

# Report Test Day S11L5

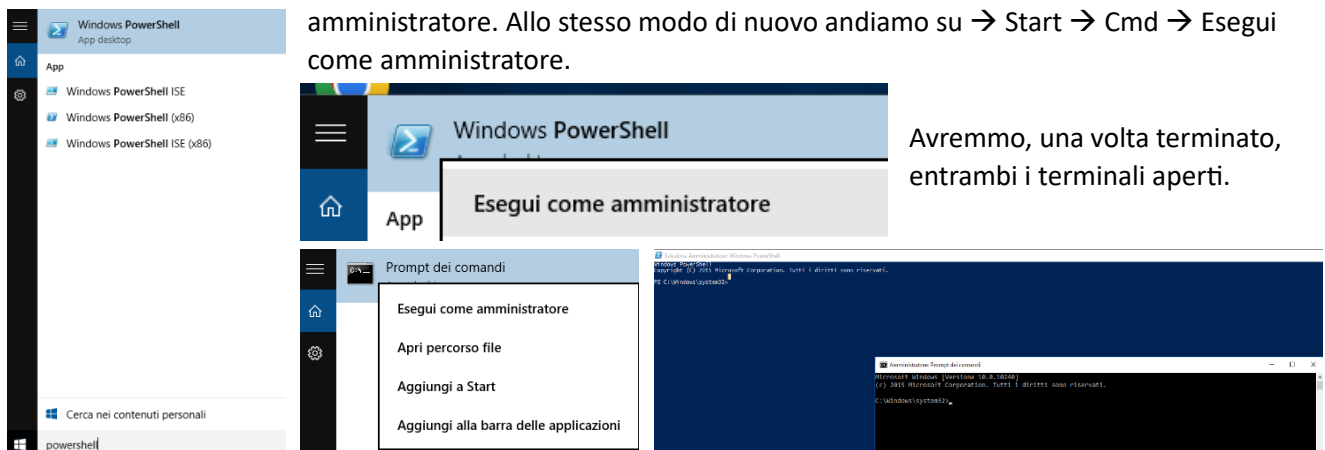
## Esercizio 1: Usare Windows Power Shell

**Obiettivi** L'obiettivo del laboratorio è esplorare alcune delle funzioni di PowerShell.

- Parte 1: Accedere alla console PowerShell.
- Parte 2: Esplorare i comandi del Prompt dei Comandi e di PowerShell.
- Parte 3: Esplorare i cmdlet.
- Parte 4: Esplorare il comando netstat usando PowerShell.
- Parte 5: Svuotare il cestino usando PowerShell.

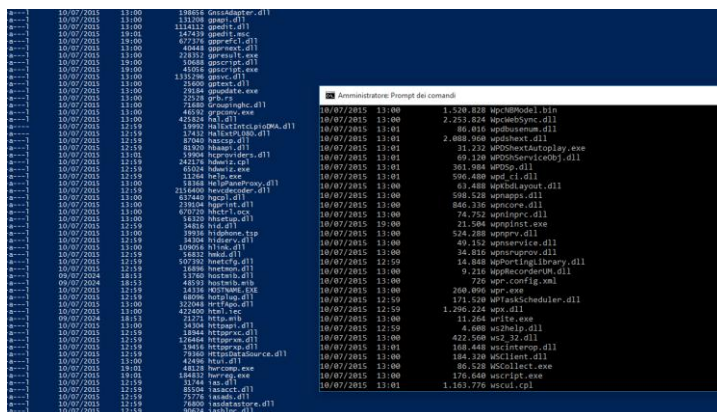
## Parte 1: Accedere alla console PowerShell

Una volta avviata la nostra VM windows 10, andiamo su → Start → PowerShell → Esegui come amministratore. Allo stesso modo di nuovo andiamo su → Start → Cmd → Esegui come amministratore.



## Parte 2: Esplorare i comandi del Prompt dei Comandi e di PowerShell

A questo punto, come richiesto nell'esercizio, andiamo a digitare il dir in entrambe le console.



Questo sarà il nostro output.

**D:** a) Quali sono gli output del comando dir?

**R:** Il comando `dir` serve per **elenicare i file e le cartelle** presenti in una directory (cartella) del file system. È uno strumento fondamentale sia in **CMD** (Prompt dei comandi) che in **PowerShell**, anche se con comportamenti leggermente diversi.

## In CMD (cmd.exe)

- Il comando dir è **nativo di CMD**.
- Elenca i file e le cartelle presenti nella directory corrente.
- Mostra:
  - La data e l'ora di modifica
  - <DIR> per le cartelle
  - La dimensione dei file
  - Il numero totale di file/cartelle e lo spazio libero su disco

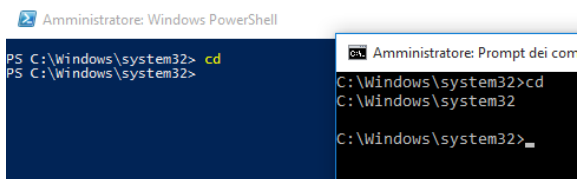
## In PowerShell

- dir **funziona** anche in PowerShell, ma **non è lo stesso comando**.
- In realtà, dir è un **alias** per il cmdlet Get-ChildItem.
- L'output è più **orientato agli oggetti**, non a testo puro come in CMD.

b) Prova un altro comando che hai usato nel prompt dei comandi, come ping, cd e ipconfig.

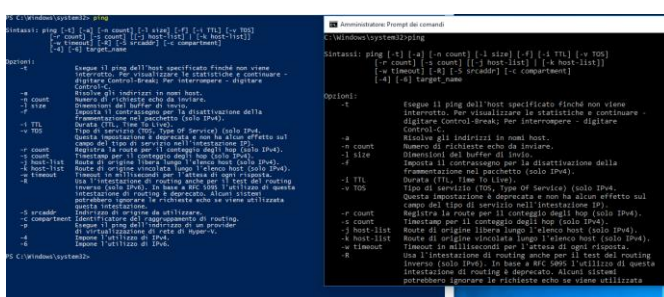
**D:** Quali sono i risultati?

