

Relazione su HTTP

Relazione su HTTP

🔖 Tag: [#http](#) [#tcpdump](#) [#wireshark](#) [#tls](#) [#cybersecurity](#)

Introduzione

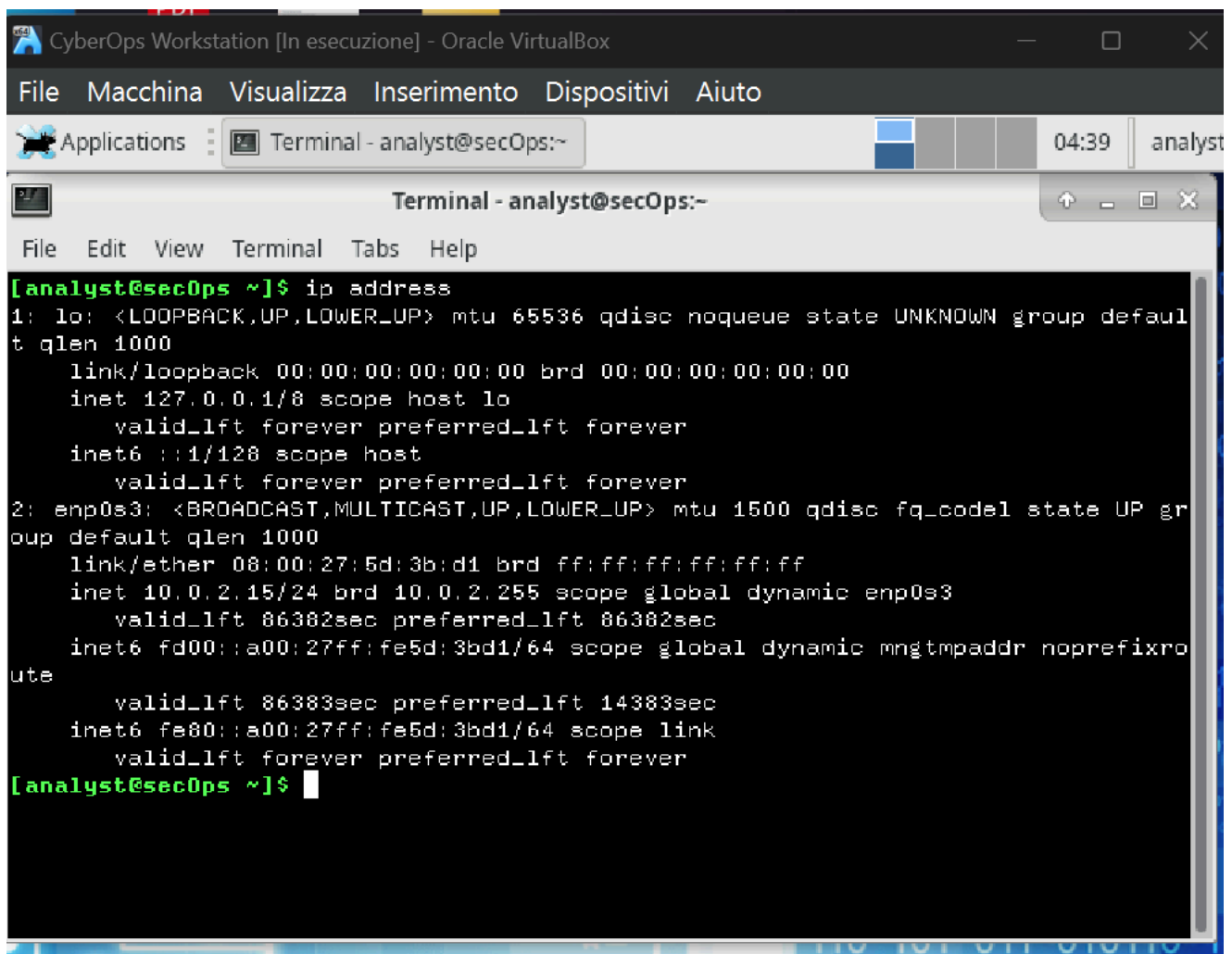
Durante l'analisi di rete eseguita su una macchina, è stato catturato del traffico HTTP e HTTPS. Le immagini mostrano l'utilizzo di **tcpdump** per l'acquisizione dei pacchetti e **Wireshark** per l'analisi dettagliata del traffico. Questo documento offre una descrizione dettagliata delle richieste HTTP e delle connessioni HTTPS catturate e analizzate.

