

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@sec0ps ~]$ 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.

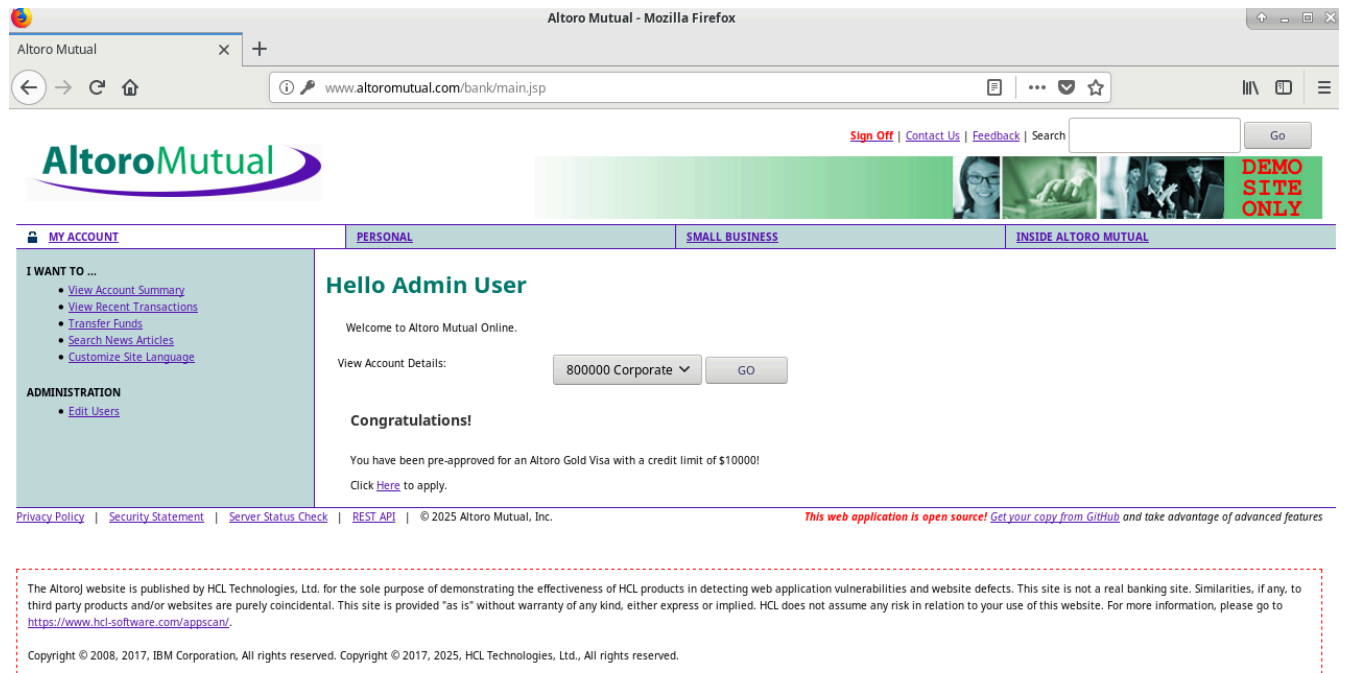
```
[analyst@sec0ps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

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:

httpdump.pcap [Wireshark 2.5.1]						
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help						
Filter: http Expression... Clear Apply Save						
No.	Time	Source	Destination	Protocol	Length	Info
11	0.057103	10.0.2.15	34.107.221.82	HTTP	342	GET /success.txt HTTP/1.1
13	0.076485	34.107.221.82	10.0.2.15	HTTP	270	HTTP/1.1 200 OK (text/plain)
72	2.106964	10.0.2.15	95.100.171.40	OCSP	485	Request
76	2.112344	10.0.2.15	95.100.171.40	OCSP	485	Request
82	2.134041	95.100.171.40	10.0.2.15	OCSP	944	Response
84	2.143285	95.100.171.40	10.0.2.15	OCSP	944	Response
124	2.342182	10.0.2.15	95.100.171.40	OCSP	485	Request
126	2.369054	95.100.171.40	10.0.2.15	OCSP	943	Response
250	2.905293	10.0.2.15	95.100.171.40	OCSP	485	Request
252	2.905607	10.0.2.15	95.100.171.40	OCSP	485	Request
257	2.932956	95.100.171.40	10.0.2.15	OCSP	943	Response
263	2.934174	10.0.2.15	95.100.171.40	OCSP	485	Request
264	2.934297	10.0.2.15	95.100.171.40	OCSP	485	Request
265	2.934382	10.0.2.15	95.100.171.40	OCSP	485	Request
271	2.936465	95.100.171.40	10.0.2.15	OCSP	943	Response
273	2.961488	95.100.171.40	10.0.2.15	OCSP	943	Response
275	2.961515	95.100.171.40	10.0.2.15	OCSP	943	Response

▶ Frame 11: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)

▶ Ethernet II, Src: PcsCompu_6d:a9:71 (08:00:27:6d:a9:71), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)

▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.107.221.82

▶ Transmission Control Protocol, Src Port: 44230, Dst Port: 80, Seq: 1, Ack: 1, Len: 288

▶ Hypertext Transfer Protocol

```

0000 52 55 0a 00 02 02 08 00 27 6d a9 71 08 00 45 00  RU.....'m.q..E.
0010 01 48 2a 5b 40 00 40 06 03 89 0a 00 02 0f 22 6b  .H*[@. ...."k
0020 dd 52 ac c6 00 50 ad 08 71 a7 00 00 fa 02 50 18  .R...P. q.....P
0030 72 10 0d 07 00 00 47 45 54 20 2f 73 75 63 63 65  r....GET/succe

```

File: "/home/analyst/httpdump.pcap" ... Packets: 3200 · Displayed: 67 (2.1%) · Load time: 0:00.042 Profile: Default

uid: Admin

passw: Admin

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

▶ Frame 2604: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits)	
▶ Ethernet II, Src: PcsCompu_6d:a9:71 (08:00:27:6d:a9:71), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)	
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 65.61.137.117	
▶ Transmission Control Protocol, Src Port: 40682, Dst Port: 80, Seq: 1492, Ack: 33763, Len: 535	
▶ Hypertext Transfer Protocol	
HTML Form URL Encoded: application/x-www-form-urlencoded	
▶ Form item: "uid" = "Admin"	
▶ Form item: "passw" = "Admin"	
▶ Form item: "btnSubmit" = "Login"	

```

0000 52 55 0a 00 02 02 08 00 27 6d a9 71 08 00 45 00  RU.....'m.q..E.
0010 02 3f 18 3d 40 00 40 06 49 bb 0a 00 02 0f 41 3d  .?=@. I.....A=
0020 89 75 9e ea 00 50 5f 06 ce 10 00 57 6d e4 50 18  ....P. ...Wm.P
0030 fd 20 d8 f2 00 00 50 4f 53 54 20 2f 64 6f 4c 6f  ....PO ST/doLo

```

File: "/home/analyst/httpdump.pcap" ... Packets: 3200 · Displayed: 67 (2.1%) · Load time: 0:00.042 Profile: Default

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

[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

```

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.

```
▶ Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
▶ Ethernet II, Src: PcsCompu_82:75:df (08:00:27:82:75:df), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 104.16.248.249
▶ Transmission Control Protocol, Src Port: 52556, Dst Port: 443, Seq: 1, Ack: 1, Len: 56
▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 51
    Encrypted Application Data: 7fa9037731c6e38e6213aacc15a0a7281f94046fdb237be9...
```