Dispense Universitarie: Fondamenti di Network, Modello ISO/OSI e Packet Tracer

Queste dispense sono state elaborate basandosi sul materiale didattico del corso "Cyber Security & Ethical Hacking - Fondamenti di Network". Il contenuto è strutturato per fornire una comprensione approfondita, accademica e orientata alla pratica professionale.

---

1. Introduzione e Obiettivi del Modulo

1. 📖 Spiegazione Approfondita

Il modulo introduce i pilastri fondamentali delle reti di calcolatori, essenziali per qualsiasi professionista di Cybersecurity. L'obiettivo primario non è solo la memorizzazione teorica, ma l'acquisizione di una *forma mentis* architetturale. Vengono presentati due strumenti cardine:

1. **Il Modello ISO/OSI:** Un framework concettuale sviluppato dall'ISO (International Organization for Standardization) per standardizzare le comunicazioni tra diversi sistemi informatici. Permette l'interoperabilità tra vendor diversi e facilita la risoluzione dei problemi (troubleshooting) scomponendo la complessità della rete in livelli gestibili.
2. **Cisco Packet Tracer:** Un software di simulazione di rete che permette di progettare, configurare e gestire reti virtuali, colmando il divario tra teoria e pratica.

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave:** Il modello ISO/OSI è uno standard di riferimento a 7 livelli per la progettazione e la comprensione delle architetture di rete logiche e fisiche.
- **Contesto Reale:** In un SOC (Security Operations Center), quando si analizza un incidente, si parla spesso di "attacco a Livello 7" (es. SQL Injection) o "problema a Livello 2" (es. ARP Spoofing). Capire i livelli è vitale per la diagnosi.

---

2. Il Modello ISO/OSI: Architettura a 7 Livelli

1. 📖 Spiegazione Approfondita

Il modello divide la comunicazione di rete in sette strati (layers) distinti. Ogni strato serve il livello superiore e viene servito da quello inferiore. I livelli sono raggruppati in **Media Layers** (i più bassi, legati all'hardware e alla trasmissione) e **Host Layers** (i più alti, legati al software).

Dall'alto verso il basso (Top-Down):

1. **Livello 7 - Applicazione (Application):** È l'interfaccia diretta con l'utente e il software. Fornisce servizi di rete alle applicazioni (es. browser, client mail). Protocolli: HTTP, SMTP, FTP. PDU (Protocol Data Unit): *Data*.
2. **Livello 6 - Presentazione (Presentation):** Si occupa della traduzione, compressione e cifratura dei dati. Assicura che i dati inviati dall'applicazione siano leggibili dal sistema ricevente (es. codifica ASCII,

JPEG, crittografia SSL/TLS). PDU: *Data*.
3. **Livello 5 - Sessione (Session):** Gestisce l'instaurazione, il mantenimento e la chiusura delle sessioni di comunicazione tra host. Sincronizza il dialogo. PDU: *Data*.
4. **Livello 4 - Trasporto (Transport):** Gestisce la segmentazione dei dati e il riassemblaggio. Garantisce l'affidabilità (TCP) o la velocità (UDP) della comunicazione end-to-end. PDU: *Segment*.
5. **Livello 3 - Rete (Network):** Determina il percorso migliore (routing) e gestisce l'indirizzamento logico (Indirizzi IP). Qui operano i Router. PDU: *Packet* (Pacchetto).
6. **Livello 2 - Data Link (Collegamento Dati):** Gestisce l'indirizzamento fisico (MAC Address), l'accesso al mezzo e il rilevamento errori. È diviso in LLC (Logical Link Control) e MAC (Media Access Control). Qui operano gli Switch. PDU: *Frame*.
7. **Livello 1 - Fisico (Physical):** Trasmissione binaria pura (bit) su mezzi fisici (cavi rame, fibra ottica, onde radio). Definisce voltaggi, frequenze e connettori. PDU: *Bit*.

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave (PDU):** Ogni livello ha la sua unità dati: **Data** (L7-L5) -> **Segment** (L4) -> **Packet** (L3) -> **Frame** (L2) -> **Bit** (L1).
- **Mnemonica:** "All People Seem To Need Data Processing" (Application, Presentation, Session, Transport, Network, Data Link, Physical).

