Dispense Universitarie Master: Fondamenti di Network e Modello ISO/OSI (Livelli 3-7)

Queste dispense sono state elaborate analizzando rigorosamente il materiale didattico del corso "Cyber Security & Ethical Hacking - Fondamenti di Network". Il contenuto è stato riorganizzato, corretto tecnicamente ed espanso per fornire una guida di studio di livello avanzato.

Introduzione al Networking e VLAN

1. 📖 Spiegazione Approfondita

Lo studio delle reti è il pilastro fondamentale della Cybersecurity. Senza comprendere come i dati viaggiano, vengono indirizzati e gestiti, è impossibile proteggere un'infrastruttura o condurre attività di Ethical Hacking.

Il primo concetto chiave trattato è la **VLAN (Virtual Local Area Network)**. Una VLAN è una tecnologia che permette di segmentare una rete fisica (livello 2) in più reti logiche distinte. Immaginate uno switch fisico con 24 porte: senza VLAN, tutti i dispositivi collegati appartengono allo stesso dominio di broadcast (sentono il traffico di tutti). Con le VLAN, possiamo dire allo switch che le porte 1-10 appartengono al reparto "Vendite" e le porte 11-20 al reparto "IT". Anche se fisicamente vicini, logicamente questi due gruppi sono isolati come se fossero su switch separati.

Benefici principali delle VLAN:

- **Sicurezza:** Separando il traffico sensibile (es. Management o Finance) da quello generico, si riduce la superficie di attacco e si prevengono accessi non autorizzati laterali.
- **Prestazioni:** Segmentare la rete riduce il **Dominio di Broadcast**. Meno broadcast significa meno "rumore" di fondo sulla rete, liberando banda per il traffico dati effettivo.
- **Gestione Semplificata:** Le policy di sicurezza e QoS (Quality of Service) possono essere applicate per intere subnet logiche anziché per porta fisica.
- **Flessibilità:** Un utente può spostarsi fisicamente in un altro ufficio; se la porta a cui si collega è assegnata alla sua VLAN, manterrà il suo indirizzo IP e i suoi permessi senza riconfigurare la rete.

Tipologie di Porte sugli Switch: Per far funzionare le VLAN, le porte degli switch vengono configurate in due modalità principali:

1. **Access Ports (Porte di Accesso):** Collegano i dispositivi finali (PC, Stampanti). Una porta in modalità *access* appartiene a una sola VLAN specifica. Il dispositivo finale non è "consapevole" della VLAN (non riceve traffico taggato).
2. **Trunk Ports (Porte di Trunk):** Collegano gli switch tra loro (o switch e router). Queste porte devono trasportare il traffico di *tutte* (o molteplici) VLAN. Per distinguere a quale VLAN appartiene un pacchetto, viene aggiunto un "tag" (etichetta) al frame Ethernet (protocollo 802.1Q).

Tipi di VLAN comuni:

- **VLAN di Default (VLAN 1):** La configurazione di fabbrica di Cisco. Tutte le porte partono qui. È una best practice di sicurezza *non* usarla per il traffico dati.
- **VLAN Dati/Accesso:** Create per gruppi di utenti (es. HR, Studenti).

- **VLAN di Management:** Dedicata esclusivamente all'accesso amministrativo agli apparati (SSH/Telnet verso switch/router).
- **VLAN Voice:** Dedicata al traffico VoIP per garantire priorità e bassa latenza.
- **VLAN Nativa:** Una VLAN su un trunk che non viene taggata (di solito coincide con la VLAN 1, ma può essere cambiata per sicurezza).

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave:** Una VLAN segmenta un dominio di broadcast fisico in molteplici domini di broadcast logici, isolando il traffico a livello 2.
- **Contesto Reale:** In azienda, le telecamere IP sono spesso su una VLAN separata dai PC degli impiegati. Se un attaccante compromette una telecamera, non ha accesso diretto (Layer 2) ai PC, ma deve passare per un firewall/router (Layer 3), dove può essere bloccato.

5. ⚠ Focus Esame

- **Domanda trabocchetto:** "Due PC su due VLAN diverse collegate allo stesso switch possono comunicare direttamente?"
  - **Risposta:** NO. Essendo domini di broadcast separati, è necessario un dispositivo di Livello 3 (Router o Switch L3) per fare *Inter-VLAN Routing*. Lo switch L2 da solo non basta.
- **Tagging:** Ricorda che i PC non vedono i tag VLAN. Il tag viene inserito dallo switch quando il frame entra in una porta trunk e rimosso quando esce verso una porta access.

