📘 Dispense Universitarie: Fondamenti di Networking e Indirizzamento IP

Modulo: Cyber Security & Ethical Hacking - Network Basics

Introduzione alle Reti e Rilevanza per l'Ethical Hacking

1. 📖 Spiegazione Approfondita

Lo studio delle reti di calcolatori non è un'opzione accessoria per un professionista della sicurezza offensiva, ma un prerequisito assoluto. Come suggerito dall'analogia proposta, tentare di effettuare un *penetration test* senza conoscere il networking è paragonabile a voler scrivere un romanzo senza conoscere l'alfabeto.

Una **Rete di Computer** è un'infrastruttura che abilita la comunicazione tra persone, applicazioni e server, superando i limiti geografici. Internet rappresenta l'esempio più vasto di questa interconnessione. Affinché hardware e software eterogenei possano comunicare, è necessario l'utilizzo di **protocolli di comunicazione** standardizzati. Questi protocolli regolano lo scambio di informazioni che viaggiano sotto forma di **pacchetti** (flussi di bit trasmessi tramite segnali elettrici su cavi LAN o onde radio Wi-Fi).

Per un Ethical Hacker, comprendere la rete significa:

1. **Identificare Vulnerabilità:** Saper leggere il traffico permette di trovare falle nel trasporto o nella configurazione.
2. **Sfruttare Vulnerabilità (Exploitation):** Manipolare i protocolli a proprio vantaggio.
3. **Protezione (Blue Teaming):** Implementare misure di mitigazione efficaci.

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave:** Una rete è un insieme di dispositivi interconnessi che condividono risorse e dati attraverso un mezzo trasmissivo comune e regole condivise (protocolli).
- **Contesto Reale:** Durante un attacco *Man-in-the-Middle* (MITM), l'hacker deve comprendere come i pacchetti fluiscono tra client e router per poterli intercettare e modificare.

5. ⚠ Focus Esame

- **Domanda:** Perché un protocollo è necessario?
- **Risposta:** Per garantire l'interoperabilità tra dispositivi con hardware e sistemi operativi differenti.

Struttura del Pacchetto IP e Header

1. 📖 Spiegazione Approfondita

L'unità fondamentale della comunicazione in rete è il **pacchetto**. Esso è strutturato in due macro-sezioni, analogamente a una busta da lettere:

1. **Header (Intestazione):** Contiene i metadati necessari per il trasporto e la consegna. La sua struttura dipende dal protocollo (es. Protocollo IP). Include informazioni critiche come:
    - **Source Address:** Indirizzo IP del mittente.
    - **Destination Address:** Indirizzo IP del destinatario.
    - **TTL (Time To Live):** Durata di vita del pacchetto per evitare loop infiniti.
    - **Protocol:** Indica quale protocollo di livello superiore è incapsulato (es. TCP, UDP).
    - **Version:** Es. IPv4 o IPv6.
2. **Payload (Carico utile):** È l'informazione vera e propria che si vuole trasmettere (es. il testo di una email, una parte di un'immagine, un comando).

Il compito dell'Header è assicurare che il dispositivo ricevente possa interpretare correttamente il Payload e gestire la connessione.

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave:** L'**Header IP** contiene gli indirizzi logici (Sorgente e Destinazione) che permettono ai router di instradare il pacchetto attraverso la rete fino alla destinazione corretta.

4. 🔗 Cross-Connection Master

- **Integrazione Pentesting:** Strumenti come **Wireshark** permettono di catturare i pacchetti ("sniffing") e visualizzare in chiaro i campi dell'header. Un hacker analizza questi campi per capire la topologia della rete o per attacchi di *IP Spoofing* (falsificazione dell'indirizzo sorgente).

Sistema Binario e Conversioni

1. 📖 Spiegazione Approfondita

I calcolatori elaborano le informazioni esclusivamente in formato binario (base 2, cifre 0 e 1), mentre gli esseri umani utilizzano il sistema decimale (base 10, cifre 0-9). La comprensione della conversione tra questi due sistemi è vitale per calcolare indirizzi IP e Subnet Mask.

Conversione Binario $\to$ Decimale

Ogni posizione in un numero binario rappresenta una potenza di 2, partendo da destra (2^0) verso sinistra. Esempio: 1011_2

- $1 \times 2^3 = 8$
- $0 \times 2^2 = 0$
- $1 \times 2^1 = 2$
- $1 \times 2^0 = 1$
- Totale: $8 + 0 + 2 + 1 = 11_{10}$

Conversione Decimale $\to$ Binario

Si utilizza il metodo delle divisioni successive per 2. Si divide il numero n > 0 per 2 e si annota il resto. Si continua a dividere il quoziente finché non diventa 0. La sequenza dei resti, letta dall'ultimo al primo, fornisce il numero binario. Esempio: 123_{10}

1. $123 / 2 = 61$ (Resto 1)
2. $61 / 2 = 30$ (Resto 1)
3. $30 / 2 = 15$ (Resto 0)
4. $15 / 2 = 7$ (Resto 1)
5. $7 / 2 = 3$ (Resto 1)
6. $3 / 2 = 1$ (Resto 1)
7. $1 / 2 = 0$ (Resto 1) Risultato (leggendo dal basso): 1111011_2

3. 🧠 Analisi Tecnica & Memorizzazione

- **Tabella Potenze del 2 (da memorizzare per il subnetting):**
  - $2^7 = 128$
  - $2^6 = 64$
  - $2^5 = 32$
  - $2^4 = 16$
  - $2^3 = 8$
  - $2^2 = 4$
  - $2^1 = 2$
  - $2^0 = 1$

Classificazione delle Reti: Geografica e Topologica

1. 📖 Spiegazione Approfondita

Le reti vengono classificate secondo due criteri principali: l'estensione geografica e la topologia fisica (collegamenti).

