


Analisi del Traffico di Rete con Wireshark: HTTP vs HTTPS

Questo documento guida studenti di sicurezza informatica e professionisti IT attraverso un'analisi comparativa del traffico di rete HTTP e HTTPS utilizzando Wireshark. L'obiettivo è dimostrare la vulnerabilità dei dati trasmessi tramite HTTP e l'importanza della crittografia offerta da HTTPS per proteggere le informazioni sensibili durante la comunicazione online.

 **by Luca Tavani**

Lab 1: Analisi del Traffico HTTP

Setup Iniziale

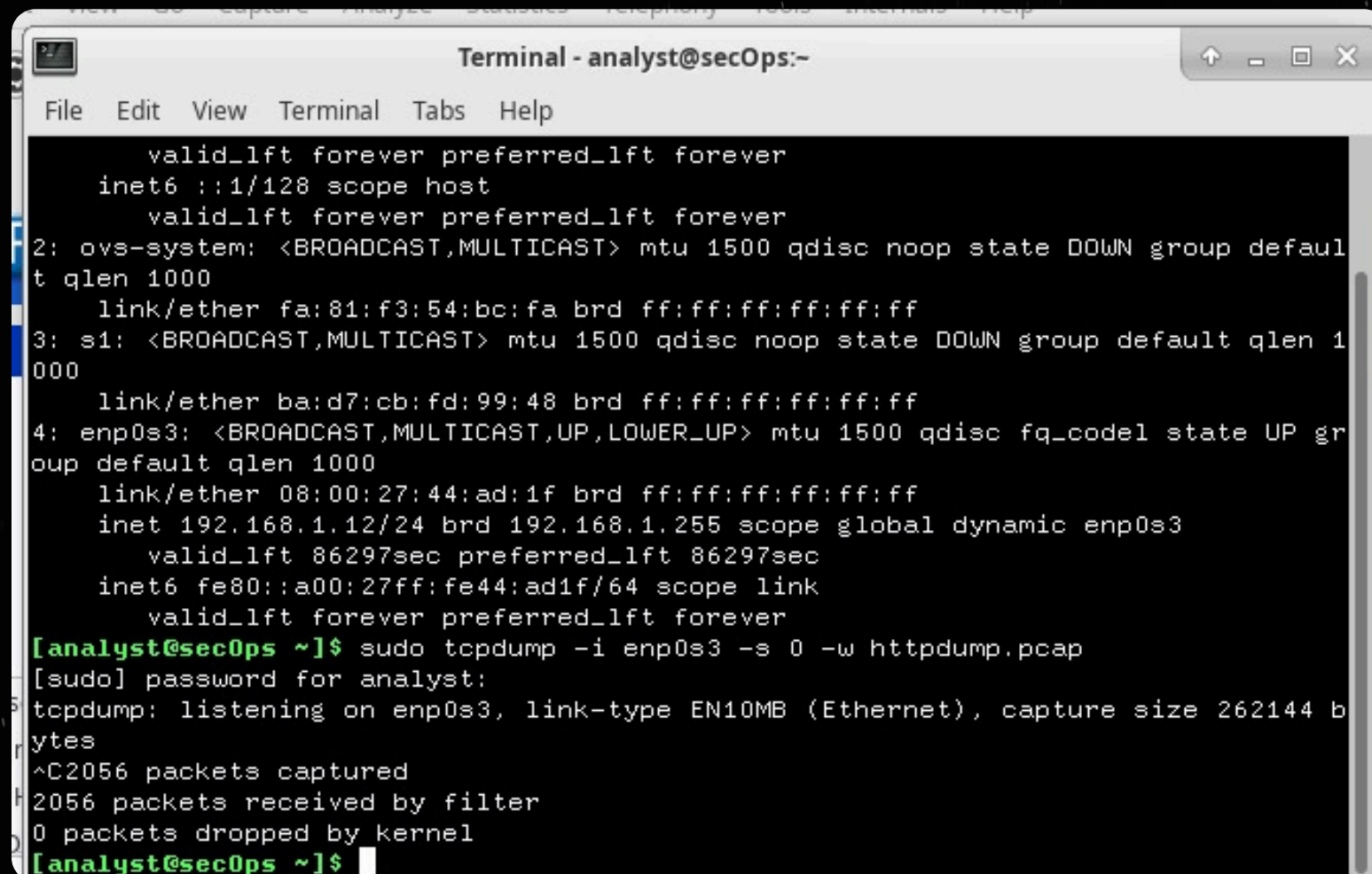
Per questo laboratorio, utilizzeremo la VM CyberOps Workstation. Assicurati che l'interfaccia di rete **enp0s3** sia attiva e configurata per ricevere un indirizzo IP tramite DHCP. Una volta configurata la rete, avvia la cattura del traffico utilizzando il comando **tcpdump**:

```
sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
```

Questo comando catturerà tutto il traffico sull'interfaccia **enp0s3** e lo salverà nel file **httpdump.pcap**.

