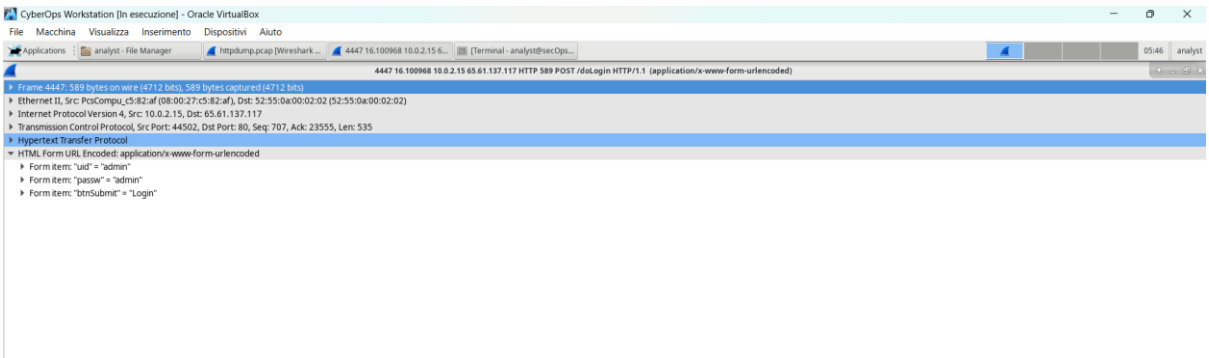
Relazione: Analisi del Traffico HTTP e HTTPS con Wireshark

Obiettivi: Questa esercitazione ha lo scopo di esaminare e confrontare il traffico HTTP e HTTPS utilizzando Wireshark. L'analisi permette di comprendere la differenza tra i due protocolli in termini di sicurezza e accessibilità dei dati trasmessi.

Scenario: L'HyperText Transfer Protocol (HTTP) è un protocollo di livello applicativo che trasmette dati in chiaro, rendendoli vulnerabili ad attacchi di tipo man-in-the-middle. L'HyperText Transfer Protocol Secure (HTTPS), invece, utilizza la crittografia TLS per proteggere le informazioni scambiate, evitando l'accesso non autorizzato ai dati trasmessi.

Parte 1: Cattura e Analisi del Traffico HTTP

1. Avvio della macchina virtuale CyberOps Workstation e accesso con le credenziali fornite.
2. Avvio di un terminale e utilizzo del comando `tcpdump` per catturare il traffico HTTP sull'interfaccia di rete.
3. Navigazione su un sito HTTP non sicuro (http://www.altoromutual.com/login.jsp), inserimento delle credenziali di accesso e chiusura del browser.
4. Interruzione della cattura del traffico e apertura del file generato (`httpdump.pcap`) con Wireshark.
5. Applicazione del filtro HTTP in Wireshark e analisi del traffico catturato.
6. Identificazione di credenziali trasmesse in chiaro nel pacchetto POST (`Admin/Admin`).



Parte 2: Cattura e Analisi del Traffico HTTPS

1. Avvio di una nuova sessione di `tcpdump` per catturare il traffico HTTPS.

2. Navigazione su un sito HTTPS (`www.netacad.com`), accesso con credenziali personali e chiusura del browser.
3. Interruzione della cattura del traffico e analisi del file risultante (`httpsdump.pcap`) con Wireshark.
4. Applicazione del filtro per il traffico HTTPS (`tcp.port==443`).
5. Analisi dei pacchetti catturati e confronto con il traffico HTTP.
6. Osservazione della sezione Secure Sockets Layer (SSL/TLS 1.2), che protegge i dati trasmessi impedendone la lettura in chiaro.

Riflessioni Finali:

1. **Vantaggi dell'uso di HTTPS rispetto a HTTP:**
    a. Protezione della trasmissione dei dati mediante crittografia.
    b. Minore vulnerabilità agli attacchi di tipo man-in-the-middle.
    c. Maggiore affidabilità per gli utenti.
2. **Affidabilità dei siti HTTPS:**
    a. L'uso di HTTPS non garantisce automaticamente la sicurezza del sito.
    b. I malintenzionati possono comunque utilizzare certificati validi per truffe e attacchi di phishing.
    c. Si consiglia di verificare sempre la legittimità di un sito web prima di inserire dati sensibili.

Questa esercitazione ha dimostrato l'importanza dell'uso di HTTPS per proteggere le informazioni trasmesse su Internet e ha evidenziato i rischi derivanti dall'uso di HTTP senza crittografia.