Livello 3: Network (Rete)

1. 📖 Spiegazione Approfondita

Saliamo al livello 3 del modello ISO/OSI. Se il livello 2 (Data Link) si occupa di consegnare i frame all'interno della stessa rete locale usando i MAC Address, il **Livello Network** si occupa dell'**instradamento (routing)** dei pacchetti tra reti diverse attraverso internet o WAN.

Il protagonista è il **Router** (o Gateway). Il Router è un dispositivo intelligente che connette reti diverse. Ogni interfaccia del router appartiene a una rete differente e funge da "porta di uscita" (Default Gateway) per i dispositivi di quella rete.

Differenza cruciale tra Indirizzamento L2 e L3:

- **Indirizzo IP (Logico/Gerarchico):** Identifica la destinazione finale (End-to-End). L'IP sorgente e l'IP destinazione **NON CAMBIANO** durante il viaggio del pacchetto (a meno che non ci sia NAT, vedi dopo).
- **Indirizzo MAC (Fisico/Piatto):** Identifica il prossimo dispositivo fisico (Hop-to-Hop). Il MAC Address cambia a ogni salto.

Il processo di instradamento (Routing): Quando Alice (Rete A) vuole inviare un pacchetto a Carol (Rete B):

1. **Incapsulamento Iniziale:** Alice crea un pacchetto IP con Destinazione = IP di Carol.
2. **Delivery Locale:** Alice capisce che Carol non è nella sua rete locale (la subnet non corrisponde). Quindi deve inviare il pacchetto al suo **Gateway Predefinito** (il Router).
3. **Frame Creation:** Alice incapsula il pacchetto in un Frame Ethernet.

    - MAC Destinazione: MAC del Router (non di Carol!).
    - IP Destinazione: IP di Carol.
4. **Routing:** Il Router riceve il frame, controlla il MAC (è per lui), scarta l'intestazione L2 (frame) e legge l'intestazione L3 (IP). Consulta la sua **Routing Table** per decidere su quale interfaccia inoltrare il pacchetto verso Carol.
5. **Re-incapsulamento:** Il router crea un *nuovo* frame per l'interfaccia di uscita.
    - Nuovo MAC Sorgente: MAC dell'interfaccia di uscita del Router.
    - Nuovo MAC Destinazione: MAC di Carol (o del router successivo).
    - IP Sorgente/Destinazione: Rimangono invariati (Alice -> Carol).

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave:** Il Router è un dispositivo di Livello 3 che interconnette reti eterogenee e decide il percorso migliore per i pacchetti consultando la Routing Table.
- **Next Hop:** Il concetto di "prossimo salto". Il computer non sa dov'è Google fisicamente; sa solo che deve passare il pacchetto al router (Next Hop).

4. 🔗 Cross-Connection Master (Sistemi Linux)

In Linux, puoi visualizzare la routing table con il comando: `route -n` oppure `ip route show`. Vedrai una riga `0.0.0.0` (o `default`) che indica il Gateway verso cui viene spedito tutto il traffico che non ha una destinazione locale specifica.

5. ⚠ Focus Esame

- **Domanda:** "Cosa cambia e cosa rimane uguale in un pacchetto che attraversa un router?"
    - **Risposta:** Cambiano gli indirizzi MAC (intestazione Frame L2). Rimangono invariati gli indirizzi IP (intestazione Pacchetto L3).
- **Nota:** Il router *non* cambia gli IP (a meno che non stia eseguendo NAT).

Livello 4: Trasporto (TCP vs UDP)

1. 📖 Spiegazione Approfondita

Il Livello 4 gestisce la comunicazione logica **End-to-End** tra le applicazioni. Non si preoccupa di *come* arrivare a destinazione (compito del router), ma di *come gestire i dati* una volta arrivati o partiti. Introduce i concetti di **Segmentazione** (dividere dati grandi in pezzi piccoli) e **Multiplexing** (gestire più app contemporaneamente tramite le Porte).

I due protocolli dominanti sono:

TCP (Transmission Control Protocol)

È il protocollo "affidabile" e "orientato alla connessione" (Connection-oriented).

- **Affidabilità:** Garantisce che i dati arrivino, siano integri, in ordine e senza duplicati.
- **Controllo di Flusso:** Se il ricevente è lento, il mittente rallenta (Windowing).
- **Handshake a 3 vie (Three-Way Handshake):** Prima di inviare dati, stabilisce un circuito logico.

