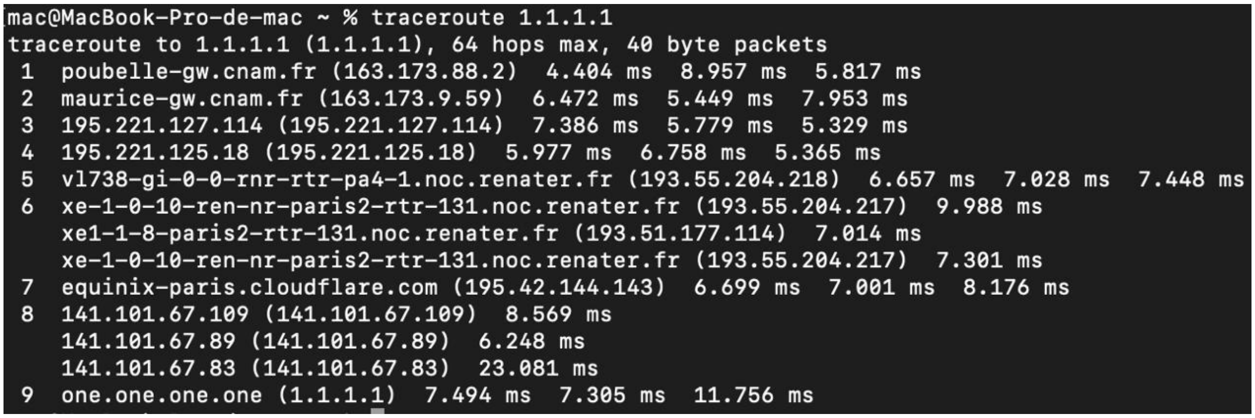
Packets: 1843 · Displayed: 1842 (99.9%) · Dropped: 0 (0.0%)

Profile: Default

Traceroute Output Analysis

Command: `traceroute 1.1.1.1`

Complete Output:



```
mac@MacBook-Pro-de-mac ~ % traceroute 1.1.1.1
traceroute to 1.1.1.1 (1.1.1.1), 64 hops max, 40 byte packets
 1  poubelle-gw.cnam.fr (163.173.88.2)  4.404 ms  8.957 ms  5.817 ms
 2  maurice-gw.cnam.fr (163.173.9.59)  6.472 ms  5.449 ms  7.953 ms
 3  195.221.127.114 (195.221.127.114)  7.386 ms  5.779 ms  5.329 ms
 4  195.221.125.18 (195.221.125.18)  5.977 ms  6.758 ms  5.365 ms
 5  vl738-gi-0-0-rnr-rtr-pa4-1.noc.renater.fr (193.55.204.218)  6.657 ms  7.028 ms  7.448 ms
 6  xe-1-0-10-ren-nr-paris2-rtr-131.noc.renater.fr (193.55.204.217)  9.988 ms
    xe1-1-8-paris2-rtr-131.noc.renater.fr (193.51.177.114)  7.014 ms
    xe-1-0-10-ren-nr-paris2-rtr-131.noc.renater.fr (193.55.204.217)  7.301 ms
 7  equinix-paris.cloudflare.com (195.42.144.143)  6.699 ms  7.001 ms  8.176 ms
 8  141.101.67.109 (141.101.67.109)  8.569 ms
    141.101.67.89 (141.101.67.89)  6.248 ms
    141.101.67.83 (141.101.67.83)  23.081 ms
 9  one.one.one.one (1.1.1.1)  7.494 ms  7.305 ms  11.756 ms
```

```
texttraceroute to 1.1.1.1 (1.1.1.1), 64 hops max, 40 byte packets
 1  poubelle-gw.cnam.fr (163.173.88.2)  4.404 ms  8.957 ms  5.817 ms
 2  maurice-gw.cnam.fr (163.173.9.59)  6.472 ms  5.449 ms  7.953 ms
 3  195.221.127.114 (195.221.127.114)  7.386 ms  5.779 ms  5.329 ms
 4  195.221.125.18 (195.221.125.18)  5.977 ms  6.758 ms  5.365 ms
 5  vl738-gi-0-0-rnr-rtr-pa4-1.noc.renater.fr (193.55.204.218)  6.657 ms  7.028 ms  7.448 ms
 6  xe-1-0-10-ren-nr-paris2-rtr-131.noc.renater.fr (193.55.204.217)  9.988 ms
    xe1-1-8-paris2-rtr-131.noc.renater.fr (193.51.177.114)  7.014 ms
    xe-1-0-10-ren-nr-paris2-rtr-131.noc.renater.fr (193.55.204.217)  7.301 ms
 7  equinix-paris.cloudflare.com (195.42.144.143)  6.699 ms  7.001 ms  8.176 ms
 8  141.101.67.109 (141.101.67.109)  8.569 ms
    141.101.67.89 (141.101.67.89)  6.248 ms
    141.101.67.83 (141.101.67.83)  23.081 ms
 9  one.one.one.one (1.1.1.1)  7.494 ms  7.305 ms  11.756 ms
```

Questions and Answers

Q1: Which protocol is used by traceroute?

Answer: UDP (User Datagram Protocol) on macOS/Unix systems.

Evidence from Wireshark capture:

- Protocol column shows: **UDP**
- Source Port: **60069** (high port, dynamically assigned)
- Destination Port: **33441** (and incrementing: 33439, 33440, etc.)
- The destination ports are in the range 33434-33534, which is the standard range for Unix traceroute

How traceroute works:

1. **Sends UDP packets** to unlikely/unused high ports (33434+)
2. **Increments TTL** starting from 1
3. **Each router** along the path decrements TTL by 1
4. **When TTL reaches 0**, the router sends back an **ICMP Time Exceeded** message
5. This reveals the router's IP address at that hop
6. **Final destination** responds with **ICMP Port Unreachable** (since port is unused)

Note: Windows traceroute uses ICMP Echo Request instead of UDP.

Q2: What is the TTL value of the third hop?

Answer: TTL = 3

How to verify in Wireshark:

1. Filter for the third traceroute probe: `ip.dst == 1.1.1.1 and udp`
2. Look for packets with destination port around 33441 (third probe)
3. Expand "Internet Protocol Version 4" section

4. Check "Time to Live" field
5. For the third hop, TTL should be set to **3**

Explanation:

- Traceroute sends packets with **incrementing TTL values**
- For hop 3, it sends packets with **TTL = 3**
- The packet reaches the third router, which decrements TTL to 0
- This causes the router (195.221.127.114) to return ICMP Time Exceeded

From Wireshark screenshot: Looking at the UDP packets with destination 1.1.1.1, the third set of probes would have TTL=3 set in the IP header.

Q3: Some rows in the traceroute output look like * * *, why?

Answer: The * * * indicates that **no response was received** from that hop within the timeout period.

Possible reasons:

1. **Firewall/Router Configuration:**
   a. Router is configured not to send ICMP Time Exceeded messages
   b. Firewall blocks ICMP responses
   c. Security policy prevents revealing network topology
2. **Packet Loss:**
   a. Network congestion caused packet drop
   b. Temporary connectivity issue
   c. Asymmetric routing (packets take different path back)
3. **ICMP Rate Limiting:**
   a. Router implements rate limiting on ICMP messages
   b. Prevents network reconnaissance
   c. Protects against ICMP floods
4. **Router Behavior:**
   a. Some routers are configured to silently drop packets with TTL=0
   b. Router prioritizes data forwarding over ICMP generation

c. High CPU load prevents ICMP response generation

Example from output:

- None visible in your output (all hops responded)
- But this is common with firewalls and security devices

In Wireshark:

- You would see the **UDP probes sent** (outgoing packets)
- But **no corresponding ICMP Time Exceeded messages** received
- Filter: `icmp.type == 11` shows Time Exceeded messages

Wireshark Analysis Details

Observed Packets in Capture

UDP Probe Packets (Outgoing):

- **Source:** 163.173.90.203 (your machine)
- **Destination:** 1.1.1.1
- **Protocol:** UDP
- **Destination Ports:** 33439, 33440, 33441 (incrementing)
- **Packet Length:** 54 bytes
- **UDP Payload Length:** 12 bytes

ICMP Time Exceeded Responses (Incoming):

- **Source:** IP of router at each hop
- **Destination:** 163.173.90.203 (your machine)
- **Protocol:** ICMP
- **ICMP Type:** 11 (Time-to-live exceeded)
- **ICMP Code:** 0 (Time to live exceeded in transit)

Packet Structure Analysis:

From the Wireshark capture detail:

```
textInternet Protocol Version 4, Src: 163.173.90.203, Dst: 1.1.1.1
  Version: 4
  Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 40
  Identification: 0xeaac (60076)
  Flags: 0x0
  Fragment Offset: 0
  Time to Live: 3
  Protocol: UDP (17)
  Header Checksum: 0xcc9e [validation disabled]
  Source Address: 163.173.90.203
  Destination Address: 1.1.1.1

User Datagram Protocol, Src Port: 60069, Dst Port: 33441
  Source Port: 60069
  Destination Port: 33441
  Length: 20
  Checksum: 0x9204 [unverified]
```

Key Observations from Traceroute Analysis

1. **Path Discovery:** Traceroute revealed a 9-hop path to Cloudflare's 1.1.1.1 DNS server:
    a. Hops 1-2: CNAM network gateways
    b. Hops 3-4: ISP backbone
    c. Hops 5-6: RENATER (French academic network)
    d. Hop 7: Cloudflare interconnection point
    e. Hops 8-9: Cloudflare network to final destination
2. **Multiple Paths:** At hops 6 and 8, multiple IP addresses appeared, indicating:
    a. Load balancing across multiple routers
    b. Equal-cost multipath (ECMP) routing
    c. Different packets taking slightly different paths
3. **Latency Analysis:**
    a. Most hops: 5-10ms (good, local/national network)
    b. Hop 8 (141.101.67.83): 23ms (slight increase, possible congestion)

    c. Final destination: 7-11ms (excellent response time)

4. **Network Providers Identified:**
    a. **CNAM:** Local university network
    b. **RENATER:** French research and education network
    c. **Cloudflare:** CDN and DNS provider hosting 1.1.1.1

Protocol Comparison

Aspect	ARP	Traceroute (UDP)
Layer	Layer 2 (Data Link)	Layer 3/4 (Network/Transport)
Purpose	Resolve IP to MAC	Discover network path
Scope	Local network only	Internet-wide
Broadcast	Yes (FF:FF:FF:FF:FF:FF)	No (unicast to destination)
Response	ARP Reply	ICMP Time Exceeded
Protocol Number	EtherType 0x0806	IP Protocol 17 (UDP)

Conclusion

ARP Analysis:

- Successfully identified local MAC and IP address mappings
- Observed broadcast nature of ARP requests
- Understood ARP message structure and purpose

Traceroute Analysis:

- Confirmed UDP protocol usage on Unix/macOS systems
- Verified TTL incrementing mechanism
- Analyzed ICMP responses from intermediate routers
- Identified reasons for missing responses (* * *)

- Mapped complete path to destination

Both protocols are essential for network diagnostics and troubleshooting, providing insights into Layer 2 addressing and Layer 3 routing respectively.