A. Classificazione Geografica (Distanza)

1. **PAN (Personal Area Network):** Raggio d'azione di pochi metri, attorno a una persona.
   - *Esempio:* Smartphone collegato via Bluetooth a cuffie o smartwatch.
2. **LAN (Local Area Network):** Rete locale confinata in un singolo edificio o ufficio. Alta velocità.
   - *Esempio:* Rete di una scuola o di un ufficio aziendale.
3. **WLAN (Wireless LAN):** Estensione della LAN che utilizza onde radio (Wi-Fi) invece di cavi.
4. **MAN (Metropolitan Area Network):** Copre un'area urbana o metropolitana.
   - *Esempio:* Interconnessione tra diverse filiali di una banca nella stessa città o rete in fibra ottica cittadina.
5. **WAN (Wide Area Network):** Copre grandi distanze geografiche (nazioni, continenti).
   - *Esempio:* Internet è la WAN per eccellenza.

B. Classificazione Topologica (Layout Fisico)

1. **Topologia a Bus:** Tutti i dispositivi condividono un unico cavo dorsale (*backbone*).
   - *Pro:* Economica e semplice per reti piccole.
   - *Contro:* Se il cavo principale si rompe, l'intera rete cade. Alta collisione di dati.
2. **Topologia ad Anello (Token Ring):** Ogni nodo è collegato al successivo formando un cerchio chiuso. I dati viaggiano in una direzione.

    - *Uso:* Ambienti enterprise legacy o reti in fibra specifiche (FDDI).
3. **Topologia a Stella (Star):** Tutti i nodi sono collegati singolarmente a un dispositivo centrale (**Switch** o **Hub**).
    - *Pro:* Se un cavo si rompe, solo quel PC viene isolato; il resto della rete funziona.
    - *Sicurezza:* È la più sicura e performante. Lo switch gestisce il traffico in modo intelligente.

5. ⚠ Focus Esame

- **Domanda:** Qual è la differenza principale tra Bus e Stella in termini di *Fault Tolerance* (tolleranza ai guasti)?
- **Risposta:** Nel Bus, un guasto al cavo principale blocca tutto. Nella Stella, un guasto a un cavo periferico isola solo un host.

Protocollo IP e Indirizzamento IPv4

1. 📖 Spiegazione Approfondita

Il **Protocollo IP (Internet Protocol)** gestisce l'indirizzamento e l'instradamento dei pacchetti. Attualmente coesistono due versioni:

IPv4 (Versione 4)

È lo standard dominante. Un indirizzo IPv4 è un identificativo univoco a **32 bit**, diviso in **4 ottetti** (gruppi da 8 bit) separati da punti (Notazione *Dotted-Decimal*).

- Ogni ottetto varia da 0 a 255 (2^8 combinazioni).
- *Esempio:* `192.168.1.254`.
- Struttura binaria: 4 Byte totali (32 bit).

IPv6 (Versione 6)

Introdotto per l'esaurimento degli indirizzi IPv4.

- Lunghezza: **128 bit**.
- Notazione: Esadecimale, separata da due punti.
- *Esempio:* `2001:0db8:85a3:0000:0000:8a2e:0370:7334`.

Classi di Indirizzi (Classful vs Classless)

Storicamente (Classful), gli IP erano divisi rigidamente:

- **Classe A:** 0-127 (Grandi reti).
- **Classe B:** 128-191 (Medie reti).
- **Classe C:** 192-223 (Piccole reti/LAN).
- **Classe D:** 224-239 (Multicast).
- **Classe E:** 240-255 (Sperimentale).

Oggi si utilizza il **CIDR (Classless Inter-Domain Routing)**, che permette una gestione flessibile tramite la **Subnet Mask variabile**.

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave:** Un indirizzo IP è la "targa" logica di un dispositivo. Non va confuso con il MAC Address (targa fisica).

Subnet Mask e Subnetting

1. 📖 Spiegazione Approfondita

La **Subnet Mask** è un filtro a 32 bit che indica al computer quale parte dell'indirizzo IP identifica la **Rete (Network ID)** e quale identifica l'**Host (dispositivo specifico)**.

- I bit impostati a **1** rappresentano la Rete.
- I bit impostati a **0** rappresentano l'Host.

Esempio: IP: `192.168.1.1` Mask: `255.255.255.0` (o /24 in CIDR) Significa che `192.168.1` è la rete fissa, e l'ultimo ottetto (`.1`) è disponibile per gli host.

