
Verifica 21/02/25

CONSEGNA 1

Laboratorio -

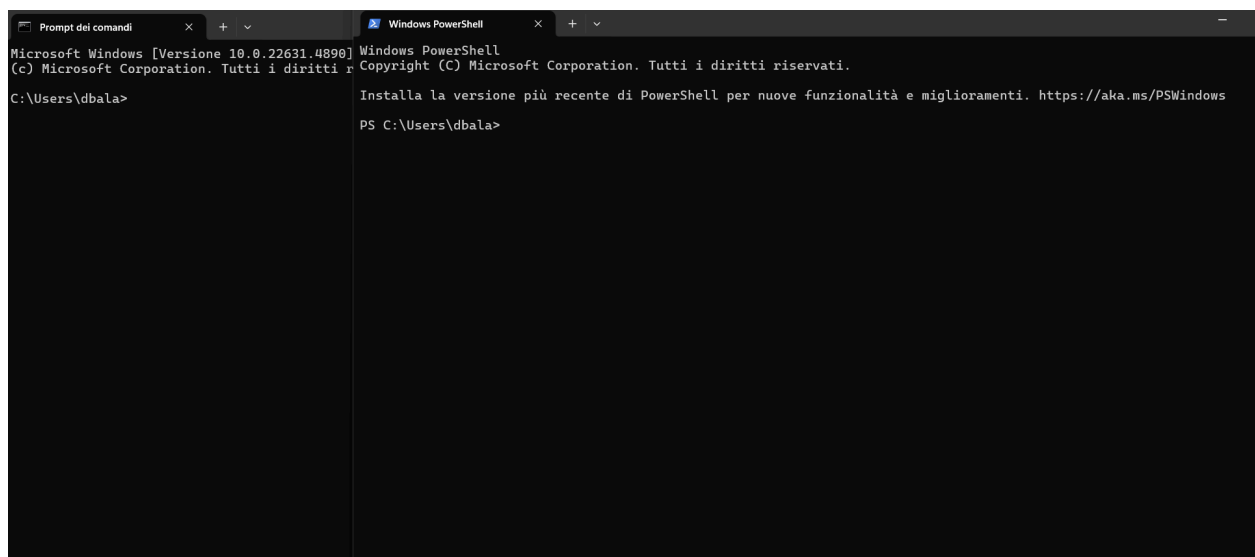
Utilizzo di Windows PowerShell In questo laboratorio, esploreremo alcune delle funzioni di Cyber Security & Ethical Hacking Cisco CyberOps PowerShell .

<https://itexamanswers.net/3-3-11-lab-using-windows-powershell-answers.html>

PASSAGGI

Part 1: Access PowerShell console.

- Click **Start**. Search and select **powershell**.
- Click **Start**. Search and select **command prompt**.



Part 2: Explore Command Prompt and PowerShell commands.

a. Enter **dir** at the prompt in both windows.

What are the outputs to the **dir** command?

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

PS C:\Users\dbala> DIR

Directory: C:\Users\dbala

Mode                LastWriteTime         Length Name
----                -
d-----          27/11/2024         12:16      .ms-ad
d-----          10/02/2025         11:32      .splunk
d-----          14/02/2025         15:41      .VirtualBox
d-----          19/09/2024         15:17      .vscode
d-----          16/10/2024         18:03      ansel
d-----          10/01/2025         11:31      Cisco Packet Tracer 8.2.2
d-----          18/09/2024         10:42      Contacts
d-----          24/09/2024         19:12      Documents
d-----          14/02/2025         16:21      Downloads
d-----          03/12/2024          09:50      eserciziC
d-----          04/12/2024         11:26      eserciziVssEpicode
d-----          18/09/2024         10:42      Favorites
d-----          18/09/2024         10:42      Links
d-----          18/09/2024         10:42      Music
d-----          28/10/2024         14:10      My project
d-----          25/11/2024         17:24      OneDrive
d-----          08/10/2024         12:49      PROGETTI
d-----          18/09/2024         10:42      Saved Games
d-----          19/09/2024         14:36      Searches
d-----          10/02/2025         16:37      splunk ssh
d-----          09/01/2025          00:51      Tracing

Prompt dei comandi
Microsoft Windows [Versione 10.0.22631.4890]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\dbala>dir

Il volume nell'unità C è Acer
Numero di serie del volume: 06D9-D6D6

Directory di C:\Users\dbala

14/02/2025  15:41  <DIR>      .
19/09/2024  13:36  <DIR>      ..
08/10/2024  11:47          58 .gitconfig
27/11/2024  12:16  <DIR>      .ms-ad
10/01/2025  00:35      176 .packettracer
10/02/2025  11:32  <DIR>      .splunk
14/02/2025  15:41  <DIR>      .VirtualBox
19/09/2024  14:17  <DIR>      .vscode
16/10/2024  17:03  <DIR>      ansel
10/01/2025  11:31  <DIR>      Cisco Packet Tracer 8.2.2
18/09/2024  09:42  <DIR>      Contacts
24/09/2024  18:12  <DIR>      Documents
14/02/2025  16:21  <DIR>      Downloads
03/12/2024  09:50  <DIR>      eserciziC
04/12/2024  11:26  <DIR>      eserciziVssEpicode
18/09/2024  09:42  <DIR>      Favorites
18/09/2024  09:42  <DIR>      Links
18/09/2024  09:42  <DIR>      Music
28/10/2024  14:10  <DIR>      My project
25/11/2024  17:24  <DIR>      OneDrive
08/10/2024  11:49  <DIR>      PROGETTI
18/09/2024  09:42  <DIR>      Saved Games
19/09/2024  13:36  <DIR>      Searches
10/02/2025  16:37  <DIR>      splunk ssh
09/01/2025  00:51  <DIR>      Tracing
```

Both windows provide a list of subdirectories and files, and associated information like type, file size, date and time of last write. In PowerShell, the attributes/modes are also shown.

b. Try another command that you have used in the command prompt, such as **ping**, **cd**, and **ipconfig**.

What are the results?

```
Windows PowerShell x + - Prompt dei comandi x + -
d----- 03/12/2024 09:50      eserciziC      04/12/2024 11:26      <DIR>      eserciziVssEpicode
d----- 04/12/2024 11:26      eserciziVssEpicode 18/09/2024 09:42      <DIR>      Favorites
d----- 18/09/2024 10:42      Favorites          18/09/2024 09:42      <DIR>      Links
d----- 18/09/2024 10:42      Links             18/09/2024 09:42      <DIR>      Music
d----- 18/09/2024 10:42      Music             28/10/2024 14:10      <DIR>      My project
d----- 28/10/2024 14:10      My project        25/11/2024 17:24      <DIR>      OneDrive
d----- 25/11/2024 17:24      OneDrive          08/10/2024 11:49      <DIR>      PROGETTI
d----- 08/10/2024 12:49      PROGETTI          18/09/2024 09:42      <DIR>      Saved Games
d----- 18/09/2024 10:42      Saved Games       19/09/2024 13:36      <DIR>      Searches
d----- 19/09/2024 14:36      Searches          10/02/2025 16:37      <DIR>      splunk ssh
d----- 10/02/2025 16:37      splunk ssh        09/01/2025 00:51      <DIR>      Tracing
d----- 09/01/2025 00:51      Tracing           12/01/2025 18:37      <DIR>      3.012 Untitled-1.html
d----- 23/09/2024 15:15      Videos           23/09/2024 14:15      <DIR>      Videos
d----- 12/02/2025 12:39      VirtualBox VMs    12/02/2025 12:39      <DIR>      VirtualBox VMs
-a----- 08/10/2024 12:47      58 .gitconfig      3 File      3.246 byte
-a----- 10/01/2025 00:35      176 .packettracer     25 Directory 183.979.216.896 byte disponibili
-a----- 12/01/2025 18:37      3012 Untitled-1.html