(Comando cd)



**R:** Proviamo a scrivere cd all'interno delle nostre console. Cd sta per "change directory", digitando solo cd ci mostra la directory corrente sia su Cmd che su Powershell.

Comando ping

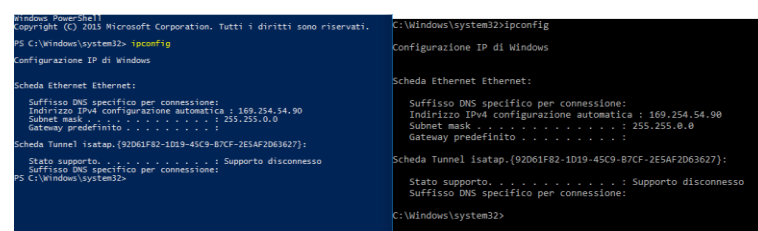


**R:** Se invece digitassimo solo il comando ping senza nessun argomento e premiamo Invio, il comando non viene eseguito correttamente. Invece, il sistema (sia in **CMD** che in **PowerShell**) ti mostra una **guida sintetica** sull'uso del comando ping. Questo accade perché ping ha bisogno **almeno di un indirizzo o un nome di dominio** come destinazione da contattare (come ping

google.com). Senza, non sa cosa fare e mostra l'**help integrato** del comando.

Quindi: se digiti solo ping, **non viene eseguito alcun test**, ma ti viene mostrata la modalità d'uso del comando.

Comando ipconfig



**R:** Se digitassimo invece solo ipconfig e premessimo invio il comando viene eseguito e il sistema restituisce un riepilogo delle **configurazioni di rete attive** sul tuo computer.

In particolare, ti mostra:

- l'indirizzo IPv4 assegnato a ogni scheda di rete (Ethernet, Wi-Fi, ecc.),
- la subnet mask,
- il gateway predefinito (se presente).

Non è come ping che richiede un argomento: ipconfig funziona anche da solo, ed è pensato proprio per darti una panoramica **rapida e utile della rete locale**. Può essere usato sia in **CMD** che in **PowerShell**, con lo stesso risultato.

## Parte 3: Esplorare i cmdlet

- I comandi PowerShell, chiamati cmdlet, sono costruiti nella forma di una stringa verbo-nome. Per identificare il comando PowerShell per elencare le sottodirectory e i file in una directory, inserisci Get-ChildItem al prompt di PowerShell.

Digitando Get-ChildItem al prompt, la console ci avvisa che non è un comando compatibile con PowerShell.

```
Amministratore: Windows PowerShell
PS C:\Windows\system32> Get-ChildItem dir

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

**D:** Qual è il comando PowerShell per dir?

**R:** Ci avvisa in realtà già la console che per 'dir' → Get-ChildItem' cioè per dir in PowerShell dobbiamo usare Get-ChildItem. Non ci è infatti servito fare

nessuna ricerca su internet come richiesto nell'esercizio, in quanto la console già ci fornisce gli strumenti per sapere quale è il comando giusto.

## Parte 4: Esplorare il comando netstat usando PowerShell

```
PS C:\Windows\system32> netstat -r

=====
Elenco interfacce
4...08 00 27 67 99 8F .....Intel(R) PRO/1000 MT Desktop Adapter
1.....Software Loopback Interface 1
6...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
5...00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter

