**S11/L3**

**Wireshark  
  
Relazione Tecnica: Analisi della Rete e Monitoraggio del Traffico**

**Contesto**

Dalle immagini fornite, viene simulata una rete utilizzando Mininet, uno strumento comunemente usato per la creazione e simulazione di topologie di rete virtuali. Il traffico di rete tra due nodi (H1 e H4) è stato catturato per analisi tramite strumenti come tcpdump e Wireshark.

**Configurazione della Rete**

1. **Mininet CLI**:

La rete configurata include i nodi H1, H4 e un router (R1).

Le interfacce del router sono configurate con indirizzi IP per comunicare su due sottoreti differenti:

10.0.0.0/24 con gateway 10.0.0.1.

172.16.0.0/24 con gateway 172.16.0.40.

Gli host H1 e H4 sono connessi rispettivamente alle sottoreti 10.0.0.0/24 e 172.16.0.0/24 tramite il router R1.

1. **Comandi Eseguiti sui Nodi**:

Su **H1**:

È stato avviato il browser Firefox per accedere al server web su H4.

È stato eseguito il comando tcpdump per catturare il traffico sulla propria interfaccia di rete, salvando il risultato in un file capture.pcap.

* + Su **H4**:

È stato avviato un server web Nginx, come mostrato dalla pagina di benvenuto accessibile all’indirizzo http://172.16.0.40/.

Sono presenti errori relativi alla richiesta di un file favicon.ico non trovato, generando una risposta HTTP 404 Not Found.

**Analisi del Traffico**

1. **Cattura e Analisi del Traffico con Wireshark**:

Il traffico analizzato mostra una connessione TCP stabilita tra i nodi H1 e H4.

Dettagli dei pacchetti:

**Pacchetti di handshake TCP**:

H1 (10.0.0.11) invia un pacchetto SYN alla porta 80 di H4 (172.16.0.40).

H4 risponde con SYN/ACK, e la connessione è stabilita tramite un ACK finale da H1.

**Richieste HTTP**:

H1 invia una richiesta GET per favicon.ico, ma il server Nginx su H4 risponde con 404 Not Found.

**Keep-Alive TCP**:

Sono presenti pacchetti di tipo "Keep-Alive" per mantenere la connessione attiva.

1. **Errori Riscontrati**:

La richiesta HTTP per favicon.ico genera un errore 404 Not Found sul server.

Questo è dovuto all’assenza del file richiesto nella directory root del server web.

**Conclusioni**

1. **Funzionalità della Rete**:

La configurazione della rete è corretta: gli host possono comunicare tra sottoreti diverse tramite il router R1.

Il traffico HTTP è visibile e ben analizzato con strumenti come tcpdump e Wireshark.

1. **Miglioramenti Possibili**:

Configurare un file favicon.ico o disabilitare la sua richiesta per evitare errori 404.

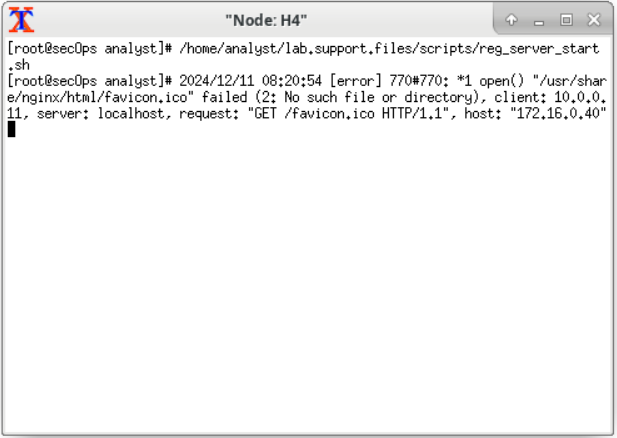
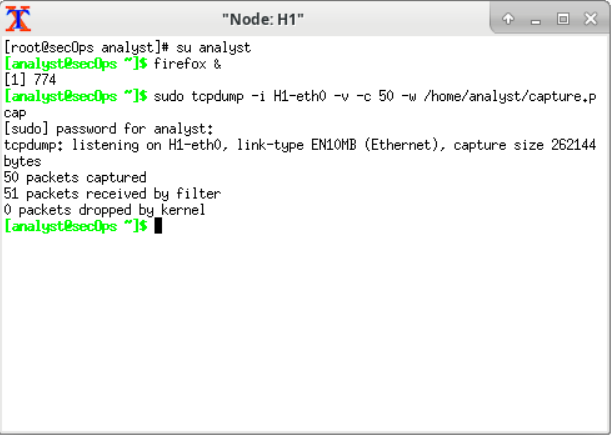
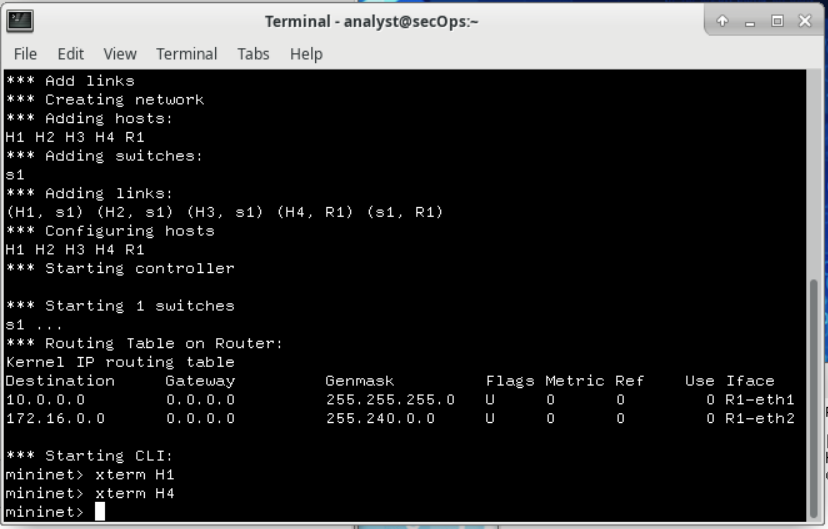
Ottimizzare i log del server per evitare informazioni superflue o ripetitive.

Utilizzare filtri specifici su Wireshark per isolare traffico di interesse (ad esempio, richieste HTTP o pacchetti TCP).

**Allegati**

File di cattura del traffico (capture.pcap) per ulteriori analisi.

Screenshot della configurazione e dei log mostrati durante l’esperimento.

****