📝

TryHackme Week05 Notes

Networking Concepts

OSI Model (Open Systems Interconnection)

Purpose:

A conceptual model that explains **how data moves through a network**, layer by layer.

Developed by: ISO (International Organization for Standardization)

The 7 Layers (Bottom → Top)

Layer 1 — Physical

- How data physically travels
- Media: cables, fiber, wireless
- Represents data as bits (0s and 1s)

Layer 2 — Data Link

- Data transfer between devices on the **same network segment**
- Defines how devices agree to communicate locally
- Examples:
  - Ethernet (802.3)
  - Wi-Fi (802.11)

Layer 3 — Network

- Communication **between different networks**

- Logical addressing and routing
- Examples:
    - IP
    - ICMP
    - IPSec

Layer 4 — Transport

- End-to-end communication between applications
- Controls reliability and delivery
- Examples:
    - TCP
    - UDP

Layer 5 — Session

- Establishes, maintains, and synchronizes sessions
- Manages connections between applications
- Examples:
    - NFS
    - RPC

Layer 6 — Presentation

- Data formatting and transformation
- Handles:
    - Encoding
    - Compression
    - Encryption

Layer 7 — Application

- Interfaces directly with user applications
- Provides network services
- Examples:
    - HTTP / HTTPS
    - DNS
    - FTP
    - SMTP
    - POP3
    - IMAP

TCP/IP Model

Purpose:

A practical networking model used on the internet.

Mapping OSI → TCP/IP

TCP/IP Layer	OSI Layers
Application	7, 6, 5
Transport	4
Internet	3
Link	2

Subnet

Network inside a network

IP Addresses & Subnets (Private Ranges)

Private IP ranges (memorize):

- `10.0.0.0 – 10.255.255.255` → **10/8**
- `172.16.0.0 – 172.31.255.255` → **172.16/12**

- `192.168.0.0 – 192.168.255.255` → **192.168/16**

Used for internal networks and labs.

Encapsulation

Definition:

The process where **each network layer adds its own header** (and sometimes a trailer) to data as it moves down the stack.

High-level idea:

Application data → wrapped multiple times → transmitted → unwrapped on receipt.

Telnet

- Protocol for remote terminal access
- Allows sending text commands to a remote system
- **Insecure** (plaintext communication)
- High risk if exposed

Networking Core Protocols

DNS traffic uses UDP port 53 and TCP port 53 as a default fall back

WHOIS

> Command whois
>
> provides information about that entity that registered a domain name, name, phone #, email, address.

NMAP - The Basics

Nmap uses multiple ways to specify its targets:

> IP range using -
>
> > For example: scan 192.168.0.1 to 192.168.0.10 = 192.168.0.1-10

IP subnet using /

For example: scan 192.168.0.1/24 = 192.168.0.0-255

Hostname

for example: example.com

Option	Explanation
Target Listing	
`-sL`	List scan – list targets without scanning
Host Discovery	
`-sn`	Ping scan – host discovery only
`-Pn`	Treat all hosts as online – scan hosts that appear to be down
Port Scanning	
`-sT`	TCP connect scan – complete three-way handshake
`-sS`	TCP SYN scan – only first step of the three-way handshake
`-sU`	UDP scan
`-F`	Fast mode – scans the 100 most common ports
`-p [range]`	Specifies a range of port numbers – `-p-` scans all ports
Service Detection	
`-O`	OS detection
`-sV`	Service version detection
`-A`	OS detection, version detection, scripts, and traceroute
Timing	
`-T0` – `-T5`	Timing templates: paranoid (0), sneaky (1), polite (2), normal (3), aggressive (4), insane (5)
`--min-parallelism <num>`	Minimum number of parallel probes
`--max-parallelism <num>`	Maximum number of parallel probes
`--min-rate <num>`	Minimum rate (packets per second)
`--max-rate <num>`	Maximum rate (packets per second)
`--host-timeout <time>`	Maximum amount of time to wait for a target host

Option	Explanation
Real-Time Output	
`-v`	Verbosity level (e.g., `-vv` , `-v4`)
`-d`	Debugging level (e.g., `-d` , `-d9`)
Report Output	
`-oN <filename>`	Normal output
`-oX <filename>`	XML output
`-oG <filename>`	Grep-able output
`-oA <basename>`	Output in all major formats