Build Week 3

Esercizio 4

LANDA

TRACKER SPA

In questo laboratorio, esplorerai e catturerai il traffico HTTP e HTTPS usando Wireshark.

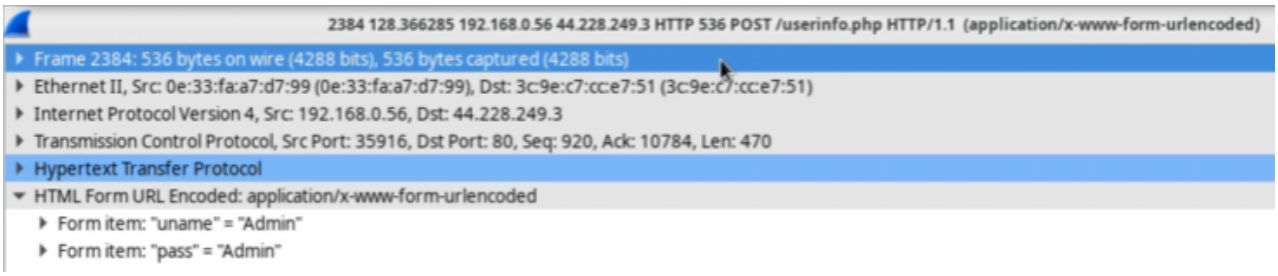
- Parte 1 Catturare e visualizzare il traffico HTTP
- Parte 2 Catturare e visualizzare il traffico HTTPS

Per l'analisi abbiamo utilizzato tcpdump sull'interfaccia eth0 per la cattura dei pacchetti nel seguente modo:

```
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -i eth0 -s -0 -w httpsgambiling.pcap
[sudo] password for kali:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C13131 packets captured
13133 packets received by filter
0 packets dropped by kernel
```

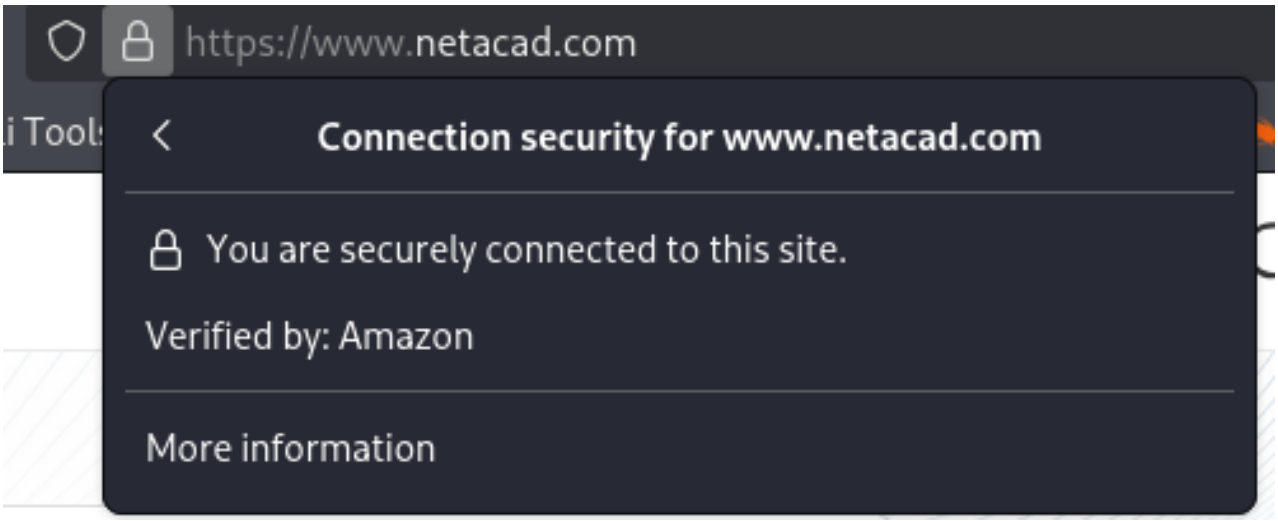
Quali due informazioni vengono visualizzate?

