

indice

CYBER SECURITY

Utilizzo di Windows PowerShell

Pg 2-7

Utilizzo di Wireshark per Esaminare il Traffico HTTP e HTTPS

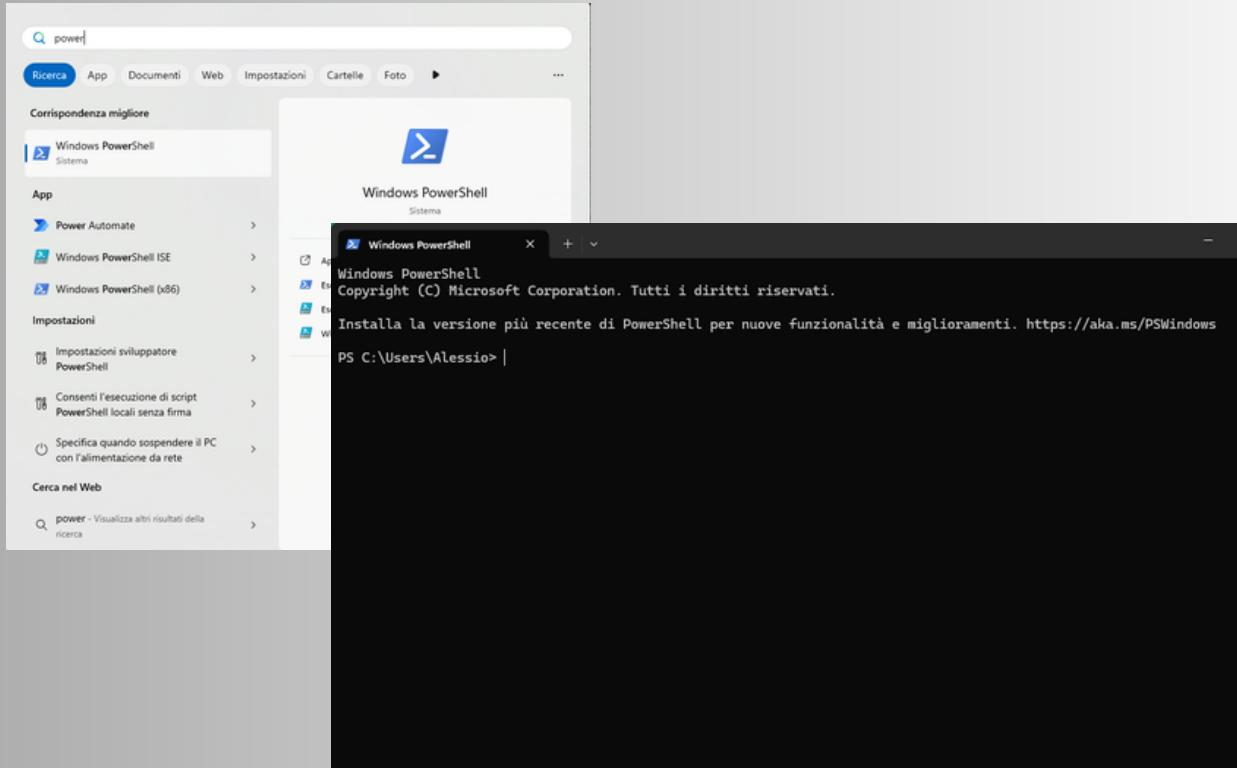
Pg 8-12

Esplorazione di Nmap

Pg 13-16

Utilizzo di Windows PowerShell

- Fai clic su Avvia. Cerca e seleziona PowerShell.
- Fai clic su Start. Cerca e seleziona il Prompt dei comandi.



- Immettere il comando **dir** al prompt (apre tutte le directory)
- Proviamo il comando **ping**

A screenshot of a Windows PowerShell window. The title bar says 'Windows PowerShell'. The command 'dir' is run, listing files in the current directory C:\Users\Alessio. The output shows a table with columns 'Mode', 'LastWriteTime', and 'Name'. The 'Name' column lists files like '.idlerc', '.insomniac', and several log files from May 2024. Below this, the command 'ping 8.8.8.8' is run, showing the results of the ping test. The output indicates four packets sent to 8.8.8.8 with a TTL of 115 and a response time of 18ms.

- Comando **Get-Alias** dir

Il comando Get-Alias in PowerShell serve a ottenere informazioni sugli alias configurati nel sistema. Un alias è un nome alternativo o abbreviato per un cmdlet o una funzione, creato per rendere più rapido o familiare l'utilizzo dei comandi. Quando esegui Get-Alias dir, PowerShell verifica e restituisce quale cmdlet si nasconde dietro l'alias dir. Nel caso specifico, l'alias dir è associato al cmdlet Get-ChildItem, che è utilizzato per elencare file e directory in una posizione specificata.

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

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

- Immettere per visualizzare le opzioni disponibili per il comando.**netstat -h**

1° Il comando netstat (Network Statistics) viene utilizzato per visualizzare statistiche e informazioni relative alle connessioni di rete, alla tabella di routing, alle porte aperte e altro. È uno strumento utile per monitorare lo stato della rete.