=====
IPv4 Tabella route

Route attive:
Indirizzo rete      Mask      Gateway      Interfaccia Metrica
-----
0.0.0.0             0.0.0.0   192.168.1.254 192.168.1.160 10
127.0.0.0           255.0.0.0 On-link      127.0.0.1      306
127.0.0.1           255.255.255.255 On-link      127.0.0.1      306
127.255.255.255     255.255.255.255 On-link      127.0.0.1      306
192.168.1.0         255.255.255.0 On-link      192.168.1.160 266
192.168.1.160       255.255.255.255 On-link      192.168.1.160 266
192.168.1.255       255.255.255.255 On-link      192.168.1.160 266
224.0.0.0           240.0.0.0 On-link      127.0.0.1      306
224.0.0.0           240.0.0.0 On-link      192.168.1.160 266
255.255.255.255     255.255.255.255 On-link      127.0.0.1      306
255.255.255.255     255.255.255.255 On-link      192.168.1.160 266
```

**D:** Qual è il gateway IPv4?

**R:** Il Gateway è 192.168.1.254

The screenshot shows the Windows Task Manager window with the 'Processi' tab selected. The process 'TCPVCS.exe' is highlighted. The 'Proprietà' dialog box for 'TCPVCS.exe' is open, showing the 'Dettagli' tab. The details include: Descrizione: TCP/IP Services Application, Versione: 10.0.0.0, Nome prodotto: Microsoft Windows® Operating System, Lingua: Inglese (Stati Uniti d'America), and Nome file originale: TCPVCS.EXE.

**D:** Quali informazioni puoi ottenere dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID selezionato?

**R:** Dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID 2032 (TCPSVCS.EXE) si ottengono le seguenti informazioni:

- **Copyright:** © Microsoft Corporation. All rights reserved.
- **Dimensione:** 12.0 KB

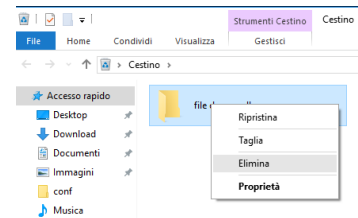
- **Ultima modifica:** 10/07/2015 12:59
- **Lingua:** Inglese (Stati Uniti d'America)
- **Nome file originale:** TCPSVCS.EXE
- **Descrizione:** TCP/IP Services Application
- **Tipo:** Applicazione

- **Versione file:** 10.0.10240.16384
- **Nome prodotto:** Microsoft® Windows® Operating Syst...
- **Versione:** 10.0.10240.16384

## Parte 5: Svuotare il cestino usando PowerShell

**D:** Cosa è successo ai file nel Cestino?

**R:** Il file viene eliminato definitivamente.



### Domanda di Riflessione

PowerShell è stato sviluppato per l'automazione delle attività e la gestione della configurazione. Usando internet, ricerca comandi che potresti usare per semplificare i tuoi compiti come analista di sicurezza. Registra le tue scoperte.

### Comandi PowerShell Chiave per Analisti di Sicurezza

PowerShell automatizza efficacemente le attività di sicurezza informatica, semplificando i compiti quotidiani degli analisti attraverso comandi mirati e potenti.

#### Comandi Essenziali

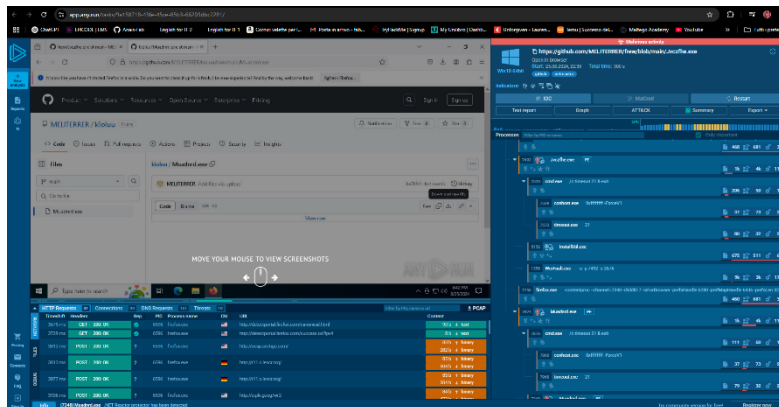
- **Test-NetConnection** verifica rapidamente la connettività di rete e identifica porte aperte. Esempio: `Test-NetConnection -ComputerName "server.com" -Port 443` per testare connessioni HTTPS.
- **Get-FileHash** calcola hash crittografici per verificare l'integrità dei file. `Get-FileHash -Algorithm SHA256 "file.exe"` crea impronte digitali per rilevare modifiche non autorizzate.
- **Get-Process** analizza i processi in esecuzione. `Get-Process | Where-Object {$_.Path -eq $null}` identifica processi sospetti senza percorso definito, spesso indicatori di malware.
- **Get-WinEvent** esamina i log di sistema per eventi di sicurezza. `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4625}` filtra i tentativi di login falliti.
- **Get-NetTCPConnection** monitora le connessioni di rete attive. `Get-NetTCPConnection | Where-Object {$_.State -eq "Established"}` rivela comunicazioni stabilite potenzialmente sospette.
- **Get-ItemProperty** accede alle chiavi di registro critiche. `Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Run` esamina i programmi di avvio automatico, comuni vettori di persistenza malware.

#### Valore Strategico

Questi comandi permettono automazione di controlli di routine, accelerazione delle indagini forensi e monitoraggio continuo dell'infrastruttura. La loro padronanza trasforma l'approccio reattivo in una postura di sicurezza proattiva, riducendo significativamente i tempi di risposta agli incidenti.

## Esercizio 2: Studio loc

## Report Analisi IoC - Muadnrd.exe



### Panoramica della Minaccia

L'analisi ANY.RUN ha identificato il file Muadnrd.exe come campione malware con comportamenti sospetti multipli. Il file è stato analizzato in ambiente Windows 10 64-bit per 360 secondi, rivelando attività malevole significative. Indicatori di Compromissione (IoC)

### File Principale

- Nome: Muadnrd.exe
- Origine: <https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe>
- Classificazione: Attività Malevola Confermata

### Comunicazioni di Rete Sospette

L'analisi ha rivelato connessioni HTTP verso domini altamente sospetti:

Domini C2 Identificati:

- <http://detectportal.firefox.com/canonical.html>
- <http://detectportal.firefox.com/success.txt>
- <http://ncap.sectigo.com/>
- <http://r11.o.lencr.org/>

Caratteristiche delle Comunicazioni:

- Richieste POST da 200-504 byte verso server remoti
- Comunicazioni verso indirizzi IP internazionali (US, DE)
- Pattern di traffic consistenti con beacon C2

### Comportamenti del Processo

Catena di Esecuzione Osservata:

- Processo padre: Jvczfhe.exe (PID 7472)
- Spawn di processi figlio: cmd.exe, conhost.exe, timeout.exe
- Injection in processi legittimi come firefox.exe

Attività Sospette:

- Creazione di processi multipli per evasione
- Utilizzo di timeout.exe per ritardi controllati
- Persistenza attraverso InstallUtil.exe

### Classificazione della Minaccia

Tipo di Malware

Trojan Dropper/Loader con capacità di:

- Download di payload aggiuntivi
- Comunicazione con server C2
- Evasione delle difese attraverso process injection
- Possibile data exfiltration

## Livello di Rischio

ALTO - Il malware presenta comportamenti tipici di advanced persistent threat (APT) con:

- Comunicazioni cifrate verso infrastructure C2
- Tecniche di evasion avanzate
- Capacità di lateral movement

## Raccomandazioni Immediate

### Contenimento:

- Isolamento immediato dei sistemi compromessi
- Blocco dei domini C2 identificati a livello firewall
- Scansione completa della rete per lateral movement

### Remediation:

- Rimozione completa del malware e processi correlati
- Reset delle credenziali potenzialmente compromesse
- Analisi forense dei log per determinare l'estensione della compromissione

### Prevenzione:

- Implementazione di regole di detection basate sugli IoC identificati
- Monitoraggio proattivo per comunicazioni verso i domini C2
- Aggiornamento delle signature antimalware con gli hash del campione

## Bonus Parte 1: Esplorazione di Nmap

- Avvia la VM CyberOps Workstation.
- Apri un terminale.
- Al prompt del terminale, inserisci `man nmap`.

### D: Cos'è Nmap? Per cosa viene usato nmap?

```
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 an open source tool for network exploration
  and security auditing. It was designed to rapidly scan large networks,
  although it works fine against single hosts. Nmap uses raw IP packets
  in novel ways to determine what hosts are available on the network,
  what services (application name and version) those hosts are offering,
  what operating systems (and OS versions) they are running, what types of
  packet filters/firewalls are in use; and dozens of other characteristics.
  While Nmap is commonly used for security audits, many systems and network
  administrators find it useful for routine tasks such as network inventory,
  managing service upgrade schedules, and monitoring host or service uptime.

