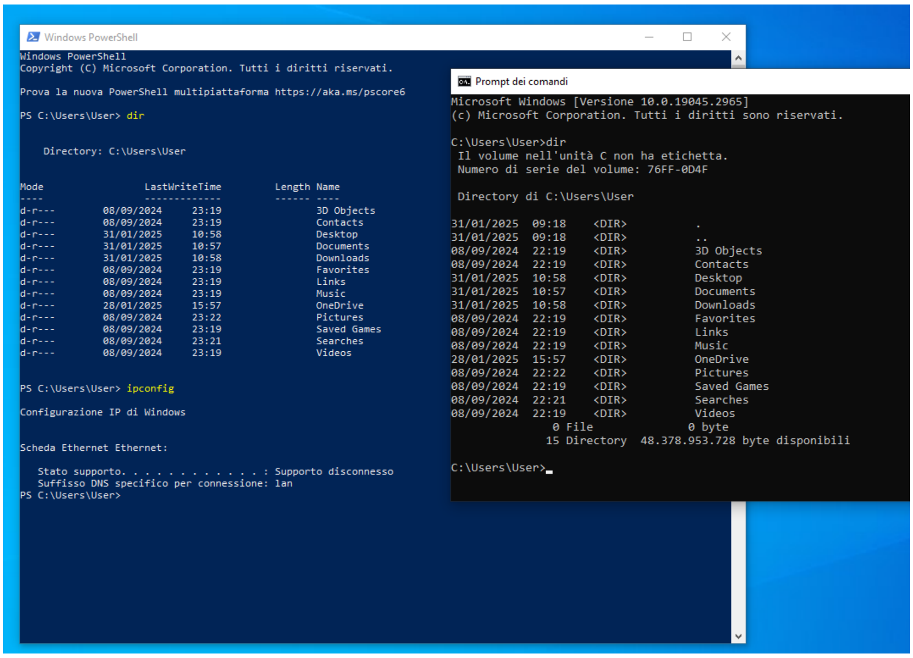
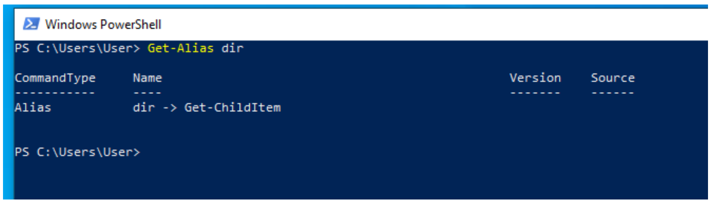
Progetto S11L5

1. In questo laboratorio ho utilizzato qualche comando della powershell di windows

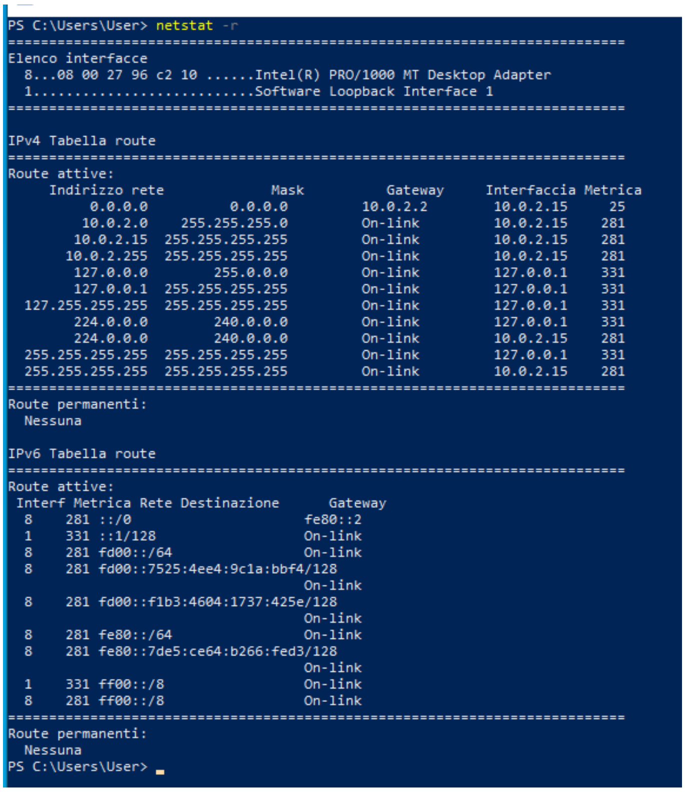


```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Prova la nuova PowerShell multipiattaforma https://aka.ms/pscore6

PS C:\Users\User> dir


    Directory: C:\Users\User


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        08/09/2024     23:19                3D Objects
d-r---        08/09/2024     23:19                Contacts
d-r---        31/01/2025     10:58                Desktop
d-r---        31/01/2025     10:57                Documents
d-r---        31/01/2025     10:58                Downloads
d-r---        08/09/2024     23:19                Favorites
d-r---        08/09/2024     23:19                Links
d-r---        08/09/2024     23:19                Music
d-r---        28/01/2025     15:57                OneDrive
d-r---        08/09/2024     23:22                Pictures
d-r---        08/09/2024     23:19                Saved Games
d-r---        08/09/2024     23:21                Searches
d-r---        08/09/2024     23:19                Videos


PS C:\Users\User> ipconfig

Configurazione IP di Windows


Scheda Ethernet Ethernet:

   Stato supporto. . . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione: lan
PS C:\Users\User>
```