5. ⚠ Focus Esame

- **Domanda:** Qual è la differenza tra Livello 3 e Livello 2?
  - *Risposta:* Il Livello 3 usa indirizzi Logici (IP) per il routing tra reti diverse; il Livello 2 usa indirizzi Fisici (MAC) per la consegna all'interno della stessa rete locale (LAN).

---

3. Il Concetto di Incapsulamento

1. 📖 Spiegazione Approfondita

L'incapsulamento è il processo mediante il quale i dati, scendendo lungo lo stack ISO/OSI dal mittente, vengono avvolti da intestazioni (header) aggiuntive specifiche di ogni livello.

1. L'applicazione genera i Dati.
2. Il livello Trasporto aggiunge l'header TCP/UDP (porte).
3. Il livello Rete aggiunge l'header IP (indirizzi IP sorgente/destinazione).
4. Il livello Data Link aggiunge l'header MAC e il trailer (FCS) per formare il Frame.
5. Il frame viene convertito in segnali fisici (bit).

Il ricevente esegue il processo inverso, detto **decapsulamento**, rimuovendo gli header strato per strato fino a ottenere i dati originali.

4. 🔗 Cross-Connection Master (Pentesting)

Comprendere l'incapsulamento è fondamentale per l'analisi dei pacchetti con **Wireshark**. Quando analizzi un pacchetto catturato, vedi visivamente questa struttura a "matrioska".

---

4. Livello 1: Fisico e Sistema Binario

1. 📖 Spiegazione Approfondita

Il livello fisico non comprende il significato dei dati, ma si occupa solo di trasmettere segnali. L'unità minima di informazione è il **Bit** (Binary Digit), che può assumere valore `0` o `1`. I computer non utilizzano il sistema decimale, ma quello binario.

- **Bit:** Unità elementare.
- **Byte:** Sequenza di 8 bit.

3. 🧠 Analisi Tecnica & Memorizzazione

I mezzi trasmissivi determinano come i bit viaggiano: impulsi elettrici (rame), impulsi di luce (fibra), onde elettromagnetiche (wireless).

---

5. Livello 2: Data Link, MAC Address e Switching

1. 📖 Spiegazione Approfondita

Questo livello organizza i bit in **Frame**. Elemento cruciale è l'indirizzamento fisico tramite il **MAC Address** (Media Access Control).

- **MAC Address:** È un identificativo univoco assegnato dal produttore alla scheda di rete (NIC).
    - **Lunghezza:** 48 bit (6 byte).
    - **Formato:** 12 cifre esadecimali (0-9, A-F), solitamente scritte a coppie (es. `00:AA:11:BB:22:CC`).
    - **Struttura:** I primi 3 byte identificano il produttore (OUI), gli ultimi 3 sono univoci per la scheda.
- **Dispositivo Hardware: Lo Switch** Lo Switch opera a Livello 2. A differenza degli hub (obsoleti), lo switch apprende quale MAC address è collegato a quale porta fisica e inoltra i dati solo al destinatario corretto (**Unicast**), riducendo le collisioni. Tuttavia, lo switch ha un comportamento particolare con il **Broadcast**: se riceve un pacchetto destinato a `FF:FF:FF:FF:FF:FF` (indirizzo broadcast), lo inoltra a *tutte* le porte connesse (tranne quella da cui è arrivato). L'insieme delle macchine che ricevono questo messaggio forma un **Dominio di Broadcast**.

2. 🛠 Sintassi & Comandi (Cleaning)

Per visualizzare il proprio MAC Address e la configurazione di rete:

- **Windows:**

  > `ipconfig /all` *Mostra IP, Subnet Mask, Gateway e Indirizzo Fisico (MAC).*

- **Linux / macOS:**

  > `ifconfig` (o il più moderno `ip link show`) *Mostra le interfacce e l'indirizzo HWaddr o ether.*

5. ⚠ Focus Esame

- **Trabocchetto:** Cos'è `FF:FF:FF:FF:FF:FF`?
    - È l'indirizzo MAC di Broadcast. Indica "tutti i dispositivi nel segmento di rete".

- **Domanda:** Cosa succede se uno switch non conosce il MAC di destinazione?
    - Effettua il "flooding", ovvero invia il frame a tutte le porte (comportandosi momentaneamente come un hub) finché il destinatario non risponde.