2° Il comando netstat -h fornisce una guida rapida con l'elenco delle opzioni disponibili per il comando netstat.

```

PS C:\Users\Alessio> netstat -n
Visualizza statistiche relative ai protocolli e alle connessioni di rete TCP/IP correnti.

NETSTAT[-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

-a Visualizza tutte le connessioni e le porte di ascolto.
-b Visualizza il file eseguibile utilizzato per la creazione di ogni connessione o
porta di ascolto. Alcuni file eseguibili conosciuti includono
più componenti indipendenti. In tali casi
viene visualizzata la sequenza dei componenti utilizzati per la creazione della connessione
o porta di ascolto e il
nome del file eseguibile viene visualizzato in fondo, tra parentesi quadre ([]). Nell'PS C:\Users\Alessio> netstat
-e visualizza, fino al raggiungimento di TCP/IP. Se si utilizza questa opzione,
l'esecuzione del comando può richiedere molto tempo e riuscirà solo se si dispone di
sufficienti
-sufficien
-e Visualizza le statistiche Ethernet. Può essere utilizzata insieme all'opzione -s.

-f Visualizza i nomi di dominio completi (FQDN, Fully Qualified Domain Name) per gli ind
esterni.
-i Visualizza il tempo trascorso da una connessione TCP nel suo stato corrente.
-n Visualizza indirizzi e numeri di porta in forma numerica.
-o Visualizza l'ID del processo proprietario associato a ogni connessione.
-p proto Visualizza le connessioni relative ad un protocollo specificato da "proto",
come TCP o UDP. Può essere utilizzato insieme all'opzione -s
per le statistiche per protocollo. "proto" può essere:
IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6
-q Visualizza tutte le connessioni, le porte di ascolto
e le porte TCP non di ascolto associate. Le porte non di ascolto associate possono es
a una connessione attiva.
-r Visualizza la tabella di routing.
-s Visualizza le statistiche per protocollo. Per impostazione predefinita, vengono
visualizzate le statistiche per IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6
-t Per specificare un sottosinsieme dei valori predefiniti, è possibile utilizzare l'opzi
interval
-v Visualizza lo stato di offload della connessione corrente.
-x Visualizza le connessioni, i listener e gli endpoint
condivisi.
-y Visualizza il modello di connessione TCP per tutte le connessioni.
Non può essere
utilizzata in combinazione con le altre opzioni.
interval Ripete la visualizzazione delle statistiche selezionate, con una pausa di un numero d
pari a "interval" dopo ogni visualizzazione. Per interrompere la ripetizione
della visualizzazione delle statistiche, premere CTRL+C. Se questa opzione viene one
verranno visualizzate una volta sola.

PS C:\Users\Alessio> |

```

- immettere al prompt **netstat -r**

Il comando netstat -r viene utilizzato per visualizzare la tabella di routing del sistema. Questa tabella mostra come il traffico di rete viene instradato attraverso la rete. È utile per diagnosticare problemi di connessione e comprendere la configurazione di rete.

```
Windows PowerShell x + v
255.255.255.255 255.255.255.255      On-link      192.168.56.1    281
255.255.255.255 255.255.255.255      On-link      192.168.1.10    281
255.255.255.255 255.255.255.255      On-link      25.22.23.158    271
=====
Route permanenti:
Nessuna

IPv6 Tabella route
=====
Route attive:
Interf Metrica Rete Destinazione      Gateway
 5   9015 ::/0                          2620:9b::1900:1
 1   331 ::1/128                        On-link
 5   271 2620:9b::/64                   On-link
 5   271 2620:9b::/96                   On-link
 5   271 2620:9b::1916:179e/128     On-link
 8   281 fe80::/64                      On-link
13   281 fe80::/64                      On-link
 5   271 fe80::/64                      On-link
 5   271 fe80::407e:b975:ebfd:dc85/128
                                         On-link
 8   281 fe80::8cfcd:5098:5fb2:8cdc/128
                                         On-link
13   281 fe80::de88:dbec:77cb:6b64/128
                                         On-link
 1   331 ff00::/8                        On-link
 8   281 ff00::/8                        On-link
13   281 ff00::/8                        On-link
 5   271 ff00::/8                        On-link
=====
Route permanenti:
Interf Metrica Rete Destinazione      Gateway
 0 4294967295 2620:9b::/96            On-link
 0   9000 ::/0                          2620:9b::1900:1
=====

PS C:\Users\Alessio> |
```

Il gateway IPv4 è un dispositivo di rete (spesso un router) che funge da punto di accesso o di uscita tra una rete locale (LAN) e altre reti, come Internet. È essenziale per instradare il traffico tra reti diverse, poiché i dispositivi all'interno di una rete locale possono comunicare direttamente solo se appartengono alla stessa subnet.

- Entriamo come amministratore

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

Installa la versione più recente di PowerShell per nuove funzionalità e miglioramenti. https://aka.ms/PSWindows