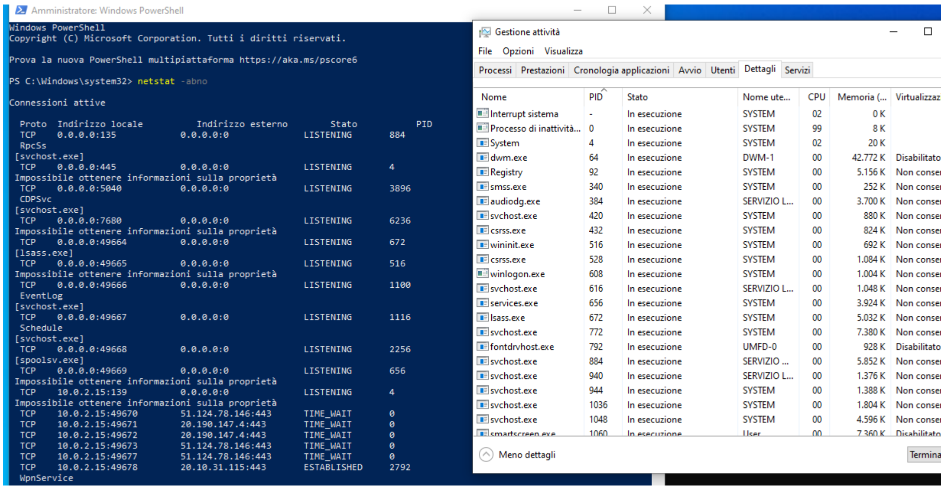
```
Microsoft Windows [Versione 10.0.19045.2965]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\User>dir
 Il volume nell'unità C non ha etichetta.
 Numero di serie del volume: 76FF-0D4F

 Directory di C:\Users\User

31/01/2025  09:18    <DIR>          .
31/01/2025  09:18    <DIR>          ..
08/09/2024  22:19    <DIR>          3D Objects
08/09/2024  22:19    <DIR>          Contacts
31/01/2025  10:58    <DIR>          Desktop
31/01/2025  10:57    <DIR>          Documents
31/01/2025  10:58    <DIR>          Downloads
08/09/2024  22:19    <DIR>          Favorites
08/09/2024  22:19    <DIR>          Links
08/09/2024  22:19    <DIR>          Music
28/01/2025  15:57    <DIR>          OneDrive
08/09/2024  22:22    <DIR>          Pictures
08/09/2024  22:19    <DIR>          Saved Games
08/09/2024  22:21    <DIR>          Searches
08/09/2024  22:19    <DIR>          Videos
               0 File              0 byte
              15 Directory  48.378.953.728 byte disponibili

C:\Users\User>
```



```
PS C:\Users\User> Get-Alias dir

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Alias           dir -> Get-ChildItem


PS C:\Users\User>
```