PS C:\Users\dbala> ping 8.8.8.8

Esecuzione di Ping 8.8.8.8 con 32 byte di dati:
Risposta da 8.8.8.8: byte=32 durata=13ms TTL=114
Risposta da 8.8.8.8: byte=32 durata=13ms TTL=114
Risposta da 8.8.8.8: byte=32 durata=13ms TTL=114
Risposta da 8.8.8.8: byte=32 durata=13ms TTL=114
Risposta da 8.8.8.8: byte=32 durata=13ms TTL=114

Statistiche Ping per 8.8.8.8:
Pacchetti: Trasmessi = 4, Ricevuti = 4,
Persi = 0 (0% persi)
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 13ms, Massimo = 13ms, Medio = 13ms
PS C:\Users\dbala> cd Downloads
PS C:\Users\dbala\Downloads>

C:\Users\dbala> ping 8.8.8.8

Esecuzione di Ping 8.8.8.8 con 32 byte di dati:
Risposta da 8.8.8.8: byte=32 durata=13ms TTL=114
Risposta da 8.8.8.8: byte=32 durata=28ms TTL=114
Risposta da 8.8.8.8: byte=32 durata=13ms TTL=114
Risposta da 8.8.8.8: byte=32 durata=51ms TTL=114

Statistiche Ping per 8.8.8.8:
Pacchetti: Trasmessi = 4, Ricevuti = 4,
Persi = 0 (0% persi)
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 13ms, Massimo = 51ms, Medio = 26ms

C:\Users\dbala> cd Downloads
C:\Users\dbala\Downloads>
```

The output in both windows are similar.

Part 3: Explore cmdlets.

a. PowerShell commands, cmdlets, are constructed in the form of *verb-noun* string. To identify the PowerShell command to list the subdirectories and files in a directory, enter **Get-Alias dir** at the PowerShell prompt.

What is the PowerShell command for **dir**?

```
PS C:\Users\dbala\Downloads> Get-Alias dir

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

Get-ChildItem

b. For more detailed information about cmdlets, perform an internet search for **Microsoft powershell cmdlets**.

Che cos'è un comando di PowerShell (cmdlet)?

Articolo • 08/11/2024 • 3 contributori

[Commenti e suggerimenti](#)

In questo articolo

[Che cos'è un cmdlet?](#)

[Nomi dei cmdlet](#)

[Passaggi successivi](#)

I comandi per PowerShell sono noti come cmdlet (pronunciati command-let). Oltre ai cmdlet, PowerShell consente di eseguire qualsiasi comando disponibile nel sistema.

1. Get-Module -All

Se vuoi ottenere una panoramica iniziale di tutti i moduli PowerShell importati puoi utilizzare il comando **Get-Module -All**.

shell

```
Get-Module -All
```

2. Get-Command

Esistono centinaia di comandi PowerShell predefiniti. Se hai bisogno di avere una panoramica dei comandi PowerShell a tua disposizione puoi utilizzare **Get-Command**. Il comando ti fornirà un elenco chiaro di tutte le azioni possibili e ti spiegherà brevemente a cosa serve ciascun cmdlet. Questo vale anche se hai installato moduli aggiuntivi.

shell

```
Get-Command
```

3. Get-Help

L'elenco generato da Get-Command ti fornisce una panoramica iniziale dei comandi a tua disposizione. Tuttavia, se hai bisogno di informazioni più dettagliate relative a un comando e alle possibilità che offre, puoi utilizzare il cmdlet **Get-Help**. Questo comando accede alle risorse del tuo PC e ti fornisce tutte le informazioni disponibili. Per attivare questa guida, combina Get-Help con il comando di cui desideri visualizzare la sintassi.

shell

```
Get-Help [[-Name] <String>] [-Path <String>] [-Category <String[]>] [-Component <String[]>] [-F
```

c. Close the Command Prompt window when done.

Part 4: Explore the netstat command using PowerShell.

a. At the PowerShell prompt, enter `netstat -h` to see the options available for the `netstat` command.

```
PS C:\Users\dbala\Downloads> netstat -h

Visualizza statistiche relative ai protocolli e alle connessioni di rete TCP/IP correnti.

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

-a          Visualizza tutte le connessioni e le porte di ascolto.
-b          Visualizza il file eseguibile utilizzato per la creazione di ogni connessione o
           porta di ascolto. Alcuni file eseguibili conosciuti includono
           più componenti indipendenti. In tali casi
           viene visualizzata la sequenza dei componenti utilizzati per la creazione della connes
           o porta di ascolto e il
           nome del file eseguibile viene visualizzato in fondo, tra parentesi quadre ([]). Nella
           e così via, fino al raggiungimento di TCP/IP. Se si utilizza questa opzione,
           l'esecuzione del comando può richiedere molto tempo e riuscirà solo se si dispone di a
           sufficienti.
-e          Visualizza le statistiche Ethernet. Può essere utilizzata insieme all'opzione -s.
-f          Visualizza i nomi di dominio completi (FQDN, Fully Qualified Domain Name) per gli indi
           esterni.
-i          Visualizza il tempo trascorso da una connessione TCP nel suo stato corrente.
-n          Visualizza indirizzi e numeri di porta in forma numerica.
-o          Visualizza l'ID del processo proprietario associato a ogni connessione.
-p proto    Visualizza le connessioni relative al protocollo specificato da "proto",
           che può essere TCP, UDP, TCPv6 o UDPv6. Se utilizzato insieme all'opzione -s
           per le statistiche per protocollo, "proto" può essere:
           IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
-q          Visualizza tutte le connessioni, le porte di ascolto
           e le porte TCP non di ascolto associate. Le porte non di ascolto associate possono ess
           a una connessione attiva.
-r          Visualizza la tabella di routing.
-s          Visualizza le statistiche per protocollo. Per impostazione predefinita, vengono
           visualizzate le statistiche per IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6.
           Per specificare un sottoinsieme dei valori predefiniti, è possibile utilizzare l'opzio
-t          Visualizza lo stato di offload della connessione corrente.
-x          Visualizza le connessioni, i listener e gli endpoint
           condivisi.
-y          Visualizza il modello di connessione TCP per tutte le connessioni.
Non può essere utilizzata in combinazione con le altre opzioni.
interval    Ripete la visualizzazione delle statistiche selezionate, con una pausa di un numero di
```

b. To display the routing table with the active routes, enter `netstat -r` at the prompt.

IPv4 Tabella route

=====

Route attive:

Indirizzo rete	Mask	Gateway	Interfaccia	Metrica
0.0.0.0	0.0.0.0	<u>192.168.1.1</u>	192.168.1.44	35
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
192.168.1.0	255.255.255.0	On-link	192.168.1.44	291
192.168.1.44	255.255.255.255	On-link	192.168.1.44	291
192.168.1.255	255.255.255.255	On-link	192.168.1.44	291
192.168.56.0	255.255.255.0	On-link	192.168.56.1	281
192.168.56.1	255.255.255.255	On-link	192.168.56.1	281
192.168.56.255	255.255.255.255	On-link	192.168.56.1	281
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	192.168.56.1	281
224.0.0.0	240.0.0.0	On-link	192.168.1.44	291
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	192.168.56.1	281
255.255.255.255	255.255.255.255	On-link	192.168.1.44	291

=====

What is the IPv4 gateway?

