Consegna S11-L3

Consegna: Utilizzo di Wireshark per Esaminare le Catture TCP e UDP

In questa pratica, l'obiettivo principale è comprendere il funzionamento della stretta di mano TCP a tre vie e approfondire l'analisi dei pacchetti utilizzando strumenti avanzati come Wireshark e tcpdump.

Struttura del Laboratorio

1. **Parte 1: Preparare gli host per catturare il traffico**
    - Configurare un ambiente adatto per catturare il traffico di rete generato durante una sessione TCP.
    - Effettuare tutte le verifiche necessarie per garantire che le configurazioni siano corrette.
2. **Parte 2: Analizzare i pacchetti utilizzando Wireshark**
    - Utilizzare Wireshark per catturare e analizzare una sessione TCP, evidenziando la sequenza di SYN, SYN-ACK e ACK.
    - Identificare eventuali anomalie o problemi nei pacchetti catturati.
3. **Parte 3: Visualizzare i pacchetti utilizzando tcpdump**
    - Utilizzare tcpdump per acquisire una sessione TCP e visualizzare i dettagli direttamente nel terminale.
    - Esportare i risultati in un file per ulteriori analisi.

Bonus: Laboratorio - Esaminare le Catture TCP e UDP

- Identificare i campi dell'intestazione TCP e analizzarne il funzionamento utilizzando una cattura di sessione FTP in Wireshark.
- Identificare i campi dell'intestazione UDP e analizzarne il funzionamento utilizzando una cattura di sessione TFTP in Wireshark.

Consegna

1. **Screenshot:**
   - Fornire screenshot dettagliati che mostrano:
     - La cattura della stretta di mano TCP a tre vie in Wireshark.
     - L'utilizzo di tcpdump per catturare e analizzare i pacchetti TCP.
     - L'analisi delle intestazioni TCP e UDP nei rispettivi bonus.
2. **Relazione:**
   - Scrivere una relazione tecnica che includa:
     - La spiegazione dei passaggi effettuati in ciascuna parte del laboratorio.
     - Un'analisi dei risultati ottenuti con Wireshark e tcpdump.
     - Eventuali problemi riscontrati durante la configurazione e le soluzioni adottate.
3. **File Pcap:**
   - Allegare i file Pcap generati durante l'analisi con Wireshark e tcpdump per una valutazione dettagliata.

🔑 Chiavi: [wireshark, tcpdump, tcp, udp, cybersecurity]