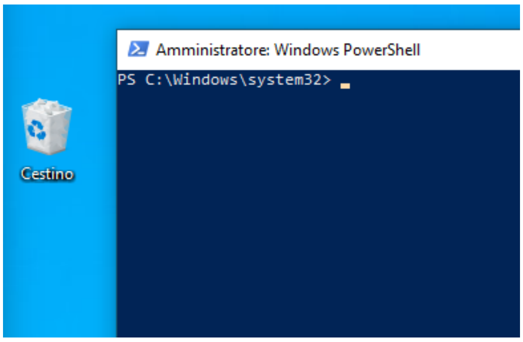


```
PS C:\Users\User> netstat -r
===========================================================================
Elenco interfacce
  8...08 00 27 96 c2 10 ......Intel(R) PRO/1000 MT Desktop Adapter
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Tabella route
===========================================================================
Route attive:
     Indirizzo rete                 Mask          Gateway     Interfaccia Metrica
          0.0.0.0          0.0.0.0         10.0.2.2        10.0.2.15     25
         10.0.2.0    255.255.255.0         On-link         10.0.2.15    281
        10.0.2.15  255.255.255.255         On-link         10.0.2.15    281
       10.0.2.255  255.255.255.255         On-link         10.0.2.15    281
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link         10.0.2.15    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link         10.0.2.15    281
===========================================================================
Route permanenti:
  Nessuna

IPv6 Tabella route
===========================================================================
Route attive:
 Interf Metrica Rete Destinazione      Gateway
  8    281 ::/0                     fe80::2
  1    331 ::1/128                  On-link
  8    281 fd00::/64                On-link
  8    281 fd00::7525:4ee4:9c1a:bbf4/128
                                    On-link
  8    281 fd00::f1b3:4604:1737:425e/128
                                    On-link
  8    281 fe80::/64                On-link
  8    281 fe80::7de5:ce64:b266:fed3/128
                                    On-link
  1    331 ff00::/8                 On-link
  8    281 ff00::/8                 On-link
===========================================================================
Route permanenti:
  Nessuna
PS C:\Users\User>
```

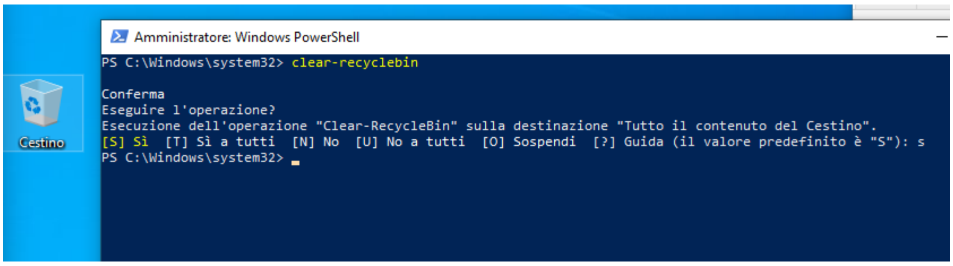


```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Prova la nuova PowerShell multipiattaforma https://aka.ms/pscore6

PS C:\Windows\system32> netstat -abno

Connessioni attive

  Proto  Indirizzo locale          Indirizzo esterno        Stato           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       884
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       3896
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       6236
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       672
 [lsass.exe]
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       516
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1100
  EventLog
 [svchost.exe]
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1116
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       2256
 [spoolsv.exe]
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       656
 Impossibile ottenere informazioni sulla proprietà
  TCP    10.0.2.15:139          0.0.0.0:0              LISTENING       4
 Impossibile ottenere informazioni sulla proprietà
  TCP    10.0.2.15:49670        51.124.78.146:443      TIME_WAIT       0
  TCP    10.0.2.15:49671        20.190.147.4:443       TIME_WAIT       0
  TCP    10.0.2.15:49672        20.190.147.4:443       TIME_WAIT       0
  TCP    10.0.2.15:49673        51.124.78.146:443      TIME_WAIT       0
  TCP    10.0.2.15:49677        51.124.78.146:443      TIME_WAIT       0
  TCP    10.0.2.15:49678        20.10.31.115:443       ESTABLISHED     2792
  WpnService
```