Verifica Interfaccia Attiva

Per verificare che l'interfaccia sia attiva e configurata correttamente, utilizza il comando **ip address** e verifica l'assegnazione di un indirizzo IP.



```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

    valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: ovs-system: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default
t qlen 1000
    link/ether fa:81:f3:54:bc:fa brd ff:ff:ff:ff:ff:ff
3: s1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1
000
    link/ether ba:d7:cb:fd:99:48 brd ff:ff:ff:ff:ff:ff
4: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:44:ad:1f brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.12/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 86297sec preferred_lft 86297sec
    inet6 fe80::a00:27ff:fe44:ad1f/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 b
ytes
^C2056 packets captured
2056 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$
```

Navigazione HTTP e Acquisizione Credenziali

Simulazione di Login

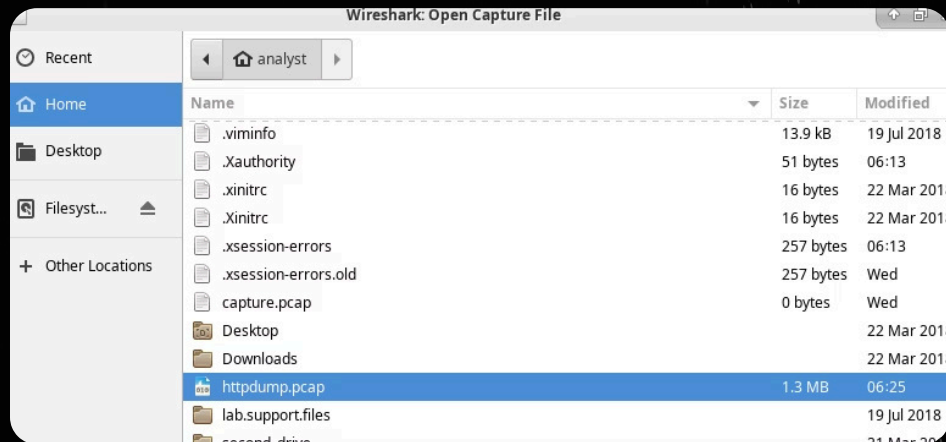
Per generare traffico HTTP non cifrato, effettua un login sul sito. Utilizza le credenziali **admin / admin** per accedere. Questo sito è appositamente progettato per essere vulnerabile e mostrare la trasmissione di credenziali in chiaro.

Interfaccia del Sito di Login

La pagina di login del sito presenta un semplice form dove inserire username e password. L'assenza di HTTPS rende questa pagina vulnerabile all'intercettazione delle credenziali.

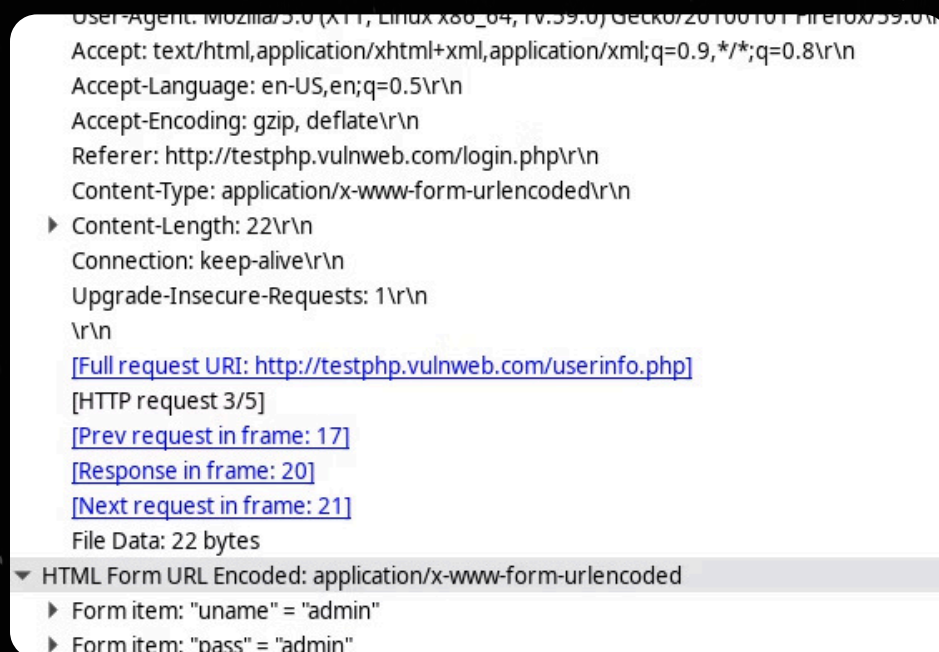
Analisi del Traffico HTTP con Wireshark

Isolamento del Pacchetto POST



Dopo aver completato la cattura, apri il file **httpdump.pcap** in Wireshark. Applica il filtro **http** per visualizzare solo il traffico HTTP. Individua il pacchetto contenente la richiesta **POST** con le credenziali inviate durante il login.