Dettagli dell'analisi

1. Configurazione dell'indirizzo IP

- **Comando eseguito:** `ip address`
- Mostra l'indirizzo IP della macchina: 10.0.2.15, con configurazione IPv4 e IPv6 attiva.
- Interfaccia attiva: enp0s3

🔖 Tag: [#ip_address](#) [#network_config](#)



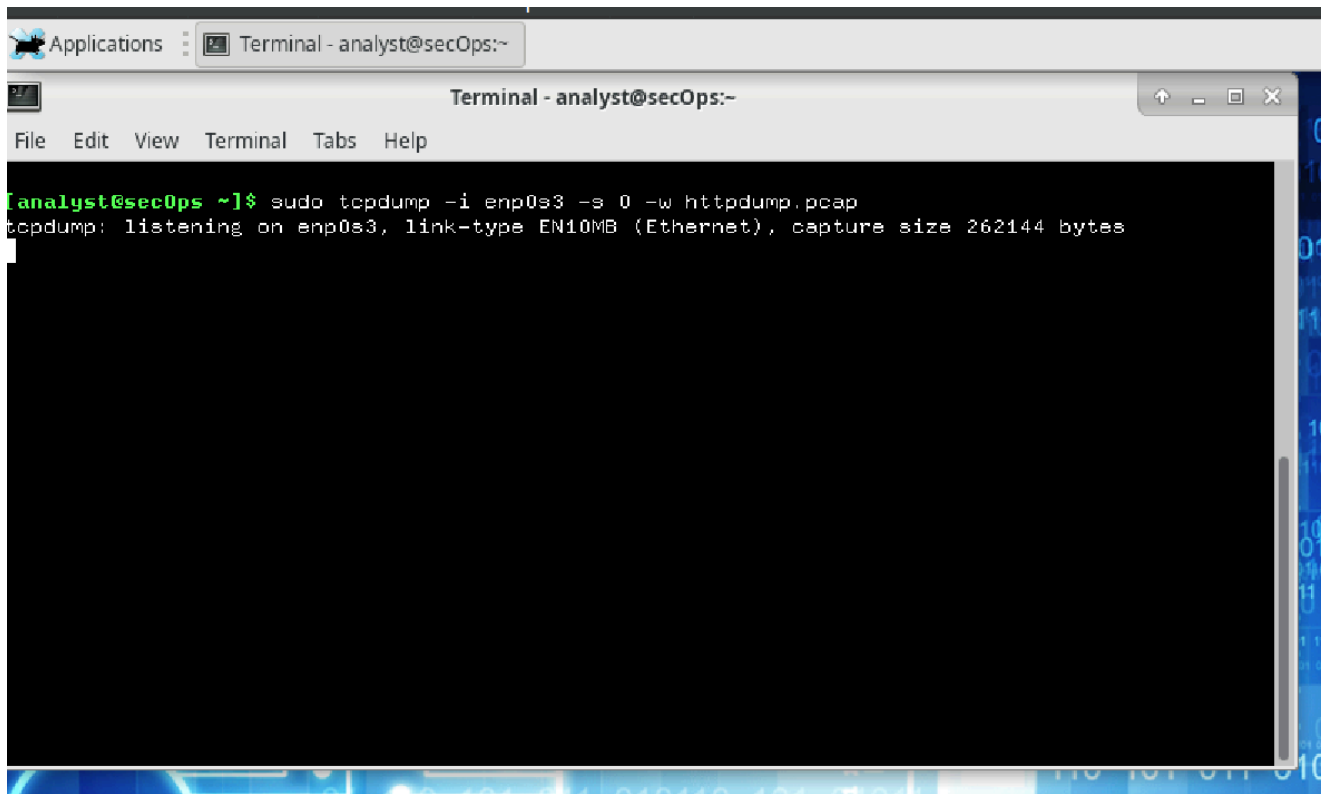
The screenshot shows a terminal window titled "Terminal - analyst@secOps:~" within a "CyberOps Workstation [In esecuzione] - Oracle VirtualBox" environment. The terminal displays the output of the command `ip address`. It shows details for the loopback interface `lo` (127.0.0.1) and the ethernet interface `enp0s3` (10.0.2.15). The `enp0s3` interface is in the "UP" state and has a MAC address of `08:00:27:5d:3b:d1`. The terminal output is as follows:

```
[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 08:00:27:5d:3b:d1 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86382sec preferred_lft 86382sec
    inet6 fd00::a00:27ff:fe5d:3bd1/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86383sec preferred_lft 14383sec
    inet6 fe80::a00:27ff:fe5d:3bd1/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