The gateway is 192.168.1.1

c. Open and run a second PowerShell with elevated privileges. Click **Start**. Search for PowerShell and right-click **Windows PowerShell** and select **Run as administrator**. Click **Yes** to allow this app to make changes to your device.

```

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

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

PS C:\WINDOWS\system32>

```

d. The netstat command can also display the processes associated with the active TCP connections. Enter the `netstat -abno` at the prompt.

```
PS C:\WINDOWS\system32> netstat -abno

Connessioni attive

Proto Indirizzo locale      Indirizzo esterno      Stato      PID
TCP    0.0.0.0:135              0.0.0.0:0              LISTENING  1372
RpcSs
[svchost.exe]
TCP    0.0.0.0:445              0.0.0.0:0              LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:808              0.0.0.0:0              LISTENING  4092
[OneApp.IGCC.WinService.exe]
TCP    0.0.0.0:5040             0.0.0.0:0              LISTENING  10156
CDPSvc
[svchost.exe]
TCP    0.0.0.0:5426             0.0.0.0:0              LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:7680             0.0.0.0:0              LISTENING  20384
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:8000             0.0.0.0:0              LISTENING  4544
[splunkd.exe]
TCP    0.0.0.0:8089             0.0.0.0:0              LISTENING  4544
[splunkd.exe]
TCP    0.0.0.0:8191             0.0.0.0:0              LISTENING  7760
[smss.exe]
```

e. Open the Task Manager. Navigate to the **Details** tab. Click the **PID** heading so the PID are in order.

Dettagli							
Nome	PID	Stato	Nome utente	CPU	Memoria (...)	Architet...	Descrizione
Interrupt sistema	-	In esecuzione	SYSTEM	00	0 K		Chiamate di procedura differite e ISR (Inte...
Processo di inattività...	0	In esecuzione	SYSTEM	96	8 K		Percentuale di tempo di inattività del proc...
System	4	In esecuzione	SYSTEM	00	12 K		NT Kernel & System
Registry	144	In esecuzione	SYSTEM	00	6.100 K		NT Kernel & System
smss.exe	572	In esecuzione	SYSTEM	00	8 K		Gestione sessioni di Windows
services.exe	592	In esecuzione	SYSTEM	00	3.112 K		App Servizi e Controller
lsass.exe	640	In esecuzione	SYSTEM	00	6.600 K	x64	Local Security Authority Process
dllhost.exe	648	In esecuzione	dbala	00	2.336 K	x64	COM Surrogate
csrss.exe	864	In esecuzione	SYSTEM	00	720 K		Processo runtime client server
wininit.exe	972	In esecuzione	SYSTEM	00	8 K		Applicazione di avvio di Windows
csrss.exe	980	In esecuzione	SYSTEM	00	1.188 K		Processo runtime client server
winlogon.exe	1068	In esecuzione	SYSTEM	00	556 K	x64	Applicazione Accesso a Windows
AggregatoHost.exe	1176	In esecuzione	SYSTEM	00	908 K	x64	Microsoft (R) Aggregator Host
svchost.exe	1196	In esecuzione	SYSTEM	00	8.648 K	x64	Processo host per servizi di Windows
fontdrvhost.exe	1232	In esecuzione	UMFD-1	00	896 K	x64	Usermode Font Driver Host
fontdrvhost.exe	1236	In esecuzione	UMFD-0	00	80 K	x64	Usermode Font Driver Host
svchost.exe	1372	In esecuzione	SERVIZIO D...	00	12.012 K	x64	Processo host per servizi di Windows
svchost.exe	1420	In esecuzione	SYSTEM	00	1.196 K	x64	Processo host per servizi di Windows
svchost.exe	1472	In esecuzione	SYSTEM	00	1.560 K	x64	Processo host per servizi di Windows
WUDFHost.exe	1496	In esecuzione	SERVIZIO L...	00	416 K	x64	Windows Driver Foundation - Processo hc
svchost.exe	1552	In esecuzione	SYSTEM	00	232 K	x64	Processo host per servizi di Windows
chrome.exe	1568	In esecuzione	dbala	00	2.292 K	x64	Google Chrome
svchost.exe	1572	In esecuzione	SERVIZIO L...	00	1.196 K	x64	Processo host per servizi di Windows
svchost.exe	1584	In esecuzione	SERVIZIO L...	00	592 K	x64	Processo host per servizi di Windows
svchost.exe	1592	In esecuzione	SERVIZIO L...	00	1.928 K	x64	Processo host per servizi di Windows
svchost.exe	1716	In esecuzione	SYSTEM	00	624 K	x64	Processo host per servizi di Windows
svchost.exe	1724	In esecuzione	SERVIZIO L...	00	792 K	x64	Processo host per servizi di Windows
identity.exe	1732	In esecuzione	SYSTEM	00	5.068 K	x64	identity

f. Select one of the PIDs from the results of netstat -abno. PID 756 is used in this example.

```

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

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

PS C:\WINDOWS\system32> netstat -abno

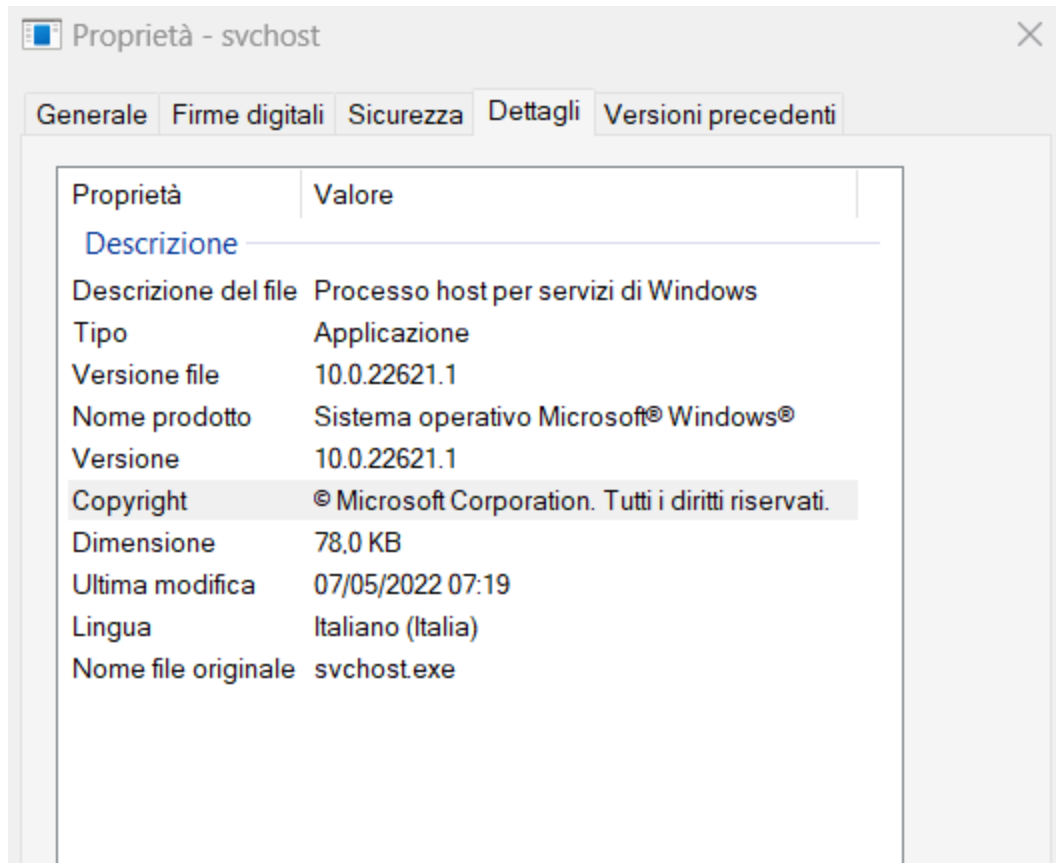
Connessioni attive

Proto Indirizzo locale      Indirizzo esterno  Stato  PID
TCP    0.0.0.0:135              0.0.0.0:0          LISTENING  1372
RpcSs
[svchost.exe]
TCP    0.0.0.0:445              0.0.0.0:0          LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:808              0.0.0.0:0          LISTENING  4092
[OneApp.IGCC.WinService.exe]
TCP    0.0.0.0:5040             0.0.0.0:0          LISTENING  10156
CDPSvc
[svchost.exe]

```

fontdrvhost.exe	1236	In esecuzione	UMFD-0	00	80
<u>svchost.exe</u>	1372	In esecuzione	<u>SERVIZIO DI RETE</u>	00	12.252
svchost.exe	1420	In esecuzione	SYSTEM	00	1.172
svchost.exe	1472	In esecuzione	SYSTEM	00	1.476

g. Locate the selected PID in the Task Manager. Right-click the selected PID in the Task Manager to open the **Properties** dialog box for more information.



