MINI-REPORT: Esercizio 4 - Usare Wireshark per Esaminare il Traffico HTTP e HTTPS

Parte 1: Catturare e visualizzare il traffico HTTP

- **Interfacce di rete rilevate con `ip address`:**
    1. `lo` (Loopback) con IP `127.0.0.1`
    2. `eth0` con IP `10.0.2.15`

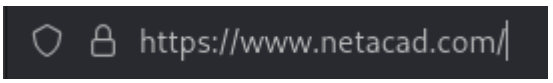
```
┌──(kali㉿kali)-[~]
└─$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 86389sec preferred_lft 86389sec
    inet6 fd17:625c:f037:2:12d8:29a2:aef5:878a/64 scope global dynamic noprefixroute
       valid_lft 86392sec preferred_lft 14392sec
    inet6 fe80::6573:6be1:2928:ba99/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- **Analisi della cattura HTTP in Wireshark:** Espandendo la sezione `HTML Form URL Encoded` nel pacchetto HTTP POST, è possibile vedere chiaramente **il nome utente e la password in chiaro** (nel nostro test: "test" e "test"). Questo dimostra che il protocollo HTTP non offre alcuna cifratura dei dati.

```
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▾ Form item: "uname" = "test"
      Key: uname
      Value: test
  ▸ Form item: "pass" = "test"
```

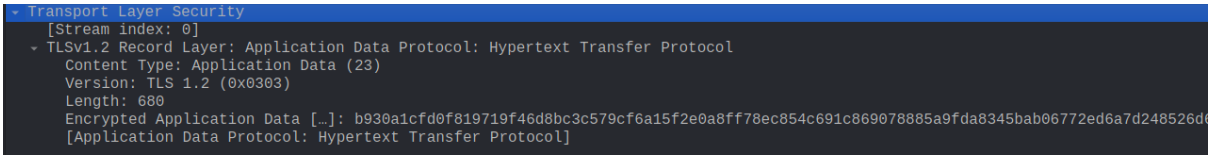
Parte 2: Catturare e Visualizzare il Traffico HTTPS

- **Osservazione dell'URL:** Navigando su NetAcad, si nota che l'URL inizia con `https://` e il browser mostra l'icona di un lucchetto, indicando una connessione sicura.



- **Analisi della cattura HTTPS in Wireshark:**

- Nel pacchetto catturato, la sezione *Hypertext Transfer Protocol* è stata sostituita da **Transport Layer Security (TLS)**.
- Cliccando su *Encrypted Application Data*, si nota che **i dati non sono più in formato leggibile** (plaintext). Sono stati trasformati in una stringa cifrata incomprensibile tramite un algoritmo matematico, rendendo impossibile per un intercettatore leggere la mail e la password inserite.



Domande di Riflessione Finali

1. **Quali sono i vantaggi dell'uso di HTTPS invece di HTTP?** A differenza di HTTP, HTTPS utilizza la crittografia. Questo nasconde il vero significato dei dati scambiati tra il computer e il server, salvaguardando informazioni sensibili come credenziali o dati personali da chiunque stia intercettando il traffico di rete.

2. **Tutti i siti web che usano HTTPS sono considerati affidabili?** No, assolutamente. Sebbene HTTPS garantisca che la *connessione* sia privata, non garantisce l'affidabilità del proprietario del sito. Molti attori malevoli utilizzano regolarmente connessioni HTTPS per nascondere le loro attività e far sembrare sicuri i loro siti di phishing o malware.