1. **SYN:** Il Client invia un segmento con flag SYN (voglio sincronizzarmi) e un numero di sequenza casuale (es. Seq=X).
2. **SYN-ACK:** Il Server riceve, risponde con SYN (voglio sincronizzarmi anch'io) e ACK (ho ricevuto il tuo X, il prossimo che aspetto è X+1).
3. **ACK:** Il Client conferma la ricezione del SYN del server. La connessione è stabilita.

- **Usi:** Web (HTTP/HTTPS), Email (SMTP/IMAP), File Transfer (FTP). Dove la precisione è più importante della velocità.

UDP (User Datagram Protocol)

È il protocollo "Best Effort" e "senza connessione" (Connectionless).

- **Inaffidabilità:** Spedisce i pacchetti ("Datagrammi") e non aspetta conferme. Se un pacchetto si perde, è perso per sempre.
- **Basso Overhead:** Header molto piccolo (8 byte) contro quello del TCP (20 byte min). Velocissimo.
- **Usi:** Streaming Video/Audio, VoIP, Gaming Online, DNS. Dove la velocità è critica e perdere qualche frame non blocca il servizio.

3. 🧠 Analisi Tecnica & Memorizzazione

- **Matematica del TCP:** Se invio un pacchetto con `Seq = 100` e lunghezza dati 10 byte, mi aspetto un `Ack = 111` (100 + 10 + 1 virtuale per il flag). Nelle slide l'esempio è semplificato: `Ack = Seq ricevuto + 1` (durante l'handshake senza dati).
- **Contesto Reale (Attacco DoS):** L'attacco **SYN Flood** sfrutta il Three-Way Handshake. L'attaccante manda milioni di pacchetti SYN ma non completa mai con l'ultimo ACK. Il server tiene le connessioni "mezze aperte" occupando tutta la memoria RAM e crasha.

5. ⚠ Focus Esame

- **Distinzione:**
  - TCP = Affidabile, Lento, Connesso (Telefono: "Pronto? Mi senti? Sì ti sento").
  - UDP = Inaffidabile, Veloce, Sconnesso (Posta prioritaria: Imbuco la lettera e spero arrivi).

Livelli Superiori (5, 6, 7)

1. 📖 Spiegazione Approfondita

Spesso raggruppati nel modello TCP/IP come un unico livello "Applicazione", nel modello ISO/OSI sono distinti:

- **Livello 5: Sessione:**
  - Gestisce il dialogo (Sessione) tra due macchine.
  - Funziona come un "vigile urbano" della conversazione: apre, gestisce e chiude le sessioni.
  - Inserisce **Checkpoint**: se sto scaricando un file di 1GB e cade la linea al 90%, grazie al livello sessione posso riprendere dal 90% senza ricominciare da zero.
- **Livello 6: Presentazione:**

    - È il "traduttore". Si assicura che i dati siano leggibili dal ricevente.
    - **Codifica/Conversione:** ASCII, EBCDIC, conversione immagini (JPG, PNG).
    - **Crittografia:** Qui avviene la cifratura/decifratura (es. TLS/SSL risiedono tecnicamente qui/innescano qui).
    - **Compressione:** Zippare i dati per spedirli più velocemente.

- **Livello 7: Applicazione:**

    - NON è il software (es. non è Chrome o Outlook), ma i **protocolli** che il software usa per comunicare in rete.
    - Fornisce l'interfaccia utente-rete.
    - Protocolli comuni:
        - **DNS (Domain Name System):** La rubrica telefonica di Internet. Converte nomi umani (`www.google.com`) in IP (`142.250.x.x`). Usa la porta 53 (UDP/TCP).
        - **DHCP (Dynamic Host Configuration Protocol):** Assegna automaticamente IP, Subnet Mask, Gateway e DNS ai dispositivi appena collegati alla rete.

Porte di Rete e Socket

1. 📖 Spiegazione Approfondita

Mentre l'indirizzo IP identifica il *computer* (Host), la **Porta** identifica il *servizio* o l'applicazione specifica all'interno di quel computer. Una porta è un numero a 16 bit ($2^{16} = 65.536$ porte disponibili).

Il concetto di **Socket** è la combinazione di `Indirizzo IP : Numero Porta` (es. `192.168.1.10:80`). Questo definisce univocamente un processo in tutta Internet.