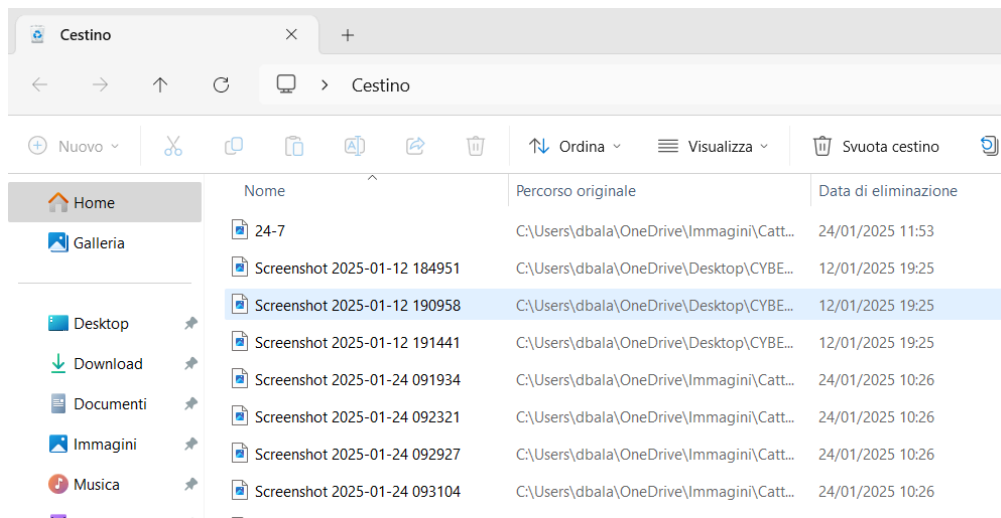
What information can you get from the Details tab and the Properties dialog box for your selected PID?

PID 756 is associated with svchost.exe process. The user for this process is SERVIZIO DI RETE and it is using 12.196K of memory.

Part 5: Empty recycle bin using PowerShell.

PowerShell commands can simplify management of a large computer network. For example, if you wanted to implement a new security solution on all servers in the network you could use a PowerShell command or script to implement and verify that the services are running. You can also run PowerShell commands to simplify actions that would take multiple steps to execute using Windows graphical desktop tools.

a. Open the Recycle Bin. Verify that there are items that can be deleted permanently from your PC. If not, restore those files.



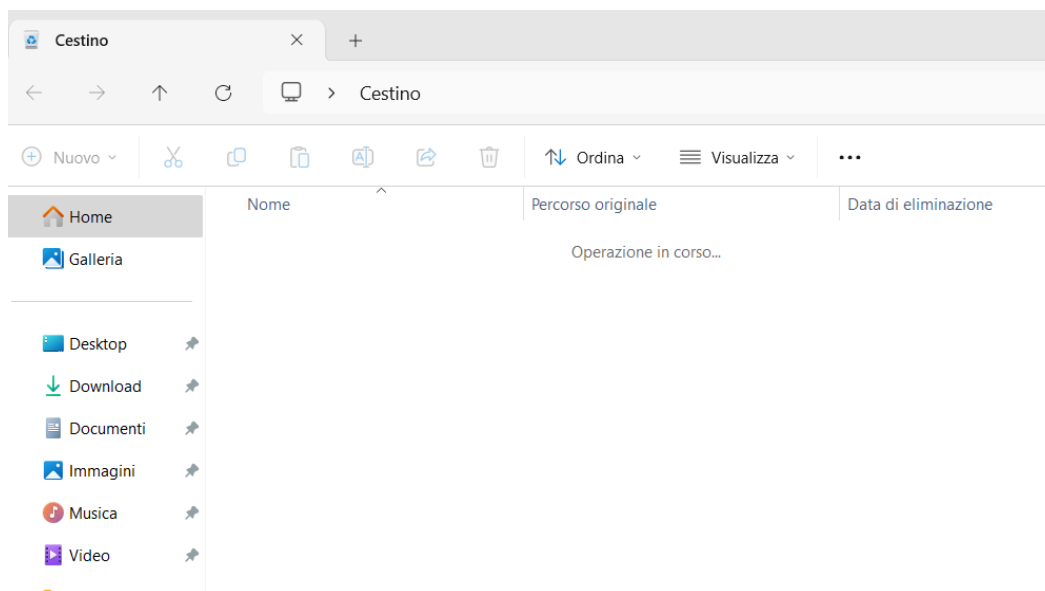
b. If there are no files in the Recycle Bin, create a few files, such as text file using Notepad, and place them into the Recycle Bin.

c. In a PowerShell console, enter `clear-recyclebin` at the prompt.

```
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>
```

What happened to the files in the Recycle Bin?



The files in the Recycle Bin are deleted permanently.

CONSEGNA 2

Esercizio 2 Cyber Security & Ethical Hacking Cisco CyberOps Studiare questo link di anyrun e spiegare queste minacce in un piccolo report. <https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/>

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

The screenshot displays the AnyRun analysis interface. On the left, a browser window shows the GitHub repository for MELTERRER/frew. The main panel shows a list of HTTP requests, including GET and POST requests to various URLs. On the right, a sidebar shows the 'Malicious activity' section, highlighting the 'firefox.exe' process. The process details show the file path 'C:\Program Files\Mozilla Firefox\firefox.exe' and the command line arguments. A circular progress indicator shows 47 out of 100.

PASSAGGI

1. Verifica informazioni di base

Per cominciare identifichiamo il nome del programma analizzato, ovvero

The screenshot shows the AnyRun interface with the file path 'C:\Program Files\Mozilla Firefox\Jvczfhe.exe' highlighted in a red circle. The interface includes a Windows logo, the URL 'https://github.com/MELTERRER/frew/blob/main/Jvczfhe.exe', and the text 'Open in browser'. Below this, it shows 'Start: 25.08.2024, 22:38' and 'Total time: 300 s'. The 'Indicators' section at the bottom shows various icons representing different types of indicators.