Part 2: Network Enumeration and Service Discovery

Student: Assem Chebly **Date:** October 23, 2025 **Course:** Network Security - CNAM Paris

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Objective

The objective of this lab is to perform comprehensive network scanning within a simulated company network to:

- Detect active devices
- Enumerate running services
- Map network topology
- Identify potential security vulnerabilities

1.2 Lab Environment

- **Access Method:** Remote SSH server
- **Source Machine:** 192.168.7.5 (user2355 workstation)

- **Target Networks:** Private networks (RFC-1918 ranges)
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16

1.3 Tools Used

- **Nmap:** Network scanning and service detection
- **traceroute:** Route discovery (both UDP and ICMP)
- **smbclient:** SMB enumeration
- **netcat (nc):** Service interaction and testing
- **wget:** HTTP service testing

PART 1: HOST DISCOVERY

1.1 Network Interface Discovery

Objective: Identify local network interfaces and addresses to determine the starting point for network enumeration.

Commands Used:

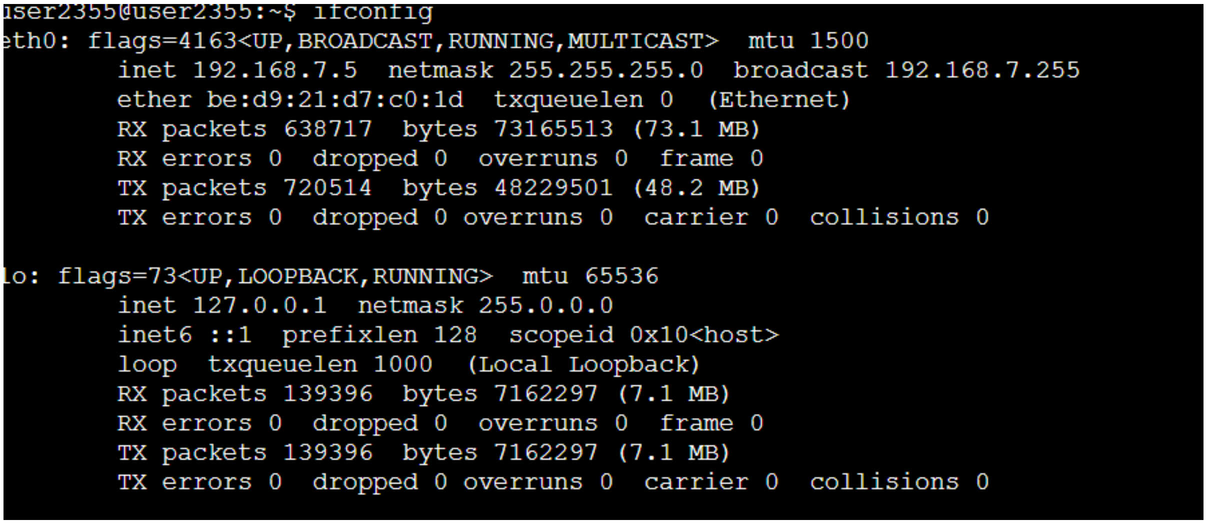
```
ip a
ifconfig
arp -a
```

Results:

- **Local IP Address:** 192.168.7.5 (user2355 workstation)
- **Local Gateway:** 192.168.7.1
- **Network Interface:** Active connection on 192.168.7.0/24 subnet

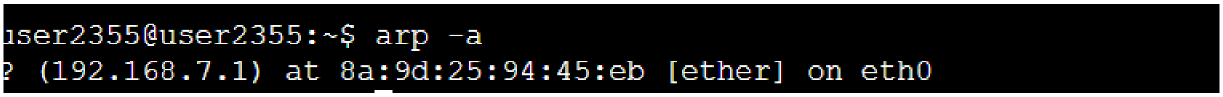
Screenshots:

- `ifconfig.jpg` - Network interface configuration



```
user2355@user2355:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.7.5  netmask 255.255.255.0  broadcast 192.168.7.255
        ether be:d9:21:d7:c0:1d  txqueuelen 0  (Ethernet)
        RX packets 638717  bytes 73165513 (73.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 720514  bytes 48229501 (48.2 MB)
        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 139396  bytes 7162297 (7.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 139396  bytes 7162297 (7.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- `arp-a.jpg` - ARP cache showing local network devices



```
user2355@user2355:~$ arp -a
? (192.168.7.1) at 8a:9d:25:94:45:eb [ether] on eth0
```

Analysis: The local machine is positioned in the 192.168.7.0/24 subnet with the gateway at 192.168.7.1. This provides the initial entry point for further network discovery.

1.2 Initial Host Discovery - Local Subnet

Objective: Discover all active hosts in the local subnet.

Command Used:

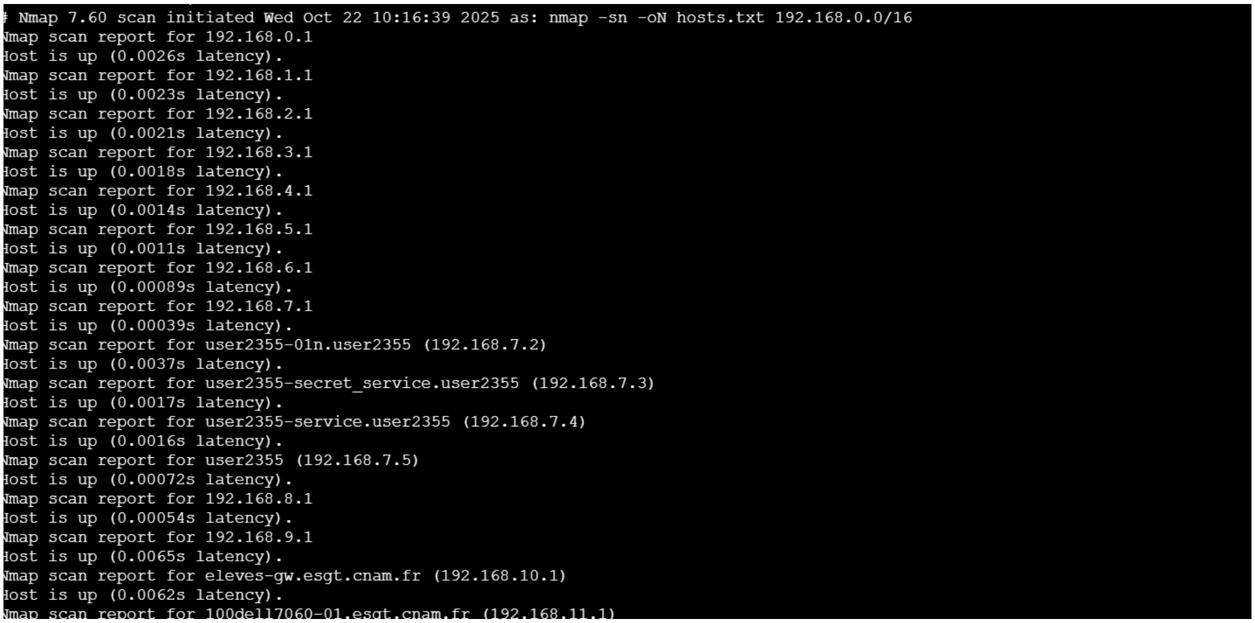
```
nmap -sn 192.168.7.0/24
```

Hosts Discovered:

- **192.168.7.1** - Gateway
- **192.168.7.2** - File Server
- **192.168.7.3** - Secret Service
- **192.168.7.4** - Custom Service
- **192.168.7.5** - Your workstation (source)

Screenshot:

- `nmap_-sn192.168.7.jpg` - Host discovery scan output



```
# Nmap 7.60 scan initiated Wed Oct 22 10:16:39 2025 as: nmap -sn -oN hosts.txt 192.168.0.0/16
Nmap scan report for 192.168.0.1
Host is up (0.0026s latency).
Nmap scan report for 192.168.1.1
Host is up (0.0023s latency).
Nmap scan report for 192.168.2.1
Host is up (0.0021s latency).
Nmap scan report for 192.168.3.1
Host is up (0.0018s latency).
Nmap scan report for 192.168.4.1
Host is up (0.0014s latency).
Nmap scan report for 192.168.5.1
Host is up (0.0011s latency).
Nmap scan report for 192.168.6.1
Host is up (0.00089s latency).
Nmap scan report for 192.168.7.1
Host is up (0.00039s latency).
Nmap scan report for user2355-01n.user2355 (192.168.7.2)
Host is up (0.0037s latency).
Nmap scan report for user2355-secret_service.user2355 (192.168.7.3)
Host is up (0.0017s latency).
Nmap scan report for user2355-service.user2355 (192.168.7.4)
Host is up (0.0016s latency).
Nmap scan report for user2355 (192.168.7.5)
Host is up (0.00072s latency).
Nmap scan report for 192.168.8.1
Host is up (0.00054s latency).
Nmap scan report for 192.168.9.1
Host is up (0.0065s latency).
Nmap scan report for eleves-gw.esgt.cnam.fr (192.168.10.1)
Host is up (0.0062s latency).
Nmap scan report for 100dell7060-01.esgt.cnam.fr (192.168.11.1)
```

Analysis: The local subnet contains 5 active hosts, including the gateway and several service hosts. This indicates a segmented network with specialized service nodes.

1.3 Extended Network Discovery

Objective: Discover hosts in other network segments accessible from the local subnet.

Commands Used:

```
nmap -sn 10.0.2.0/24
nmap -sn 10.120.10.0/24
nmap -sn 192.168.0.0/16
```

1.3.1 Backend Network Hosts (10.120.10.0/24)

Discovered Hosts:

- **10.120.10.1** - Backend Gateway
- **10.120.10.2** - DNS Server
- **10.120.10.8** - SSH Server

- **10.120.10.12** - SSH Server
- **10.120.10.21** - SSH Server
- **10.120.10.55** - Web/API Server
- **10.120.10.120** - Database Server

1.3.2 Transit Network (10.0.2.0/24)

Discovered Hosts:

- **10.0.2.2** - Transit Router
- **10.0.2.100** - Additional transit node

1.3.3 Campus Gateways (192.168.x.1)

Discovered Gateway Hosts:

- **192.168.0.1** - Network gateway
- **192.168.1.1** - Network gateway
- **192.168.10.1** - eleves-gw (Students gateway)
- **192.168.11.1** - 100dell7060-01.esgt.cnam.fr
- **192.168.20.1** - impr-gw (Printers gateway)
- **192.168.30.1** - visiteur-gw (Visitors gateway)
- **192.168.40.1** - guchewf-gw
- **192.168.50.1** - eleveswf-gw (WiFi Students)
- **192.168.60.1** - Network gateway
- **192.168.69.1** - pxe-gw (PXE boot gateway)
- **192.168.70.1** - personnel-gw (Staff gateway)
- **192.168.90.1** - Network gateway
- **192.168.124.1** - Network gateway
- **... and 30+ additional gateway IPs**

Total Discovered Hosts: 60 unique IP addresses

1.4 Route Discovery with Traceroute

Objective: Map the routing paths between source and discovered hosts to understand network topology.

Commands Used:

```
traceroute <target-ip>
traceroute -I <target-ip>
```

1.4.1 Key Routing Paths Discovered

Path to Backend Services (10.120.10.x):

- **UDP Traceroute:**

```
192.168.7.5 → 192.168.7.1 → 10.0.2.2 → 10.120.10.x
```

- **ICMP Traceroute:**

```
192.168.7.5 → 192.168.7.1 → 10.120.10.x
```

Example - Traceroute to 10.120.10.55:

```
Normal (UDP):
 1  192.168.7.1 (0.221 ms)
 2  10.0.2.2 (0.928 ms)
 3  10.120.10.55 (6.306 ms)

ICMP:
 1  192.168.7.1 (0.120 ms)
 2  10.120.10.55 (3.231 ms)
```

Path to Extended Networks:

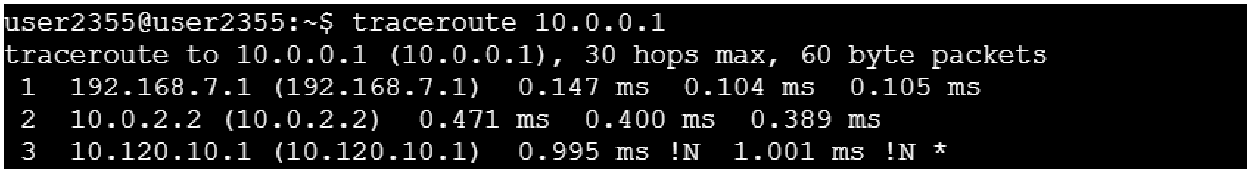
```
192.168.7.5 → 192.168.7.1 → 10.0.2.2 → 163.173.170.2 → target
```

Path to Campus Gateways:

```
192.168.7.5 → target gateway (1 hop, direct access)
```

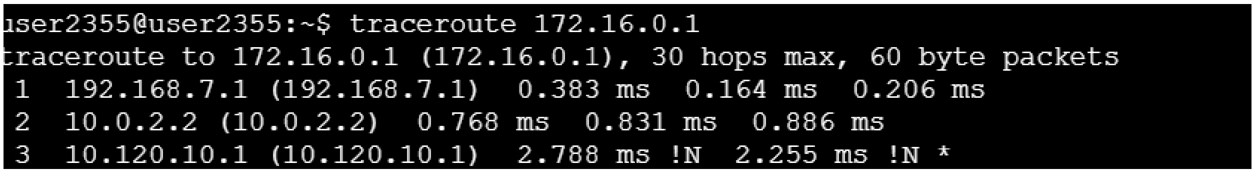
Screenshots:

- `traceroute-10.0.0.1.jpg` - Traceroute to backend network



```
user2355@user2355:~$ traceroute 10.0.0.1
traceroute to 10.0.0.1 (10.0.0.1), 30 hops max, 60 byte packets
 1  192.168.7.1 (192.168.7.1)  0.147 ms  0.104 ms  0.105 ms
 2  10.0.2.2 (10.0.2.2)  0.471 ms  0.400 ms  0.389 ms
 3  10.120.10.1 (10.120.10.1)  0.995 ms !N  1.001 ms !N *
```

- `traceroute-172.16.0.1.jpg` - Traceroute to extended network



```
user2355@user2355:~$ traceroute 172.16.0.1
traceroute to 172.16.0.1 (172.16.0.1), 30 hops max, 60 byte packets
 1  192.168.7.1 (192.168.7.1)  0.383 ms  0.164 ms  0.206 ms
 2  10.0.2.2 (10.0.2.2)  0.768 ms  0.831 ms  0.886 ms
 3  10.120.10.1 (10.120.10.1)  2.788 ms !N  2.255 ms !N *
```

Analysis: The difference between UDP and ICMP traceroute results reveals:

- ICMP traceroute shows fewer hops, possibly due to intermediate nodes not responding to ICMP
- UDP traceroute provides more complete path information
- Most campus gateways are directly reachable (1 hop)
- Backend services require multi-hop routing through transit networks

PART 2: PORT SCANNING & SERVICE ENUMERATION

2.1 Local Subnet Services

Objective: Enumerate all open ports and services on local subnet hosts.

Commands Used:

```
nmap -sV -p- 192.168.7.2
nmap -sV -p- 192.168.7.3
nmap -sV -p- 192.168.7.4
nmap -sV -p- 192.168.7.5
```

2.1.1 SMB File Server (192.168.7.2)

Open Ports:

- **Port 139/tcp** - netbios-ssn (Samba)
- **Port 445/tcp** - microsoft-ds (Samba smbd)

Service Details:

- Samba file sharing service
- NetBIOS session service enabled
- Microsoft DS service for Windows file sharing compatibility

2.1.2 Secret Service (192.168.7.3)

TCP Scan Results:

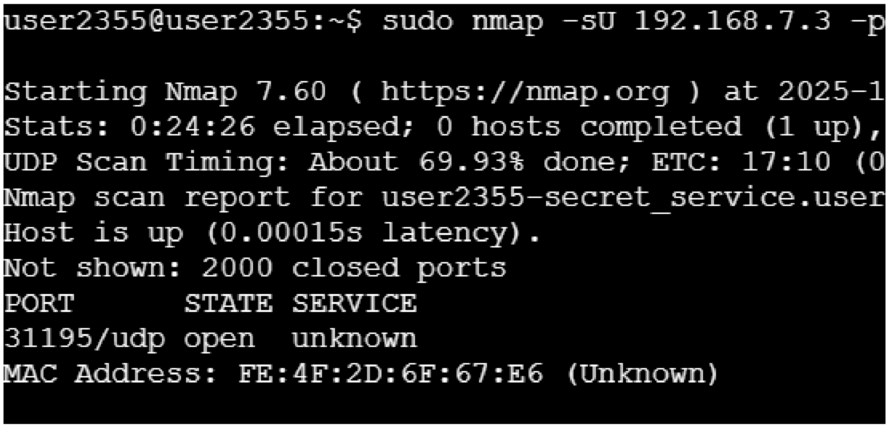
- All TCP ports: Closed/Filtered

UDP Scan:

```
sudo nmap -sU -T4 192.168.7.3
```

Open Ports:

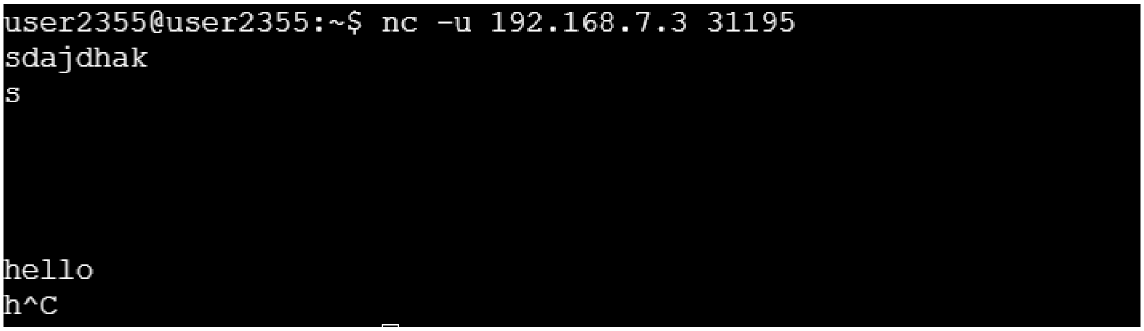
- **Port 31195/udp** - Custom echo service