Nome	PID	Stato	Nome ute...	CPU	Memoria (...	Virtualizzaz
Interrupt sistema	-	In esecuzione	SYSTEM	02	0 K	
Processo di inattività...	0	In esecuzione	SYSTEM	99	8 K	
System	4	In esecuzione	SYSTEM	02	20 K	
dwm.exe	64	In esecuzione	DWM-1	00	42.772 K	Disabilitato
Registry	92	In esecuzione	SYSTEM	00	5.156 K	Non conse
smss.exe	340	In esecuzione	SYSTEM	00	252 K	Non conse
audiodg.exe	384	In esecuzione	SERVIZIO L...	00	3.700 K	Non conse
svchost.exe	420	In esecuzione	SYSTEM	00	880 K	Non conse
csrss.exe	432	In esecuzione	SYSTEM	00	824 K	Non conse
wininit.exe	516	In esecuzione	SYSTEM	00	692 K	Non conse
csrss.exe	528	In esecuzione	SYSTEM	00	1.084 K	Non conse
winlogon.exe	608	In esecuzione	SYSTEM	00	1.004 K	Non conse
svchost.exe	616	In esecuzione	SERVIZIO L...	00	1.048 K	Non conse
services.exe	656	In esecuzione	SYSTEM	00	3.924 K	Non conse
lsass.exe	672	In esecuzione	SYSTEM	00	5.032 K	Non conse
svchost.exe	772	In esecuzione	SYSTEM	00	7.380 K	Non conse
fontdrvhost.exe	792	In esecuzione	UMFD-0	00	928 K	Disabilitato
svchost.exe	884	In esecuzione	SERVIZIO ...	00	5.852 K	Non conse
svchost.exe	940	In esecuzione	SERVIZIO L...	00	1.376 K	Non conse
svchost.exe	944	In esecuzione	SYSTEM	00	1.388 K	Non conse
svchost.exe	1036	In esecuzione	SYSTEM	00	1.804 K	Non conse
svchost.exe	1048	In esecuzione	SYSTEM	00	4.596 K	Non conse
smartscreen.exe	1060	In esecuzione	User	00	7.360 K	Disabilitato



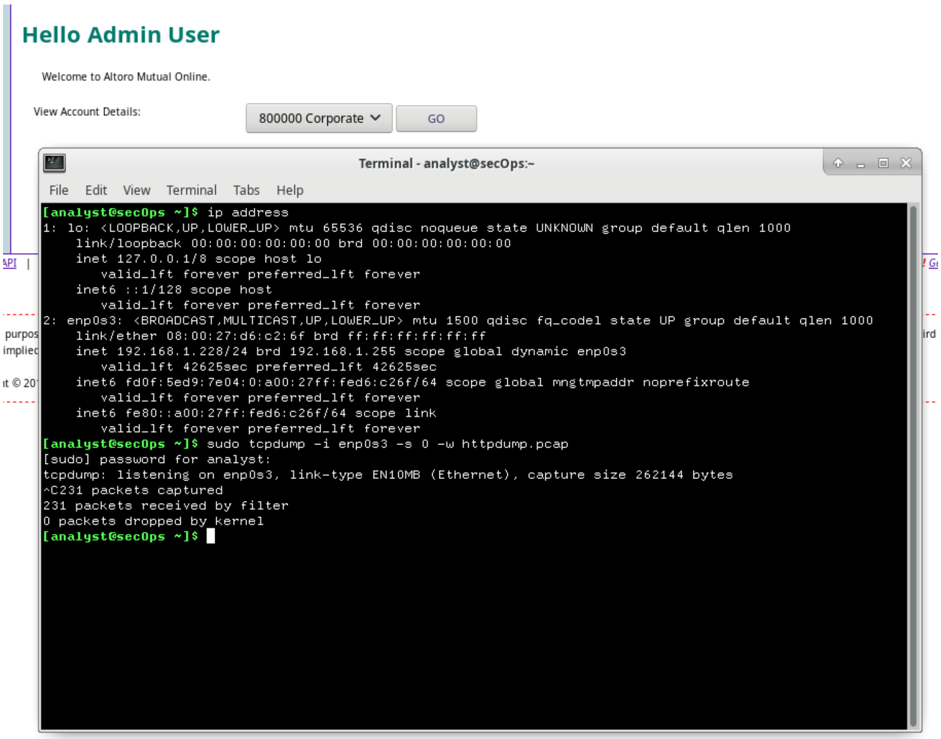
```
PS C:\Windows\system32> _
```



```
PS C:\Windows\system32> clear-recyclebin

Conferma
Eseguire l'operazione?
Esecuzione dell'operazione "Clear-RecycleBin" sulla destinazione "Tutto il contenuto del Cestino".
[S] Sì  [T] Sì a tutti  [N] No  [U] No a tutti  [O] Sospendi  [?] Guida (il valore predefinito è "S"): s
PS C:\Windows\system32> _
```