2. Acquisizione del traffico HTTP con tcpdump

- **Comando eseguito:** `sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap`
- L'acquisizione dei pacchetti è stata effettuata con tcpdump sull'interfaccia `enp0s3` e salvata nel file `httpdump.pcap`. Sono stati catturati 8666 pacchetti senza perdite.

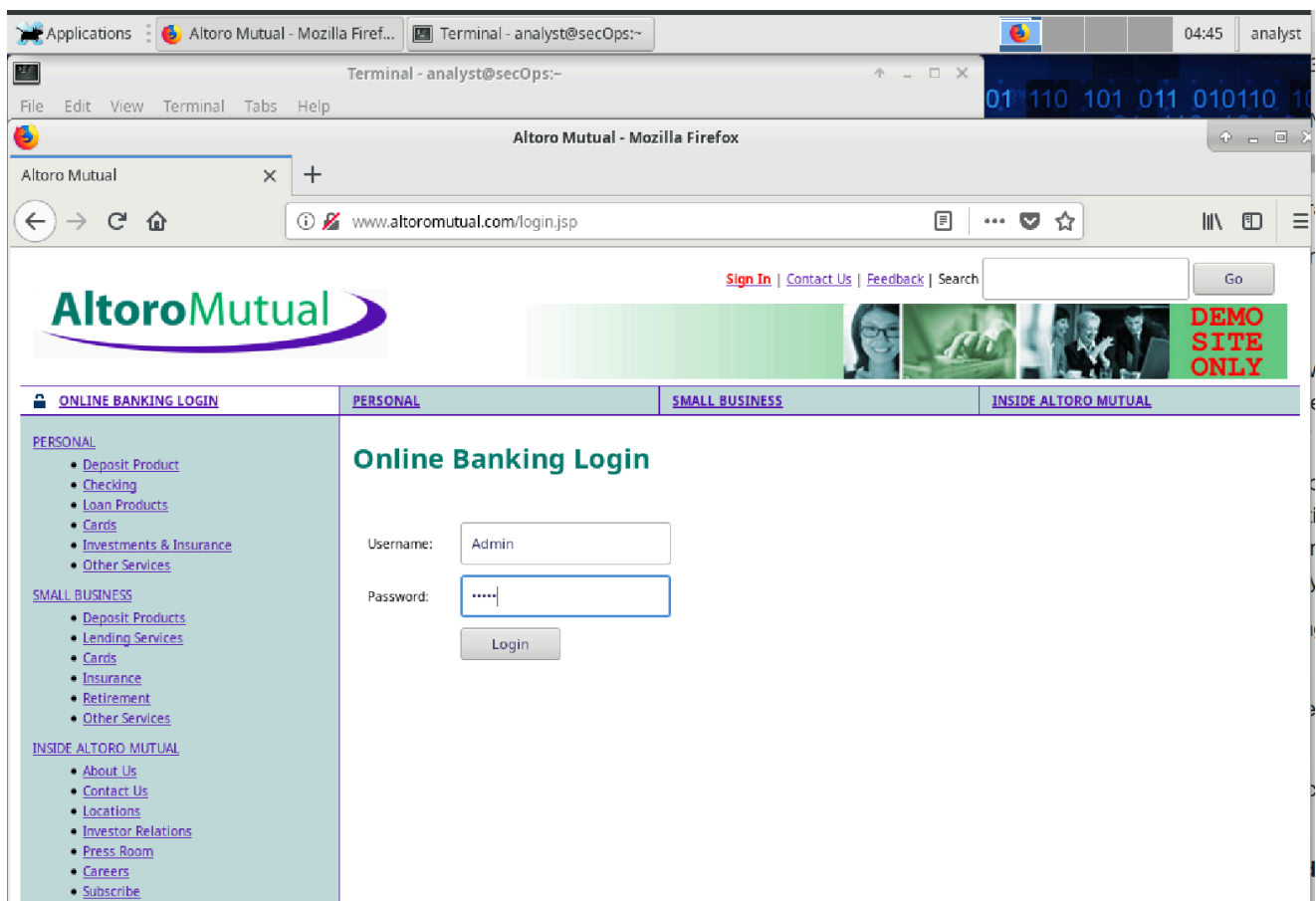
🌟 Tag: [#tcpdump](#) [#pcap_capture](#)



3. Tentativo di login al sito Altoro Mutual

- Durante la sessione di login al sito, è stato inserito lo username "Admin" con una password.
- Il traffico HTTP generato è stato catturato da tcpdump.

🌸 Tag: [#http_login](#) [#web_traffic](#)



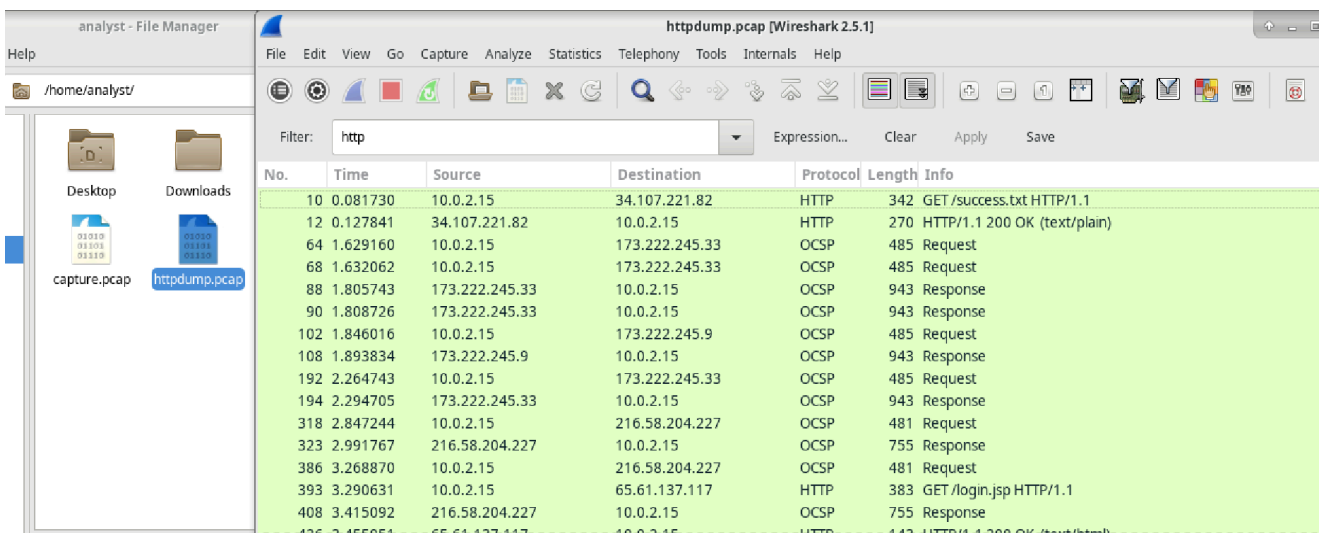
4. Analisi del traffico HTTP con Wireshark

- **File analizzato:** httpdump.pcap
- L'analisi di Wireshark ha mostrato richieste **GET** e **POST**. Tra queste, vi è stata una richiesta POST che includeva le credenziali inserite nel form di login.

🔖 Tag: #wireshark #http_analysis

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

[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C8642 packets captured
8656 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$
```