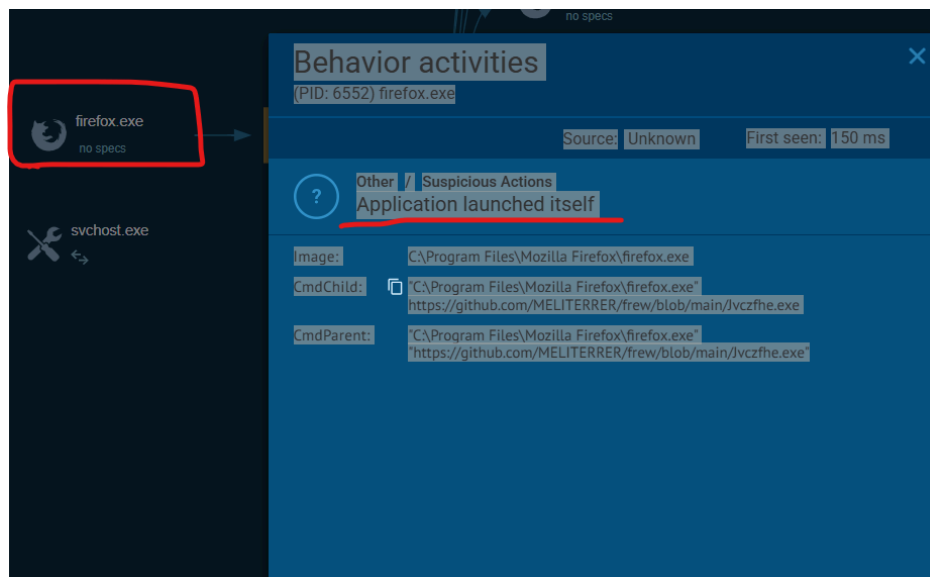
Jvczfhe.exe

Apriamo quindi l'albero dei processi per una visualizzazione più organica e procediamo con un'analisi step-by-step

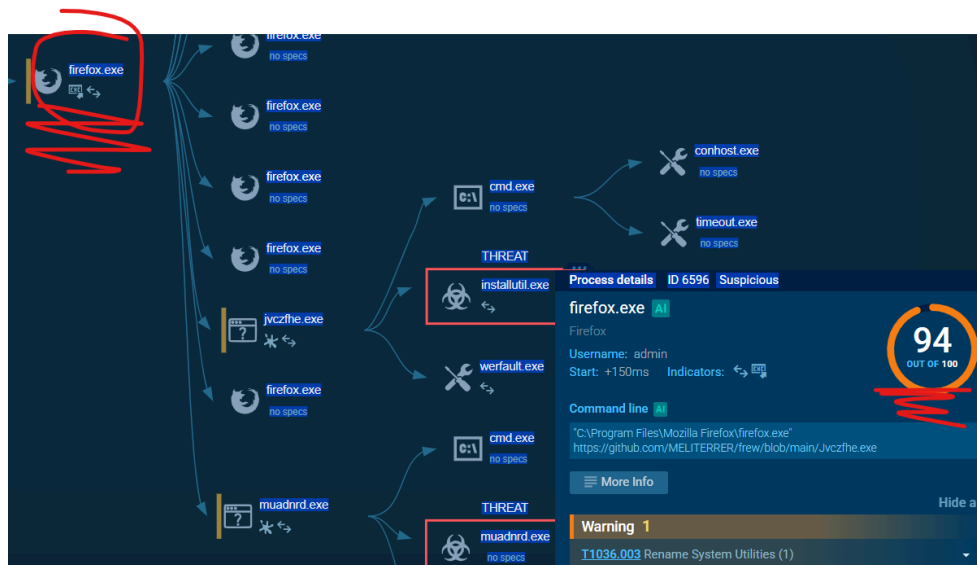


2.ANALISI PRIMO PROCESSO FIREFOX

Facendo doppio click sul primo processo notiamo che:



L'esecuzione sembra essere stata lanciata da una fonte sconosciuta, un comportamento tipico dei malware che vengono avviati da remoto o sono automatizzati per eseguirsi in totale autonomia, puntando verso il processo firefox vediamo che:



il processo sembra aver 'droppato' ovvero eseguito il **download** di un file **.exe** da una o più repository github, inoltre abbiamo un **Warning** relativo al fatto che il processo sembra stia tentando di effettuare una rinomina del file droppato in modo da farlo passare per un file di sistema '**legittimo**'.

Techniques details

Get to know what this threat is about

Warning (1)

Subtechniques ▼ [T1036](#)

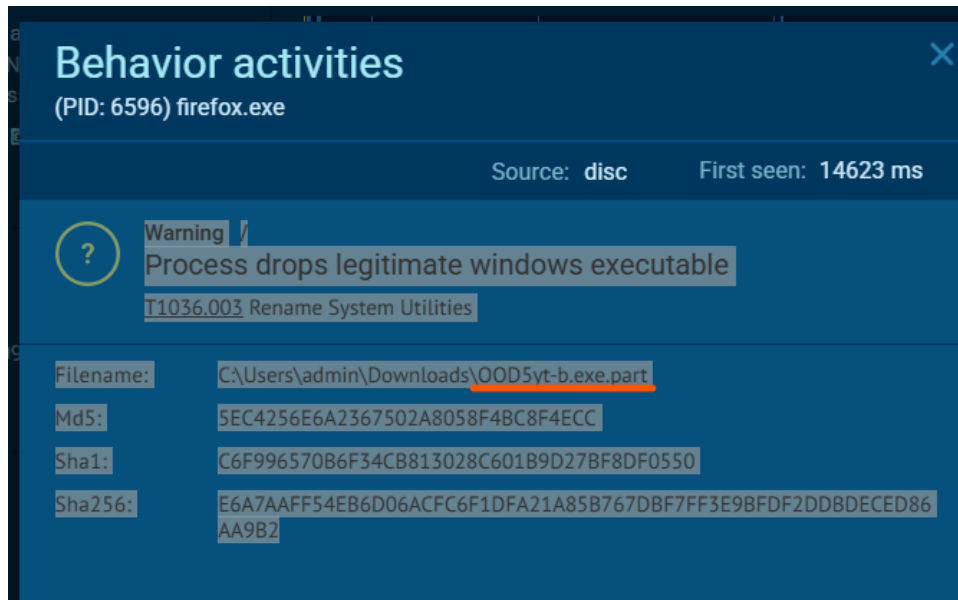
"Masquerading"

Permissions required:

Data sources: Service: Service Creation, Scheduled Job: Scheduled Job Metadata, Scheduled Job: Scheduled Job Modification, Service: Service Metadata, File: File

Rename System Utilities ▲

- Process drops legitimate windows executable (1)
6596 firefox.exe (1)



Andiamo quindi a fare un'ispezione più approfondita sulle azioni effettuate dal processo e notiamo che

Main Information	Put the slider in the desired position or select the desired segment by yourself (?)
Code signing Valid	4.559 s +14.18 s 318.437 s
Process dump 0	
Events	
Modified files 243	
Registry changes 90	
Synchronization 473	
HTTP requests 28	
Connections 71	
Network threats 0	
Modules 168	
Debug 0	
[6596] Firefox.exe	
[6744] Firefox.exe	
[6816] Firefox.exe	
[7048] Firefox.exe	
[6680] Firefox.exe	
[6368] Firefox.exe	
[6384] Firefox.exe	
[6340] Firefox.exe	

Time	Type	Size	Path and MD5
			tion-twitter-digest256-1.vlpset 0e74baccab7b2923ce25b62f282edd71f
+14184 ms	binary	293 b	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protec tion-twitter-digest256.vlpset 0e74baccab7b2923ce25b62f282edd71f
+14473 ms	executable	105 Kb	C:\Users\admin\Downloads\OOD5vt-b.exe.part 5ec4256e6a2367502a8058f4bc8f4ecc
+14489 ms	binary	264 b	C:\Users\admin\AppData\Local\Low\Microsoft\CryptnetUrlCache\MetaData\37C951188967C8EB88D99893D9D191FE fb64a9ebcd48d3895381d5b7d80743d
+14727 ms	text	19 Kb	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\prefs-1.js 16356b99f12bbb2dfaab7c487cd8c03a
+14727 ms	text	19 Kb	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\prefs.js 16356b99f12bbb2dfaab7c487cd8c03a
+14786 ms	executable	105 Kb	C:\Users\admin\Downloads\jvczffe.exe 5ec4256e6a2367502a8058f4bc8f4ecc

