Report Test Day S11L5

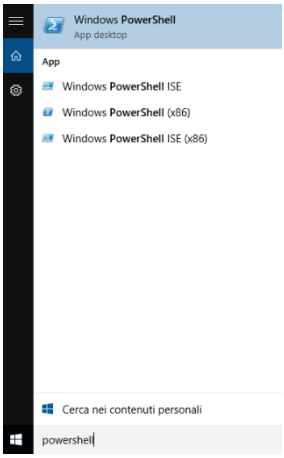
Esercizio 1: Usare Windows Power Shell

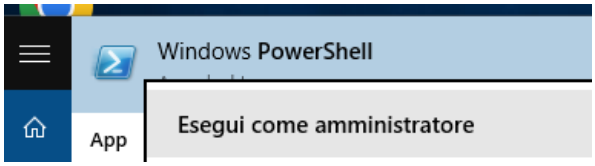
Obiettivi L'obiettivo del laboratorio è esplorare alcune delle funzioni di PowerShell.

- 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.

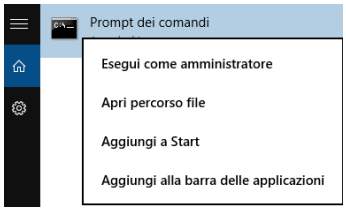
Parte 1: Accedere alla console PowerShell

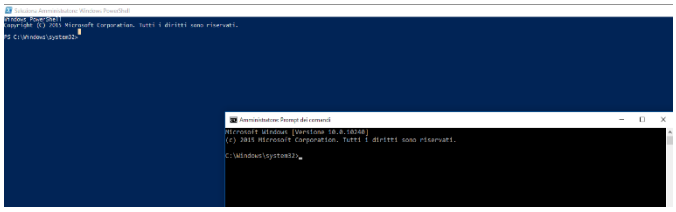
Una volta avviata la nostra VM windows 10, andiamo su → Start → PowerShell → Esegui come amministratore. Allo stesso modo di nuovo andiamo su → Start → Cmd → Esegui come amministratore.





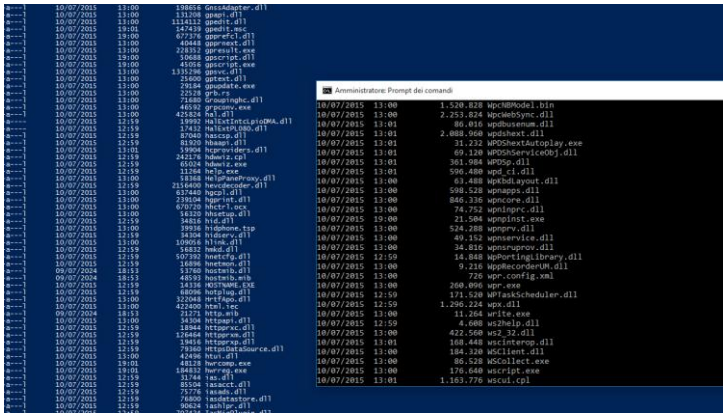
Avremmo, una volta terminato, entrambi i terminali aperti.





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 **elencare 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)

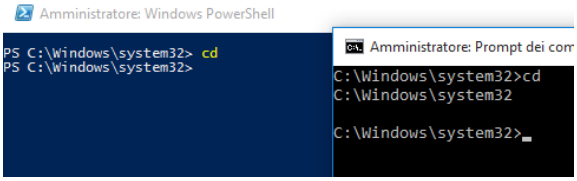
- Il comando dir è **nativo di CMD**.
- Elenca i file e le cartelle presenti nella directory corrente.
- Mostra:
    - La data e l'ora di modifica
    - <DIR> per le cartelle
    - La dimensione dei file
    - Il numero totale di file/cartelle e lo spazio libero su disco

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.

