

## S11 L5 - Analisi avanzate: Un approccio pratico - Lab 2

### 10.6.7 Lab – Utilizzo di Wireshark per esaminare il traffico HTTP e HTTPS (risposte)

#### Obiettivi

---

- **Parte 1: Cattura e visualizza il traffico HTTP**
- **Parte 2: Cattura e visualizza il traffico HTTPS**

#### Parte 1: Cattura e visualizza il traffico HTTP

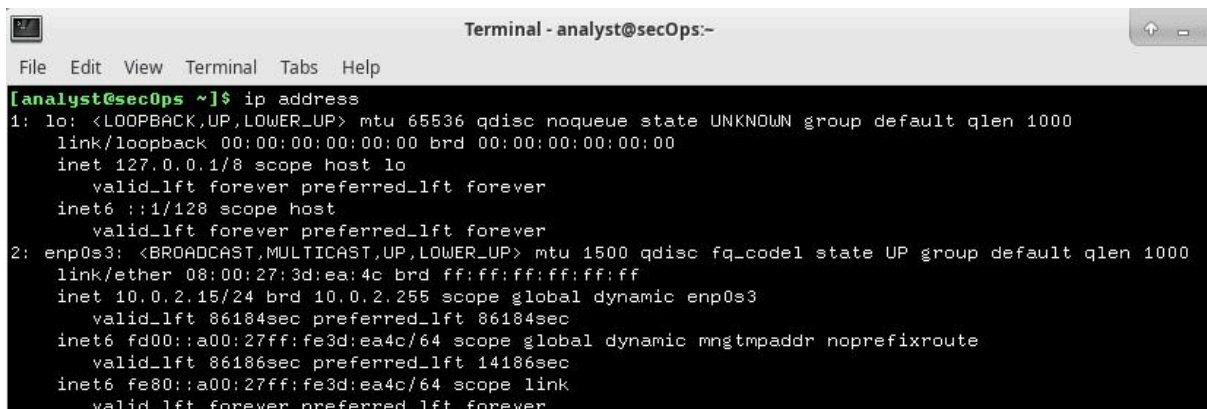
In questa parte, utilizzerai tcpdump per catturare il contenuto del traffico HTTP. Utilizzerai le opzioni di comando per salvare il traffico in un file di cattura dei pacchetti (pcap). Questi record possono quindi essere analizzati utilizzando diverse applicazioni che leggono i file pcap, tra cui Wireshark.

#### Passaggio 1: avviare la macchina virtuale ed effettuare l'accesso.

Avviare la VM CyberOps Workstation.

#### Passaggio 2: aprire un terminale e avviare tcpdump.

Aprire un'applicazione terminale e immettere il comando [ip address](#).



```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ 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  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:3d:ea:4c brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3  
        valid_lft 86184sec preferred_lft 86184sec  
    inet6 fd00::a00:27ff:fe3d:ea4c/64 scope global dynamic mngtmpaddr noprefixroute  
        valid_lft 86186sec preferred_lft 14186sec  
    inet6 fe80::a00:27ff:fe3d:ea4c/64 scope link  
        valid_lft forever preferred_lft forever
```

**Elencare le interfacce e i relativi indirizzi IP visualizzati nell'output dell'indirizzo IP .**

enp0s3 con 10.0.2.15/24 e lo con 127.0.0.1

Mentre sei nell'applicazione terminale, inserisci il comando **sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap**.

```
[analyst@sec0ps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

L' **-i** opzione command consente di specificare l'interfaccia.

L' **-s** opzione command specifica la lunghezza dello snapshot per ogni pacchetto. Impostando snaplen su 0 lo imposti al valore predefinito di 262144.

L' **-w** opzione command viene utilizzata per scrivere il risultato del comando tcpdump in un file.

Aprire un browser Web dalla barra di avvio all'interno della VM CyberOps Workstation. Andare su <http://www.altoromutual.com/login.jsp>

Inserisci il nome utente **Admin** e la password **Admin** e fai clic su **Accedi**



Ritornare alla finestra del terminale in cui è in esecuzione tcpdump. Digitare **CTRL+C** per interrompere la cattura del pacchetto.