  The output from Nmap is a list of scanned targets, with supplemental
  information on each depending on the options used. Key among that
  information is the "interesting ports table". That table lists the
  port number and protocol, service name, and state. The state is either
  open, filtered, closed, or unfiltered. Open means that an application
  on the target machine is listening for connections/packets on that
  port. Filtered means that a firewall, filter, or other network
  device is blocking the port so that Nmap cannot tell whether it is
  open or closed. Closed ports have no application listening on them,
  though they could open up at any time. Ports are classified as
  unfiltered when they are responsive to Nmap's probes, but Nmap cannot
  determine whether they are open or closed. Nmap reports the state
  combinations open/filtered and closed/filtered when it cannot determine
  which of the two states describe a port. The port table may also
  include software version details when version detection has been
  requested. When an IP protocol scan is requested (-sS), Nmap provides
  information on supported IP protocols rather than listening ports.

  In addition to the interesting ports table, Nmap can provide further
  information on targets, including reverse DNS names, operating system
  guesses, device types, and MAC addresses.

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

  Example 1. A representative Nmap scan

  # nmap -n -iL scanme.nmap.org

  Nmap scan report for scanme.nmap.org (74.207.244.223)
  Manual page nmap(1) line 1 (press h for help or q to quit)
```

### R: Cos'è Nmap?

Nmap (Network Mapper) è uno strumento di scansione di rete che scopre host attivi, porte aperte e servizi in esecuzione.

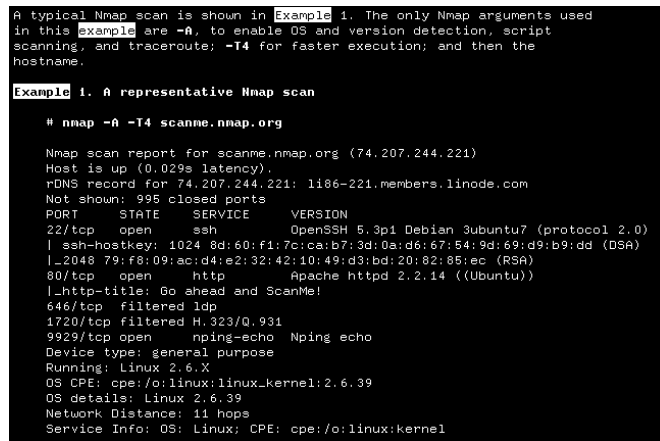
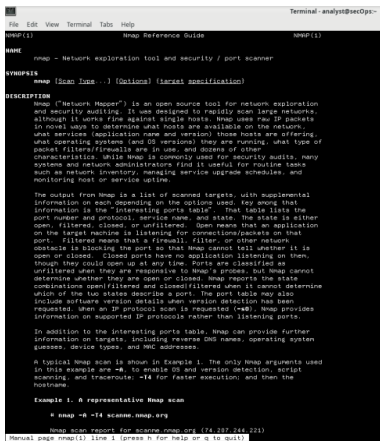
### Utilizzi:

- **Sicurezza:** Penetration testing e vulnerability assessment
- **Amministrazione:** Inventario di rete e monitoraggio
- **Troubleshooting:** Diagnosi problemi di connettività

### Funzioni principali:

- Scoperta host
- Scansione porte
- Rilevamento OS e servizi

È lo standard per la scansione di rete in ambito IT e cybersecurity.

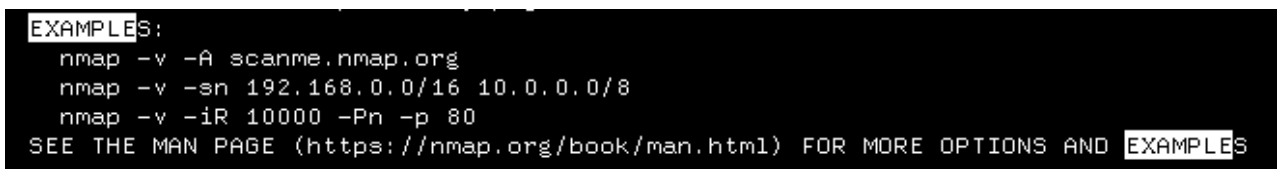


e. Nella prima istanza di

example, vedi tre corrispondenze. Per passare alla corrispondenza successiva, premi n.

**D:** Qual è il comando nmap usato?

**R:**



**D:** Cosa fa l'opzione-A? Cosa fa l'opzione-T4?

**R:**

Opzione -A

Esegue scansione aggressiva che combina:

- Rilevamento OS (-O)
- Rilevamento versioni servizi (-sV)
- Script scanning (-sC)
- Traceroute (--traceroute)

Opzione -T4

Imposta il timing template su "aggressive":

- Scansione più veloce
- Timeout ridotti
- Più probe simultanei
- Bilanciamento tra velocità e accuratezza

T4 è ideale per reti moderne con buona banda e bassa latenza.

## Parte 2: Scansione delle Porte Aperte

Passo 1: Scansiona il tuo localhost.

a. Se necessario, apri un terminale sulla VM. Al prompt, inserisci `nmap -A -T4 localhost`. A seconda della tua rete locale e dei dispositivi, la scansione richiederà da pochi secondi a pochi minuti.



## D: Quali porte e servizi sono aperti?

```
[analyst@sec0ps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 05:41 EDT
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)
|_ --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 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: 1 IP address (1 host up) scanned in 11.41 seconds
```

## R: Porte e Servizi Aperti:

Porta 21/tcp - FTP

- Servizio: vsftpd 2.0.8 o successivo
- Login anonimo consentito (FTP code 230)

Porta 22/tcp - SSH

- Servizio: OpenSSH 7.7 (protocollo 2.0)

Totale: 2 porte aperte, 998 porte chiuse

## Passo 2: Scansiona la tua rete.

a. Al prompt dei comandi del terminale, inserisci ip address per determinare l'indirizzo IP e la subnet mask per questo host.

## D: A quale rete appartiene la tua VM?