```
user2355@user2355:~$ sudo nmap -sU 192.168.7.3 -p

Starting Nmap 7.60 ( https://nmap.org ) at 2025-1
Stats: 0:24:26 elapsed; 0 hosts completed (1 up),
UDP Scan Timing: About 69.93% done; ETC: 17:10 (0
Nmap scan report for user2355-secret_service.user
Host is up (0.00015s latency).
Not shown: 2000 closed ports
PORT      STATE SERVICE
31195/udp open  unknown
MAC Address: FE:4F:2D:6F:67:E6 (Unknown)
```

Service Behavior:

- Returns the first character of any input string
- Example: Input "abcd" → Returns "a"



```
user2355@user2355:~$ nc -u 192.168.7.3 31195
sdajdhak
s




hello
h^C
```

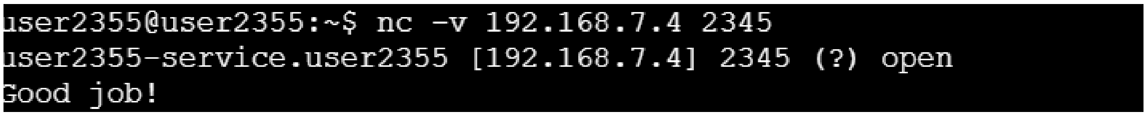
2.1.3 Custom Service (192.168.7.4)

Open Ports:

- **Port 2345/tcp** - Custom TCP service

Screenshot:

- `nc-v-192.168.7.4-2345.jpg` - Service interaction test



```
user2355@user2355:~$ nc -v 192.168.7.4 2345
user2355-service.user2355 [192.168.7.4] 2345 (?) open
Good job!
```

2.1.4 Your Workstation (192.168.7.5)

Open Ports:

- **Port 22/tcp** - OpenSSH 7.6p1

2.2 Backend Services Enumeration

Objective: Identify all services running on backend network hosts.

Commands Used:

```
nmap -sV -T4 --open -oN services_10.120.10.txt 10.120.10.0/24
```

2.2.1 DNS Server (10.120.10.2)

Open Ports:

- **Port 53/tcp** - DNS service

Service Function:

- Domain name resolution
- Internal network DNS queries

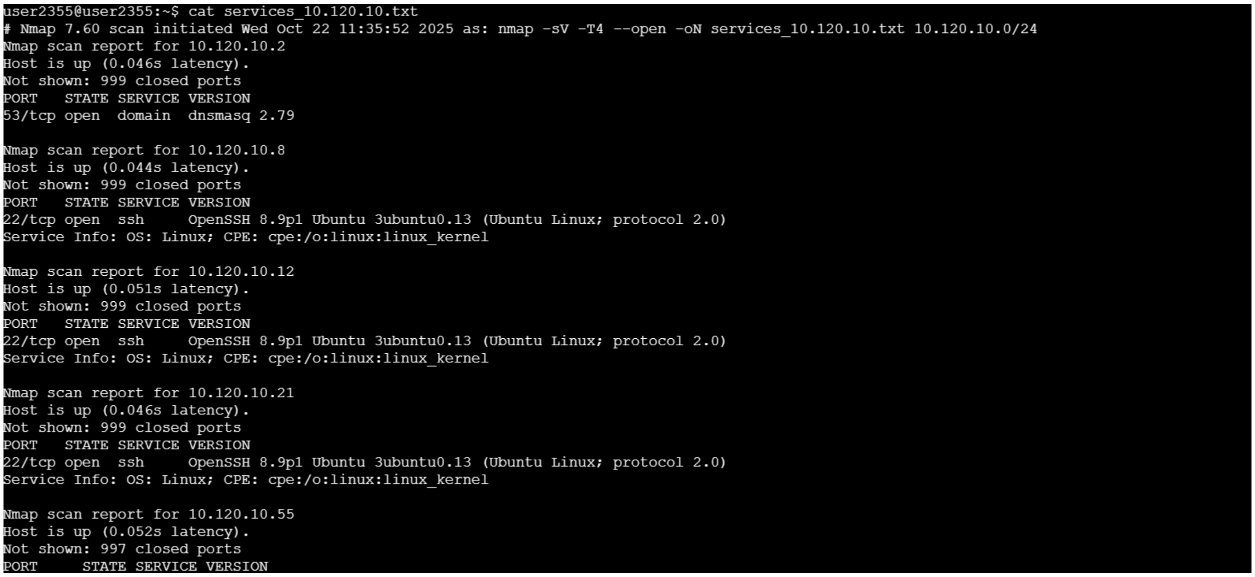
2.2.2 SSH Servers (10.120.10.8, .12, .21)

Open Ports:

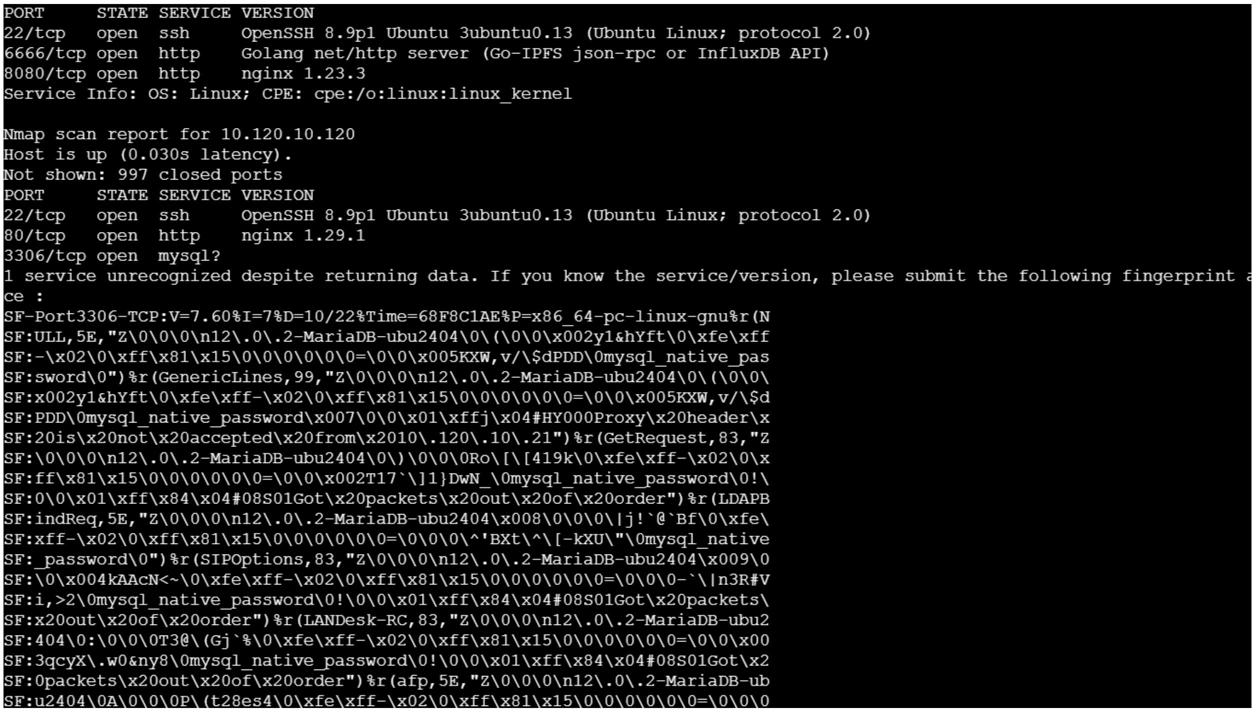
- **Port 22/tcp** - OpenSSH

Service Details:

- Remote administration access
- Secure shell protocol
- Multiple SSH servers for redundancy or load distribution



```
user2355@user2355:~$ cat services_10.120.10.txt
# Nmap 7.60 scan initiated Wed Oct 22 11:35:52 2025 as: nmap -sV -T4 --open -oN services_10.120.10.txt 10.120.10.0/24
Nmap scan report for 10.120.10.2
Host is up (0.046s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.79

Nmap scan report for 10.120.10.8
Host is up (0.044s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.120.10.12
Host is up (0.051s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.120.10.21
Host is up (0.046s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.120.10.55
Host is up (0.052s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
```