Credenziali in Chiaro



Analizzando il payload del pacchetto POST, noterai che i dati trasmessi (username e password) sono leggibili in chiaro all'interno del payload HTTP, dimostrando l'assenza di crittografia. Wireshark permette di visualizzare facilmente questi dati non cifrati.

Packectudnls
siruricmp sake(keg Socure,
icq katbe lerante ing fecrvatioe ba
petktepet lecunmd IP Rucralert Caw
potatd'cmd setcriplum: tistwenta van
tcritAzpcduket: lfwo; dual care
istel:-sddump:
131:159:1236684240A)...
133:1sJ:5565544 T3:
131:na6:
333:da7:

Gestione dei File .pcap

Sovrascrittura dei File

Il comando **tcpdump** sovrascrive il file **httpdump.pcap** ad ogni nuova esecuzione. Questo significa che conserverai solo l'ultima cattura effettuata. Assicurati di analizzare il file prima di avviare una nuova cattura per evitare di perdere i dati precedenti.

Conferma della Cattura

Al termine della cattura, il terminale mostrerà un messaggio di conferma indicando il numero di pacchetti raccolti. Questo ti permette di verificare che la cattura sia stata eseguita correttamente.

Conclusioni sull'Analisi HTTP

- Il protocollo HTTP trasmette i dati senza cifratura, esponendo le credenziali a eventuali attacchi di sniffing in rete locale.
- Anche su siti apparentemente sicuri, l'uso di HTTP rappresenta un grave rischio di sicurezza.
- **Wireshark** è uno strumento potente per dimostrare concretamente l'importanza dell'uso di **HTTPS** per la protezione dei dati sensibili.

Ora, confronteremo questi risultati con l'analisi del traffico HTTPS.

Lab 2: Analisi del Traffico HTTPS

L'obiettivo è dimostrare che, durante la navigazione su un sito HTTPS, i dati sensibili trasmessi non sono leggibili in chiaro grazie alla cifratura end-to-end.

Setup Iniziale per l'Analisi HTTPS

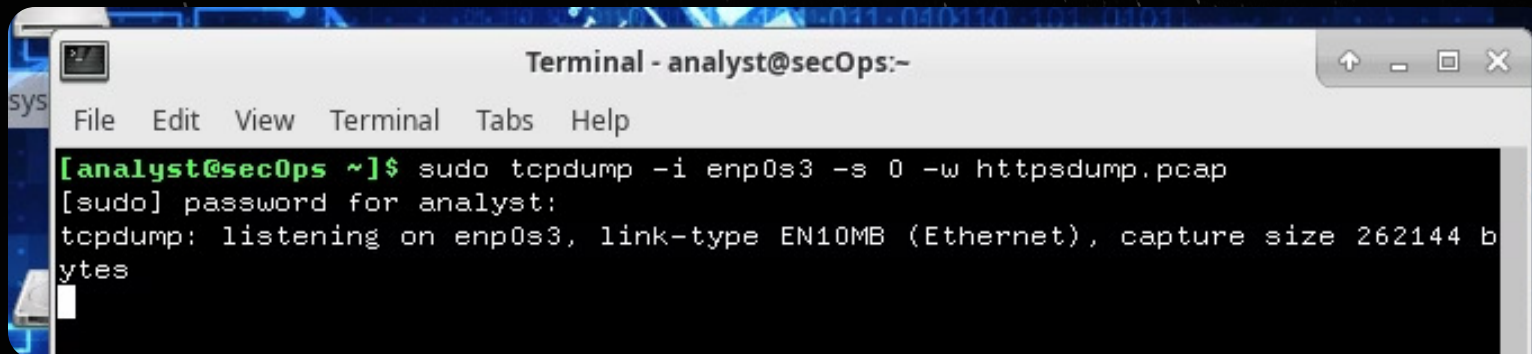
Configurazione dell'Ambiente

Come nel laboratorio precedente, utilizzeremo la VM CyberOps Workstation e l'interfaccia **enp0s3**. Assicurati che l'interfaccia sia attiva e configurata correttamente.