PS C:\windows\system32>
```

- Immettere il al prompt.**netstat -abn**

Il comando netstat -abn è un'estensione avanzata di netstat che fornisce informazioni dettagliate sulle connessioni di rete e sulle porte aperte, insieme ai processi che le utilizzano. Ogni opzione aggiunge specifici dettagli:

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

Installa la versione più recente di PowerShell per nuove funzionalità e miglioramenti. https://aka.ms/PSWindows

PS C:\windows\system32> netstat -abn

Connessioni attive

  Proto  Indirizzo locale        Indirizzo esterno      Stato      PID
  TCP    0.0.0.0:135           0.0.0.0:0              LISTENING   1280
  RpcSs

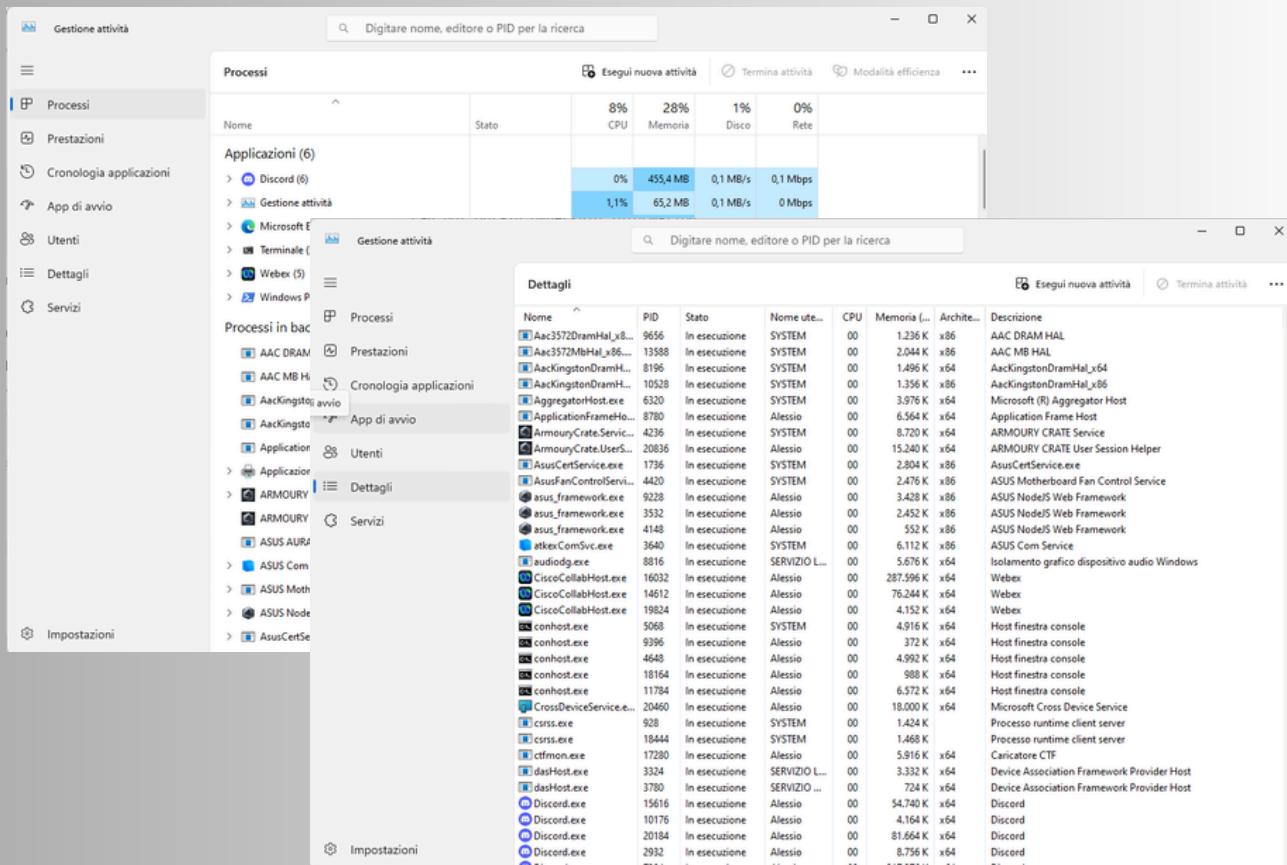
  [svchost.exe]
  TCP    0.0.0.0:445           0.0.0.0:0              LISTENING   4
  Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:1042          0.0.0.0:0              LISTENING   9228
  [asus_framework.exe]
  TCP    0.0.0.0:1043          0.0.0.0:0              LISTENING   9228
  [asus_framework.exe]
  TCP    0.0.0.0:5040          0.0.0.0:0              LISTENING   9512
  CDPsvc

  [svchost.exe]
  TCP    0.0.0.0:5357          0.0.0.0:0              LISTENING   4
  Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:7680          0.0.0.0:0              LISTENING   16840
  Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:27836         0.0.0.0:0              LISTENING   5544
  [steam.exe]
  TCP    0.0.0.0:49664         0.0.0.0:0              LISTENING   1048
  [lsass.exe]
  TCP    0.0.0.0:49665         0.0.0.0:0              LISTENING   384
  Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:49666         0.0.0.0:0              LISTENING   1804
  EventLog

  [svchost.exe]
  TCP    0.0.0.0:49667         0.0.0.0:0              LISTENING   2544
  Schedule

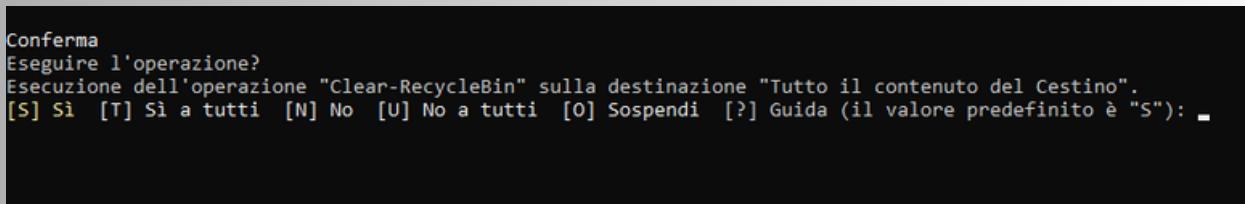
  [svchost.exe]
  TCP    0.0.0.0:49710         0.0.0.0:0              LISTENING   4788
  [spoolsv.exe]
  TCP    0.0.0.0:49721         0.0.0.0:0              LISTENING   924
  Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:50068          0.0.0.0:0              LISTENING   4940
  [NortonSecurity.exe]
  TCP    0.0.0.0:50069          0.0.0.0:0              LISTENING   4940
  [NortonSecurity.exe]
  TCP    25.22.23.158:139       0.0.0.0:0              LISTENING   4
  Impossibile ottenere informazioni sulla proprietà
  TCP    127.0.0.1:6463         0.0.0.0:0              LISTENING   7304
  [Discord.exe]
  TCP    127.0.0.1:13010        0.0.0.0:0              LISTENING   4236
  [ArmouryCrates.Service.exe]
  TCP    127.0.0.1:13030        0.0.0.0:0              LISTENING   5080
  [ROGLiveService.exe]
  TCP    127.0.0.1:13030        127.0.0.1:49720     ESTABLISHED  5080
  [ROGLiveService.exe]
  TCP    127.0.0.1:13031        0.0.0.0:0              LISTENING   20836
  [ArmouryCrates.UserSessionHelper.exe]
  TCP    127.0.0.1:13032        0.0.0.0:0              LISTENING   20836
  [ArmouryCrates.UserSessionHelper.exe]
  TCP    127.0.0.1:17532        0.0.0.0:0              LISTENING   4236
  [ArmouryCrates.Service.exe]
  TCP    127.0.0.1:17532        127.0.0.1:51935     ESTABLISHED  4236
```