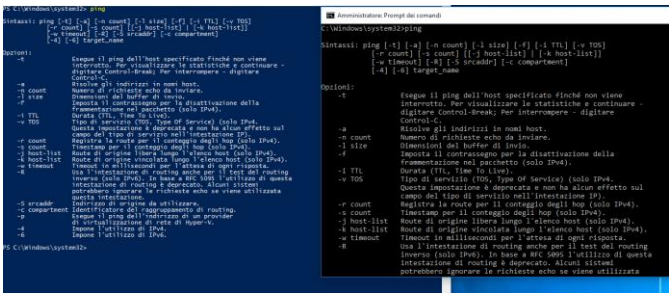
b) Prova un altro comando che hai usato nel prompt dei comandi, come ping, cd e ipconfig.
D: Quali sono i risultati?

(Comando *cd*)



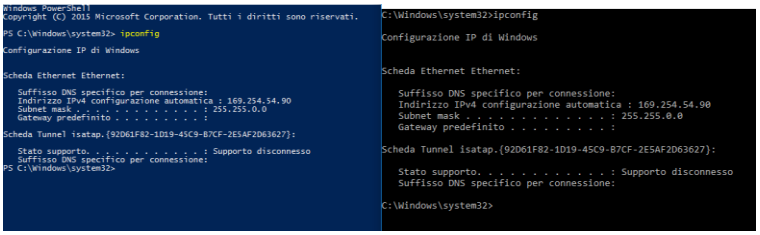
R: Proviamo a scrivere cd all'interno delle nostre console. Cd sta per ''change directory'', digitando solo cd ci mostra la directory corrente sia su Cmd che su Powershell.

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:

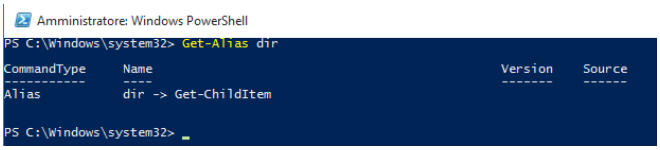
- l'indirizzo IPv4 assegnato a ogni scheda di rete (Ethernet, Wi-Fi, ecc.),
- la subnet mask,
- il gateway predefinito (se presente).

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

a. 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-Alias dir al prompt di PowerShell.

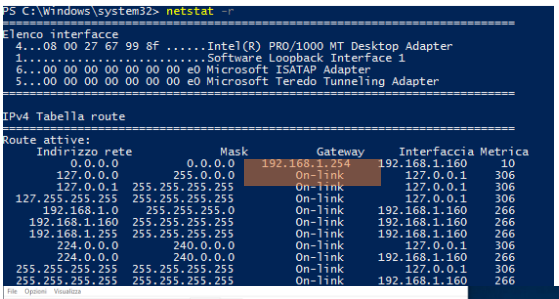
Digitando Get-Alias dir, la console ci avvisa che non è un comando compatibile con PowerShell.



D: Qual è il comando PowerShell per dir?

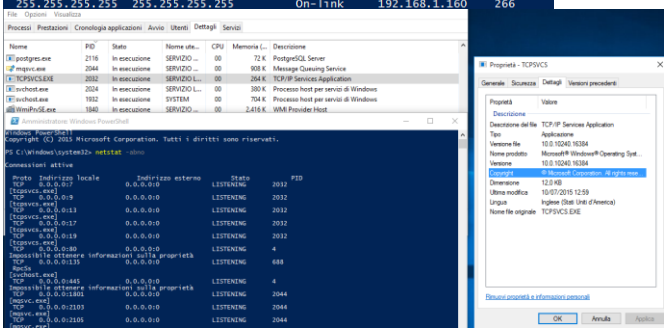
R: Ci avvisa in realtà già la console che per 'dir → Get-ChildItem' cioè per dir in PowerShell dobbiamo usare Get-ChildItem. Non ci è infatti servito fare nessuna ricerca su internet come richiesto nell'esercizio, in quanto la console già ci fornisce gli strumenti per sapere quale è il comando giusto.

Parte 4: Esplorare il comando netstat usando PowerShell



D: Qual è il gateway IPv4?