No.	Time	Source	Destination	Protocol	Length	Info
10	0.081730	10.0.2.15	34.107.221.82	HTTP	342	GET /success.txt HTTP/1.1
12	0.127841	34.107.221.82	10.0.2.15	HTTP	270	HTTP/1.1 200 OK (text/plain)
64	1.629160	10.0.2.15	173.222.245.33	OCSP	485	Request
68	1.632062	10.0.2.15	173.222.245.33	OCSP	485	Request
88	1.805743	173.222.245.33	10.0.2.15	OCSP	943	Response
90	1.808726	173.222.245.33	10.0.2.15	OCSP	943	Response
102	1.846016	10.0.2.15	173.222.245.9	OCSP	485	Request
108	1.893834	173.222.245.9	10.0.2.15	OCSP	943	Response
192	2.264743	10.0.2.15	173.222.245.33	OCSP	485	Request
194	2.294705	173.222.245.33	10.0.2.15	OCSP	943	Response
318	2.847244	10.0.2.15	216.58.204.227	OCSP	481	Request
323	2.991767	216.58.204.227	10.0.2.15	OCSP	755	Response
386	3.268870	10.0.2.15	216.58.204.227	OCSP	481	Request
393	3.290631	10.0.2.15	65.61.137.117	HTTP	383	GET /login.jsp HTTP/1.1
408	3.415092	216.58.204.227	10.0.2.15	OCSP	755	Response
426	3.455051	65.61.137.117	10.0.2.15	HTTP	142	HTTP/1.1 200 OK (text/html)