2. In questo laboratorio catturo il traffico di rete con wireshark per un sito http ed uno HTTPS

Catturo il traffico HTTP



Hello Admin User

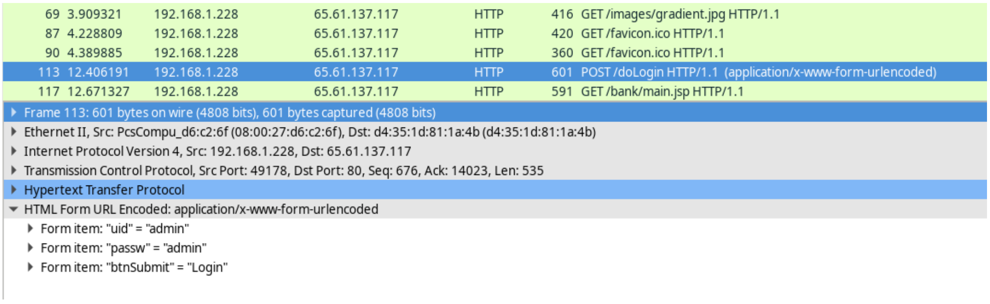
Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

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

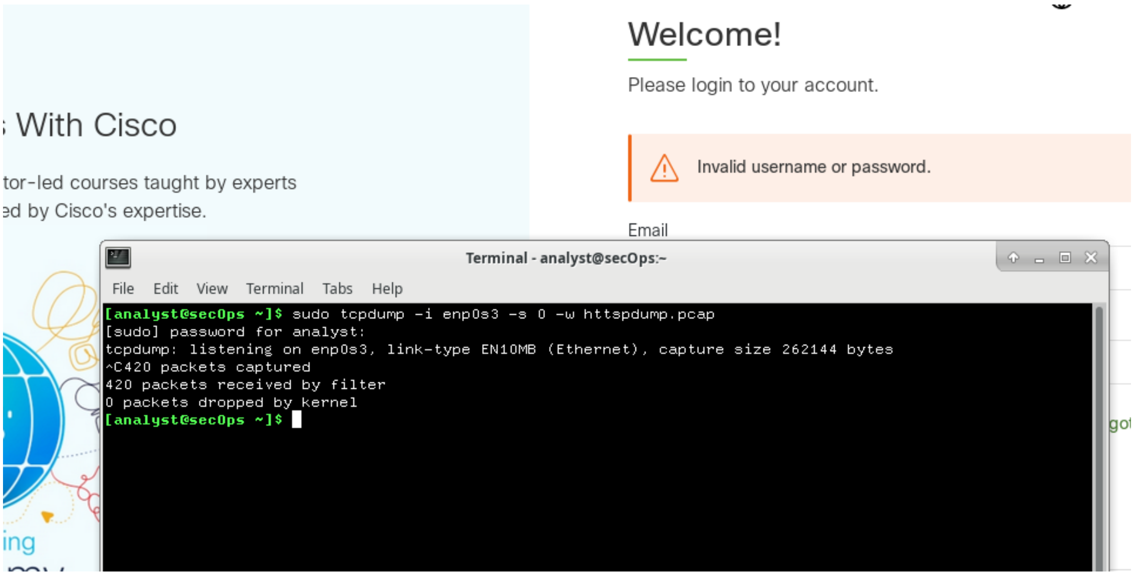
```
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       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:d6:c2:6f brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.228/24 brd 192.168.1.255 scope global dynamic enp0s3
       valid_lft 42625sec preferred_lft 42625sec
    inet6 fd0f:5ed9:7e04:0:a00:27ff:fed6:c26f/64 scope global mngtmpaddr noprefixroute
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed6:c26f/64 scope link
       valid_lft forever preferred_lft forever
[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
^C231 packets captured
231 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$
```