Avvio della Cattura HTTPS

Per catturare il traffico HTTPS, esegui il seguente comando **tcpdump**:

```
sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
```

A screenshot of a terminal window titled "Terminal - analyst@secOps:-". The terminal shows the command `sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap` being entered. The prompt `[analyst@secOps ~]` is visible. Below the command, the output shows `[sudo] password for analyst:` followed by `tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes`. The terminal window has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help".

```
Terminal - analyst@secOps:-
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Questo comando catturerà tutto il traffico sull'interfaccia **enp0s3** e lo salverà nel file **httpsdump.pcap**.

Navigazione HTTPS e Generazione di Traffico Cifrato

Visita al Sito HTTPS

Visita il sito <https://www.netacad.com>. Questo sito utilizza HTTPS, garantendo la crittografia dei dati trasmessi.

Simulazione di Inserimento Dati

Inserisci un'email fittizia nel campo di login per generare traffico reale cifrato via TLS. Non è necessario completare il login, l'obiettivo è solo generare traffico cifrato.

← Go back

Welcome!

Please login to your account.



Invalid username or email.

Email

picciopasticcio@tempmail.com

Analisi del Traffico HTTPS con Wireshark

Applicazione del Filtro

Filter:		tcp.port == 443		Expression...		Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info		
241	77.863110	34.120.5.221	192.168.1.12	TLSv1.2	135	Application Data		
242	77.863887	34.120.5.221	192.168.1.12	TLSv1.2	2866	Server Hello, Certificate		
243	77.863900	192.168.1.12	34.120.5.221	TCP	66	46442 → 443 [ACK] Seq=20		
244	77.864005	34.120.5.221	192.168.1.12	TLSv1.2	301	Server Key Exchange, Serve		
245	77.864012	192.168.1.12	34.120.5.221	TCP	66	46442 → 443 [ACK] Seq=20		
246	77.867236	192.168.1.12	34.120.5.221	TLSv1.2	159	Client Key Exchange, Chang		
250	77.898218	34.120.5.221	192.168.1.12	TLSv1.2	377	New Session Ticket, Change		
251	77.898265	34.120.5.221	192.168.1.12	TLSv1.2	135	Application Data		
252	77.903032	34.120.5.221	192.168.1.12	TCP	135	TCP Retransmission 1.443 →		
253	77.903053	192.168.1.12	34.120.5.221	TCP	78	46444 → 443 [ACK] Seq=20		
263	77.938568	192.168.1.12	34.120.5.221	TCP	66	46442 → 443 [ACK] Seq=20		
271	77.959029	34.120.5.221	192.168.1.12	TLSv1.2	135	TCP Spurious Retransmissi		
272	77.959035	192.168.1.12	34.120.5.221	TCP	78	TCP Dup ACK 263#114644		
273	77.997599	192.168.1.12	34.120.5.221	TLSv1.2	243	Application Data		
274	77.998687	192.168.1.12	34.120.5.221	TLSv1.2	313	Application Data		
275	77.999023	192.168.1.12	34.120.5.221	TLSv1.2	104	Application Data		
277	78.001021	192.168.1.12	34.120.5.221	TLSv1.2	260	Application Data		

Apri il file **httpsdump.pcap** in Wireshark. Applica il filtro **tcp.port == 443** per visualizzare solo il traffico HTTPS (porta 443 è la porta standard per HTTPS).

Protocollo TLS e Dati Cifrati

▶ [SEQ/ACK analysis]
▼ [Timestamps]
[Time since first frame in this TCP stream: 0.158880000 seconds]
[Time since previous frame in this TCP stream: 0.020461000 seconds]
TCP payload (69 bytes)
▼ Secure Sockets Layer
▼ TLSv1.2 Record Layer: Application Data Protocol: http2
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 64
Encrypted Application Data: 000000000000000199403910f20d68e9467b0206224119a...

I pacchetti identificati mostrano l'utilizzo del protocollo **TLSv1.2** e traffico criptato. Analizzando i dettagli dei pacchetti, noterai che il payload contiene **Encrypted Application Data**. A differenza del traffico HTTP, nessun contenuto del form (es. email) è visibile in chiaro. Il payload è completamente cifrato.

Conclusioni e Confronto HTTP vs HTTPS

Aspetto	HTTP	HTTPS
Visibilità dati	Visibili in chiaro (username, password)	Cifrati (Encrypted Application Data)
Sicurezza	Nessuna	Protetto da TLS
Wireshark può leggere contenuto?	✓ Sì	✗ No

Questo esperimento dimostra in modo pratico l'importanza di utilizzare **HTTPS** per proteggere i dati sensibili in transito. La cifratura offerta da HTTPS rende i dati illeggibili a eventuali intercettatori, garantendo la riservatezza delle informazioni scambiate tra il client e il server.