## **PROGETTO S1/L5**

**TRACCIA:**

Simulare, in ambiente di laboratorio virtuale, un’architettura client server in cui un client con indirizzo 192.168.32.101 richiede tramite web browser una risorsa all’hostname epicode.internal che risponde all’indirizzo 192.168.32.100. Si intercetti poi la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS. Ripetere l’esercizio, sostituendo il server HTTPS, con un server HTTP. Si intercetti nuovamente il traffico, evidenziando le differenze tra il traffico appena catturato in HTTP ed il traffico precedente in HTTPS. Spiegare, motivandole, le principali differenze.

**In http**A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

**In https**

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

**STEP1 Configurazione Iniziale:**

È stata creata un'architettura client-server in un ambiente di laboratorio virtuale sia su WINDOWS 7 che su Kali Linux.

Il client ha l'indirizzo cioè Windows 7 con l’ IP 192.168.32.101, mentre il server Kali Linux ha l'hostname epicode.internal con l'indirizzo IP 192.168.32.100.

Un server HTTPS è attivo e un servizio DNS è attivo per la risoluzione dei nomi di dominio.

**Richiesta con HTTPS:**

Il client (che parte da Windows 7), con indirizzo IP 192.168.32.101, fa una richiesta tramite un web browser al server all'hostname epicode.internal (Kali Linux).

La comunicazione avviene tramite HTTPS, il che significa che i dati sono **criptati** durante la trasmissione.

**Intercezione con Wireshark:**

Durante l'intercettazione con Wireshark, si evidenziano i MAC address di sorgente e destinazione, e il contenuto della richiesta HTTPS.

Il traffico HTTPS mostra che i dati sono cifrati, quindi l'indirizzo IP e il contenuto della richiesta **sono protetti da potenziali attacchi di intercettazione.**

**Step 2 Richiesta con HTTP:**

Si ripete l'esercizio sostituendo il server HTTPS con un server http.

**Intercezione con Wireshark (HTTP):**

Durante l'intercettazione del traffico HTTP, si noterà che l'indirizzo IP e il contenuto della richiesta **sono chiaramente visibili e non cifrati.**

Dunque nel traffico HTTPS, il contenuto è cifrato (usando SSL/TLS), il che fornisce un livello di sicurezza aggiuntivo.

Nel traffico HTTP, i dati viaggiano in chiaro sulla rete, esponendo l'indirizzo IP e il contenuto a potenziali attacchi di intercettazione come attacchi di tipo "man-in-the-middle".

L'HTTPS fornisce un livello di sicurezza superiore rispetto all'HTTP a causa della crittografia dei dati in transito.

L'utilizzo di HTTPS è particolarmente importante quando si trasmettono informazioni sensibili come password, dati personali o finanziari.

In conclusione, l'uso di HTTPS è fortemente raccomandato per garantire la sicurezza delle comunicazioni su Internet, specialmente quando sono coinvolte informazioni sensibili.

La cifratura fornita da HTTPS protegge da potenziali minacce di intercettazione e compromissione dei dati durante la trasmissione.