5. Analisi del traffico HTTPS

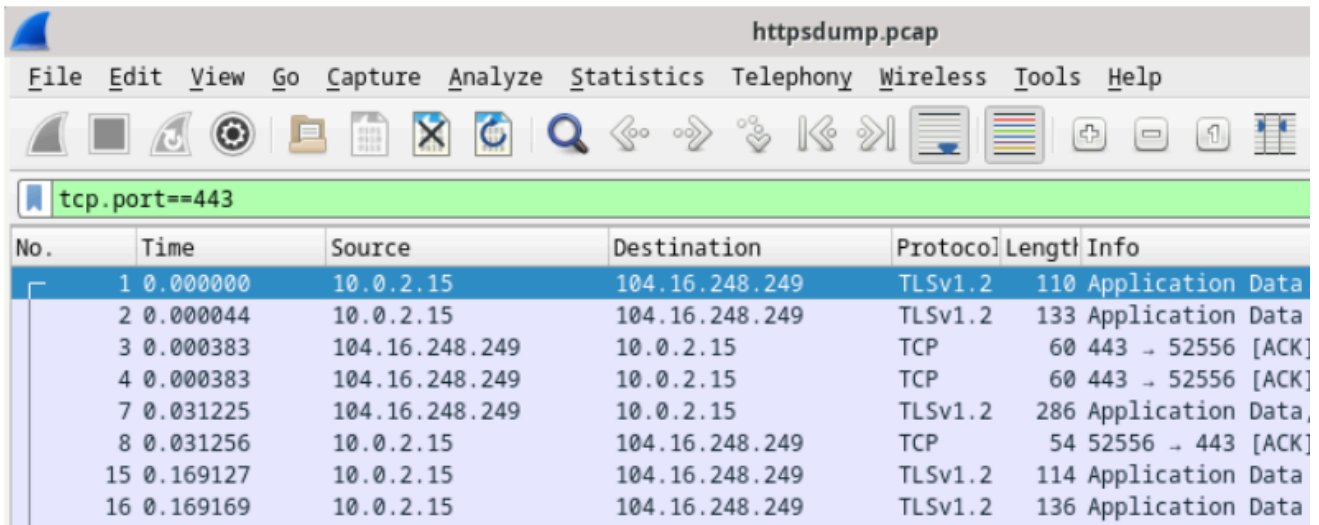
- **Filtro applicato:** `tcp.port==443`
- Pacchetti TLSv1.2 (HTTPS) sono stati catturati e analizzati. Il traffico era cifrato, quindi i dati non erano visibili in chiaro.
- Nell'ultima immagine, è mostrato un pacchetto TLSv1.2 con dati applicativi cifrati.

🔖 Tag: [#https](#) [#tls_encryption](#) [#wireshark](#)

6. Dettagli del pacchetto TLS

- L'ultima immagine mostra un pacchetto cifrato su HTTPS (porta 443). La connessione avviene tra la macchina locale (IP 10.0.2.15) e il server remoto (104.16.248.249).
- Il traffico mostra dati applicativi cifrati tramite **TLSv1.2**.

🔖 Tag: [#tls_traffic](#) [#encrypted_traffic](#) [#wireshark](#)



The image shows a Wireshark capture of a file named 'httpsdump.pcap'. The filter bar at the top displays 'tcp.port==443'. The packet list table below shows several packets, with packets 1, 2, 7, 15, and 16 being TLSv1.2 Application Data. Packets 3, 4, and 8 are TCP ACKs from 104.16.248.249 to 10.0.2.15.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.15	104.16.248.249	TLSv1.2	110	Application Data
2	0.000044	10.0.2.15	104.16.248.249	TLSv1.2	133	Application Data
3	0.000383	104.16.248.249	10.0.2.15	TCP	60	443 → 52556 [ACK]
4	0.000383	104.16.248.249	10.0.2.15	TCP	60	443 → 52556 [ACK]
7	0.031225	104.16.248.249	10.0.2.15	TLSv1.2	286	Application Data
8	0.031256	10.0.2.15	104.16.248.249	TCP	54	52556 → 443 [ACK]
15	0.169127	10.0.2.15	104.16.248.249	TLSv1.2	114	Application Data
16	0.169169	10.0.2.15	104.16.248.249	TLSv1.2	136	Application Data

Conclusione

L'analisi del traffico HTTP e HTTPS catturato tramite **tcpdump** e analizzato con **Wireshark** ha permesso di esaminare le richieste HTTP in chiaro e il traffico HTTPS cifrato. Mentre le richieste HTTP mostravano le credenziali inviate durante il login, le connessioni HTTPS erano cifrate e i dati non potevano essere letti senza decifratura.

```
▶ 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...
```

Chiavi:

[http, tcpdump, wireshark, tls, cybersecurity]