con wireshark trovo le credenziali di accesso



```
 69  3.909321   192.168.1.228   65.61.137.117   HTTP   416  GET /images/gradient.jpg HTTP/1.1
 87  4.228809   192.168.1.228   65.61.137.117   HTTP   420  GET /favicon.ico HTTP/1.1
 90  4.389885   192.168.1.228   65.61.137.117   HTTP   360  GET /favicon.ico HTTP/1.1
113 12.406191   192.168.1.228   65.61.137.117   HTTP   601  POST /doLogin HTTP/1.1  (application/x-www-form-urlencoded)
117 12.671327   192.168.1.228   65.61.137.117   HTTP   591  GET /bank/main.jsp HTTP/1.1

▸ Frame 113: 601 bytes on wire (4808 bits), 601 bytes captured (4808 bits)
▸ Ethernet II, Src: PcsCompu_d6:c2:6f (08:00:27:d6:c2:6f), Dst: d4:35:1d:81:1a:4b (d4:35:1d:81:1a:4b)
▸ Internet Protocol Version 4, Src: 192.168.1.228, Dst: 65.61.137.117
▸ Transmission Control Protocol, Src Port: 49178, Dst Port: 80, Seq: 676, Ack: 14023, 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"
```

Catturo il traffico HTTPS



With Cisco

tor-led courses taught by experts
ed by Cisco's expertise.

Welcome!

Please login to your account.

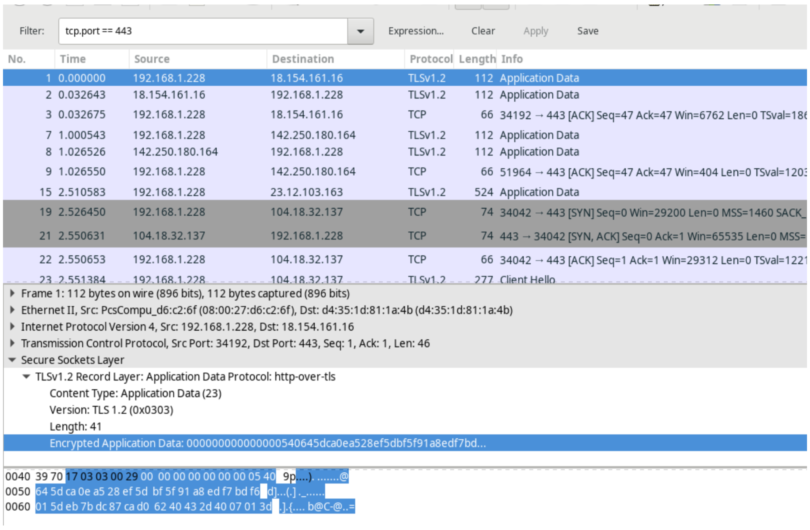
Invalid username or password.

