

L0 – HTTP vs HTTPS

Scopo

Lo scopo dell'esercizio è mostrare tramite packet sniffing, analizzando quindi il traffico in uscita dalla propria rete locale, le differenze nella trasmissione delle informazioni di login (username e password) tra i protocolli HTTP e HTTPS.

Per chi

L'esercizio è pensato e contiene passaggi adatti a un pubblico che conosca il proprio dispositivo e la propria rete locale, ma è possibile seguire le descrizioni anche con una minima conoscenza tecnica. In particolare, per svolgere l'esercizio è necessario saper installare programmi sul proprio computer e conoscere le specifiche del proprio sistema operativo.

Durata

Il tempo richiesto dipende principalmente dalla durata della fase di preparazione e installazione dei software necessari.

lo svolgimento completo è di circa 1 ora.

Livello arcobaleno

Livello L0 – The Net

Tag/keyword

Riservatezza dei dati

Difficoltà

Medio/alta.

L'esercizio non è accessibile a tutti gli utenti, ma anche senza conoscenze tecniche risultano di facile comprensione sia i passaggi intermedi che lo scopo finale dell'esercizio.

Strumenti, s.o., pacchetti/app

È necessario avere :

- un computer
- una connessione di rete
- un account personale sul sito <http://tecnocivismo.di.unimi.it/>
- Wireshark installato (riferimenti a ver. 3.6.1)

I software necessari sono specificati, con relativa guida all'installazione, nella sezione "Istruzioni Dettagliate"

Costi

Il download del software e la registrazione di un account sul sito sono gratuiti.

Istruzioni dettagliate

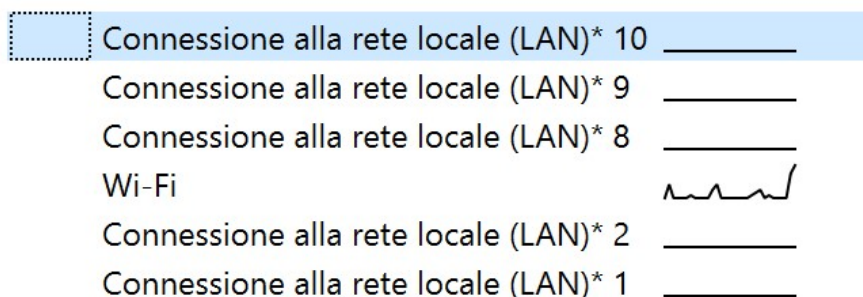
Installazione Wireshark (indicazioni per ver. 3.6.1, s.o. Win64, connessione Wi-Fi)

- Aprire il link : <https://www.wireshark.org/download.html>
 - Selezionare (se possibile dalla lista "Stable Release") la propria versione di sistema operativo per avviare il download
 - Avviare l'installazione seguendo le indicazioni dell'installer
- ATTENZIONE: Wireshark richiede l'installazione di Npcap o Winpcap, suggerite durante l'installazione, NON è invece necessario USBpcap per questo esercizio.

Avviare Wireshark

Una volta aperto Wireshark sarà disponibile una lista di interfacce di rete.

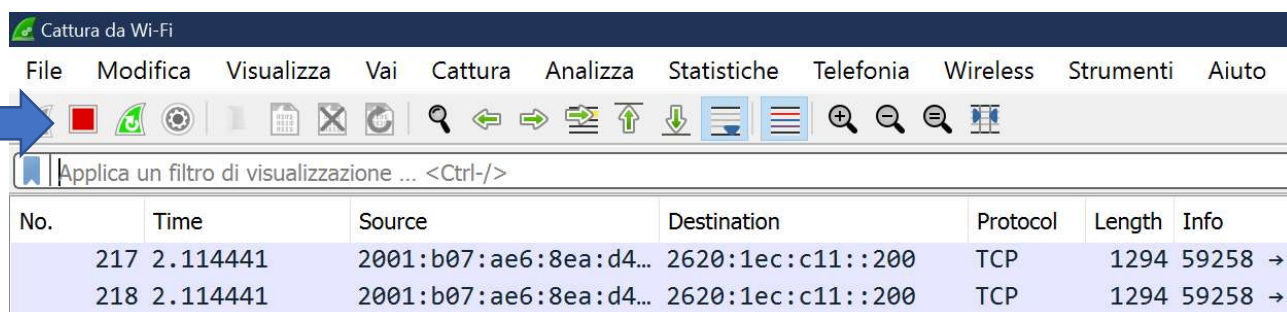
Selezionare con doppio click quella tramite cui il vostro dispositivo è connesso alla rete, il dettaglio del traffico su ogni interfaccia è visibile anche tramite grafico affiancato ai nomi (linee rette indicano assenza di traffico di pacchetti).