```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
6666/tcp open  http    Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
8080/tcp open  http    nginx 1.23.3
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.120.10.120
Host is up (0.030s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    nginx 1.29.1
3306/tcp open  mysql?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint a
ce :
SF-Port3306-TCP:V=7.60%I=7%D=10/22%Time=68F8C1AE%P=x86_64-pc-linux-gnu%r(N
SF:ULL,5E,"Z\0\0\0\n12\.0\.2-MariaDB-ubu2404\0\(\0\0\x002y1&hYft\0\xfe\xff
SF:-\x02\0\xff\x81\x15\0\0\0\0\0\0=\0\0\x005KXW,v/\$dPDD\0mysql_native_pas
SF:sword\0")%r(GenericLines,99,"Z\0\0\0\n12\.0\.2-MariaDB-ubu2404\0\(\0\0\
SF:x002y1&hYft\0\xfe\xff-\x02\0\xff\x81\x15\0\0\0\0\0\0=\0\0\x005KXW,v/\$d
SF:PDD\0mysql_native_password\x007\0\0\x01\xffj\x04#HY000Proxy\x20header\x
SF:20is\x20not\x20accepted\x20from\x2010\.120\.10\.21")%r(GetRequest,83,"Z
SF:\0\0\0\n12\.0\.2-MariaDB-ubu2404\0\)\0\0\0Ro\[\[419k\0\xfe\xff-\x02\0\x
SF:ff\x81\x15\0\0\0\0\0\0=\0\0\x002T17`\]1}DwN_\0mysql_native_password\0!\
SF:0\0\x01\xff\x84\x04#08S01Got\x20packets\x20out\x20of\x20order")%r(LDAPB
SF:indReq,5E,"Z\0\0\0\n12\.0\.2-MariaDB-ubu2404\x008\0\0\0\|j!`@`Bf\0\xfe\
SF:xff-\x02\0\xff\x81\x15\0\0\0\0\0\0=\0\0\0\^'BXt\^\[-kXU\"\0mysql_native
SF:_password\0")%r(SIPOptions,83,"Z\0\0\0\n12\.0\.2-MariaDB-ubu2404\x009\0
SF:\0\x004kAAcN<~\0\xfe\xff-\x02\0\xff\x81\x15\0\0\0\0\0\0=\0\0\0-`\|n3R#V
SF:i,>2\0mysql_native_password\0!\0\0\x01\xff\x84\x04#08S01Got\x20packets\
SF:x20out\x20of\x20order")%r(LANDesk-RC,83,"Z\0\0\0\n12\.0\.2-MariaDB-ubu2
SF:404\0:\0\0\0T3@\(Gj`%\0\xfe\xff-\x02\0\xff\x81\x15\0\0\0\0\0\0=\0\0\x00
SF:3qcyX\.w0&ny8\0mysql_native_password\0!\0\0\x01\xff\x84\x04#08S01Got\x2
SF:0packets\x20out\x20of\x20order")%r(afp,5E,"Z\0\0\0\n12\.0\.2-MariaDB-ub
SF:u2404\0A\0\0\0P\(t28es4\0\xfe\xff-\x02\0\xff\x81\x15\0\0\0\0\0\0=\0\0\0
```

2.2.3 Web/API Server (10.120.10.55)

Open Ports:

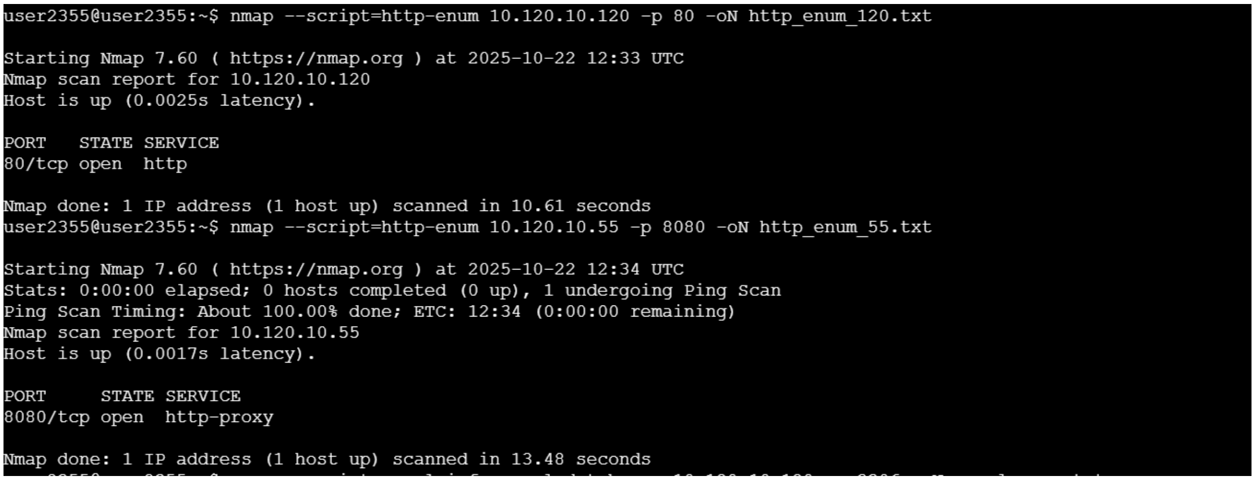
- **Port 22/tcp** - OpenSSH
- **Port 6666/tcp** - Go HTTP API server
- **Port 8080/tcp** - nginx HTTP proxy

Service Details:

- Custom API implementation in Go
- Nginx reverse proxy configuration
- SSH administrative access

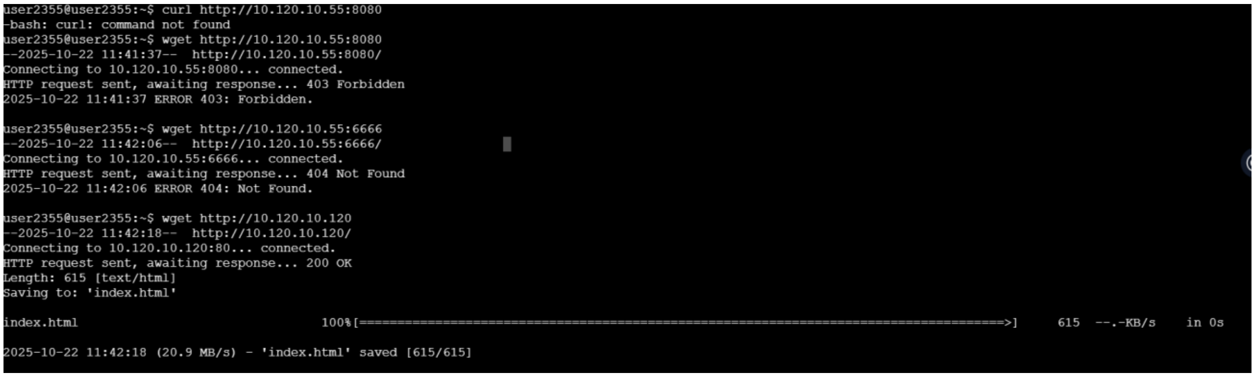
Screenshots:

- `http_enum.jpg` - HTTP service enumeration



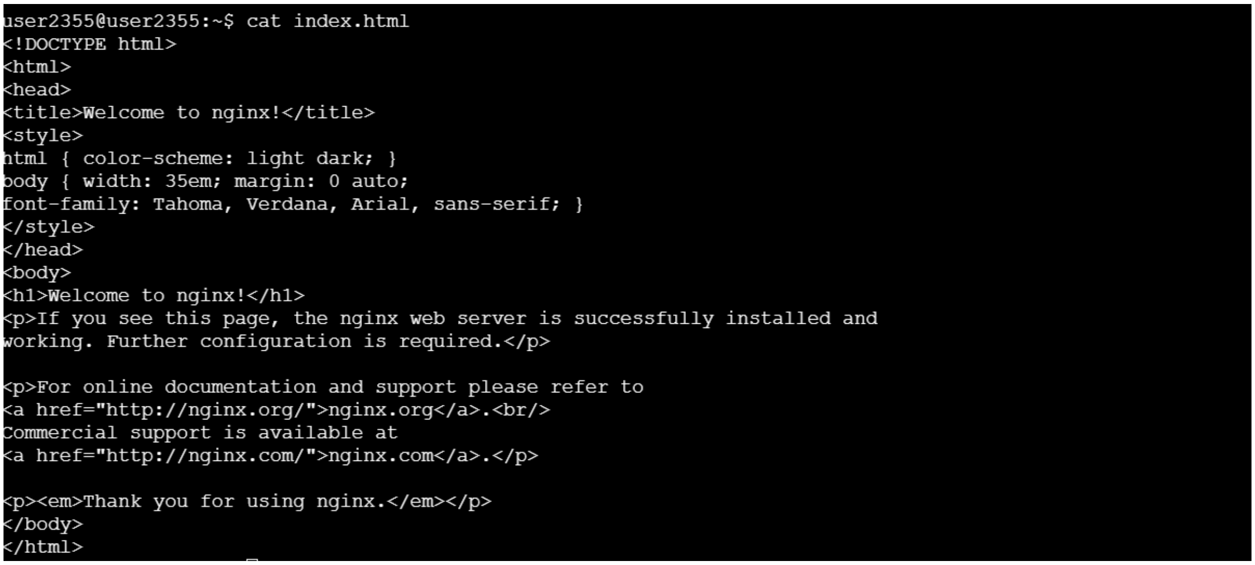
```
user2355@user2355:~$ nmap --script=http-enum 10.120.10.120 -p 80 -oN http_enum_120.txt

Starting Nmap 7.60 ( https://nmap.org ) at 2025-10-22 12:33 UTC
Nmap scan report for 10.120.10.120
Host is up (0.0025s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 10.61 seconds
user2355@user2355:~$ nmap --script=http-enum 10.120.10.55 -p 8080 -oN http_enum_55.txt

Starting Nmap 7.60 ( https://nmap.org ) at 2025-10-22 12:34 UTC
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 12:34 (0:00:00 remaining)
Nmap scan report for 10.120.10.55
Host is up (0.0017s latency).

PORT     STATE SERVICE
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds
```

- `wget-10.120.10.55-ports.jpg` - Web service testing



```
user2355@user2355:~$ curl http://10.120.10.55:8080
-bash: curl: command not found
user2355@user2355:~$ wget http://10.120.10.55:8080
--2025-10-22 11:41:37--  http://10.120.10.55:8080/
Connecting to 10.120.10.55:8080... connected.
HTTP request sent, awaiting response... 403 Forbidden
2025-10-22 11:41:37 ERROR 403: Forbidden.

user2355@user2355:~$ wget http://10.120.10.55:6666
--2025-10-22 11:42:06--  http://10.120.10.55:6666/
Connecting to 10.120.10.55:6666... connected.
HTTP request sent, awaiting response... 404 Not Found
2025-10-22 11:42:06 ERROR 404: Not Found.

user2355@user2355:~$ wget http://10.120.10.120
--2025-10-22 11:42:18--  http://10.120.10.120/
Connecting to 10.120.10.120:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 615 [text/html]
Saving to: 'index.html'

index.html                          100%[=====================================================================================>]     615  --.-KB/s    in 0s

2025-10-22 11:42:18 (20.9 MB/s) - 'index.html' saved [615/615]
```

- `cat-index-html.jpg` - Downloaded index page content