---

6. Il Protocollo ARP (Address Resolution Protocol)

1. 📖 Spiegazione Approfondita

L'ARP è il protocollo "ponte" tra il Livello 3 (IP) e il Livello 2 (MAC). Quando un computer (es. PC A) vuole comunicare con un altro (es. PC B) nella stessa rete locale, conosce l'indirizzo IP di B (logico), ma per costruire il frame Ethernet ha bisogno dell'indirizzo MAC di B (fisico).

Processo ARP:

1. **ARP Request:** PC A invia un messaggio in **Broadcast** (`FF:FF:FF:FF:FF:FF`): *"Chi ha l'indirizzo IP 192.168.1.5?"*
2. Tutti ricevono la richiesta, ma solo PC B (che possiede quell'IP) risponde.
3. **ARP Reply:** PC B risponde in **Unicast** a PC A: *"Sono io, e il mio MAC address è AA:BB:CC:..."*.
4. **ARP Cache:** PC A memorizza questa associazione (IP <-> MAC) in una tabella temporanea (Cache ARP) per evitare di dover chiedere nuovamente ad ogni pacchetto.

2. 🛠 Sintassi & Comandi

Per visualizzare la tabella ARP sul proprio computer:

> `arp -a` *Mostra la lista delle associazioni IP-MAC attualmente memorizzate nella cache.*

4. 🔗 Cross-Connection Master (Cybersecurity)

Questo meccanismo è vulnerabile all'**ARP Poisoning** (o ARP Spoofing). Un attaccante può inviare falsi ARP Reply dicendo "L'IP del Gateway corrisponde al MIO MAC address". In questo modo, tutto il traffico della vittima passa attraverso l'attaccante (Man-In-The-Middle).

---

7. Cisco Packet Tracer: Guida Pratica

1. 📖 Spiegazione Approfondita

Packet Tracer è l'ambiente di simulazione per reti Cisco.

- **Area di Lavoro:**
    - **Pannello Principale:** Dove si disegna la topologia logica.
    - **Pannello Secondario (in basso):** Selezione dispositivi (Router, Switch, Hub, Wireless, End Devices, Connections).
- **Categorie Dispositivi:**
    - **Network Devices:** Router (Livello 3), Switch (Livello 2).
    - **End Devices:** PC, Laptop, Server.
- **Cablaggio (Connections):**
    - Simbolo "Fulmine": Connessione automatica (sceglie il cavo giusto).

- Linea Nera Continua (**Copper Straight-through**): Per collegare dispositivi di tipo diverso (es. Switch <-> Router, PC <-> Switch).
- Linea Tratteggiata (**Copper Cross-over**): Per collegare dispositivi dello stesso tipo (es. Switch <-> Switch, PC <-> PC).

2. 🛠 Sintassi & Configurazione (Lab)

Configurazione End Device (PC/Laptop)

1. Cliccare sull'icona del PC -> Tab **Desktop** -> **IP Configuration**.
2. Impostare:
   - **IPv4 Address:** Indirizzo logico (es. `192.168.10.100`).
   - **Subnet Mask:** Maschera di sottorete (es. `255.255.255.0`).
   - **Default Gateway:** L'IP del router che permette di uscire dalla rete (es. `192.168.10.1`).
3. Verifica connettività:
   - Tab **Desktop** -> **Command Prompt**.
   - Comando: `ping [IP_Destinatario]` (invia pacchetti ICMP echo request).

Configurazione Router (Network Device)

1. Cliccare sul Router -> Tab **Config**.
2. Selezionare l'interfaccia corretta (es. **GigabitEthernet0/0/0**).
3. Impostare:
   - **IPv4 Address:** L'IP del Gateway per quella rete (es. `192.168.10.1`).
   - **Subnet Mask:** (es. `255.255.255.0`).
4. **CRUCIALE:** Spuntare la casella **Port Status: On**. I router Cisco hanno le interfacce spente (shutdown) di default. Senza questo passaggio, il link rimane rosso (inattivo).

5. ⚠ Focus Esame

- **Errore Comune:** Dimenticare di impostare il **Default Gateway** sul PC.
  - *Conseguenza:* Il PC può comunicare nella LAN, ma non può raggiungere Internet o altre reti.
- **Errore Comune:** Router con link rossi.
  - *Causa:* Non è stato attivato il "Port Status: On" (comando CLI reale: `no shutdown`).