Tipi di hackers

White Hat Hackers

- Conosciuti come: Ethical hackers
- Operano: Con permesso, rispettando le leggi
- Obiettivi: Identificare e risolvere vulnerabilità, migliorare la sicurezza
- Attività: Penetration tests, valutazione della sicurezza, consulenze

Black Hat Hackers

- Conosciuti come: Cracker, hacker malintenzionati
- Operano: Senza permesso, violando leggi
- Obiettivi: Rubare dati, ottenere guadagni illeciti, diffondere malware
- Attività: Sfruttamento di vulnerabilità, creazione di malware, vendita di dati rubati

Grey Hat Hackers

- Posizione: Tra white hat e black hat
- Operano: A volte senza permesso, ma non con intenzioni maligne
- Obiettivi: Scoprire vulnerabilità, segnalare ai proprietari (a volte chiedendo ricompense)
- Attività: Scansione di sistemi senza autorizzazione, segnalazione di vulnerabilità, operazione in area legale ed etica grigia

Modello ISO/OSI

Questi livelli lavorano insieme per consentire la comunicazione e il trasferimento di dati attraverso una rete.

1. **Livello Fisico (Physical Layer)**
   - **Funzione**: Trasmette bit grezzi attraverso un mezzo fisico (cavi, onde radio).
   - **Componenti**: Cavi, connettori, segnali elettrici/ottici.
2. **Livello di Collegamento Dati (Data Link Layer)**
   - **Funzione**: Gestisce la comunicazione tra dispositivi su una singola rete locale; rilevamento e correzione errori.
   - **Componenti**: Switch, schede di rete, frame.
3. **Livello di Rete (Network Layer)**
   - **Funzione**: Determina il percorso dei dati tra dispositivi su reti diverse; indirizzamento IP.
   - **Componenti**: Router, pacchetti.
4. **Livello di Trasporto (Transport Layer)**
   - **Funzione**: Garantisce la trasmissione affidabile dei dati end-to-end; controllo di flusso e segmentazione.
   - **Componenti**: TCP, UDP, segmenti.
5. **Livello di Sessione (Session Layer)**
   - **Funzione**: Gestisce le sessioni di comunicazione tra applicazioni; sincronizzazione e controllo dialogo.

    - **Componenti**: Apertura, gestione e chiusura sessioni.
6. **Livello di Presentazione (Presentation Layer)**
    - **Funzione**: Traduce i dati tra il formato di rete e il formato utilizzato dalle applicazioni; crittografia e compressione.
    - **Componenti**: Formati dati, codifica, decodifica.
7. **Livello Applicazione (Application Layer)**
    - **Funzione**: Fornisce servizi di rete direttamente alle applicazioni dell'utente.
    - **Componenti**: HTTP, FTP, SMTP, browser, applicazioni.

Modello TCP/IP

Questi livelli collaborano per consentire la trasmissione dei dati attraverso reti complesse, semplificando il processo di comunicazione end-to-end.

Livello di Accesso alla Rete (Network Interface Layer)

- **Funzione**: Gestisce la trasmissione dei dati tra il dispositivo e la rete; include i dettagli del livello fisico e del livello di collegamento dati del modello OSI.
- **Componenti**: Ethernet, Wi-Fi, frame, schede di rete.

Livello Internet (Internet Layer)

- **Funzione**: Gestisce l'instradamento dei pacchetti attraverso reti diverse; indirizzamento IP.
- **Componenti**: IP (IPv4, IPv6), ICMP, pacchetti.

Livello di Trasporto (Transport Layer)

- **Funzione**: Fornisce una comunicazione affidabile e ordinata tra dispositivi; gestione delle connessioni e controllo di flusso.
- **Componenti**: TCP, UDP, segmenti.

Livello Applicazione (Application Layer)

- **Funzione**: Fornisce servizi di rete direttamente alle applicazioni dell'utente; include funzionalità dei livelli di sessione, presentazione e applicazione del modello OSI.
- **Componenti**: HTTP, FTP, SMTP, DNS, applicazioni.

Differenze tra ISO/OSI e TCP/IP

Il modello ISO/OSI è un modello teorico esplicativo dei 7 livelli che consentono la comunicazione di rete e il relativo trasferimento dati tra dispositivi. Il modello TCP/IP è l'equivalente dell'ISO/OSI messo però in parte pratica. Raggruppa i livelli in 4 anziché 7 ed è il modello utilizzato per trasferire dati tra reti complesse come, per esempio, attraverso la rete più grande che conosciamo cioè INTERNET.

Confronto tra le macchine virtuali

Le macchine virtuali che abbiamo installato sull'applicativo Virtual Box sono Metasploitable, Kali Linux, Windows 7 e Ubuntu. Installarle è stato facile, l'utilizzo si differenzia per alcune impostazioni diverse nel codice e la familiarità avviene tramite l'utilizzo nel tempo (learning by doing).

Ping: cos'è e perchè si fa

Il comando **ping** è uno strumento fondamentale utilizzato per verificare la connettività di rete e diagnosticare problemi di rete. Il ping è utilizzato per:

- Verificare la raggiungibilità di un dispositivo.
- Diagnosticare problemi di rete.
- Misurare la latenza.
- Monitorare le prestazioni di rete.
- Verificare la configurazione dei dispositivi di rete.

Approfondimento InetSim

INetSim (Internet Services Simulation Suite) è uno strumento per simulare servizi di rete comuni (DNS, HTTP, FTP, e-mail) in un ambiente controllato. Viene utilizzato principalmente per:

1. **Analisi del Malware**: Studiare il comportamento del malware senza rischi per la rete reale.
2. **Test di Sicurezza**: Simulare attacchi e valutare misure di sicurezza.
3. **Ricerca e Sviluppo**: Sviluppare e testare nuovi strumenti di sicurezza.
4. **Formazione**: Educare su come funzionano i servizi di rete e il comportamento del malware.

Approfondimento Wireshark

Wireshark è uno strumento di analisi del traffico di rete utilizzato per catturare e visualizzare i dati che transitano attraverso una rete. Ecco una sintesi delle sue funzioni principali:

1. **Cattura del Traffico**: Wireshark cattura pacchetti di dati in tempo reale da una rete.
2. **Analisi del Traffico**: Permette di visualizzare e analizzare i dettagli dei pacchetti, incluse informazioni sui protocolli e contenuti dei dati.
3. **Diagnostica di Rete**: Aiuta a identificare problemi di rete, come ritardi, perdite di pacchetti o configurazioni errate.
4. **Sicurezza**: Consente di rilevare attività sospette o non autorizzate, come tentativi di intrusione o attacchi di rete.
5. **Formazione**: Strumento didattico per imparare come funzionano i protocolli di rete e il traffico dati.