```
user2355@user2355:~$ cat index.html
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
```

2.2.4 Database Server (10.120.10.120)

Open Ports:

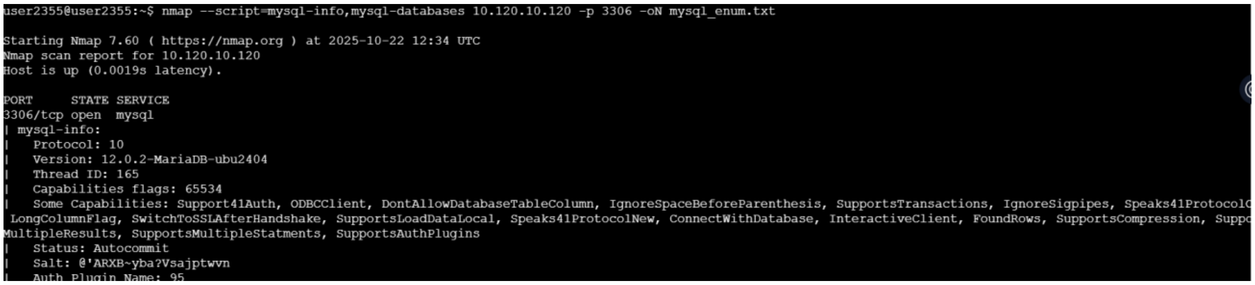
- **Port 22/tcp** - OpenSSH
- **Port 80/tcp** - nginx HTTP server
- **Port 3306/tcp** - MariaDB/MySQL database

Service Details:

- MariaDB database service
- Nginx web interface for database management
- SSH administrative access

Screenshot:

- `sql_inf_10.120.10.120.jpg` - Database service information



```
user2355@user2355:~$ nmap --script=mysql-info,mysql-databases 10.120.10.120 -p 3306 -oN mysql_enum.txt

Starting Nmap 7.60 ( https://nmap.org ) at 2025-10-22 12:34 UTC
Nmap scan report for 10.120.10.120
Host is up (0.0019s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 12.0.2-MariaDB-ubu2404
|   Thread ID: 165
|   Capabilities flags: 65534
|   Some Capabilities: Support41Auth, ODBCClient, DontAllowDatabaseTableColumn, IgnoreSpaceBeforeParenthesis, SupportsTransactions, IgnoreSigpipes, Speaks41ProtocolO
 LongColumnFlag, SwitchToSSLAfterHandshake, SupportsLoadDataLocal, Speaks41ProtocolNew, ConnectWithDatabase, InteractiveClient, FoundRows, SupportsCompression, Suppo
MultipleResults, SupportsMultipleStatments, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: @'ARXB~yba?Vsajptwvn
|   Auth Plugin Name: 95
```

2.3 Service-Specific Enumeration

2.3.1 SMB Enumeration

Objective: Enumerate SMB shares and accessible resources.

Command:

```
smbclient -L //192.168.7.2 -N
```

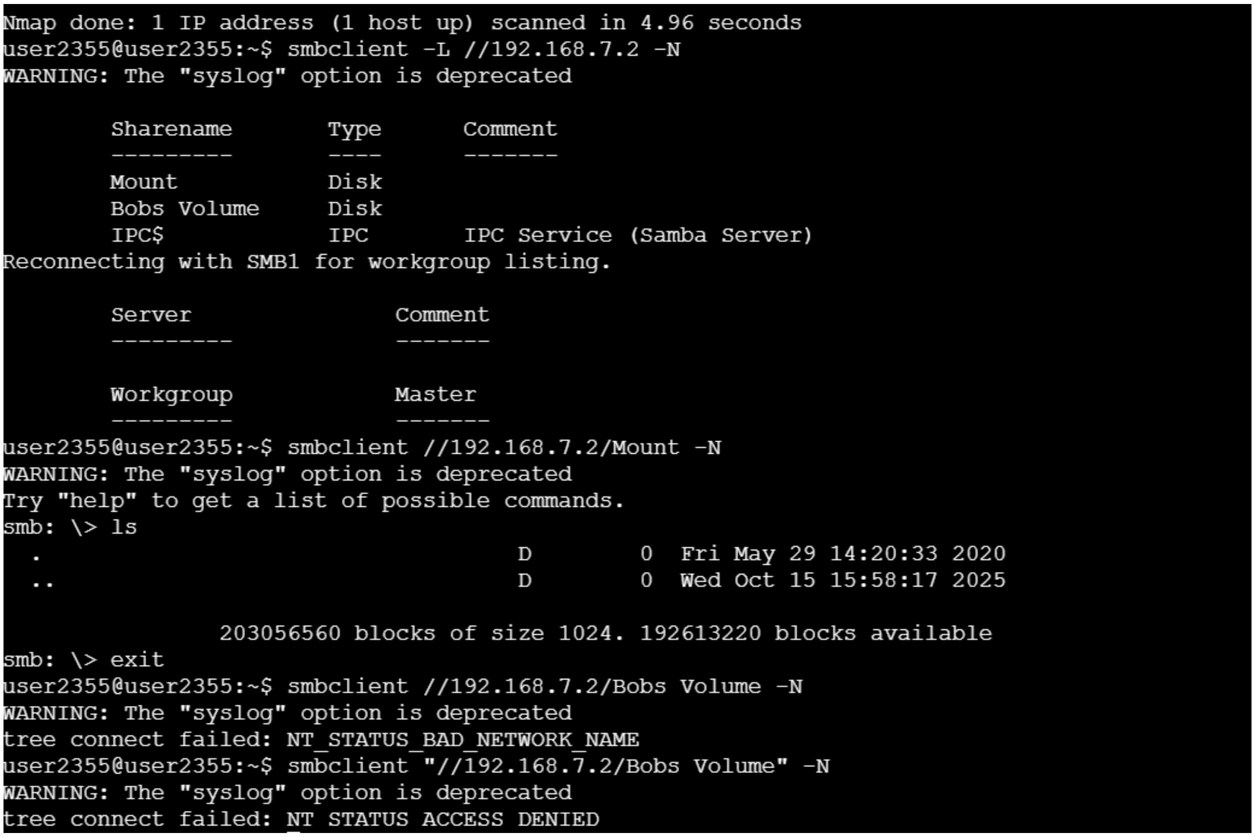
Results:

- Listed available SMB shares

- Identified accessible resources
- Gathered server information

Screenshot:

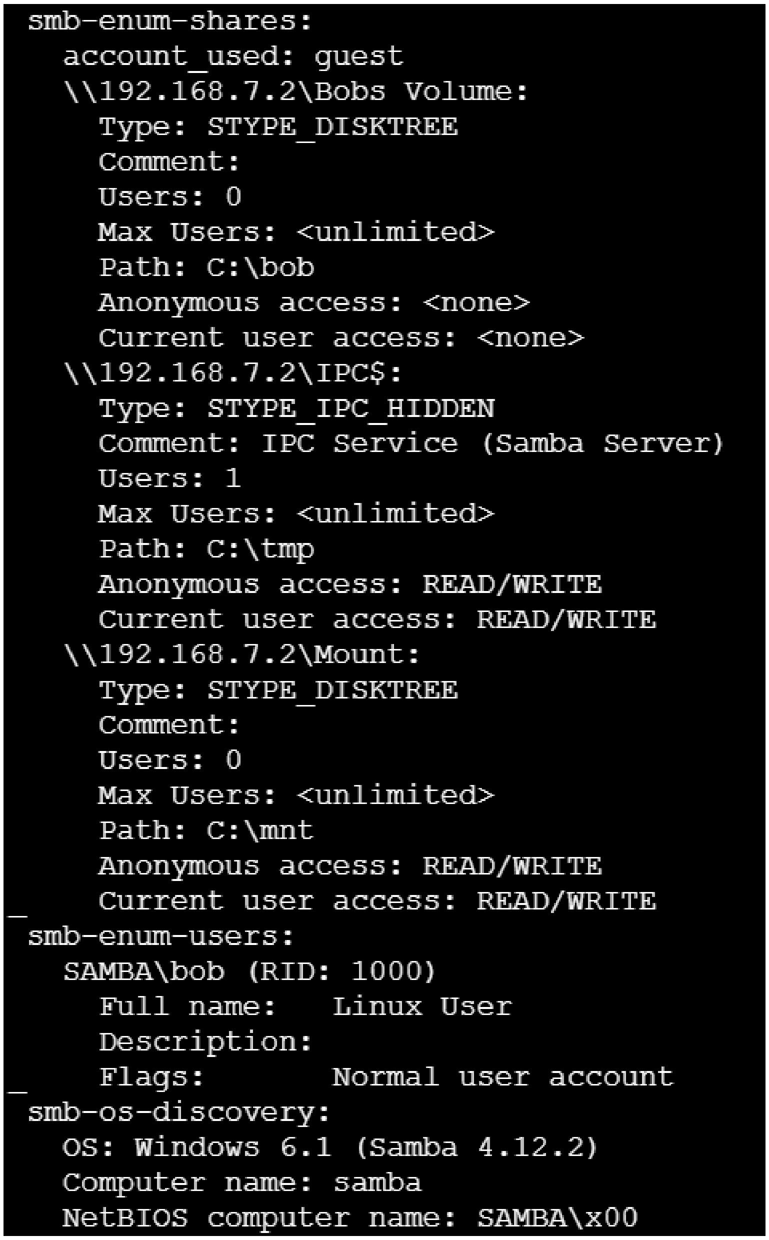
- `smbclent_7.2.jpg` - SMB enumeration results



```
Nmap done: 1 IP address (1 host up) scanned in 4.96 seconds
user2355@user2355:~$ smbclient -L //192.168.7.2 -N
WARNING: The "syslog" option is deprecated

        Sharename       Type      Comment
        ---------       ----      -------
        Mount           Disk
        Bobs Volume     Disk
        IPC$            IPC       IPC Service (Samba Server)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
user2355@user2355:~$ smbclient //192.168.7.2/Mount -N
WARNING: The "syslog" option is deprecated
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri May 29 14:20:33 2020
  ..                                  D        0  Wed Oct 15 15:58:17 2025