- Apriamo il Task Manager.
- Andiamo su dettagli e osserviamo il Pid



Il PID (Process Identifier) è un numero univoco assegnato dal sistema operativo a ciascun processo in esecuzione. Questo identificativo serve a distinguere i processi attivi e a gestirli in modo indipendente. Ogni processo in esecuzione su un computer ha un proprio PID.

- In PowerShell, immettere al prompt **.clear-recyclebin**



Il comando Clear-RecycleBin in PowerShell viene utilizzato per svuotare il Cestino di Windows su uno o più volumi del computer. È utile per liberare spazio su disco eliminando definitivamente i file attualmente nel Cestino.

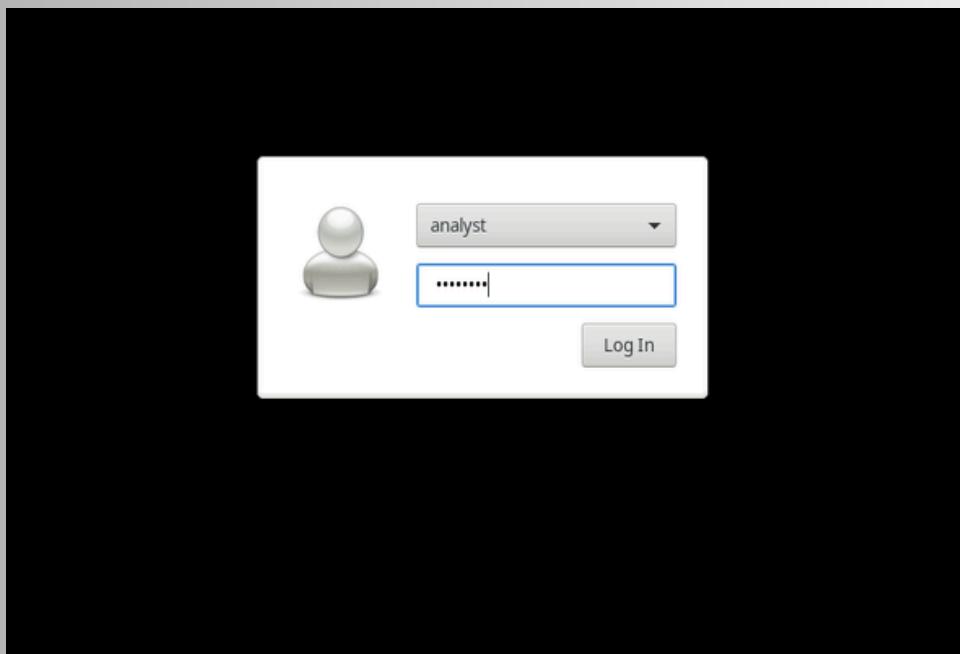
Conclusioni

In conclusione, PowerShell è uno strumento potentissimo e versatile per l'amministrazione di sistemi Windows. Grazie alla sua sintassi semplice e alla capacità di automatizzare compiti complessi, è ampiamente utilizzato da amministratori di sistema, professionisti IT e sviluppatori. PowerShell offre una vasta gamma di cmdlet per la gestione di file, processi, reti, e molto altro, permettendo anche l'integrazione con strumenti esterni e la gestione remota di macchine. La possibilità di scrivere script avanzati e di combinare comandi con pipe e variabili lo rende indispensabile per migliorare l'efficienza e la produttività. Con una solida comprensione di PowerShell, gli utenti possono ottimizzare e personalizzare il loro ambiente di lavoro, migliorando la gestione dei sistemi e automatizzando attività quotidiane.



