S11L3

Data: 11/12/24

INFORMAZIONI PRINCIPALI

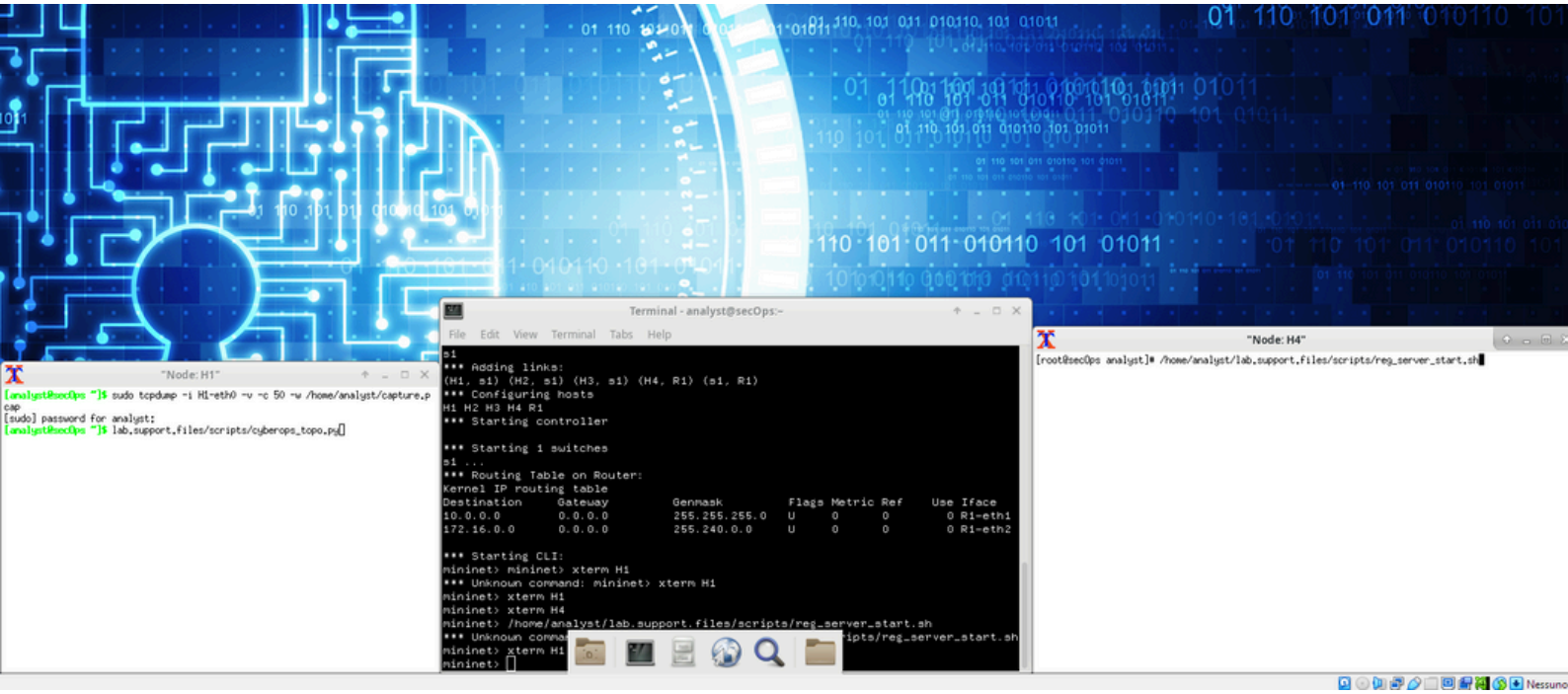
Traccia:

Parte 1: Preparare gli host per catturare il traffico
Configurare gli host utilizzando Mininet. Un host fungerà da client e l'altro da server web. Avviare una sessione di acquisizione di pacchetti utilizzando tcpdump, salvando i dati per successive analisi.

Parte 2: Analizzare i pacchetti utilizzando Wireshark
Aprire il file di cattura in Wireshark, applicherò filtri TCP e analizzare i dettagli dei pacchetti. L'attenzione sarà focalizzata sull'osservazione dei flag (SYN, ACK) e dei numeri di sequenza relativi, che permettono di comprendere il funzionamento della stretta di mano TCP a 3 vie.

Parte 3: Visualizzare i pacchetti utilizzando tcpdump
usare tcpdump per visualizzare i pacchetti catturati, filtrando solo quelli pertinenti al protocollo TCP. Questo permetterà di validare i risultati ottenuti e confrontarli con quelli di Wireshark.

INIZIO ESERCIZIO & RELAZIONE



In questo esercizio abbiamo usato Wireshark, strumento essential per l'analisi dei pacchetti di rete e l'osservazione e il how does it work dell'handshake tcp a tre vie. cattureremo il traffico con un tcp dump, dall'inizializzazione fino all'handshake completo.

PREPARAZIONE DEGLI HOST

Ho configurato due host (H1 e H4) utilizzando Mininet. H4 è stato impostato come server web, mentre H1 come client. Su H1, ho lanciato una sessione di acquisizione tramite tcpdump, salvando i pacchetti in un file .pcap. Una volta iniziata l'acquisizione, ho aperto un browser su H1 per connettermi al server, generando così il traffico necessario.

ANALISI DEI PACCHETTI

Utilizzando Wireshark, ho aperto il file di cattura per applicare un filtro sui pacchetti TCP. Questo mi ha permesso di focalizzarmi sui primi tre pacchetti dell'handshake TCP. L'analisi dettagliata ha mostrato come i pacchetti scambiati stabiliscano una connessione affidabile tra client e server, attraverso l'uso di flag specifici (SYN, ACK).

Infine, ho esplorato i dettagli dei pacchetti, come indirizzi IP, porte e flag di controllo. Ad esempio:

Il primo pacchetto presentava un flag SYN con un numero di sequenza relativo pari a 0.

Il secondo pacchetto includeva i flag SYN e ACK, con un numero di sequenza e un numero di riconoscimento relativi incrementati.

Il terzo pacchetto, infine, conteneva solo il flag ACK, confermando la stabilità della connessione.

REFLECTIONS

Ho riflettuto anche su come Wireshark possa essere utilizzato in un contesto reale. Non solo per analisi post-attacco, ma anche per comprendere meglio nuovi protocolli e servizi, identificando porte e flussi di traffico rilevanti per migliorare la sicurezza della rete.