SUBNETTING

MODULE 2 : SUBNETTING

1. What is Subnetting? (Professional Definition)

Subnetting is the process of **dividing a larger IP network into smaller, logical subnetworks** (subnets) to improve routing efficiency, security, and network management.

In simpler words:

> Subnetting breaks one big network into multiple smaller networks so traffic stays organized, secure, and easy to manage.

✅ 2. Why Subnetting Matters in Penetration Testing

As a pentester, subnetting helps you:

✔ Identify network boundaries

(e.g., internal vs DMZ vs restricted zones)

✔ Scan accurately

Avoid scanning unnecessary IP ranges.

✔ Understand attack paths

How traffic flows → where pivoting may be possible.

✔ Enumerate hidden networks

Subnetting patterns reveal additional internal IP ranges.

Example:

If you see **10.10.5.23/16**, then the **entire network ranges from 10.10.0.0 to 10.10.255.255** → a huge 65,536-host environment.

✅ 3. CIDR Notation (Very Simple Explanation)

CIDR (/xx) tells how many bits are used for the **network portion** of the IP.

Example:

- /24 means **24 bits = network**, remaining 8 bits = hosts
- /16 means **16 bits = network**, remaining 16 bits = hosts

The fewer bits for hosts → the more usable IPs.

✅ 4. Subnet Size Table (Pentester's Cheat Sheet)

CIDR	Hosts	Use Case
/30	2 usable	VPN tunnels, point-to-point links
/29	6 usable	Small server clusters
/24	254 usable	Most LAN networks
/23	510 usable	Large flat networks
/22	1022 usable	Corporate internal ranges
/16	65,534 usable	Entire enterprise network

✅ 5. How Subnetting Helps Pentesters (Real Examples)

Example 1 — Detect Network Size

IP: **192.168.1.25/24**

Meaning:

- Network: 192.168.1.0
- Broadcast: 192.168.1.255
- Hosts: 254

🛠️ Pentester action:

Scan **only the /24**, not the whole 192.168.0.0/16.

Example 2 — Multiple Internal Networks

Target host shows:

```
ip addr
10.0.2.15/24
```

Then ARP table reveals:

```
10.0.3.x
10.0.4.x
```

This indicates **multiple subnets**—good pivot targets.

✅ 6. Essential Subnetting Tools & Commands

Below are actual tools used by pentesters to identify and calculate subnets.

6.1 ipcalc (Linux Subnet Calculator)

Command

```
ipcalc 192.168.1.25/24
```

Output Understanding

- Network: 192.168.1.0
- Netmask: 255.255.255.0
- Broadcast: 192.168.1.255
- Host range: 192.168.1.1 – 192.168.1.254

6.2 sipcalc (Advanced Calculator)

Command

```
sipcalc 10.0.5.200/16
```

Shows:

- Subnet size
- Wildcard mask
- Usable hosts
- Reverse DNS zone

Excellent for large corporate ranges.

6.3 nmap Subnet Discovery

Scan a full subnet

```
nmap -sn 192.168.1.0/24
```

Scan multiple subnets

```
nmap -sn 192.168.0.0/16
```

Discover live hosts

```
nmap -sn 10.0.0.0/8 --min-rate 10000
```

6.4 netdiscover (ARP-based discovery)

Command

```
netdiscover -r 192.168.1.0/24
```

Useful when no ping responses are allowed.

6.5 traceroute for subnet inference

Command

```
traceroute 192.168.1.50
```

Shows:

- Gateway IP
- Intermediate hops

  → Helps identify backbone subnets and routing structure.

6.6 arp-scan (Layer-2 scanning)

Command

```
arp-scan --interface=eth0 192.168.1.0/24
```

Finds:

- MAC addresses
- Vendor names
- Hidden devices not responding to ping

---

7. Practical Subnetting Example (Explained)

Given:

IP: 10.10.5.23

Subnet: /16

Breakdown:

- Network bits: 16
- Host bits: 16
- Total hosts: 65,536
- Usable range: 10.10.0.1 → 10.10.255.254

Why important?

Large internal /16 networks often contain:

- DNS servers
- AD domain controllers
- File shares
- Staging servers
- Test environments

  → A full treasure map for pentesters.

---

8. Supernetting (Brief Professional Note)

Supernetting combines **multiple small networks into a larger one**.

Useful for:

- BGP routing
- ISP aggregation
- Large enterprise backbone routing

Example:

Combine 192.168.0.0/24 + 192.168.1.0/24

→ becomes **192.168.0.0/23**

Subnetting Explained SUPER Simple

Imagine you have a **big classroom** with **100 students**.

The teacher says:

> "This room is too big. Let's divide it into small groups so it's easier to manage."

So she splits the class into **smaller groups**:

- Group 1
- Group 2
- Group 3
- Group 4

That's exactly what **subnetting** does.

⭐ Subnetting = Breaking one BIG network into smaller networks

A **network** is like your big classroom.

Subnetting is cutting it into smaller **sub-classrooms**.

🧠 Why do we do this?

Because smaller groups make things:

- **Easier to control**
- **Safer**
- **Less crowded**
- **Faster**

Same with computer networks!

If 500 computers are in one big messy network, everything becomes slow and confusing.

So subnetting helps organize them.

🏠 Example Using Houses (SUPER SIMPLE)

Think of an IP address like a **house address**:

192.168.1.20

Subnetting tells you **which neighborhood the house belongs to**.

If we say **/24**:

It means:

> "All houses from 192.168.1.1 to 192.168.1.254 belong to the same neighborhood."

🎂 Subnets Are Like Cutting a Cake

You have a big cake (network).

You cut it into slices (subnets).

Smaller slice = fewer people can eat it

Bigger slice = more people can eat it

Works exactly the same for:

- /24
- /23
- /30

🎲 CIDR Explained Like a Toy Box

CIDR (the /24, /16 thing) tells you **how big your toy box is**.

Here's the simple version:

CIDR	Toy Box Size	Meaning
/30	Very tiny	Only 2 devices can fit
/24	Medium	254 devices can fit
/16	Big	65,534 devices can fit

🚦 Traffic Example (Very Simple)

Imagine cars (data packets) on a road.

- One big road = traffic jam
- Many small roads = smooth traffic

Subnetting ⟶ creates more small roads

So computers don't "bump into each other."

🧩 Real-Life Pentesting Example (Kid-Friendly)

You join a network and see:

192.168.1.20/24

You immediately know:

- This is a medium-sized network
- It goes from 192.168.1.1 → 192.168.1.254
- You can scan only these computers, not the whole world

It's like knowing:

> "Your treasure map starts here and ends there."

🛠️ Tools explained in kid-level language

🧱 ipcalc (The Calculator Tool)

It tells you:

- Which neighborhood the IP lives in

- What the first and last house numbers are

Command:

```
ipcalc 192.168.1.20/24
```

🕵️ netdiscover (Find people in the neighborhood)

```
netdiscover -r 192.168.1.0/24
```

Meaning:

> “Hey, who lives in this street?”

🚔 nmap (Check which houses have open doors)

```
nmap -sn 192.168.1.0/24
```

Meaning:

> “Knock on every door and see who answers.”

ONE-SENTENCE SUMMARY

Subnetting is cutting one big network into smaller, easier-to-manage networks—like splitting a big classroom into smaller groups so everything works smoother.