il processo effettua 243 modifiche di cui alcune inerenti file.exe, tra i quali troviamo il file appena droppato, il file oggetto dell'analisi e non solo, modifica anche due eseguibili che si trovano nella cartella di firefox, solitamente usati per le librerie, ma potenzialmente oggetto d'attacco da parte dell'hacker al fine di

camuffarsi

Modified files	243				09372174e83dbbf696ee732fd2e875bb
Registry changes	90				
Synchronization	473	+51341 ms	text	20 Kb	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\prefs-1.js db81071da69309e4cd299b6c44bf0487
HTTP requests	28				
Connections	71	+51341 ms	text	20 Kb	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\prefs.js db81071da69309e4cd299b6c44bf0487
Network threats	0				
Modules	168				
Debug	0	+51395 ms	executable	1 Mb	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\gmp-gmpopenh264\2.3.2\gmpopenh264.dll.tmp 842039753bf41fa5e11b3a1383061a87
5596] Firefox.exe		+51395 ms	executable	1 Mb	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\gmp-gmpopenh264\2.3.2\gmpopenh264.dll 842039753bf41fa5e11b3a1383061a87
[6744] Firefox.exe					

inoltre vediamo anche altre due modifiche a file eseguibili presenti nella cartella download e quindi presumibilmente appena scaricati

Events	Time	Type	Size	Path and MD5
Modified files	243	+101355 ms binary	3 Kb	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\sessionstore-backups\recovery.jsonlz496ee13ecee12a1dc7d5d0053cf78e5f3
Registry changes	90			
Synchronization	473			
HTTP requests	28			
Connections	71			
Network threats	0	+104523 ms binary	65 Kb	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\permissions.sqlite-journal88789738f7a746ded927d4c99a63ba7a
Modules	168			
Debug	0	+104971 ms executable	106 Kb	C:\Users\admin\Downloads\xtorRoyHX.exe.part9773175646f2942573bb40551b142a99
		+105216 ms executable	106 Kb	C:\Users\admin\Downloads\Muadnrd.exe9773175646f2942573bb40551b142a99

il primo, a parere mio ma senza la certezza per dirlo, potrebbe essere il file .exe che è stato precedentemente rinominato, mentre il secondo è con più probabilità il **payload** malevolo vero e proprio, ma vedremo in seguito il perchè di questa affermazione

2.2 CONNESSIONI DI RETE SOSPETTE

Dalla sezione in cui ci troviamo notiamo inoltre che il processo ha avviato un totale di 28 connessioni http. vediamo di cosa si tratta:

HTTP Requests	31	Connections	99	DNS Requests	161	Threats	19	Filter by PID, name or url	PCAP
Timeshift	Headers	Rep	PID	Process name	CN	URL	Content		
3675 ms	GET 200: OK	✓	6596	firefox.exe	🇺🇸	http://detectportal.firefox.com/canonic...	90 b ↓ text		
3729 ms	GET 200: OK	✓	6596	firefox.exe	🇺🇸	http://detectportal.firefox.com/success...	8 b ↓ text		
3812 ms	POST 200: OK	?	6596	firefox.exe	🇺🇸	http://ocsp.sectigo.com/	83 b ↑ binary 282 b ↓ binary		
3813 ms	POST 200: OK	?	6596	firefox.exe	🇩🇪	http://r11.o.lencr.org/	85 b ↑ binary 504 b ↓ binary		

Synchronization	4/3	http://ocsp.sectigo.com/
HTTP requests	28	+3662 ms POST 200: OK ? Unknown United States 83 b ↑ binary 282 b ↓ binary
Connections	71	http://r11.o.lencr.org/
Network threats	0	+3663 ms POST 200: OK ? Unknown Germany 85 b ↑ binary 504 b ↓ binary
Modules	168	http://r11.o.lencr.org/
Debug	0	+3727 ms POST 200: OK ? Unknown Germany 85 b ↑ binary 504 b ↓ binary
▼ [6596] Firefox.exe		http://o.pki.goog/wr2
[6744] Firefox.exe		+3786 ms POST 200: OK ? Unknown United States 84 b ↑ binary 472 b ↓ binary
[6816] Firefox.exe		http://r10.o.lencr.org/
[7048] Firefox.exe		+3809 ms POST 200: OK ? Unknown Germany 85 b ↑ binary 504 b ↓ binary
[6680] Firefox.exe		http://r10.o.lencr.org/
[6368] Firefox.exe		+3813 ms POST 200: OK ? Unknown Germany 85 b ↑ binary 504 b ↓ binary
[6384] Firefox.exe		
[6340] Firefox.exe		
[6360] Firefox.exe		
[6456] Firefox.exe		
▼ [7492] Jvczfhe.exe		
▼ [7520] Cmd.exe		
[7528] Cmd.exe		

Come si può notare scorrendo le richieste di tipo **POST** sembra che il processo stia tentando di avviare connessioni con una ventina di indirizzi IP diversi e di dubbia natura, vista la condizione UNKNOWN della loro ‘reputation’ e l’appartenenza a paesi diversi di cui la maggiorparte alla germania.

Passiamo in rassegna alcuni di questi indirizzi con ‘**VirusTotal**’ e verifichiamo eventuali malignità note

0

/ 96

Community Score

-25

No security vendors flagged this URL as malicious

Reanalyze Search More

http://ocsp.sectigo.com/

ocsp.sectigo.com

Status 200

Content type application/ocsp-response

Last Analysis Date 4 days ago

DETECTION

DETAILS

COMMUNITY 47

Join our Community

and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

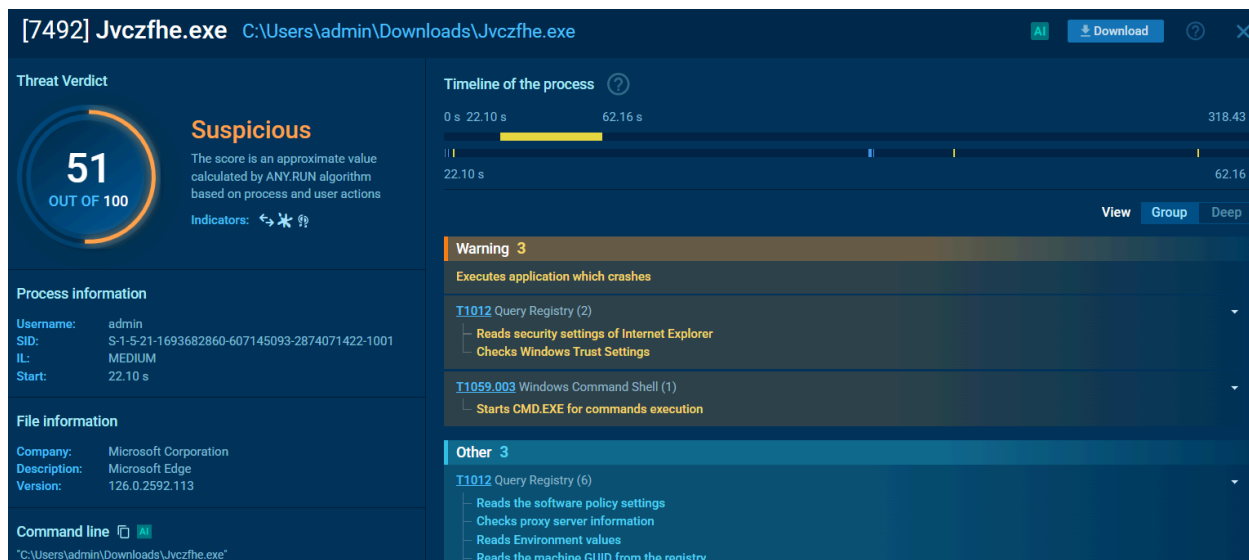
Sembra che non possa esserci d’aiuto, perciò procediamo con l’analisi.