```
[analyst@sec0ps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether 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 08:00:27:9c:e6:64 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.92/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 41950sec preferred_lft 41950sec
    inet6 fd8d:db7a:9800:9046:a00:27ff:fe9c:e564/64 scope link
        valid_lft 1758sec preferred_lft 1758sec
    inet6 2a01:e11:500d:8000:e15d:9e92/128 scope global dynamic noprefixroute
        valid_lft 85148sec preferred_lft 85148sec
    inet6 fe80::a00:27ff:fe9c:e564/64 scope link
        valid_lft forever preferred_lft forever
3: ovs-system: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether e2:6d:e7:60:e6:94 brd ff:ff:ff:ff:ff:ff
4: si: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether a6:72:19:7b:09:46 brd ff:ff:ff:ff:ff:ff
```

## R:

### Configurazione di Rete della VM:

Indirizzo IP: 192.168.1.92

Subnet Mask: 255.255.255.0 (/24)

Rete di Appartenenza:

La VM appartiene alla rete 192.168.1.0/24

## Dettagli della rete:

- Network Address: 192.168.1.0
- Broadcast Address: 192.168.1.255
- Range IP utilizzabili: 192.168.1.1 - 192.168.1.254
- Numero totale di host: 254 host possibili

- b. Per localizzare altri host su questa LAN, inserisci nmap -A -T4 indirizzo\_rete/prefisso.