Email

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

```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httspdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C420 packets captured
420 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$
```

Con wireshark vediamo che la connessione è criptata



Filter: tcp.port == 443

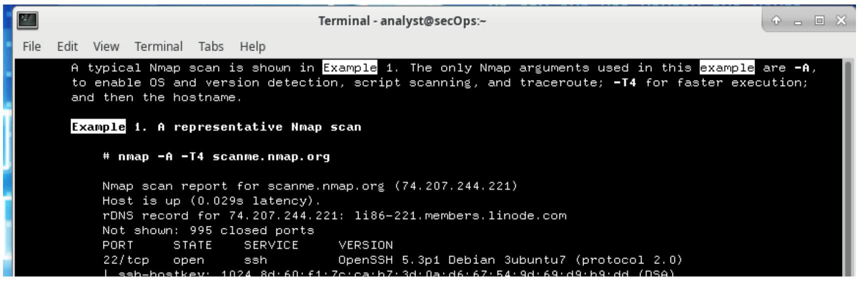
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.228	18.154.161.16	TLSv1.2	112	Application Data
2	0.032643	18.154.161.16	192.168.1.228	TLSv1.2	112	Application Data
3	0.032675	192.168.1.228	18.154.161.16	TCP	66	34192 → 443 [ACK] Seq=47 Ack=47 Win=6762 Len=0 TSval=18
7	1.000543	192.168.1.228	142.250.180.164	TLSv1.2	112	Application Data
8	1.026526	142.250.180.164	192.168.1.228	TLSv1.2	112	Application Data
9	1.026550	192.168.1.228	142.250.180.164	TCP	66	51964 → 443 [ACK] Seq=47 Ack=47 Win=404 Len=0 TSval=120
15	2.510583	192.168.1.228	23.12.103.163	TLSv1.2	524	Application Data
19	2.526450	192.168.1.228	104.18.32.137	TCP	74	34042 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_
21	2.550631	104.18.32.137	192.168.1.228	TCP	74	443 → 34042 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
22	2.550653	192.168.1.228	104.18.32.137	TCP	66	34042 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=122
23	2.551384	192.168.1.228	104.18.32.137	TLSv1.2	277	Client Hello

```
▸ Frame 1: 112 bytes on wire (896 bits), 112 bytes captured (896 bits)
▸ Ethernet II, Src: PcsCompu_d6:c2:6f (08:00:27:d6:c2:6f), Dst: d4:35:1d:81:1a:4b (d4:35:1d:81:1a:4b)
▸ Internet Protocol Version 4, Src: 192.168.1.228, Dst: 18.154.161.16
▸ Transmission Control Protocol, Src Port: 34192, Dst Port: 443, Seq: 1, Ack: 1, Len: 46
▾ Secure Sockets Layer
    ▾ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
          Content Type: Application Data (23)
          Version: TLS 1.2 (0x0303)
          Length: 41
          Encrypted Application Data: 0000000000000000540645dca0ea528ef5dbf5f91a8edf7bd...
```

```
0040  39 70 17 03 03 00 29 00  00 00 00 00 00 00 05 40   9p....). .......@
0050  64 5d ca 0e a5 28 ef 5d  bf 5f 91 a8 ed f7 bd f6   d]...(.] ._......
0060  01 5d eb 7b dc 87 ca d0  62 40 43 2d 40 07 01 3d   .].{.... b@C-@..=
```

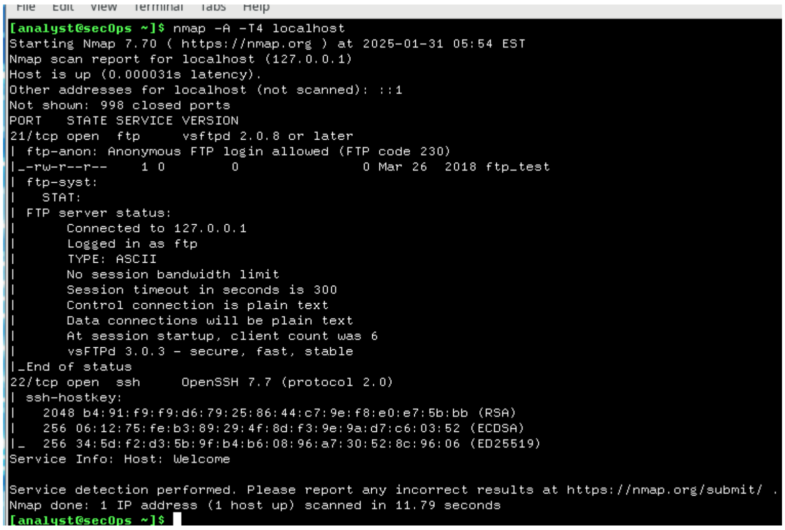
3. In questo laboratorio lavoriamo con nmap