3. PROCESSI FIGLI ESEGUITI

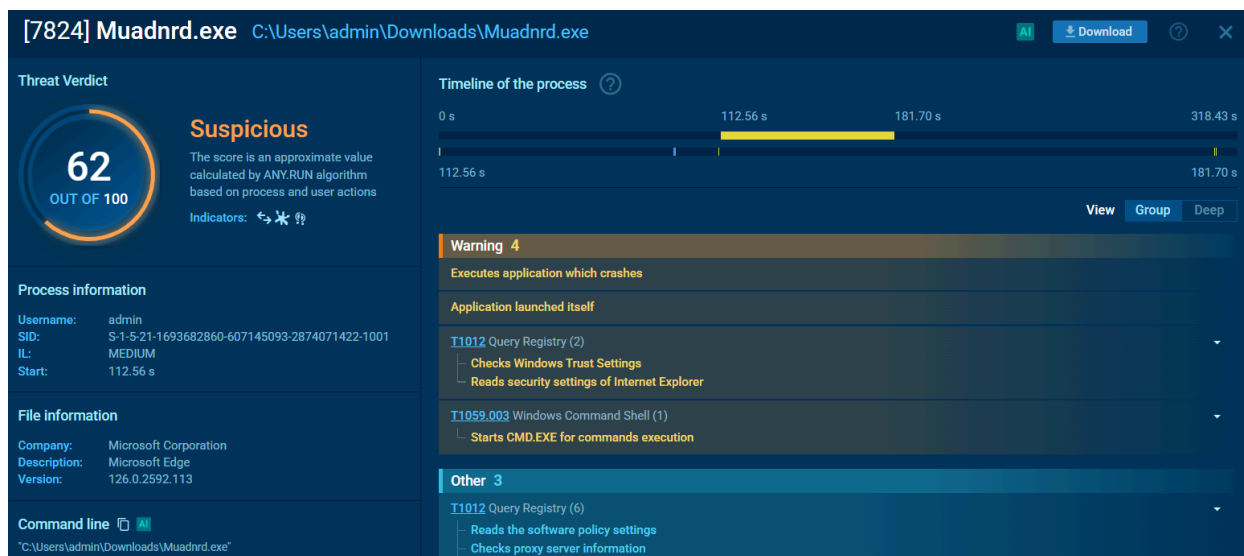
Come abbiamo visto, il processo appena analizzato da vita a diversi processi figli



Concentriamoci su quelli eseguibili, che ci vengono infatti segnalati da AnyRun come sospetti:



The screenshot shows the AnyRun interface for the process **Jvczfhe.exe** (ID: [7492]). The file path is `C:\Users\admin\Downloads\Jvczfhe.exe`. The Threat Verdict is **Suspicious** with a score of **51 OUT OF 100**. The process information shows it was started by `admin` at `22.10 s`. The file information indicates it is from `Microsoft Corporation` and `Microsoft Edge`. The command line is `"C:\Users\admin\Downloads\Jvczfhe.exe"`. The timeline shows a **Warning 3** for **Executes application which crashes**. The process actions include `T1012 Query Registry (2)` (reads security settings of Internet Explorer, checks Windows Trust Settings) and `T1059.003 Windows Command Shell (1)` (starts CMD.EXE for commands execution).

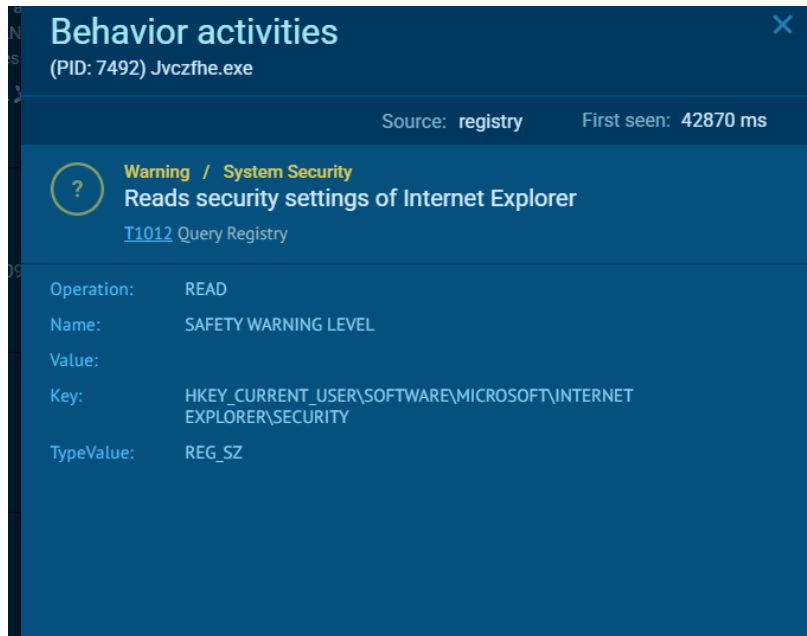


The screenshot shows the AnyRun interface for the process **Muadnrd.exe** (ID: [7824]). The file path is `C:\Users\admin\Downloads\Muadnrd.exe`. The Threat Verdict is **Suspicious** with a score of **62 OUT OF 100**. The process information shows it was started by `admin` at `112.56 s`. The file information indicates it is from `Microsoft Corporation` and `Microsoft Edge`. The command line is `"C:\Users\admin\Downloads\Muadnrd.exe"`. The timeline shows a **Warning 4** for **Executes application which crashes**. The process actions include `T1012 Query Registry (2)` (checks Windows Trust Settings, reads security settings of Internet Explorer) and `T1059.003 Windows Command Shell (1)` (starts CMD.EXE for commands execution).

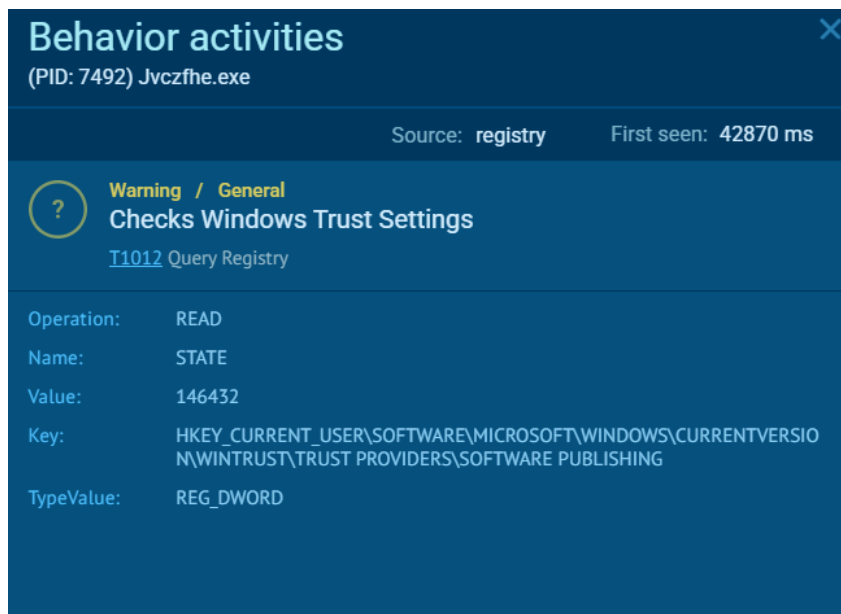
Entrambi provengono dalla cartella Downloads perciò possiamo presumere che il processo padre li abbia scaricati (entrambi o uno dei due se non altro).

Entrambi lanciano un'applicazione che poi va in crash, un comportamento tipico dei malware che tentano di aggirare misure di sicurezza o causare confusione nel loro comportamento per eludere eventuali controlli

Entrambi inoltre presentano la voce 'Launched Itself' che indica la loro automazione nell'avvio, altro elemento sospetto già visto in partenza.