```
analyst@sec0ps:~$ nmap -A -T4 192.168.1.0/24
Nmap scan report for 192.168.1.0/24
Host is up (0.000027s latency).
Other addresses for 192.168.1.0/24 (not scanned): 192.168.1.1, 192.168.1.2, 192.168.1.3, 192.168.1.4, 192.168.1.5, 192.168.1.6, 192.168.1.7, 192.168.1.8, 192.168.1.9, 192.168.1.10, 192.168.1.11, 192.168.1.12, 192.168.1.13, 192.168.1.14, 192.168.1.15, 192.168.1.16, 192.168.1.17, 192.168.1.18, 192.168.1.19, 192.168.1.20, 192.168.1.21, 192.168.1.22, 192.168.1.23, 192.168.1.24, 192.168.1.25, 192.168.1.26, 192.168.1.27, 192.168.1.28, 192.168.1.29, 192.168.1.30, 192.168.1.31, 192.168.1.32, 192.168.1.33, 192.168.1.34, 192.168.1.35, 192.168.1.36, 192.168.1.37, 192.168.1.38, 192.168.1.39, 192.168.1.40, 192.168.1.41, 192.168.1.42, 192.168.1.43, 192.168.1.44, 192.168.1.45, 192.168.1.46, 192.168.1.47, 192.168.1.48, 192.168.1.49, 192.168.1.50, 192.168.1.51, 192.168.1.52, 192.168.1.53, 192.168.1.54, 192.168.1.55, 192.168.1.56, 192.168.1.57, 192.168.1.58, 192.168.1.59, 192.168.1.60, 192.168.1.61, 192.168.1.62, 192.168.1.63, 192.168.1.64, 192.168.1.65, 192.168.1.66, 192.168.1.67, 192.168.1.68, 192.168.1.69, 192.168.1.70, 192.168.1.71, 192.168.1.72, 192.168.1.73, 192.168.1.74, 192.168.1.75, 192.168.1.76, 192.168.1.77, 192.168.1.78, 192.168.1.79, 192.168.1.80, 192.168.1.81, 192.168.1.82, 192.168.1.83, 192.168.1.84, 192.168.1.85, 192.168.1.86, 192.168.1.87, 192.168.1.88, 192.168.1.89, 192.168.1.90, 192.168.1.91, 192.168.1.93, 192.168.1.94, 192.168.1.95, 192.168.1.96, 192.168.1.97, 192.168.1.98, 192.168.1.99, 192.168.1.100, 192.168.1.101, 192.168.1.102, 192.168.1.103, 192.168.1.104, 192.168.1.105, 192.168.1.106, 192.168.1.107, 192.168.1.108, 192.168.1.109, 192.168.1.110, 192.168.1.111, 192.168.1.112, 192.168.1.113, 192.168.1.114, 192.168.1.115, 192.168.1.116, 192.168.1.117, 192.168.1.118, 192.168.1.119, 192.168.1.120, 192.168.1.121, 192.168.1.122, 192.168.1.123, 192.168.1.124, 192.168.1.125, 192.168.1.126, 192.168.1.127, 192.168.1.128, 192.168.1.129, 192.168.1.130, 192.168.1.131, 192.168.1.132, 192.168.1.133, 192.168.1.134, 192.168.1.135, 192.168.1.136, 192.168.1.137, 192.168.1.138, 192.168.1.139, 192.168.1.140, 192.168.1.141, 192.168.1.142, 192.168.1.143, 192.168.1.144, 192.168.1.145, 192.168.1.146, 192.168.1.147, 192.168.1.148, 192.168.1.149, 192.168.1.150, 192.168.1.151, 192.168.1.152, 192.168.1.153, 192.168.1.154, 192.168.1.155, 192.168.1.156, 192.168.1.157, 192.168.1.158, 192.168.1.159, 192.168.1.160, 192.168.1.161, 192.168.1.162, 192.168.1.163, 192.168.1.164, 192.168.1.165, 192.168.1.166, 192.168.1.167, 192.168.1.168, 192.168.1.169, 192.168.1.170, 192.168.1.171, 192.168.1.172, 192.168.1.173, 192.168.1.174, 192.168.1.175, 192.168.1.176, 192.168.1.177, 192.168.1.178, 192.168.1.179, 192.168.1.180, 192.168.1.181, 192.168.1.182, 192.168.1.183, 192.168.1.184, 192.168.1.185, 192.168.1.186, 192.168.1.187, 192.168.1.188, 192.168.1.189, 192.168.1.190, 192.168.1.191, 192.168.1.192, 192.168.1.193, 192.168.1.194, 192.168.1.195, 192.168.1.196, 192.168.1.197, 192.168.1.198, 192.168.1.199, 192.168.1.200, 192.168.1.201, 192.168.1.202, 192.168.1.203, 192.168.1.204, 192.168.1.205, 192.168.1.206, 192.168.1.207, 192.168.1.208, 192.168.1.209, 192.168.1.210, 192.168.1.211, 192.168.1.212, 192.168.1.213, 192.168.1.214, 192.168.1.215, 192.168.1.216, 192.168.1.217, 192.168.1.218, 192.168.1.219, 192.168.1.220, 192.168.1.221, 192.168.1.222, 192.168.1.223, 192.168.1.224, 192.168.1.225, 192.168.1.226, 192.168.1.227, 192.168.1.228, 192.168.1.229, 192.168.1.230, 192.168.1.231, 192.168.1.232, 192.168.1.233, 192.168.1.234, 192.168.1.235, 192.168.1.236, 192.168.1.237, 192.168.1.238, 192.168.1.239, 192.168.1.240, 192.168.1.241, 192.168.1.242, 192.168.1.243, 192.168.1.244, 192.168.1.245, 192.168.1.246, 192.168.1.247, 192.168.1.248, 192.168.1.249, 192.168.1.250, 192.168.1.251, 192.168.1.252, 192.168.1.253, 192.168.1.254.
Not shown: 254 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  rsh
26/tcp    open  rlogin
27/tcp    open  rcp
30/tcp    open  ncp
31/tcp    open  l2tp
33/tcp    open  l2tp
34/tcp    open  l2tp
35/tcp    open  l2tp
36/tcp    open  l2tp
37/tcp    open  l2tp
38/tcp    open  l2tp
39/tcp    open  l2tp
40/tcp    open  l2tp
41/tcp    open  l2tp
42/tcp    open  l2tp
43/tcp    open  l2tp
44/tcp    open  l2tp
45/tcp    open  l2tp
46/tcp    open  l2tp
47/tcp    open  l2tp
48/tcp    open  l2tp
49/tcp    open  l2tp
50/tcp    open  l2tp
51/tcp    open  l2tp
52/tcp    open  l2tp
53/tcp    open  l2tp
54/tcp    open  l2tp
55/tcp    open  l2tp
56/tcp    open  l2tp
57/tcp    open  l2tp
58/tcp    open  l2tp
59/tcp    open  l2tp
60/tcp    open  l2tp
61/tcp    open  l2tp
62/tcp    open  l2tp
63/tcp    open  l2tp
64/tcp    open  l2tp
65/tcp    open  l2tp
66/tcp    open  l2tp
67/tcp    open  l2tp
68/tcp    open  l2tp
69/tcp    open  l2tp
70/tcp    open  l2tp
71/tcp    open  l2tp
72/tcp    open  l2tp
73/tcp    open  l2tp
74/tcp    open  l2tp
75/tcp    open  l2tp
76/tcp    open  l2tp
77/tcp    open  l2tp
78/tcp    open  l2tp
79/tcp    open  l2tp
80/tcp    open  l2tp
81/tcp    open  l2tp
82/tcp    open  l2tp
83/tcp    open  l2tp
84/tcp    open  l2tp
85/tcp    open  l2tp
86/tcp    open  l2tp
87/tcp    open  l2tp
88/tcp    open  l2tp
89/tcp    open  l2tp
90/tcp    open  l2tp
91/tcp    open  l2tp
92/tcp    open  l2tp
93/tcp    open  l2tp
94/tcp    open  l2tp
95/tcp    open  l2tp
96/tcp    open  l2tp
97/tcp    open  l2tp
98/tcp    open  l2tp
99/tcp    open  l2tp
100/tcp   open  l2tp
101/tcp   open  l2tp
102/tcp   open  l2tp
103/tcp   open  l2tp
104/tcp   open  l2tp
105/tcp   open  l2tp
106/tcp   open  l2tp
107/tcp   open  l2tp
108/tcp   open  l2tp
109/tcp   open  l2tp
110/tcp   open  l2tp
111/tcp   open  l2tp
112/tcp   open  l2tp
113/tcp   open  l2tp
114/tcp   open  l2tp
115/tcp   open  l2tp
116/tcp   open  l2tp
117/tcp   open  l2tp
118/tcp   open  l2tp
119/tcp   open  l2tp
120/tcp   open  l2tp
121/tcp   open  l2tp
122/tcp   open  l2tp
123/tcp   open  l2tp
124/tcp   open  l2tp
125/tcp   open  l2tp
126/tcp   open  l2tp
127/tcp   open  l2tp
128/tcp   open  l2tp
129/tcp   open  l2tp
130/tcp   open  l2tp
131/tcp   open  l2tp
132/tcp   open  l2tp
133/tcp   open  l2tp
134/tcp   open  l2tp
135/tcp   open  l2tp
136/tcp   open  l2tp
137/tcp   open  l2tp
138/tcp   open  l2tp
139/tcp   open  l2tp
140/tcp   open  l2tp
141/tcp   open  l2tp
142/tcp   open  l2tp
143/tcp   open  l2tp
144/tcp   open  l2tp
145/tcp   open  l2tp
146/tcp   open  l2tp
147/tcp   open  l2tp
148/tcp   open  l2tp
149/tcp   open  l2tp
150/tcp   open  l2tp
151/tcp   open  l2tp
152/tcp   open  l2tp
153/tcp   open  l2tp
154/tcp   open  l2tp
155/tcp   open  l2tp
156/tcp   open  l2tp
157/tcp   open  l2tp
158/tcp   open  l2tp
159/tcp   open  l2tp
160/tcp   open  l2tp
161/tcp   open  l2tp
162/tcp   open  l2tp
163/tcp   open  l2tp
164/tcp   open  l2tp
165/tcp   open  l2tp
166/tcp   open  l2tp
167/tcp   open  l2tp
168/tcp   open  l2tp
169/tcp   open  l2tp
170/tcp   open  l2tp
171/tcp   open  l2tp
172/tcp   open  l2tp
173/tcp   open  l2tp
174/tcp   open  l2tp
175/tcp   open  l2tp
176/tcp   open  l2tp
177/tcp   open  l2tp
178/tcp   open  l2tp
179/tcp   open  l2tp
180/tcp   open  l2tp
181/tcp   open  l2tp
182/tcp   open  l2tp
183/tcp   open  l2tp
184/tcp   open  l2tp
185/tcp   open  l2tp
186/tcp   open  l2tp
187/tcp   open  l2tp
188/tcp   open  l2tp
189/tcp   open  l2tp
190/tcp   open  l2tp
191/tcp   open  l2tp
192/tcp   open  l2tp
193/tcp   open  l2tp
194/tcp   open  l2tp
195/tcp   open  l2tp
196/tcp   open  l2tp
197/tcp   open  l2tp
198/tcp   open  l2tp
199/tcp   open  l2tp
200/tcp   open  l2tp
201/tcp   open  l2tp
202/tcp   open  l2tp
203/tcp   open  l2tp
204/tcp   open  l2tp
205/tcp   open  l2tp
206/tcp   open  l2tp
207/tcp   open  l2tp
208/tcp   open  l2tp
209/tcp   open  l2tp
210/tcp   open  l2tp
211/tcp   open  l2tp
212/tcp   open  l2tp
213/tcp   open  l2tp
214/tcp   open  l2tp
215/tcp   open  l2tp
216/tcp   open  l2tp
217/tcp   open  l2tp
218/tcp   open  l2tp
219/tcp   open  l2tp
220/tcp   open  l2tp
221/tcp   open  l2tp
222/tcp   open  l2tp
223/tcp   open  l2tp
224/tcp   open  l2tp
225/tcp   open  l2tp
226/tcp   open  l2tp
227/tcp   open  l2tp
228/tcp   open  l2tp
229/tcp   open  l2tp
230/tcp   open  l2tp
231/tcp   open  l2tp
232/tcp   open  l2tp
233/tcp   open  l2tp
234/tcp   open  l2tp
235/tcp   open  l2tp
236/tcp   open  l2tp
237/tcp   open  l2tp
238/tcp   open  l2tp
239/tcp   open  l2tp
240/tcp   open  l2tp
241/tcp   open  l2tp
242/tcp   open  l2tp
243/tcp   open  l2tp
244/tcp   open  l2tp
245/tcp   open  l2tp
246/tcp   open  l2tp
247/tcp   open  l2tp
248/tcp   open  l2tp
249/tcp   open  l2tp
250/tcp   open  l2tp
251/tcp   open  l2tp
252/tcp   open  l2tp
253/tcp   open  l2tp
254/tcp   open  l2tp
```

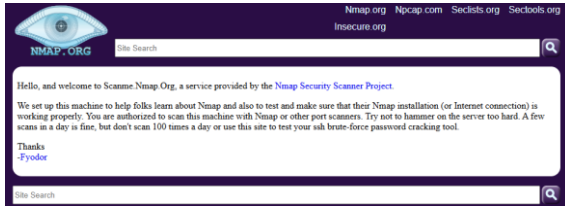
## D: Quanti host sono attivi?

## R: Un host attivo



## Passo 3: Scansiona un server remoto

a. Apri un browser web e naviga su [scanme.nmap.org](https://scanme.nmap.org). Leggi il messaggio pubblicato.



**D:** Qual è lo scopo di questo sito?

**R:** Scopo del sito Scanme.Nmap.Org:

**Obiettivo principale:** Fornire una macchina di test per imparare e testare Nmap.

### Funzioni:

- Ambiente di pratica per comandi Nmap
- Verifica del corretto funzionamento di installazioni Nmap
- Test di connessioni Internet
- Piattaforma educativa per port scanning

### Limitazioni:

- Massimo pochi scan al giorno
- Non utilizzare per brute-force di password
- Non sovraccaricare il server

È un servizio gratuito del **Nmap Security Scanner Project** per scopi didattici e di testing.

- c. Al prompt del terminale, inserisci `nmap -A -T4 scanme.nmap.org`.
- d. c. Rivedi i risultati e rispondi alle seguenti domande.

**D:** Quali porte e servizi sono aperti?

**R:** Porte e servizi aperti:

- 22/tcp: SSH (OpenSSH 6.6.1p1 Ubuntu)
- 80/tcp: HTTP (Apache httpd 2.4.7)
- 9929/tcp: nping-echo
- 31337/tcp: tcpwrapped

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 06:03 EDT
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 (ECDHE)
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 29.95 seconds
```