Categorie di Porte (IANA):

1. **Well-Known Ports (0 - 1023):** Riservate ai servizi di sistema e protocolli fondamentali.
    - **20/21:** FTP (File Transfer)
    - **22:** SSH (Secure Shell - Accesso remoto sicuro)
    - **23:** Telnet (Accesso remoto insicuro/in chiaro)
    - **25:** SMTP (Invio Email)
    - **53:** DNS (Risoluzione Nomi)
    - **80:** HTTP (Web non sicuro)
    - **443:** HTTPS (Web sicuro)
2. **Registered Ports (1024 - 49151):** Assegnate a software specifici (es. database come MySQL, giochi, ecc.).
3. **Dynamic/Private Ports (49152 - 65535):** Usate dai Client come porte "effimere" per iniziare una connessione verso un server.

2. 🛠 Sintassi & Comandi (Cleaning)

Per vedere quali porte sono aperte sul proprio computer (Listening) o connesse (Established):

- **Windows:**

```
netstat -ano
```

    - `-a`: Mostra tutte le connessioni e porte in ascolto.
    - `-n`: Mostra indirizzi e porte in formato numerico (non risolve i nomi, più veloce).
    - `-o`: Mostra il PID (Process ID) che sta usando quella porta.

- **Linux:**

```
netstat -tunp
```

    - (Oppure il più moderno `ss -tunp`)
    - `-t`: TCP
    - `-u`: UDP
    - `-n`: Numerico
    - `-p`: Mostra il nome del programma/PID.

- **MacOS:**

```
netstat -p tcp -p udp
```

    - Oppure `lsof -i -P | grep LISTEN` per un output più chiaro.

4. 🔗 Cross-Connection Master (Pentesting)

Durante una fase di **Scanning** (es. con Nmap), l'hacker cerca le "Well-Known Ports" aperte.

- Porta 22 aperta -> Tenterà un Brute Force SSH.
- Porta 80 aperta -> Cercherà vulnerabilità Web/SQL Injection. Sapere quali porte corrispondono a quali servizi è vitale per il *Reconnaissance*.

NAT (Network Address Translation) e PAT

1. 📖 Spiegazione Approfondita

Il mondo ha finito gli indirizzi IPv4 pubblici molto tempo fa. La soluzione tampone che ha "salvato" Internet è il NAT. Il NAT permette a una rete privata (con indirizzi privati non instradabili su Internet) di presentarsi al mondo esterno con un unico (o pochi) indirizzi IP Pubblici.

Classi di Indirizzi Privati (RFC 1918): Questi IP non possono viaggiare su Internet pubblico.

- **Classe A:** `10.0.0.0` - `10.255.255.255` (Grandi aziende)
- **Classe B:** `172.16.0.0` - `172.31.255.255` (Docker, Medie aziende)
- **Classe C:** `192.168.0.0` - `192.168.255.255` (Reti domestiche, SOHO)

Tipologie di NAT:

1. **Static NAT (1:1):** Un IP Privato viene mappato staticamente su un IP Pubblico specifico. Usato per Server Web interni che devono essere raggiungibili da fuori sempre allo stesso IP.
2. **Dynamic NAT:** Un pool di IP pubblici viene assegnato dinamicamente agli IP privati che ne fanno richiesta (chi prima arriva, meglio alloggia).
3. **PAT (Port Address Translation) o NAT Overload:** È quello che usiamo a casa.
    - **Problema:** Abbiamo 1 solo IP pubblico ma 10 dispositivi (PC, telefoni, TV).

    - **Soluzione:** Il router usa l'IP pubblico per tutti, ma distingue le connessioni modificando la **Porta Sorgente**.
    - Esempio:
        - PC A invia richiesta: `192.168.1.10:12345` -> Router traduce in -> `203.0.113.5:40001`.
        - PC B invia richiesta: `192.168.1.11:12345` -> Router traduce in -> `203.0.113.5:40002`.
    - Quando Google risponde alla porta 40001, il router consulta la sua **NAT Table**, capisce che corrisponde al PC A e inoltra il pacchetto ritraducendolo.

Vantaggi: Risparmio IP pubblici, Sicurezza (nasconde la topologia interna). **Svantaggi:** Rompe il principio "end-to-end", introduce latenza, complica protocolli come VoIP o P2P.

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave PAT:** Tecnica che permette a molti host privati di condividere un solo IP pubblico utilizzando numeri di porta univoci per distinguere le sessioni.
- **Tabella NAT:** Il cuore del router NAT. Mantiene la mappatura "Chi era interno <-> Chi è diventato esterno".

5. ⚠ Focus Esame

- **Domanda:** "Qual è la differenza tra NAT statico e PAT?"
    - **Risposta:** Il NAT statico è una traduzione 1 a 1 di indirizzi IP. Il PAT è una traduzione "Molti a 1" che utilizza le porte TCP/UDP per multiplexare le connessioni.