Utilizzo di Wireshark per Esaminare il Traffico HTTP e HTTPS

- Apriamo la macchina virtuale Cyberops



- Apriamo un terminale e avviamo tcpdump.
- inseriamo il comando .ip address

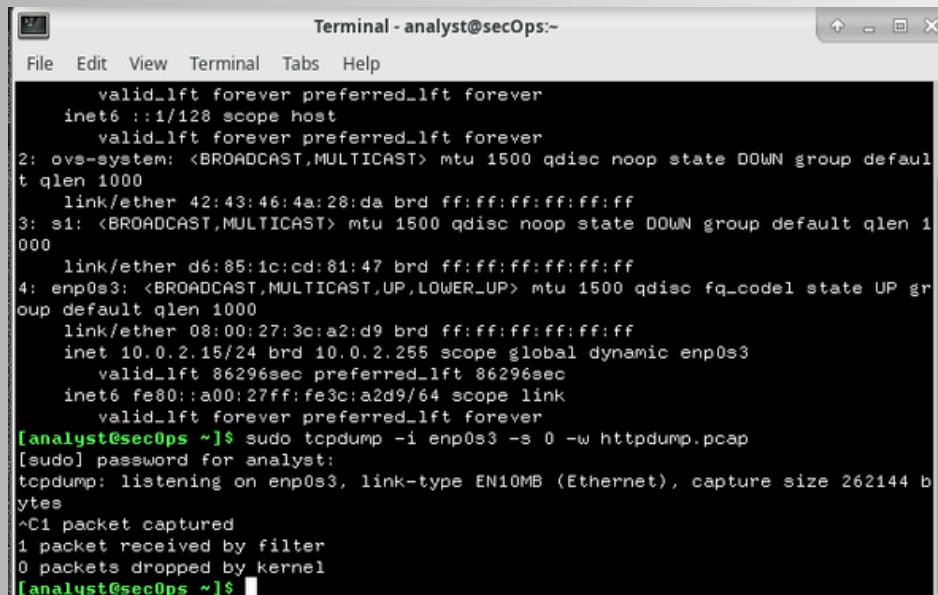
A screenshot of a terminal window titled "Terminal - analyst@secOps:~". The window shows the output of the "ip address" command. The output lists several network interfaces:

- lo: loopback interface (inet 127.0.0.1/8)
- ovs-system: ovs-system interface (inet 127.0.0.1/8)
- eth0: broadcast interface (inet 10.0.2.15/24)
- enp0s3: broadcast interface (inet 10.0.2.255/24)

The output also includes details about queueing disciplines (qdisc) and link layer information.

- Nell'applicazione terminale, immettiamo il comando **sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap**

Questo comando avvia tcpdump e registra il traffico di rete sull'interfaccia enp0s3

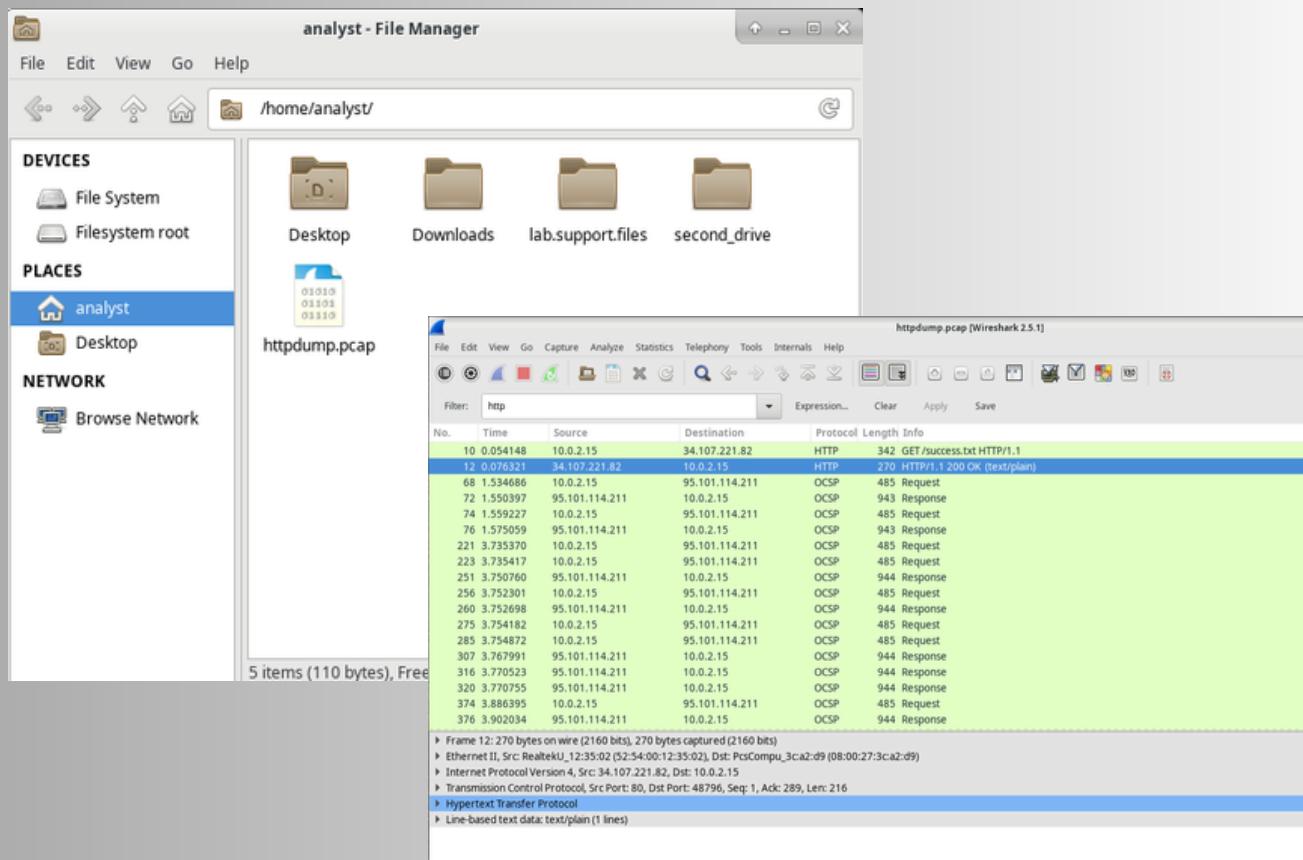


```

Terminal - analyst@secOps:~ 
File Edit View Terminal Tabs Help
    valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ovs-system: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 42:43:46:4a:28:da brd ff:ff:ff:ff:ff:ff
3: s1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether d6:85:ic:cd:81:47 brd ff:ff:ff:ff:ff:ff
4: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:3c:a2:d9 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86296sec preferred_lft 86296sec
    inet6 fe80::a00:27ff:fe3c:a2d9/64 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
^C packet captured
1 packet received by filter
0 packets dropped by kernel
[analyst@secOps ~]$ 