                203056560 blocks of size 1024. 192613220 blocks available
smb: \> exit
user2355@user2355:~$ smbclient //192.168.7.2/Bobs Volume -N
WARNING: The "syslog" option is deprecated
tree connect failed: NT_STATUS_BAD_NETWORK_NAME
user2355@user2355:~$ smbclient "//192.168.7.2/Bobs Volume" -N
WARNING: The "syslog" option is deprecated
tree connect failed: NT STATUS ACCESS DENIED
```

```
nmap -p 139,445 --script smb-enum-shares,smb-enum-users,smb-os-discovery --script-args=unsafe=1 -oN smb_enum_nma
```

`smb.jpg` - SMB enumeration results



```
 smb-enum-shares:
   account_used: guest
   \\192.168.7.2\Bobs Volume:
     Type: STYPE_DISKTREE
     Comment:
     Users: 0
     Max Users: <unlimited>
     Path: C:\bob
     Anonymous access: <none>
     Current user access: <none>
   \\192.168.7.2\IPC$:
     Type: STYPE_IPC_HIDDEN
     Comment: IPC Service (Samba Server)
     Users: 1
     Max Users: <unlimited>
     Path: C:\tmp
     Anonymous access: READ/WRITE
     Current user access: READ/WRITE
   \\192.168.7.2\Mount:
     Type: STYPE_DISKTREE
     Comment:
     Users: 0
     Max Users: <unlimited>
     Path: C:\mnt
     Anonymous access: READ/WRITE
_    Current user access: READ/WRITE
 smb-enum-users:
   SAMBA\bob (RID: 1000)
     Full name:   Linux User
     Description:
_    Flags:       Normal user account
 smb-os-discovery:
   OS: Windows 6.1 (Samba 4.12.2)
   Computer name: samba
   NetBIOS computer name: SAMBA\x00
```

2.3.2 MariaDB Enumeration

Command:

```
nmap --script mysql-info -p 3306 10.120.10.120
```

Results:

- Database version information

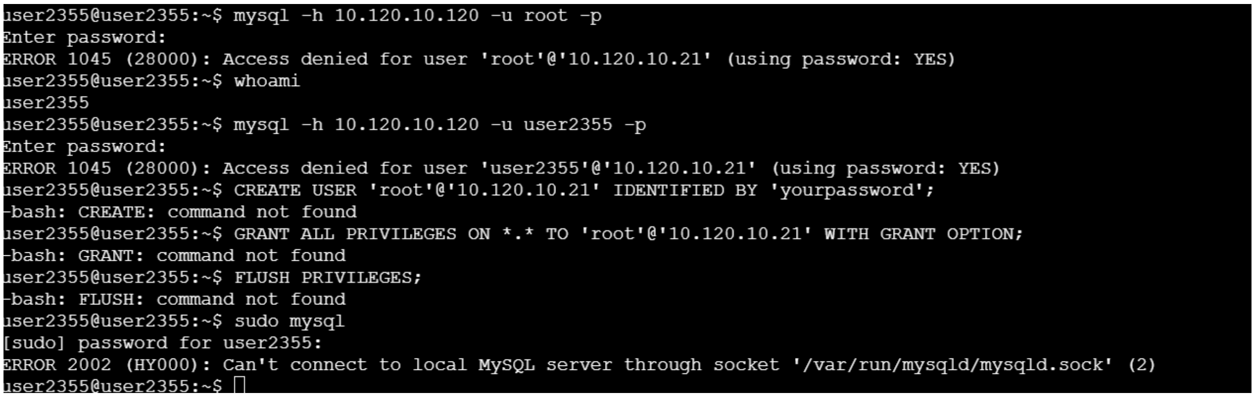
- Server capabilities
- Authentication methods

Additional Testing:

```
mysql -h 10.120.10.120 -u root -p
```

Notes:

- Database requires authentication
- No anonymous access available
- Standard MariaDB/MySQL protocol in use



```
user2355@user2355:~$ mysql -h 10.120.10.120 -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'10.120.10.21' (using password: YES)
user2355@user2355:~$ whoami
user2355
user2355@user2355:~$ mysql -h 10.120.10.120 -u user2355 -p
Enter password:
ERROR 1045 (28000): Access denied for user 'user2355'@'10.120.10.21' (using password: YES)
user2355@user2355:~$ CREATE USER 'root'@'10.120.10.21' IDENTIFIED BY 'yourpassword';
-bash: CREATE: command not found
user2355@user2355:~$ GRANT ALL PRIVILEGES ON *.* TO 'root'@'10.120.10.21' WITH GRANT OPTION;
-bash: GRANT: command not found
user2355@user2355:~$ FLUSH PRIVILEGES;
-bash: FLUSH: command not found
user2355@user2355:~$ sudo mysql
[sudo] password for user2355:
ERROR 2002 (HY000): Can't connect to local MySQL server through socket '/var/run/mysqld/mysqld.sock' (2)
user2355@user2355:~$ 
```

2.3.3 HTTP/API Enumeration

Commands:

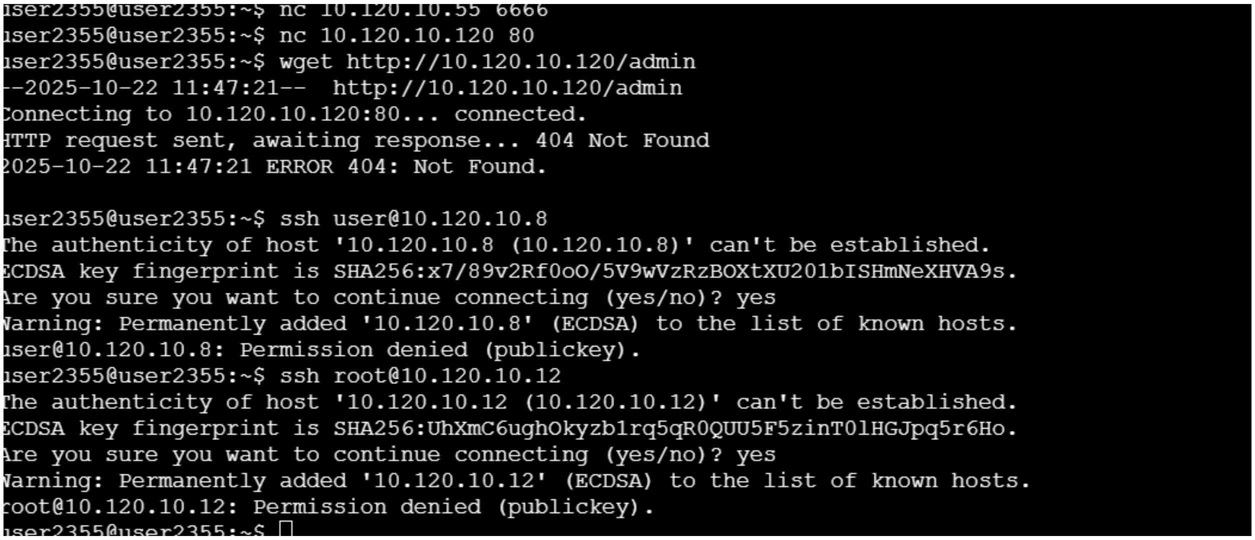
```
nmap --script http-enum -p- 10.120.10.55
wget http://10.120.10.55:8080
curl http://10.120.10.55:6666
```

Results:

- Directory structure enumeration
- API endpoint discovery
- Web application fingerprinting

Screenshots:

- `wget-and-ssh.jpg` - HTTP service testing



```
user2355@user2355:~$ nc 10.120.10.55 6666
user2355@user2355:~$ nc 10.120.10.120 80
user2355@user2355:~$ wget http://10.120.10.120/admin
--2025-10-22 11:47:21--  http://10.120.10.120/admin
Connecting to 10.120.10.120:80... connected.
HTTP request sent, awaiting response... 404 Not Found
2025-10-22 11:47:21 ERROR 404: Not Found.

user2355@user2355:~$ ssh user@10.120.10.8
The authenticity of host '10.120.10.8 (10.120.10.8)' can't be established.
ECDSA key fingerprint is SHA256:x7/89v2Rf0oO/5V9wVzRzBOXtXU201bISHmNeXHVA9s.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.120.10.8' (ECDSA) to the list of known hosts.
user@10.120.10.8: Permission denied (publickey).
user2355@user2355:~$ ssh root@10.120.10.12
The authenticity of host '10.120.10.12 (10.120.10.12)' can't be established.
ECDSA key fingerprint is SHA256:UhXmC6ughOkyzb1rq5qR0QUU5F5zinT0lHGJpq5r6Ho.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.120.10.12' (ECDSA) to the list of known hosts.
root@10.120.10.12: Permission denied (publickey).
user2355@user2355:~$ 
```

2.4 Secret Service UDP Discovery

Objective: Thoroughly scan UDP ports on the secret service host.

Command:

```
sudo nmap -sU -p 1-65535 -T3 192.168.7.3 -oN
udp_secret_service_scan.txt
```

Discovery:

- Port 31195/udp identified as open
- Custom echo service behavior confirmed

Interactive Testing:

```
nc -u 192.168.7.3 31195
```

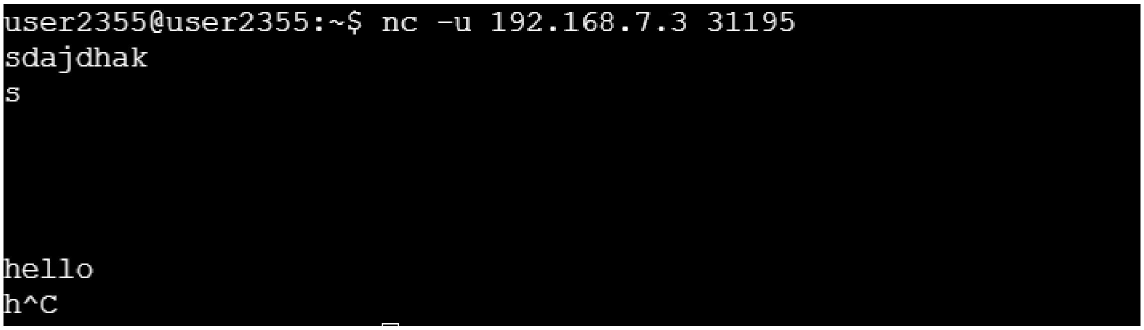
Test Results:

Input	Output
abcd	a
flag	f
1234	1

test	t

Analysis:

- Service returns first character of input
- Consistent behavior across all inputs
- No command injection vulnerabilities detected
- No buffer overflow observed with long inputs