R: Il Gateway è 192.168.1.254



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

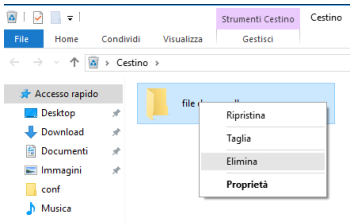
R: Dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID 2032 (TCPSVCS.EXE) si ottengono le seguenti informazioni:

- **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

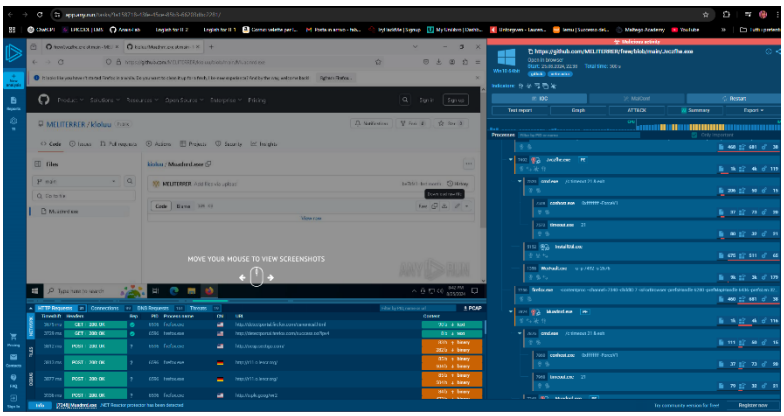
- **Test-NetConnection** verifica rapidamente la connettività di rete e identifica porte aperte. Esempio: Test-NetConnection -ComputerName "server.com" -Port 443 per testare connessioni HTTPS.
- **Get-FileHash** calcola hash crittografici per verificare l'integrità dei file. Get-FileHash -Algorithm SHA256 "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 Ioc

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:

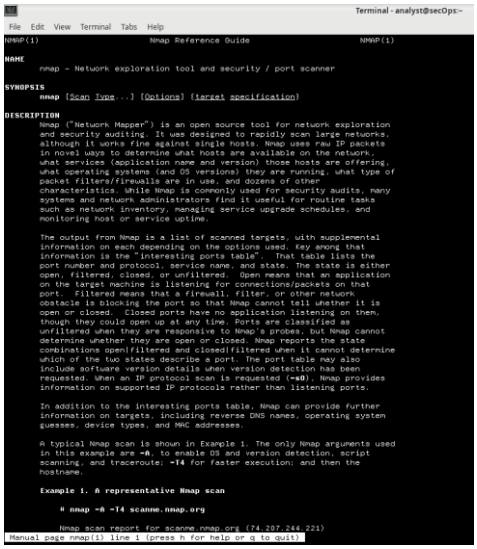
- Implementazione di regole di detection basate sugli IoC identificati
- Monitoraggio proattivo per comunicazioni verso i domini C2
- Aggiornamento delle signature antimalware con gli hash del campione

---

Bonus Parte 1: Esplorazione di Nmap

a. Avvia la VM CyberOps Workstation.
b. Apri un terminale.
c. Al prompt del terminale, inserisci man nmap.

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



R: **Cos'è Nmap?**

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

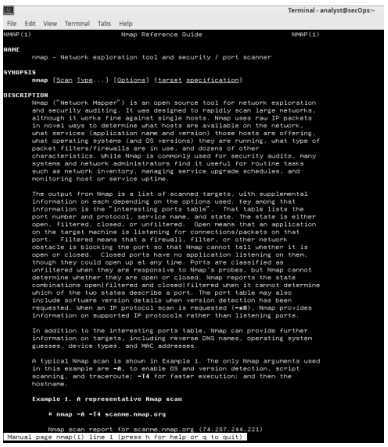
Utilizzi:

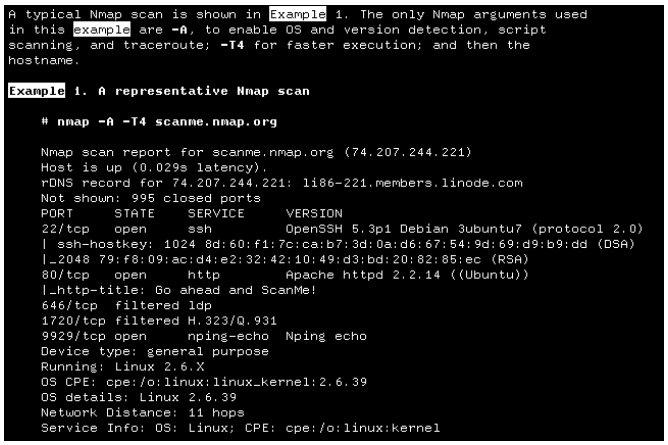
- **Sicurezza**: Penetration testing e vulnerability assessment
- **Amministrazione**: Inventario di rete e monitoraggio
- **Troubleshooting**: Diagnosi problemi di connettività