**Quali porte e servizi sono filtrati?**

**R:** Porte filtrate:

- 25/tcp: SMTP
- 135/tcp: msrpc
- 139/tcp: netbios-ssn
- 445/tcp: microsoft-ds

**Qual è l'indirizzo IP del server?**

**R:** Indirizzo IP: 45.33.32.156

**Qual è il sistema operativo?**

**R:** Sistema operativo:

Linux (Ubuntu), probabilmente Ubuntu 20.04 basato sulla versione OpenSSH 6.6.1p1

Il server mostra anche porte chiuse (1024, 3389, 255, 256) e alcune con servizi non standard come nping-echo sulla porta 9929.

## Domanda di Riflessione

### Nmap: Strumento a Doppio Taglio per la Sicurezza di Rete

Utilizzo Legittimo per la Sicurezza

Nmap è essenziale per i professionisti della sicurezza che devono identificare vulnerabilità nelle proprie reti prima che lo facciano gli attaccanti. Permette di scoprire servizi esposti involontariamente, verificare l'efficacia dei firewall e mantenere un inventario aggiornato dei sistemi di rete. Gli amministratori possono così correggere configurazioni errate e chiudere porte non necessarie, riducendo la superficie d'attacco.

### Potenziale Uso Malevolo

Gli stessi meccanismi di scansione possono essere sfruttati da criminali informatici per mappare reti target senza autorizzazione. Attraverso tecniche di fingerprinting, gli attaccanti raccolgono informazioni dettagliate su sistemi operativi e servizi in esecuzione, creando una mappa precisa per pianificare attacchi mirati. Le funzionalità stealth di Nmap permettono inoltre di evitare molti sistemi di rilevamento.

