CYBER SECURITY

Analisi del Traffico di Rete

Cos'è Wireshark

- Definizione: Wireshark è un analizzatore di protocolli di rete open-source.
- Funzione: Cattura e analizza i pacchetti di dati che transitano su una rete.
- Piattaforme: Disponibile per Windows, macOS e Linux.

A COSA SERVE WIRESHARK

- Analisi del traffico di rete: Monitoraggio e risoluzione dei problemi di rete.
- Sicurezza: Identificazione di attività sospette e vulnerabilità.
- Formazione: Strumento educativo per comprendere i protocolli di rete.

Come si installa Wireshark

- Download: Scaricare l'installer dal sito ufficiale di Wireshark.
- Installazione su Windows:
  - Eseguire l'installer e seguire le istruzioni a schermo.
  - Installare Npcap, necessario per la cattura dei pacchetti.
- Installazione su macOS e Linux:
  - Utilizzare i gestori di pacchetti come Homebrew (macOS) o apt-get (Linux).

Come si usa Wireshark

- #### Avvio
- Selezione dell'interfaccia di rete: All'avvio di Wireshark, seleziona l'interfaccia di rete da monitorare (es. Ethernet, Wi-Fi).
- Avvio della cattura: Clicca sul pulsante 'Start Capturing Packets' (icona dello squalo verde) per iniziare la cattura dei pacchetti

Come si usa Wireshark

- #### Cattura dei pacchetti
- Monitoraggio in tempo reale: Osserva i pacchetti che transitano sulla rete in tempo reale.
- Salvataggio della cattura: Puoi salvare la cattura per analisi future cliccando su 'File' > 'Save As'.

Come si usa Wireshark

- #### Filtri
- Applicazione dei filtri: Utilizza i filtri per isolare i pacchetti di interesse. Ad esempio, per visualizzare solo il traffico HTTP, inserisci `http` nella barra dei filtri.
- Esempi di filtri comuni:
- Traffico HTTP: `http`
- Traffico IP specifico: `ip.addr == 192.168.1.1`
- Traffico TCP: `tcp`
- Traffico DNS: `dns`

Come si usa Wireshark

- #### Analisi dei pacchetti
- Dettagli del pacchetto: Clicca su un pacchetto per visualizzare i dettagli. La finestra dei dettagli è divisa in tre sezioni:
- Lista dei pacchetti: Mostra tutti i pacchetti catturati con informazioni di base come numero, tempo, sorgente, destinazione, protocollo e lunghezza.
- Dettagli del pacchetto: Mostra una vista dettagliata del pacchetto selezionato, suddivisa per livelli del modello OSI (es. livello fisico, livello di rete, livello di trasporto).
- Byte del pacchetto: Visualizza i dati grezzi del pacchetto in formato esadecimale e ASCII.

Come si usa Wireshark

- #### Esempi pratici
- Analisi di una richiesta HTTP:
- Filtro: `http.request`
- Dettagli: Mostra le richieste HTTP inviate dal browser, inclusi metodi come GET e POST, URL richiesti e intestazioni HTTP.

Come si usa Wireshark

- Monitoraggio di un dispositivo specifico:
- Filtro: `ip.addr == 192.168.1.100`
- Dettagli: Visualizza tutto il traffico in entrata e uscita da un dispositivo con indirizzo IP specifico.

- Identificazione di attività sospette:
- Filtro: `tcp.flags.syn == 1 and tcp.flags.ack == 0`
- Dettagli: Isola i pacchetti SYN senza ACK, che possono indicare un tentativo di scansione delle porte.

Conclusione

- Riassunto: Wireshark è uno strumento potente per l'analisi del traffico di rete e la sicurezza.
- Risorse: Visita il sito ufficiale di Wireshark per ulteriori informazioni e tutorial.