All'interno del campo HTML Form URL Encoded troviamo le informazioni relative ai dati in chiaro.



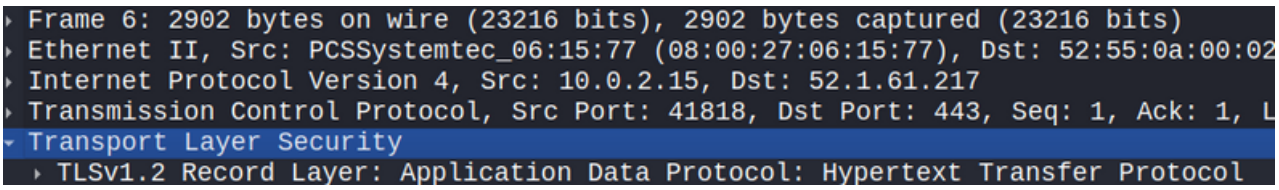
Cosa noti riguardo all'URL del sito web?

Dall'URL possiamo notare che possiede il certificato SSL/TLS verificato da **Amazon**.



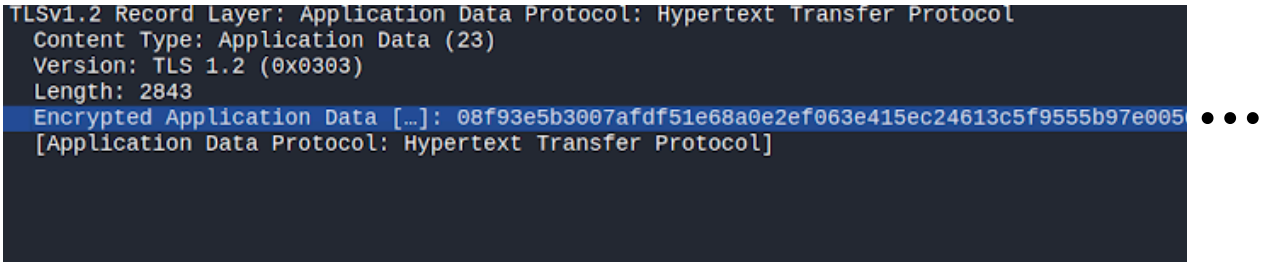
Cosa ha sostituito la sezione HTTP che era nel file di cattura precedente?

La sezione **HyperText Transfer Protocol** è stata sostituita con **Transfer Layer Security (TLS)**.



I dati dell'applicazione sono in formato plaintext o leggibile?

I dati dell'applicazione non sono leggibili o plaintex; il contenuto è cifrato tramite il **protocollo TLS 1.2**.



DOMANDE DI RIFLESSIONE

Quali sono i vantaggi dell'uso di HTTPS invece di HTTP?

L'utilizzo di **HTTPS** al posto di **HTTP** offre un'esperienza web più sicura, affidabile e moderna. Il vantaggio principale è la sicurezza offerta dalla crittografia, ciò rende i dati, come password e numeri di carte, illeggibili a chiunque cerchi di intercettarli.
HTTPS garantisce l'integrità dei dati, assicurando che i dati non siano stati manomessi o alterati in transito da malintenzionati.
Infine, attraverso il certificato **SSL/TLS**, offre autenticazione, verificando che la comunicazione sia con il vero sito interessato, e non con un imitatore.

Tutti i siti web che usano HTTPS sono considerati affidabili?

No, non tutti i siti web che usano **HTTPS** sono considerati automaticamente affidabili. Al giorno d'oggi ottenere un certificato **SSL/TLS** è diventato estremamente facile ed economico, di conseguenza, anche un sito di phishing o un sito losco può implementare l'HTTPS.
Per stabilire se un sito è davvero affidabile bisogna guardare oltre il lucchetto HTTPS e prestare particolare attenzione a URL, dettagli del certificato, recensioni e contatti e la qualità del contenuto del sito.