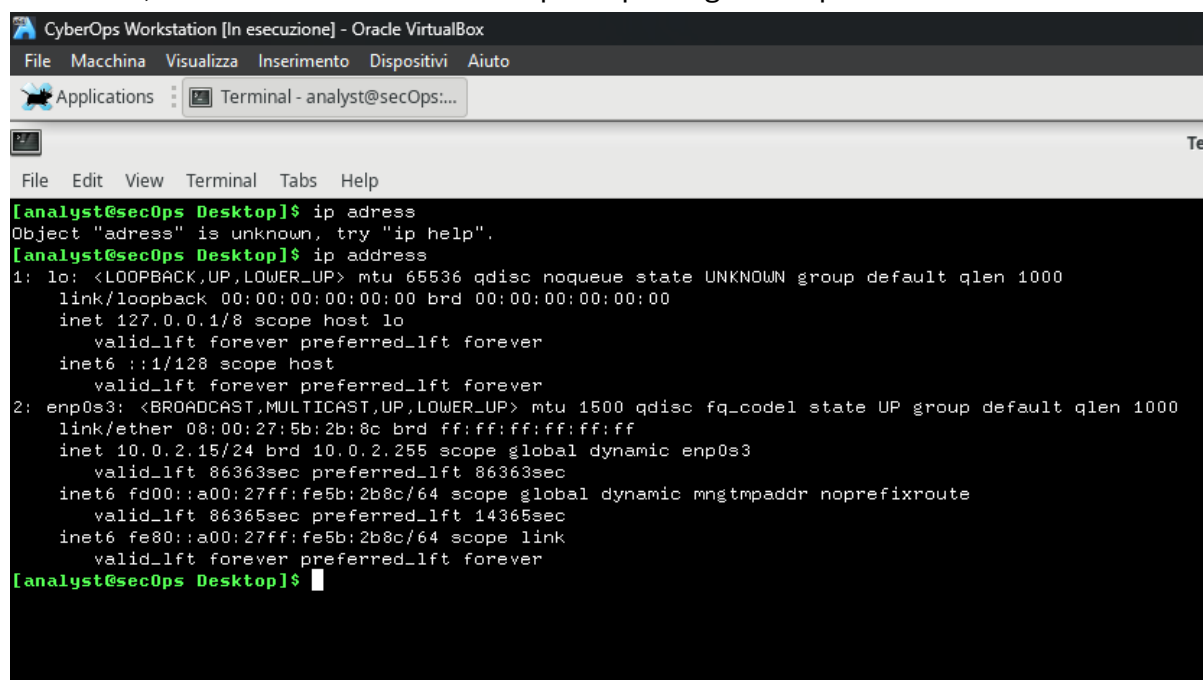


## HTTP/S TRAFFIC

Per prima cosa accediamo alla macchina virtuale CyberOps Workstation e apriamo un terminale, verifichiamo che l'indirizzo ip sia quello giusto e possiamo cominciare.



```
CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
Applications  Terminal - analyst@secOps:...

File  Edit  View  Terminal  Tabs  Help

[analyst@secOps Desktop]$ ip address
Object "adress" is unknown, try "ip help".
[analyst@secOps Desktop]$ 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 08:00:27:5b:2b:8c brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86363sec preferred_lft 86363sec
    inet6 fd00::a00:27ff:fe5b:2b8c/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86365sec preferred_lft 14365sec
    inet6 fe80::a00:27ff:fe5b:2b8c/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps Desktop]$
```

Per avviare tcpdump eseguiamo questo comando **"sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap"** dove:

- **-i**: Consente di specificare l'interfaccia, nel caso in cui non la specifichiamo tcpdump catturerà tutto il traffico su tutte le interfacce.
- **-s**: Specifica la lunghezza dello snapshot per ciascun pacchetto, si dovrebbe limitare snaplen al numero più piccolo che catturerà le informazioni sul protocollo a cui sei interessato. Impostando snaplen su 0 lo imposta sul valore predefinito di 262144, per renderlo compatibile con le versioni precedenti e recenti di tcpdump.
- **-w**: Questo comando viene utilizzato per scrivere il risultato del comando tcpdump in un file. L'aggiunta dell'estensione .pcap garantisce che i sistemi operativi e le applicazioni saranno in grado di leggere i file. Tutto il traffico registrato verrà stampato nel file httpdump.pcap nella directory home dell'analista utente.

Apriamo il browser e navighiamo su <http://www.altoromutual.com/login.jsp>, eseguiamo l'accesso e terminiamo la scansione con il comando CTRL+C. Andiamo ad aprire il file con Wireshark e esaminiamolo, aprendo la voce "HTML Form URL Encoded: application/x-www-form-urlencoded" vedremo l'username e la password.

479	12.743955	142.250.180.131	10.0.2.15	TCP	60	ITCP Keep-Alive ACK! 80 → 43872 (ACK! Seq=1403 Ack=855 Win=65535 Len=0)
480	14.124154	10.0.2.15	65.61.137.117	HTTP	589	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
481	14.124437	65.61.137.117	10.0.2.15	TCP	60	80 → 54310 (ACK! Seq=15920 Ack=1219 Win=65535 Len=0)
482	14.291655	65.61.137.117	10.0.2.15	HTTP	318	HTTP/1.1 302 Found
483	14.291672	10.0.2.15	65.61.137.117	TCP	54	54310 → 80 (ACK! Seq=1219 Ack=16184 Win=63360 Len=0)
484	14.294335	10.0.2.15	65.61.137.117	HTTP	609	GET /bank/main.jsp HTTP/1.1
485	14.294552	65.61.137.117	10.0.2.15	TCP	60	80 → 54310 (ACK! Seq=16184 Ack=1774 Win=65535 Len=0)
486	14.435760	65.61.137.117	10.0.2.15	TCP	4194	80 → 54310 (PSH, ACK! Seq=16184 Ack=1774 Win=65535 Len=4140 (TCP segment of a reassembled PDU))
487	14.435785	10.0.2.15	65.61.137.117	TCP	54	54310 → 80 (ACK! Seq=1774 Ack=20324 Win=64800 Len=0)
488	14.436163	65.61.137.117	10.0.2.15	TCP	1434	80 → 54310 (PSH, ACK! Seq=20324 Ack=1774 Win=65535 Len=1380 (TCP segment of a reassembled PDU))
489	14.437005	65.61.137.117	10.0.2.15	HTTP	982	HTTP/1.1 200 OK (text/html)
490	14.437013	10.0.2.15	65.61.137.117	TCP	54	54310 → 80 (ACK! Seq=1774 Ack=22632 Win=64800 Len=0)
▶ Frame 480: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits) ▶ Ethernet II, Src: PcsCompu_5b:2b:8c (08:00:27:5b:2b:8c), 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: 54310, Dst Port: 80, Seq: 684, Ack: 15920, Len: 535 ▶ Hypertext Transfer Protocol ▼ HTML Form URL Encoded: application/x-www-form-urlencoded ▶ Form item: "uid" = "admin" ▶ Form item: "passwd" = "admin" ▶ Form item: "btnSubmit" = "Login"						

Per quanto riguarda invece l'HTTPS il risultato è ben diverso, eseguiamo tcpdump e questa volta entriamo su [www.netacad.com](http://www.netacad.com) tenendo la registrazione accesa. Facciamo l'accesso, interrompiamo tcpdump e andiamolo ad analizzare.

```

▶ 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...
```

Come possiamo notare questa volta i nostri dati sono criptati e quindi non visibili.