Utilizzo di Wireshark per Analizzare il Traffico HTTP e HTTPS

Utilizzo di Wireshark per Analizzare il Traffico HTTP e HTTPS

Parte 1: Cattura e Analisi del Traffico HTTP

Passo 1: Avvio della macchina virtuale e accesso

Ho avviato la CyberOps Workstation VM e ho effettuato l'accesso con le credenziali fornite:

- **Username**: analyst
- **Password**: cyberops

Passo 2: Avvio di tcpdump

- Ho aperto un terminale ed eseguito il comando ip address per identificare le interfacce di rete disponibili. Ho trovato:
  - **enp0s3**: con IP 10.0.2.15
  - **lo**: con IP 127.0.0.1

```
[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 08:00:27:6d:a9:71 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 86161sec preferred_lft 86161sec
    inet6 fd00::a00:27ff:fe6d:a971/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86163sec preferred_lft 14163sec
    inet6 fe80::a00:27ff:fe6d:a971/64 scope link
       valid_lft forever preferred_lft forever
```

- Successivamente, ho avviato tcpdump per catturare il traffico HTTP:

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

  Ho inserito la password richiesta e il comando ha iniziato a registrare il traffico sulla mia interfaccia di rete.

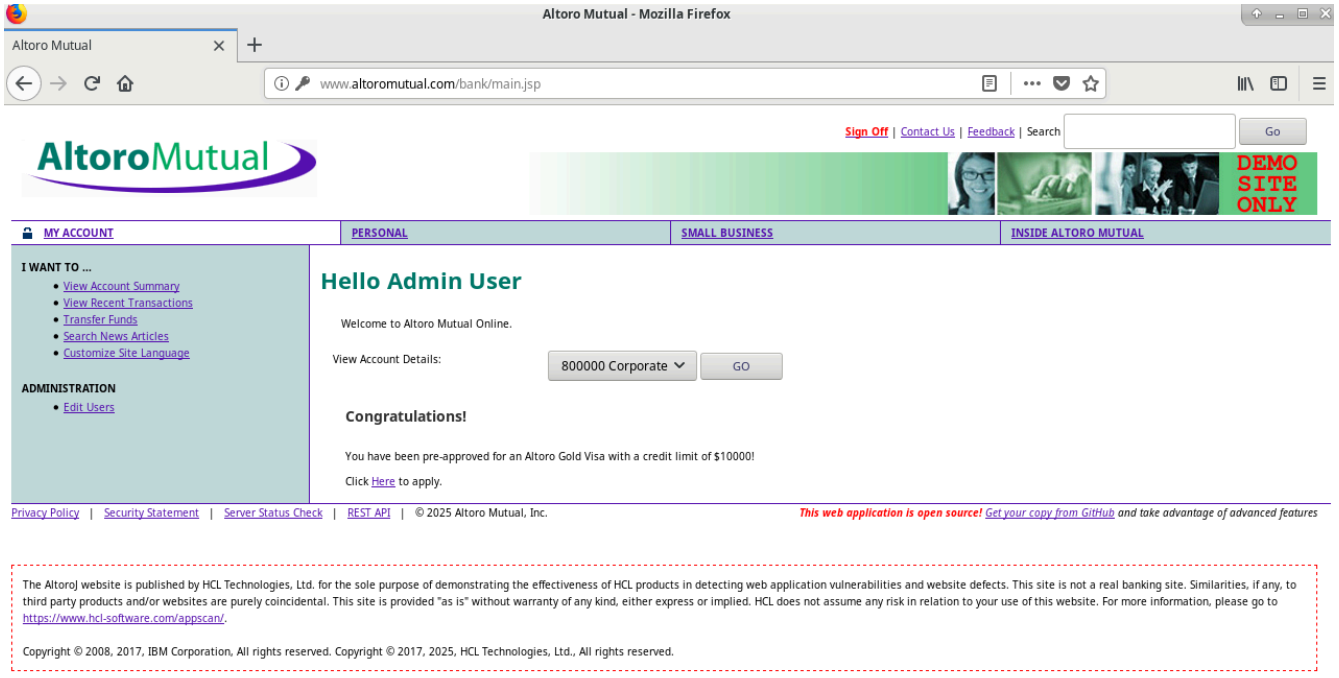
```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Passo 3: Generazione di traffico HTTP

- Ho aperto un browser e visitato il sito web http://www.altoromutual.com/login.jsp. Poiché utilizza HTTP, i dati non sono crittografati. Ho inserito:

  Username: Admin

Password: Admin

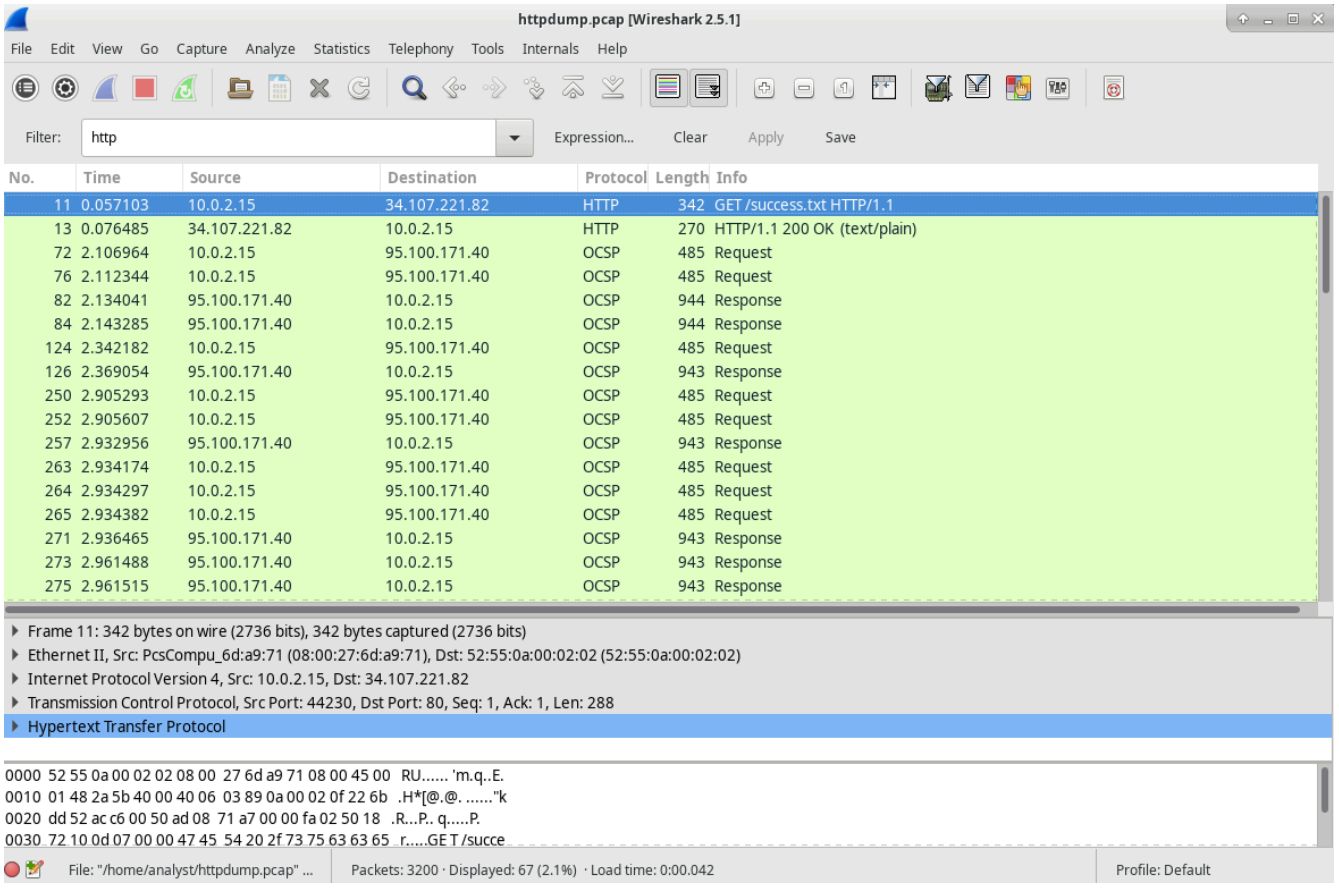


- Dopo aver effettuato l'accesso, ho chiuso il browser e interrotto la cattura dei pacchetti con CTRL+C.