Apro il manuale di nmap


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

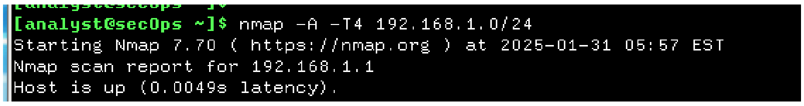
```
       A typical Nmap scan is shown in Example 1. The only Nmap arguments used in this example are -A,
       to enable OS and version detection, script scanning, and traceroute; -T4 for faster execution;
       and then the hostname.

       Example 1. A representative Nmap scan

           # nmap -A -T4 scanme.nmap.org

           Nmap scan report for scanme.nmap.org (74.207.244.221)
           Host is up (0.029s latency).
           rDNS record for 74.207.244.221: li86-221.members.linode.com
           Not shown: 995 closed ports
           PORT     STATE    SERVICE     VERSION
           22/tcp   open     ssh         OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
           | ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
```

scansiono la mia macchina e trovo delle porte aperte



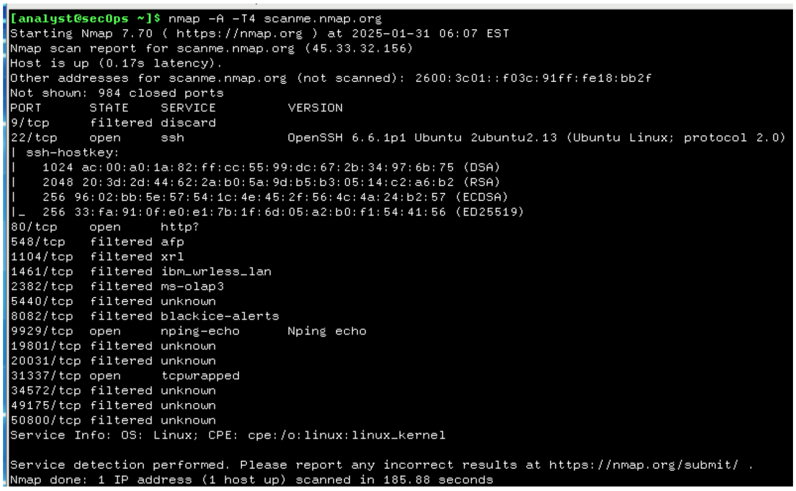
```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-01-31 05:54 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000031s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0               0 Mar 26  2018 ftp_test
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 127.0.0.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 6
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 b4:91:f9:f9:d6:79:25:86:44:c7:9e:f8:e0:e7:5b:bb (RSA)
|   256 06:12:75:fe:b3:89:29:4f:8d:f3:9e:9a:d7:c6:03:52 (ECDSA)
|_  256 34:5d:f2:d3:5b:9f:b4:b6:08:96:a7:30:52:8c:96:06 (ED25519)
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.79 seconds
[analyst@secOps ~]$
```

Con questo comando scansiono l'intera rete



```
[analyst@secOps ~]$
[analyst@secOps ~]$ nmap -A -T4 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2025-01-31 05:57 EST
Nmap scan report for 192.168.1.1
Host is up (0.0049s latency).
```

Con nmap possiamo scansionare anche siti web



```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-01-31 06:07 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.17s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 984 closed ports
PORT      STATE    SERVICE        VERSION
9/tcp     filtered discard
22/tcp    open     ssh            OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open     http?
548/tcp   filtered afp
1104/tcp  filtered xrl
1461/tcp  filtered ibm_wrless_lan
2382/tcp  filtered ms-olap3
5440/tcp  filtered unknown
8082/tcp  filtered blackice-alerts
9929/tcp  open     nping-echo     Nping echo
19801/tcp filtered unknown
20031/tcp filtered unknown
31337/tcp open     tcpwrapped
34572/tcp filtered unknown
49175/tcp filtered unknown
50800/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 185.88 seconds
```