### Conclusione

La differenza fondamentale tra uso legittimo e malevolo sta nell'autorizzazione e nell'intento. Nmap è uno strumento neutro la cui eticità dipende da chi e come viene utilizzato. Per questo motivo, le organizzazioni devono implementare sistemi di monitoraggio per rilevare scansioni non autorizzate e utilizzare proattivamente Nmap per anticipare le mosse degli attaccanti.

## Bonus 2: Attacco a un database MySQL

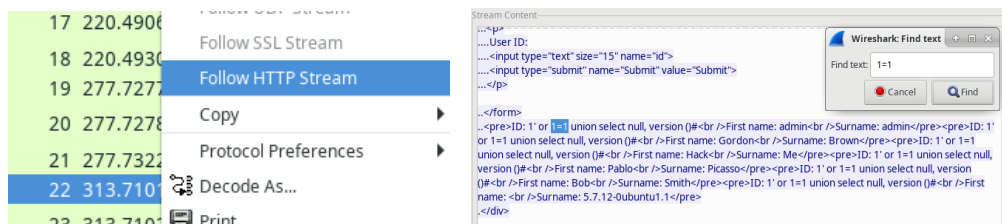
a.b.c.d.e. Aperto wireshark e caricando il file PCAP – analizziamolo.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.4	10.0.2.15	TCP	74	35614 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=45838 TSecr=0 WS=128
2	0.000315	10.0.2.15	10.0.2.4	TCP	74	80 → 35614 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=38535 TSecr=45838 WS=12
3	0.000349	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=45838 TSecr=38535
4	0.000681	10.0.2.4	10.0.2.15	HTTP	654	POST /dwa/login.php HTTP/1.1 (application/x-www-form-urlencoded)
5	0.002149	10.0.2.15	10.0.2.4	TCP	66	80 → 35614 [ACK] Seq=1 Ack=589 Win=30208 Len=0 TSval=38536 TSecr=45838
6	0.005700	10.0.2.15	10.0.2.4	HTTP	430	HTTP/1.1 302 Found
7	0.005700	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=589 Ack=365 Win=30336 Len=0 TSval=45840 TSecr=38536
8	0.014383	10.0.2.4	10.0.2.15	HTTP	496	GET /dwa/index.php HTTP/1.1
9	0.015485	10.0.2.15	10.0.2.4	HTTP	3107	HTTP/1.1 200 OK (text/html)
10	0.015485	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1019 Ack=3406 Win=36480 Len=0 TSval=45843 TSecr=38539
11	0.068625	10.0.2.4	10.0.2.15	HTTP	429	GET /dwa/dwa/css/main.css HTTP/1.1
12	0.070400	10.0.2.15	10.0.2.4	HTTP	1511	HTTP/1.1 200 OK (text/css)
13	174.254430	10.0.2.4	10.0.2.15	HTTP	536	GET /dwa/vulnerabilities/sql/?id=1%3D1&Submit=Submit HTTP/1.1
14	174.254581	10.0.2.15	10.0.2.4	TCP	66	80 → 35638 [ACK] Seq=1 Ack=471 Win=235 Len=0 TSval=82101 TSecr=98114
15	174.257989	10.0.2.15	10.0.2.4	HTTP	1861	HTTP/1.1 200 OK (text/html)
16	220.490531	10.0.2.4	10.0.2.15	HTTP	577	GET /dwa/vulnerabilities/sql/?id=1%27+or+%270%27%3D%270+&Submit=Submit HTTP/1.1
17	220.490637	10.0.2.15	10.0.2.4	TCP	66	80 → 35640 [ACK] Seq=1 Ack=512 Win=235 Len=0 TSval=93660 TSecr=111985
18	220.493085	10.0.2.15	10.0.2.4	HTTP	1918	HTTP/1.1 200 OK (text/html)
19	277.727722	10.0.2.4	10.0.2.15	HTTP	630	GET /dwa/vulnerabilities/sql/?id=1%27+or+1%3D1+union+select+database%28%29%2C+user%28%29%23&Submit=Submit HTTP/1.1

**D:** Quali sono i due indirizzi IP coinvolti in questo attacco di SQL injection in base alle informazioni visualizzate?

**R:**  
10.0.2.15 Target  
10.0.2.4 Attaccante

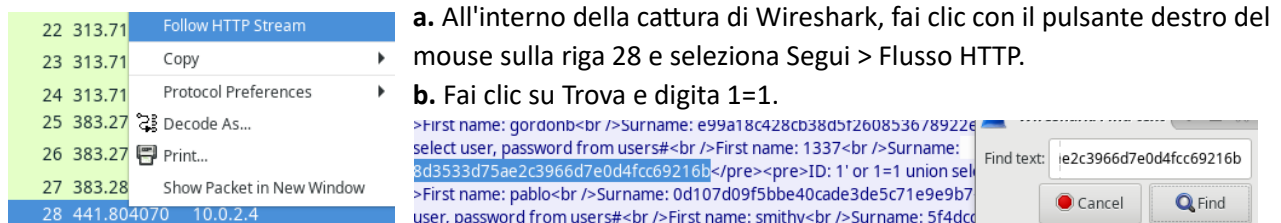
## L'attacco di SQL Injection fornisce informazioni di sistema



**D:** Qual è la versione?

**R:** La versione è 5.7.12-0ubuntu1.1.

## L'attacco di SQL Injection e le informazioni sulle tabelle



- All'interno della cattura di Wireshark, fai clic con il pulsante destro del mouse sulla riga 28 e seleziona Segui > Flusso HTTP.
- Fai clic su Trova e digita 1=1.

**D:** Quale utente ha l'hash della password di 8d3533d75ae2c3966d7e0d4fcc69216b?

c. Usando un sito web come <https://crackstation.net/>, copia l'hash della password nel cracker di hash di password e inizia a decifrare.

**R:** La password appartiene all'utente 1337.

**D:** Quale è la password in chiaro?



**R:** La password in chiaro è 'charley'.