Il Subnetting

È la pratica di suddividere una rete IP principale in sottoreti (subnet) più piccole. **Vantaggi:**

1. **Ottimizzazione:** Riduce lo spreco di indirizzi IP.
2. **Sicurezza:** Isola segmenti di rete (es. Reparto HR separato da Reparto IT).
3. **Performance:** Riduce il traffico di broadcast (domini di broadcast più piccoli).

Metodo di Calcolo (Il "Numero Magico")

Per calcolare i range di una sottorete dato un CIDR (es. /22):

1. **Identificare l'ottetto interessante:** Dove cade l'ultimo bit a 1 della maschera?
   - /22 = `11111111.11111111.11111100.00000000`
   - Terzo ottetto.
2. **Calcolare il valore decimale della maschera nell'ottetto:**
   - `11111100` binario = `252` decimale.
3. **Applicare la regola:** $256 - \text{Valore Maschera} = \text{Blocco (Numero Magico)}$.
   - $256 - 252 = 4$.
4. Le sottoreti avanzeranno di 4 in 4 nel terzo ottetto (0, 4, 8, 12...).

2. 🛠 Definizioni Operative (Calcolo Subnet)

Per ogni subnet calcolata esistono 3 indirizzi speciali:

- **Network IP (Indirizzo di Rete):** Il primo indirizzo (tutti i bit host a 0). Identifica la rete stessa. *Non assegnabile a un PC.*
- **Gateway IP:** Solitamente il primo indirizzo utile (es. Network + 1). È l'indirizzo del router per uscire dalla rete.
- **Broadcast IP:** L'ultimo indirizzo del range (tutti i bit host a 1). Usato per parlare con *tutti* nella subnet. *Non assegnabile a un PC.*

- **Host Range:** Tutti gli indirizzi compresi tra Network+1 e Broadcast-1.

5. ⚠ Focus Esame

Esercizio Tipo: Dato `172.16.0.0/22`:

- **Magic Number:** 4 (nel 3° ottetto).
- **Subnet 1:** 172.16.0.0
- **Next Subnet:** 172.16.4.0
- **Broadcast Subnet 1:** È l'indirizzo appena prima della Next Subnet -> 172.16.3.255.
- **Range Host Subnet 1:** 172.16.0.1 (Gateway) fino a 172.16.3.254.

Esercizi Svolti e Soluzioni

Classificazione IP (Esercizio 1)

Identificare la classe basandosi sul primo ottetto (Regole Classful):

- `192.168.1.1` -> Inizia con 192 -> **Classe C** (Range 192-223).
- `150.10.1.1` -> Inizia con 150 -> **Classe B** (Range 128-191).
- `10.1.1.1` -> Inizia con 10 -> **Classe A** (Range 0-127).
- `223.1.1.1` -> Inizia con 223 -> **Classe C**.
- `172.16.1.1` -> Inizia con 172 -> **Classe B**.

Calcolo Host Disponibili (Esercizio 2)

Formula: $2^h - 2$ (dove h è il numero di bit 0 nella maschera).

1. **Mask 255.255.255.192 (/26):**
   - 32 - 26 = 6 bit di host.
   - $2^6 - 2 = 64 - 2 = \textbf{62 host}$.
2. **Mask 255.255.252.0 (/22):**
   - 32 - 22 = 10 bit di host.
   - $2^{10} - 2 = 1024 - 2 = \textbf{1022 host}$.
3. **Mask 255.255.255.0 (/24):**
   - 32 - 24 = 8 bit di host.
   - $2^8 - 2 = 256 - 2 = \textbf{254 host}$.

Identificazione Rete (Esercizio 3)

Data una coppia IP/Mask, trovare l'ID di Rete (operazione AND logico).

1. **IP:** 192.168.10.45 **Mask:** /24 (255.255.255.0)
   - Rete: **192.168.10.0** (i primi 3 ottetti sono bloccati).
2. **IP:** 172.16.25.78 **Mask:** /16 (255.255.0.0)
   - Rete: **172.16.0.0** (i primi 2 ottetti sono bloccati, il resto va a 0).
3. **IP:** 10.0.1.33 **Mask:** /26 (255.255.255.192)
   - Block size = 256 - 192 = 64.
   - Range: 0-63. L'IP 33 cade nel primo blocco.

- Rete: **10.0.1.0**.

Strumenti di Laboratorio

Cisco Packet Tracer

Per mettere in pratica questi concetti (routing, switching, subnetting), si utilizza il simulatore **Cisco Packet Tracer**. È fondamentale scaricare la versione per il proprio sistema operativo (Windows/Linux) tramite il portale *Cisco NetAcad* o link alternativi forniti, previa registrazione.

4. 🔗 Cross-Connection Master

In fase di esame e lavoro, non si usa solo Packet Tracer. Si utilizzeranno strumenti reali come:

- `ping`: per testare la raggiungibilità.
- `ipconfig` (Windows) / `ifconfig` o `ip a` (Linux): per vedere il proprio IP e Mask.
- `netmask` o calcolatori IP online: per verificare velocemente il subnetting durante i pentest.