```
[analyst@sec0ps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C1798 packets captured
1798 packets received by filter
0 packets dropped by kernel
```


### Passaggio 3: visualizzare l'acquisizione HTTP.

Il tcpdump, eseguito nel passaggio precedente, ha stampato l'output in un file denominato httpdump.pcap.

Fare clic sull'icona File Manager sul desktop e andare alla cartella home dell'analista utente . Fare doppio clic sul file httpdump.pcap, nella finestra di dialogo Apri con scorrere fino a Wireshark e quindi fare clic su Apri .



Nell'applicazione Wireshark, filtra per http e fai clic su Applica .

Filter:	<input type="text" value="http"/>		Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info
9	0.060264	10.0.2.15	34.107.221.82	HTTP	342	GET /success.txt HTTP/1.1
11	0.081600	34.107.221.82	10.0.2.15	HTTP	270	HTTP/1.1 200 OK (text/plain)
53	2.326306	10.0.2.15	95.100.181.18	OCSP	485	Request
57	2.328176	10.0.2.15	95.100.181.18	OCSP	485	Request
59	2.349057	95.100.181.18	10.0.2.15	OCSP	943	Response
61	2.351912	95.100.181.18	10.0.2.15	OCSP	943	Response
160	2.835177	10.0.2.15	95.100.181.18	OCSP	485	Request

Nella finestra inferiore viene visualizzato il messaggio. Espandi la sezione **HTML Form URL Encoded**

1033	7.523073	216.58.204.131	10.0.2.15	OCSP	756	Response
1156	41.821239	10.0.2.15	65.61.137.117	HTTP	589	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
1160	41.986294	65.61.137.117	10.0.2.15	HTTP	299	HTTP/1.1 302 Found

▼ HTML Form URL Encoded: application/x-www-form-urlencoded
▶ Form item: "uid" = "admin"
▶ Form item: "passw" = "admin"
▶ Form item: "btnSubmit" = "Login"

**Quali due informazioni vengono visualizzate?**

L'UID e password dell'amministratore

## Parte 2: Cattura e visualizza il traffico HTTPS

Ora utilizzerai tcpdump dalla riga di comando di una workstation Linux per catturare il traffico HTTPS. Dopo aver avviato tcpdump, genererai traffico HTTPS mentre tcpdump registra il contenuto del traffico di rete. Questi record saranno nuovamente analizzati utilizzando Wireshark.

**Passaggio 1: avviare tcpdump da un terminale.**

a. Mentre sei nell'applicazione terminale, immetti il comando **sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap**. Immetti la password cyberops per l'analista utente quando richiesto.

Questo comando avvierà tcpdump e registrerà il traffico di rete sull'interfaccia enp0s3 della workstation Linux..

Tutto il traffico registrato verrà stampato nel file httpsdump.pcap nella directory home dell'analista utente.

```
[analyst@sec0ps ~]$ 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
```

Ho dovuto aggiornare il giorno e l'ora con il seguente comando, cambiando il giorno e l'ora correnti.

```
[analyst@sec0ps ~]$ sudo date -s "31 JANUARY 2025 11:41:30"  
Fri Jan 31 11:41:30 EST 2025
```

Aprire un browser Web dalla barra di avvio all'interno della VM CyberOps Workstation. Andare su [www.netacad.com](http://www.netacad.com).



Ritornare alla finestra del terminale in cui è in esecuzione tcpdump. Digitare **CTRL+C** per interrompere la cattura del pacchetto.

Fare clic sull'icona File Manager sul desktop e andare alla cartella home dell'analista utente. Fare doppio clic sul file **httpsdump.pcap**, nella finestra di dialogo Apri con scorrere fino a Wireshark e quindi fare clic su **Apri**.



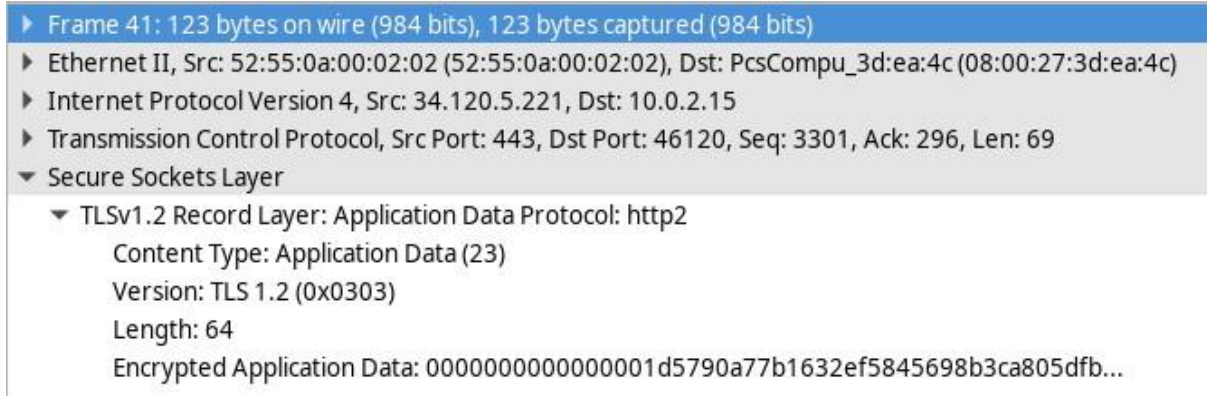
httpsdump.pcap

Nell'applicazione Wireshark, espandere verticalmente la finestra di acquisizione e quindi filtrare in base al traffico HTTPS tramite la porta 443.

Immetti **tcp.port==443**

No.	Time	Source	Destination	Protocol	Length	Info
39	2.764396	34.120.5.221	10.0.2.15	TLSv1.2	123	Application Data
40	2.775019	34.120.5.221	10.0.2.15	TLSv1.2	365	New Session Ticket, C
41	2.776622	34.120.5.221	10.0.2.15	TLSv1.2	123	Application Data

Nella finestra inferiore viene visualizzato il messaggio



**Cosa noti riguardo all'URL del sito web?**

Si è aggiunta la sezione Secure Sockets Layer.

### Domande di riflessione

---

**Quali sono i vantaggi dell'utilizzo di HTTPS anziché HTTP?**

Quando si utilizza HTTPS, il carico di dati di un messaggio viene crittografato

**Tutti i siti web che utilizzano HTTPS sono considerati affidabili?**

No, perché anche i siti web dannosi possono utilizzare HTTPS.