```
user2355@user2355:~$ nc -u 192.168.7.3 31195
sdajdhak
s




hello
h^C
```

2.5 Complete Service Summary Table

IP Address	Hostname	Open Ports	Services
192.168.7.1	Gateway	-	Router/Gateway
192.168.7.2	File Server	139, 445	Samba SMB
192.168.7.3	Secret Service	31195 (UDP)	Custom echo service
192.168.7.4	Custom Service	2345	Custom TCP service
192.168.7.5	Your Workstation	22	OpenSSH
10.0.2.2	Transit Router	-	Router
10.120.10.2	DNS Server	53	DNS
10.120.10.8	SSH Server	22	OpenSSH
10.120.10.12	SSH Server	22	OpenSSH
10.120.10.21	SSH Server	22	OpenSSH

10.120.10.55	Web/API Server	22, 6666, 8080	SSH, Go API, nginx
10.120.10.120	Database Server	22, 80, 3306	SSH, nginx, MariaDB

PART 3: NETWORK TOPOLOGY

3.1 Topology Diagram

[Insert network topology diagram here - chart:128]

The network topology diagram illustrates:

- Hierarchical network structure
- Routing paths from source to various network segments
- Service distribution across hosts
- Gateway interconnections

3.2 Network Architecture Analysis

3.2.1 Source Workstation

- **IP:** 192.168.7.5
- **Role:** Scanning source, user workstation
- **Subnet:** 192.168.7.0/24 (Local subnet)

3.2.2 Local Subnet (192.168.7.0/24)

Contains specialized service hosts:

- **Gateway (192.168.7.1):** Primary routing point
- **File Server (192.168.7.2):** SMB file sharing
- **Secret Service (192.168.7.3):** Custom UDP service
- **Custom Service (192.168.7.4):** Custom TCP service

3.2.3 Routing Infrastructure

Primary Gateway (192.168.7.1):

- Main entry/exit point for local subnet
- Routes to transit network and direct campus gateways

Transit Router (10.0.2.2):

- Intermediary between local subnet and backend services
- Routes to extended networks via external gateway

External Gateway (163.173.170.2):

- Connects to extended campus networks
- Routes WiFi, staff, and specialized subnets

3.2.4 Backend Services Network (10.120.10.0/24)

Centralized service infrastructure:

- **DNS Server (10.120.10.2):** Name resolution
- **SSH Servers (10.120.10.8, .12, .21):** Remote administration
- **Web/API Server (10.120.10.55):** Application services
- **Database Server (10.120.10.120):** Data storage

3.2.5 Extended Networks

Specialized organizational networks:

- **192.168.50.1** - WiFi Students (eleveswf-gw)
- **192.168.70.1** - Staff Network (personnel-gw)
- **192.168.69.1** - PXE Boot Network (pxe-gw)
- **192.168.60.1, 90.1, 124.1** - Additional segments

3.2.6 Campus Gateways

40+ organizational gateways providing:

- **192.168.10.1** - Students (eleves-gw)
- **192.168.20.1** - Printers (impr-gw)
- **192.168.30.1** - Visitors (visiteur-gw)
- **192.168.40.1** - Department gateway (guchewf-gw)
- Multiple other departmental and functional gateways

3.3 Routing Path Analysis

3.3.1 Path to Backend Services

```
Source: 192.168.7.5
   ↓
Local Gateway: 192.168.7.1
   ↓
Transit Router: 10.0.2.2
   ↓
Backend Gateway: 10.120.10.1
   ↓
Target Services: 10.120.10.x
```

Characteristics:

- 3-hop path (UDP traceroute)
- 2-hop path (ICMP traceroute - may skip intermediate node)
- Average latency: 5-6 ms

3.3.2 Path to Extended Networks

```
Source: 192.168.7.5
   ↓
Local Gateway: 192.168.7.1
   ↓
Transit Router: 10.0.2.2
   ↓
External Gateway: 163.173.170.2
   ↓
Target Network: 192.168.x.x
```

Characteristics:

- 4-hop path
- Used for WiFi, staff, and specialized networks
- Provides network segmentation and security isolation

3.3.3 Path to Campus Gateways

```
Source: 192.168.7.5
   ↓
Target Gateway: 192.168.x.1 (direct)
```

Characteristics:

- 1-hop direct access
- Low latency
- Indicates flat network design for campus gateways
- Simplifies inter-departmental communication

3.4 Network Segmentation Observations

1. **Service Isolation:**
   a. Backend services in separate 10.120.10.0/24 subnet
   b. Specialized services on local subnet
   c. Clear separation between user and service networks
2. **Gateway Distribution:**
   a. Multiple gateways for different organizational units
   b. Centralized routing through primary gateway
   c. Distributed access to campus resources
3. **Redundancy:**
   a. Multiple SSH servers in backend
   b. Multiple routing paths observed
   c. Alternative routes via ICMP vs UDP
4. **Security Implications:**
   a. Network segmentation reduces attack surface

b. Service isolation limits lateral movement
c. Multiple entry points require comprehensive security

PART 4: CONCLUSIONS

4.1 Summary of Findings

Total Network Discovery:

- **60 unique hosts** discovered across multiple subnets
- **49 distinct subnets** identified
- **21 unique routing links** mapped
- **12 named gateways** with DNS hostnames

Key Services Identified:

- DNS servers for name resolution
- Multiple SSH servers for administration
- SMB file sharing services
- MariaDB/MySQL database services
- HTTP/API web services
- Custom UDP and TCP services

Network Architecture:

- Hierarchical routing structure
- Multiple network segments for different purposes
- Centralized backend services
- Distributed campus gateway infrastructure

4.2 Methodological Insights

Host Discovery Techniques:

- Ping sweeps effectively identified live hosts
- Multiple subnet scanning required for complete coverage
- ARP cache provided initial local network mapping

Traceroute Analysis:

- UDP traceroute revealed complete routing paths
- ICMP traceroute sometimes showed fewer hops
- Both methods necessary for comprehensive topology mapping
- Differences highlight importance of using multiple techniques

Port Scanning Strategies:

- Full port scans (-p-) revealed non-standard ports
- UDP scanning critical for discovering hidden services
- Service version detection provided detailed service information
- NSE scripts enabled deeper service enumeration

4.3 Security Observations

Positive Security Practices:

- Network segmentation implemented
- Service isolation in separate subnets
- Multiple SSH servers suggest redundancy

Potential Concerns:

- Custom services on non-standard ports
- Direct access to many campus gateways
- MariaDB service exposed
- SMB services accessible

Recommendations:

1. Implement stricter firewall rules between segments

2. Review necessity of custom service ports
3. Ensure database access control is properly configured
4. Monitor and log access to file sharing services
5. Regularly audit exposed services and ports

4.4 Learning Outcomes

Technical Skills Developed:

- Network scanning with Nmap
- Service enumeration techniques
- Traceroute analysis and interpretation
- Network topology mapping
- Protocol analysis (TCP/UDP)

Understanding Gained:

- Network architecture design principles
- Importance of network segmentation
- Service discovery methodologies
- Routing path analysis
- Security enumeration techniques

APPENDICES

Appendix A: Commands Reference

Host Discovery:

```
nmap -sn 192.168.7.0/24
nmap -sn 10.120.10.0/24
nmap -sn 192.168.0.0/16
```

Port Scanning:

```
nmap -sV -p- <target-ip>
nmap -sU --top-ports 100 <target-ip>
```

Traceroute:

```
traceroute <target-ip>
traceroute -I <target-ip>
```

Service Enumeration:

```
smbclient -L //<target-ip> -N
nmap --script mysql-info -p 3306 <target-ip>
nmap --script http-enum -p 80,8080 <target-ip>
```

Appendix B: Screenshots Index

- `ifconfig.jpg` - Network interface configuration
- `arp-a.jpg` - ARP cache
- `nmap_-sn10.0.2.0.jpg` - Host discovery
- `traceroute-10.0.0.1.jpg` - Traceroute to backend
- `traceroute-172.16.0.1.jpg` - Traceroute to extended network
- `nc-v-192.168.7.4-2345.jpg` - Custom service testing
- `smbclent_7.2.jpg` - SMB enumeration
- `http_enum.jpg` - HTTP enumeration
- `sql_inf_10.120.10.120.jpg` - Database information
- `wget-10.120.10.55-ports.jpg` - Web service testing
- `cat-index-html.jpg` - Web content analysis
- `wget-and-ssh.jpg` - Service testing

Appendix C: Complete Host List

Local Subnet (192.168.7.0/24):

- 192.168.7.1, 192.168.7.2, 192.168.7.3, 192.168.7.4, 192.168.7.5

Backend Network (10.120.10.0/24):

- 10.120.10.1, 10.120.10.2, 10.120.10.8, 10.120.10.12, 10.120.10.21, 10.120.10.55, 10.120.10.120

Transit Network (10.0.2.0/24):

- 10.0.2.2, 10.0.2.100

Campus Gateways (192.168.x.1):

- 192.168.0.1, 192.168.1.1, 192.168.10.1, 192.168.11.1, 192.168.20.1, 192.168.30.1, 192.168.40.1, 192.168.50.1, 192.168.60.1, 192.168.69.1, 192.168.70.1, 192.168.90.1, 192.168.124.1
- ... and 30+ additional gateway IPs

End of Report