```

- Visualizziamo l'acquisizione HTTP.



- Nella finestra inferiore viene visualizzato il messaggio. Espandiamo la sezione URL del modulo HTML codificato: application/x-www-form-urlencoded.

```
Frame 150: 637 bytes on wire (5096 bits), 637 bytes captured (5096 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: 65.61.137.117
Transmission Control Protocol, Src Port: 41156, Dst Port: 80, Seq: 1, Ack: 1, Len: 583
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
```

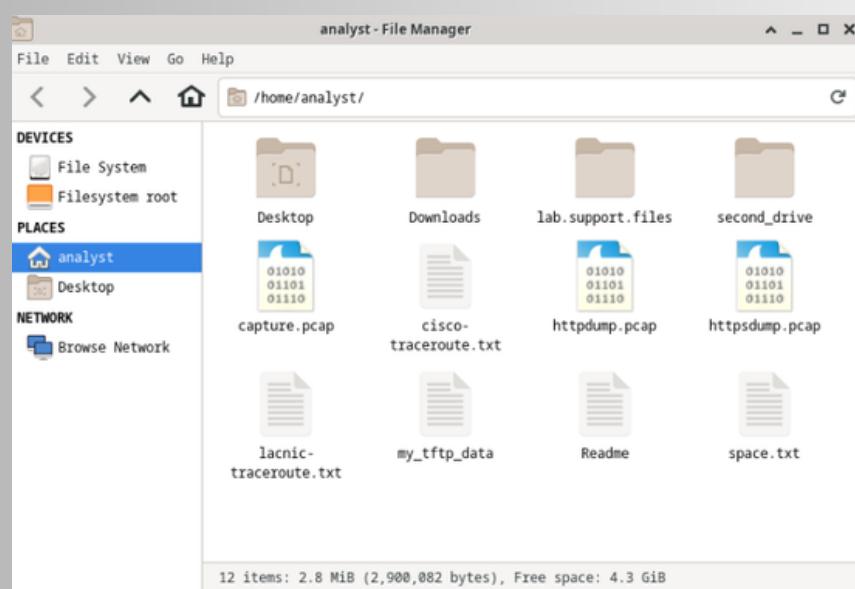
Quando si parla di application/x-www-form-urlencoded, si fa riferimento al tipo di contenuto (content type) utilizzato per inviare i dati da un modulo HTML attraverso una richiesta HTTP POST. Questo tipo di codifica è il più comune per i moduli web, in quanto i dati del modulo vengono inviati nel corpo della richiesta come una stringa di query, simile a quella che appare nell'URL di una richiesta GET.

- Acquisizione e visualizzazione del traffico HTTPS.

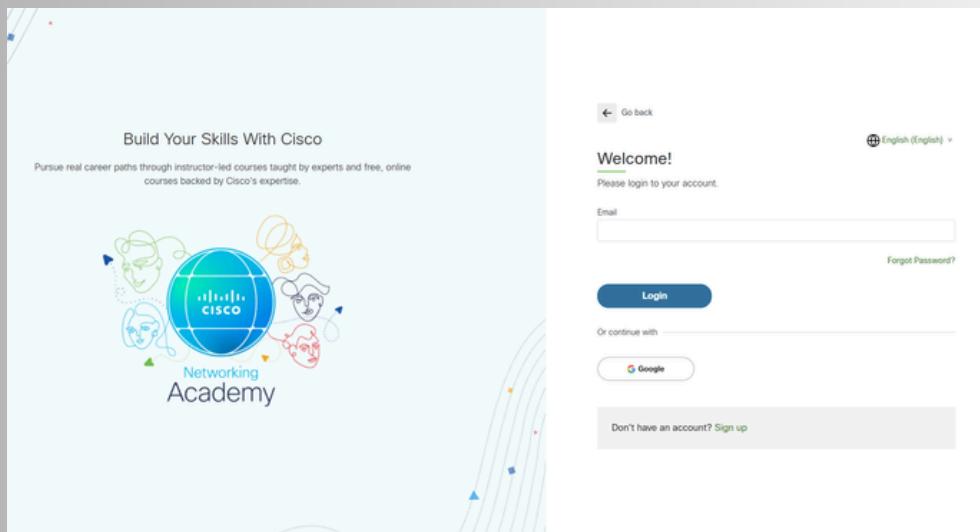
Immettiamo il codice **sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap**

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

Tutto il traffico registrato verrà registrato nel file httpsdump.pcap nella directory.