Funzioni principali:

- Scoperta host
- Scansione porte
- Rilevamento OS e servizi

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

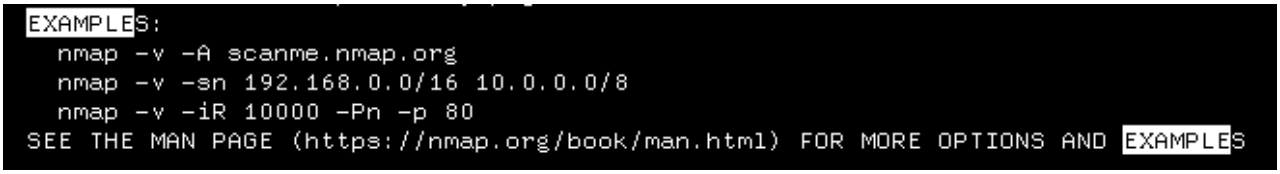




e. Nella prima istanza di example, vedi tre corrispondenze. Per passare alla corrispondenza successiva, premi n.

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@secOps ~]$ 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: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@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 08:00:27:9c:e5:64 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 global dynamic mngtmpaddr noprefixroute
       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:e5:94 brd ff:ff:ff:ff:ff:ff
4: s1: <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

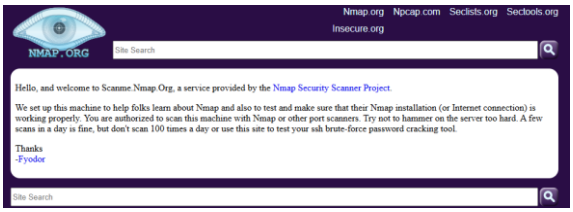
b. Per localizzare altri host su questa LAN, inserisci nmap -A -T4 indirizzo_rete/prefisso.

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. 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.

```
[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 (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 29.95 seconds
```

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

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

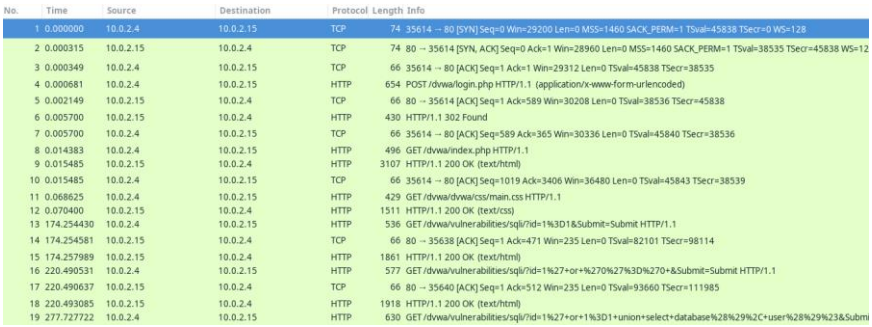
Nmap è essenziale per i professionisti della sicurezza che devono identificare vulnerabilità nelle proprie reti prima che lo facciano gli attaccanti. Permette di scoprire servizi esposti involontariamente, verificare l'efficacia dei firewall e mantenere un inventario aggiornato dei sistemi di rete. Gli 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

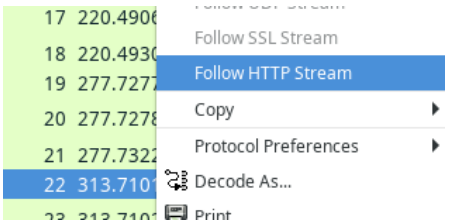
a.b.c.d.e. Aperto wireshark e caricando il file PCAP – analizziamolo.