Le indicazioni successive saranno riferite a una connessione Wi-Fi.

A schermo compare una lista di pacchetti identificati da Wireshark sull'interfaccia selezionata.

Premere sul pulsante "ferma la cattura dei pacchetti" raffigurato come quadrato rosso presente in alto a sinistra.



Interpretare le informazioni

La schermata è divisa in tre fasce, la prima mostra l'elenco dei pacchetti intercettati.

Qui è possibile notare le colonne:

No. | Time | Source | Destination | Protocol | Length | Info

Cliccando su uno dei pacchetti (possibilmente per una spiegazione più chiara selezionare un pacchetto con Protocollo = TCP la cui riga NON sia evidenziata in nero) è possibile analizzarne il contenuto nelle due sezioni sottostanti, o tramite doppio click può essere aperto in una nuova finestra.

Dalla prima delle due sezioni è possibile espandere gli attributi, ad esempio, di Internet Protocol Version 4 e Transmission Control Protocol, mentre nella sezione più in basso è presente una rappresentazione cifrata del contenuto.

Selezionare le informazioni

Per lo scopo di questo esercizio è necessario isolare il traffico in uscita dal proprio dispositivo dal resto.

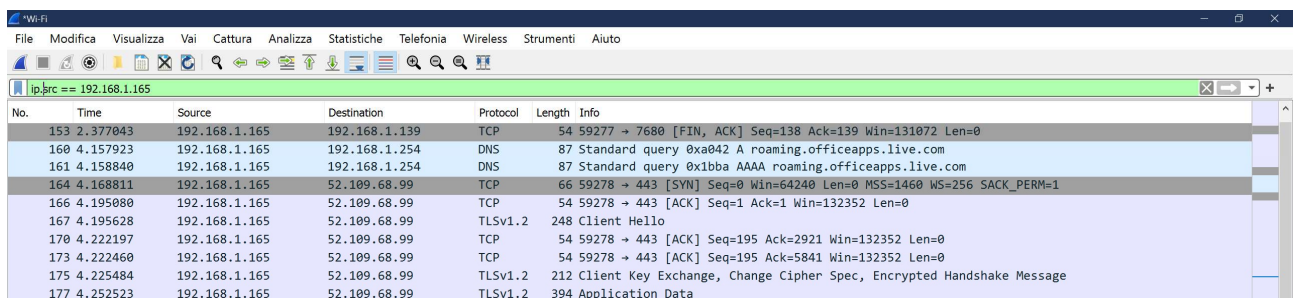
Per farlo è necessario conoscere il proprio indirizzo IPv4, visualizzabile dalle proprietà di rete o seguendo queste indicazioni :

START - cmd - "ipconfig"+INVIO

la voce che ci interessa è "Indirizzo IPv4" sotto "Scheda LAN wireless Wi-Fi".

Ora, tornati su Wireshark, è possibile applicare filtri di selezione ai pacchetti intercettati, digitando le formule di selezione nella barra in alto.

Un esempio di comando da inserire è : "ip.src == *IPv4*" inserendo il proprio IPv4 (es. ip.src == 192.186.1.115) per visualizzare solo i pacchetti in uscita dal dispositivo.



No.	Time	Source	Destination	Protocol	Length	Info
153	2.377043	192.168.1.165	192.168.1.139	TCP	54	59277 → 7680 [FIN, ACK] Seq=138 Ack=139 Win=131072 Len=0
160	4.157923	192.168.1.165	192.168.1.254	DNS	87	Standard query 0xa042 A roaming.officeapps.live.com
161	4.158840	192.168.1.165	192.168.1.254	DNS	87	Standard query 0x1bba AAAA roaming.officeapps.live.com
164	4.168811	192.168.1.165	52.109.68.99	TCP	66	59278 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
166	4.195080	192.168.1.165	52.109.68.99	TCP	54	59278 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
167	4.195628	192.168.1.165	52.109.68.99	TLSv1.2	248	Client Hello
170	4.222197	192.168.1.165	52.109.68.99	TCP	54	59278 → 443 [ACK] Seq=195 Ack=2921 Win=132352 Len=0
173	4.222460	192.168.1.165	52.109.68.99	TCP	54	59278 → 443 [ACK] Seq=195 Ack=5841 Win=132352 Len=0
175	4.225484	192.168.1.165	52.109.68.99	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
177	4.252523	192.168.1.165	52.109.68.99	TLSv1.2	394	Application Data