- Apriamo un Web browser dalla barra di avvio all'interno della macchina virtuale CyberOps Workstation. Vai a www.netacad.com.



- Nell'applicazione Wireshark, espandiamo la finestra di acquisizione, quindi filtriamo il traffico HTTPS tramite la porta 443.

Inseriamo **tcp.port==443** come filtro



- Sfogliamo i diversi messaggi HTTPS e selezioniamo dati dell'applicazione

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] Seq=1 Ack=57 Win=65535 Len=0
4	0.000383	104.16.248.249	10.0.2.15	TCP	60	443 - 52556 [ACK] Seq=1 Ack=136 Win=65535 Len=4
7	0.031225	104.16.248.249	10.0.2.15	TLSv1.2	286	Application Data, Application Data
8	0.031256	10.0.2.15	104.16.248.249	TCP	54	52556 - 443 [ACK] Seq=136 Ack=233 Win=63900 Len=4
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

- Espandiamo il Secure Sockets Layer
Facciamo clic su Dati dell'applicazione crittografati

```

> 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: 7fa037731c6e38e6213aacc15a0a7281f94046fdb237be9...
  
```

Conclusioni

Wireshark è uno strumento potente per analizzare il traffico di rete, incluso HTTP e HTTPS.

HTTP: Wireshark cattura e mostra facilmente le richieste e risposte HTTP, inclusi gli header e i contenuti delle risorse come HTML, CSS, e JavaScript. È utile per monitorare le interazioni tra client e server.

HTTPS: Poiché HTTPS è crittografato, Wireshark non può visualizzare direttamente i contenuti. Tuttavia, può catturare le informazioni di handshake SSL/TLS, come i certificati e i cipher suites. Per decriptare il traffico, è necessario configurare Wireshark con le chiavi appropriate o usare metodi come SSLKEYLOGFILE.

In sintesi, Wireshark è essenziale per analizzare il traffico di rete HTTP, mentre l'analisi di HTTPS richiede configurazioni speciali per la decrittazione.



Esplorazione di Nmap

- Inseriamo il comando man nmap per esplorare i comandi

The screenshot shows a terminal window titled "Terminal - analyst@secOps:~". The window displays the Nmap(1) man page. The man page includes sections for NAME, SYNOPSIS, and DESCRIPTION. The DESCRIPTION section provides a detailed explanation of what Nmap is and how it works, mentioning its use for network exploration and security auditing. It describes how Nmap can discover services running on hosts and determine their characteristics, such as operating systems and network administrators. The SYNOPSIS section shows the command syntax: nmap [Scan Type...] [Options] {target specification}. The man page concludes with an example scan of a target host, followed by a note about the latest version of Nmap and a link to the official book.

```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
NMAP(1) Nmap Reference Guide NMAP(1)  
NAME  
nmap - Network exploration tool and security / port scanner  
SYNOPSIS  
nmap [Scan Type...] [Options] {target specification}  
DESCRIPTION  
Nmap ("Network Mapper") is a network exploration tool and security auditing. It was originally designed to quickly determine what services (application and/or network layer) are listening on a host, although it works fine again in novel ways to determine what services (application and/or network layer) are listening on a host, what operating systems (and OS versions) are running, and what packet filters/firewalls are in place. While Nmap is primarily used by systems and network administrators for such as network inventory, monitoring, and security audits, it is also used by monitoring host or service users.  
The output from Nmap is a list of information on each dependency. The most interesting information is the "interesting ports": those ports which are open, filtered, closed, or unfiltered. On the target machine is listed every port. Filtered means that some obstacle is blocking the port, whether it is open or closed. Closed ports are those which could open up at any time, though they could open up at any time. Unfiltered ports are those which are ready to accept connections. Open ports are those which are accepting connections. Determining whether they are open, filtered, or closed is done by sending combinations of open/filtered probe packets to each port and determining which of the two states described above best fits the responses received. When an IP protocol is selected, Nmap will attempt to determine supported IP options for that protocol.  
Manual page nmap(1) line 1 (press h for help or q to quit)  
  
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:0:a:d6:67:54:9d:69:d9:b9:dd (RSA)  
|_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85 (RSA)  
80/tcp    open  http     Apache httpd 2.2.14 ((Ubuntu))  
|_http-title: Go ahead and ScanMe!  
646/tcp   filtered ldp  
1720/tcp  filtered H.323/Q.931  
9929/tcp  open  nping-echo  Nping echo  
Device type: general purpose  
Running: Linux 2.6.X  
OS CPE: cpe:/o:linux:linux_kernel:2.6.39  
OS details: Linux 2.6.39  
Network Distance: 11 hops  
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel  
  
TRACEROUTE (using port 53/tcp)  
HOP RTT      ADDRESS  
[Cut first 10 hops for brevity]  
1  17.65 ms  li86-221.members.linode.com (74.207.244.221)  
  
Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds  
  
The newest version of Nmap can be obtained from https://nmap.org. The newest version of this man page is available at https://nmap.org/book/man.html. It is also included as a chapter of Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning (see https://nmap.org/book/).  
Manual page nmap(1) line 48 (press h for help or q to quit)
```

Nmap (Network Mapper) è uno strumento open-source utilizzato principalmente per la scansione e la mappatura delle reti. È uno degli strumenti più popolari e potenti per l'analisi della sicurezza delle reti, ma viene anche impiegato in ambito amministrativo per scoprire dispositivi connessi e raccogliere informazioni sui sistemi.