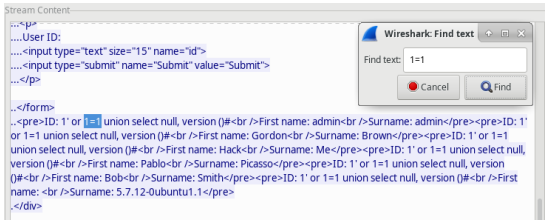


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.4	10.0.2.15	TCP	74	35614 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=45838 TSecr=0 WS=128
2	0.000315	10.0.2.15	10.0.2.4	TCP	74	80 → 35614 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=38535 TSecr=45838 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 /dvwa/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 /dvwa/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 /dvwa/dvwa/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 /dvwa/vulnerabilities/sqli/?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 /dvwa/vulnerabilities/sqli/?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 /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+database%28%29%2C+user%28%29%23&Submi

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

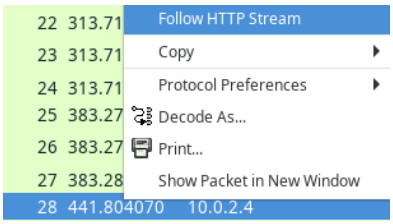




D: Qual è la versione?

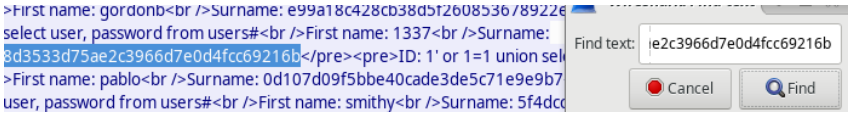
R: La versione è 5.7.12-0ubuntu1.1.

L'attacco di SQL Injection e le informazioni sulle tabelle



a. All'interno della cattura di Wireshark, fai clic con il pulsante destro del mouse sulla riga 28 e seleziona Segui > Flusso HTTP.

b. Fai clic su Trova e digita 1=1.

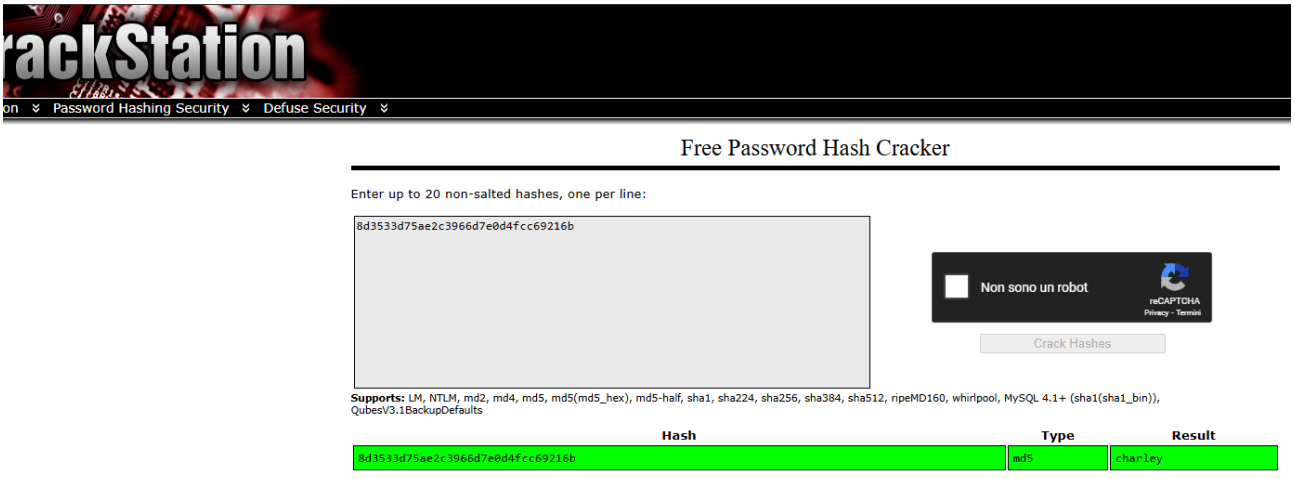


D: Quale utente ha l'hash della password di 8d3533d75ae2c3966d7e0d4fcc69216b?

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'.

Fabriani Anais
13/06/2025