```
[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 bytes
^C3200 packets captured
3200 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$
```

Passo 4: Analisi del traffico HTTP con Wireshark

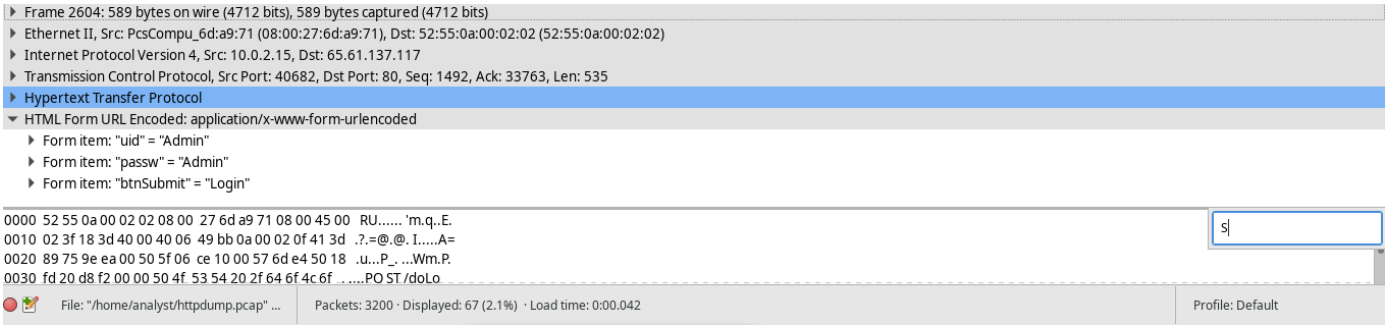
- Ho aperto il file httpdump.pcap con Wireshark e applicato il filtro http. Scorrendo tra i pacchetti, ho individuato un messaggio POST, e nella sezione HTML Form URL Encoded, ho trovato i dati in chiaro:



uid: Admin

passw: Admin

Questa dimostrazione evidenzia la vulnerabilità dell'HTTP, in quanto trasmette credenziali senza protezione.



Parte 2: Cattura e Analisi del Traffico HTTPS

Passo 1: Avvio di tcpdump

- Ho avviato una nuova cattura di pacchetti HTTPS con il comando:

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

Passo 2: Generazione di traffico HTTPS

Ho aperto un browser e visitato https://www.netacad.com. L'URL mostrava il lucchetto, segno della crittografia attiva. Ho effettuato l'accesso inserendo le credenziali NetAcad e poi ho chiuso il browser.

```
[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
^C4826 packets captured
4826 packets received by filter
0 packets dropped by kernel
```

Passo 3: Analisi del traffico HTTPS con Wireshark

- Ho aperto il file httpsdump.pcap in Wireshark, applicando il filtro:
  `tcp.port==443`

Scorrendo i pacchetti, ho trovato un messaggio Application Data. A differenza di HTTP, qui la sezione HTTP è stata sostituita da TLS 1.2, dimostrando che il traffico è crittografato. Espandendo la sezione Secure Sockets Layer, ho verificato che il payload dell'applicazione risultava illeggibile, confermando l'uso della crittografia TLS.