HTTP

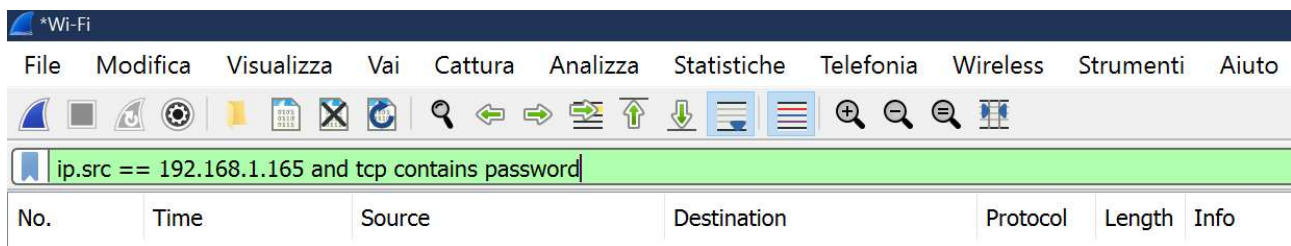
Per analizzare come HTTP trasmette le informazioni di login (username e password) è necessario seguire i seguenti passaggi.

IMPORTANTE

Prima di iniziare la procedura sotto descritta assicurarsi di non avere le informazioni di login salvate nei cookie del sito o di non aver effettuato l'accesso da meno di 24 ore.

- Cliccare sull'icona in alto a sinistra a forma di pinna di squalo blu per iniziare una nuova scansione. Non è necessario salvare i risultati della scansione precedente.
- Aprire sul proprio browser il sito <http://tecnocivismo.di.unimi.it/>
- Selezionare una scheda del sito per attivare la pagina di login
- Inserire username e password
- Attendere qualche secondo o navigare nel sito per qualche secondo
- Tornare su Wireshark e interrompere la scansione tramite pulsante (quadrato rosso in alto)
- Riapplicare il filtro relativo al proprio indirizzo IP

Filtri da inserire : "tcp contains password" + INVIO



Applicato questo filtro individuare nella lista dei pacchetti, se non ne resta solo uno, quello che corrisponde alle seguenti caratteristiche :

- Source = *IPv4*
- Protocol = HTTP
- Info = POST /user/login...

Selezionandolo ed espandendo la voce "HTML from URL encoded:" nella sezione a centro schermo (la seconda delle tre di Wireshark) è possibile notare, in chiaro e tra le voci "data[user]", i campi username e password con i valori inseriti in fase di login.

È possibile salvare queste informazioni in formato testuale facendo tasto destro su "HTML from URL encoded:" e selezionando "Copia -> Tutti gli elementi visibili dell'albero selezionato" salvandoli su un documento di testo.

HTTPS

Ora per mostrare come vengono rappresentate le informazioni di login trasmesse da un sito che usa HTTPS è necessario :

- Iniziare una nuova scansione cliccando sul simbolo a forma di pinna di squalo blu.
- Aprire il browser ed eseguire un login su un sito a piacere che utilizzi HTTPS (es. login google)
- Attendere qualche secondo
- Fermare la scansione su Wireshark

Ora il filtro usato in precedenza non restituirebbe più nessun pacchetto.

È possibile notare che nella colonna "Protocol" sono presenti oltre a TCP anche TLSv1.1/TLSv1.2/TLSv1.3. Questi sono protocolli di transfer layer security che criptano i dati trasmessi.

Selezionando un pacchetto è possibile visualizzarne il contenuto intercettato con :
tasto destro -> segui -> flusso TCP

Le informazioni di login, così come il resto delle informazioni contenute, sono impossibili da interpretare.

Risultati attesi

Eseguiti gli step indicati dovrebbe essere chiara la differenza di sicurezza fornita dai due protocolli in esame. HTTP e HTTPS nello specifico, ma più in generale protocolli diversi usano cifrature ed encryption diversi, che si traduce in una differenza nell'esposizione dei contenuti a un osservatore in rete.

Obiettivi formativi

L'obiettivo dell'esercizio è rendere consapevoli gli utenti del livello di riservatezza delle informazioni personali trasmesse, prendendo in esempio una fase delicata come il login.

L'invito rivolto al lettore è quello di ragionare sull'idea di riservatezza come concetto applicabile a ogni fase

di esistenza di un dispositivo all'interno della rete, oltre che ai pacchetti e alle informazioni trasmesse in rete.

Suggerimenti per variazioni

È possibile ampliare l'esercizio per testare vari siti web che utilizzano i protocolli HTTP e HTTPS. Inoltre, lo strumento Wireshark apre a molte possibilità di analisi della rete, per cui si rimanda a forum e tutorial presenti numerosi in rete.

See also, prosegui con, propedeuticità

È possibile approfondire i funzionamenti dei protocolli analizzati, è quindi consigliato soffermarsi ad esempio sulla sequenza di pacchetti che rappresentano i processi di handshake, HTTP GET/POST, ... o sul contenuto dei campi in HTTP.

Autore

Daniele Scaccabarozzi