- Scansioniamo il nostro localhost **nmap -A -T4 localhost**.

```

Terminal - analyst@secOps:~ 
File Edit View Terminal Tabs Help
!_http-title: Go ahead and ScanMe!
!_9292/tcp open nping-echo Nping echo
!_1337/tcp open tcprwapped
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 30.70 seconds
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 04:19 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000027s 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)
          _rwd-r--r--  1 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 4
            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:fb: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 11.54 seconds
[analyst@secOps ~]$ 

```

Il risultato di Nmap mostrato nell'immagine è il resoconto di una scansione di rete condotta su localhost (127.0.0.1) con l'opzione -A (che abilita la rilevazione del sistema operativo, la versione del servizio, la scansione delle porte e altre informazioni dettagliate). La scansione è stata eseguita con una priorità -T4, che riduce il tempo di scansione. Ecco una sintesi delle informazioni mostrate:

Porta 21 (FTP):

La porta 21 è aperta, con il servizio FTP (File Transfer Protocol) in esecuzione.

Versione del servizio: vsftpd 2.0.8 o successiva.

Autenticazione FTP: La connessione FTP consente l'accesso anonimo (FTP code 230).

Un file di test denominato `ftp_test` è stato trovato nella directory `/srv/ftp`.

Porta 22 (SSH):

La porta 22 è aperta, con il servizio SSH (Secure Shell) in esecuzione.

Versione del servizio: OpenSSH 7.7. Connessione stabilita, la connessione di rete è di tipo plain text.

- Inseriamo il comando **ip address** e andiamo a vedere il nostro indirizzo ip e la subnet mask

```
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
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 00:00:00:00:00:00 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 brd 00:00:00:00:00:00 scope host
        valid_lft forever preferred_lft forever
2: ovs-system: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default
    link/ether 5e:a6:26:90:d0:7a brd ff:ff:ff:ff:ff:ff
3: si: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether d6:85:1c:cd:81:47 brd ff:ff:ff:ff:ff:ff
4: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:3c:a2:d9 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 85592sec preferred_lft 85592sec
    inet6 fe80::a00:27ff:fe3c:a2d9/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

- Conosciuto l'indirizzo ip inseriamo il comando **nmap -A -T4 10.0.2.0/24**

```
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 04:29 EST
Nmap scan report for 10.0.2.15
Host is up (0.000033s latency).
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 10.0.2.15
|   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 5
|   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: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: 256 IP addresses (1 host up) scanned in 39.87 seconds
```

Risultati della scansione:

Host: È stato trovato un host attivo all'indirizzo IP 10.0.2.15.

Porte aperte:

Porta 21/tcp: È aperta e fornisce il servizio FTP (File Transfer Protocol). Il server FTP in uso è vsftpd versione 2.0.8 o successiva.

Porta 22/tcp: È aperta e fornisce il servizio SSH (Secure Shell). Il server SSH in uso è OpenSSH versione 7.7.

- Eseguiamo la scansione di un server remoto

Digitiamo **nmap -A -T4 scanme.nmap.org**

```
[analyst@sec0ps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 04:31 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
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         Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
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 30.56 seconds
```

Risultati della scansione:

Host: È stato trovato un host attivo all'indirizzo IP 45.33.32.156.

Porte aperte:

Porta 22/tcp: È aperta e fornisce il servizio SSH (Secure Shell). Il server SSH in uso è OpenSSH versione 6.6.1p1 su un sistema operativo Ubuntu Linux.

Porta 80/tcp: È aperta e fornisce il servizio HTTP (Hypertext Transfer Protocol). Il server web in uso è Apache versione 2.4.7 su un sistema operativo Ubuntu.

Porta 9929/tcp: È aperta e fornisce un servizio custom chiamato "Nping echo".

Porta 31337/tcp: È aperta ma lo stato del servizio è "tcpwrapped", il che significa che il servizio è nascosto o filtrato in qualche modo.

Conclusioni

In conclusione, Nmap si rivela uno strumento fondamentale per l'esplorazione e la mappatura delle reti, nonché per la valutazione della sicurezza di sistemi remoti. Le sue potenti funzionalità, come la scansione delle porte, il rilevamento dei servizi, la determinazione del sistema operativo e la versione del software, lo rendono essenziale per amministratori di rete e professionisti della sicurezza. Anche se le informazioni raccolte durante una scansione possono rivelare vulnerabilità potenziali, è cruciale utilizzare Nmap in modo etico, rispettando sempre le leggi e le policy di sicurezza, per evitare rischi di intrusione non autorizzata. In definitiva, Nmap offre un'analisi approfondita e accurata delle reti, aiutando a migliorare la gestione e la protezione delle infrastrutture IT.