Jvczfhe.exe inoltre come possiamo vedere dal warning, esegue una ‘scansione’ delle nostre impostazioni di sicurezza inerenti internet explorer



il presunto malware fa inoltre una scansione (o una modifica...?) anche delle nostre impostazioni di sistema inerenti le policy di sicurezza, probabilmente al fine di aggirare le impostazioni che bloccherebbero l’avvio di eventuali eseguibili, o che potrebbero rilevarli come sospetti.

dei comportamenti analoghi li esegue anche il secondo programma ovvero

MuadRnd.exe

Behavior activities

(PID: 7492) Jvczfhe.exe

Source: process First seen: 18150 ms

?

Warning / General
Starts CMD.EXE for commands execution
[T1059.003](#) Windows Command Shell

Image:

C:\Windows\SysWOW64\cmd.exe

Cmdline:

"CMD" /C TIMEOUT 21 & EXIT

Behavior activities

(PID: 7824) Muadnrd.exe

Source: process First seen: 108.22 s

?

Warning / General
Starts CMD.EXE for commands execution
[T1059.003](#) Windows Command Shell

Image:

C:\Windows\SysWOW64\cmd.exe

Cmdline:

"CMD" /C TIMEOUT 21 & EXIT

vediamo inoltre che i programmi avviano una **command shell** per l'esecuzione di comandi, quindi a questo punto siamo piuttosto certi si tratti di file malevoli.

Code signing	Untrusted	22.105 s							+21.95 s	62.1
Process dump	0									
▼ Events										
Modified files	0									
Registry changes	23									
Synchronization	37									
HTTP requests	0									
Connections	1									
Network threats	0									
Modules	119									

Time	Type	Rep	CN	Src IP	Port	Dst IP	Port	ASN	↑ Send	↓ Recv
+21956 ms	TCP	?	🇺🇸	185.199.110.133	443	VM	49790	FASTLY	417 b	5 Mb

Advanced details of process

Main information

Code signing

Untrusted

Process dump

0

▼ Events

Modified files

0

Registry changes

22

Synchronization

37

HTTP requests

0

Connections

1

Network threats

0

Modules

116

[7824] Muadnrd.exe

C:\Users\admin\Downloads\Muadnrd.exe

Put the slider in the desired position or select the desired segment by yourself

112.567 s

+20.75 s

181.704 s

Time	Type	Rep	CN	Src IP	Port	Dst IP	Port	ASN	↑ Send	↓ Recv
+20754 ms	TCP	?		185.199.110.133	443	VM	59019	FASTLY	415 b	5 Mb

in ultimo possiamo notare come sia **Jvczfhe.exe** che **Muadnrd.exe** effettuino un unica connessione verso un indirizzo **IP 105.199.110.133** . Questo potrebbe indurci a pensare che tutte le altre connessioni aperte dal processo padre come visto in precedenza attraverso firefox non siano altro che sistemi di mascheraggio per la vera connessione ‘malevola’ aperta dai nostre due eseguibili in questione, ma queste sono speculazioni...

3. PROCESSI ULTIMO STADIO

Come abbiamo visto fino ad ora, i processi avviati dal presunto malware iniziale proseguono come sotto indicato



Anyrun ci segnala due possibili Threat proprio in questa fase dei processi:

[5152] InstallUtil.exe C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe

Threat Verdict

No verdict

The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions

Indicators:

Process information

Username: admin
SID: S-1-5-21-1693682860-607145093-2874071422-1001
IL: MEDIUM
Start: 58.99 s

File information

Company: Microsoft Corporation
Description: .NET Framework installation utility
Version: 4.8.9037.0 built by: NET481REL1

Command line

"C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe"

Timeline of the process

0 s 58.99 s 318.43 s

Warning 1

T1571 Non-Standard Port (1)

Connects to unusual port

Other 3

.NET Reactor protector has been detected

T1012 Query Registry (4)

- Reads Environment values
- Reads the machine GUID from the registry
- Reads the computer name
- Checks supported languages

T1082 System Information Discovery (4)

- Reads Environment values
- Reads the machine GUID from the registry

InstallUtil.exe è un framework di microsoft che viene utilizzato genericamente per installare applicazioni **‘.net’**,ma il warning ci segnala la connessione ad una porta sospetta

Behavior activities

(PID: 5152) InstallUtil.exe

Source: **network** First seen: **56587 ms**

?

Warning / Unusual Activities
Connects to unusual port
[T1571 Non-Standard Port](#)

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
IpDst:	91.92.253.47
PortDst:	7702
PortSrc:	59005
Protocol:	TCP

indicata infatti come ‘NON-Standard port’ . questo ci fa pensare che il file processo stia cercando di scaricare codice malevolo sulla macchina o altri payload di varia natura.

[7248] Muadnrd.exe

C:\Users\admin\Downloads\Muadnrd.exe

Threat Verdict

0

OUT OF 100

No verdict

The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions

Indicators:

Process information

Username: admin
SID: S-1-5-21-1693682860-607145093-2874071422-1001
IL: MEDIUM
Start: 179.71 s

File information

Company: Microsoft Corporation
Description: Microsoft Edge
Version: 126.0.2592.113

Timeline of the process

0 s 179.71 s 210.12 s

179.71 s

Other 3

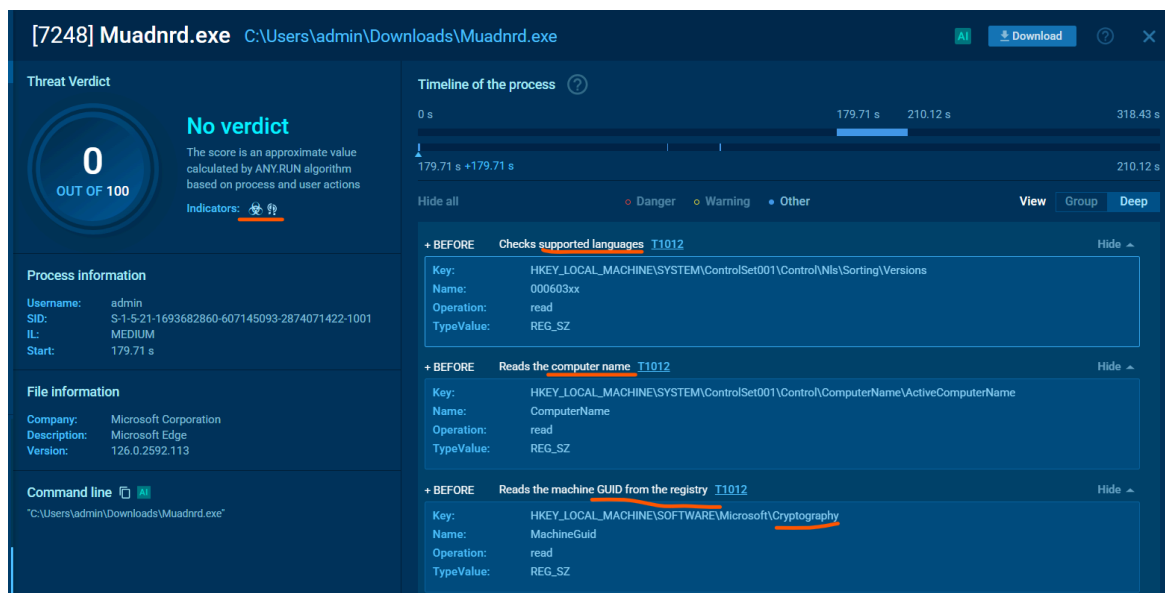
T1012 Query Registry (3)

- Reads the machine GUID from the registry
- Reads the computer name
- Checks supported languages

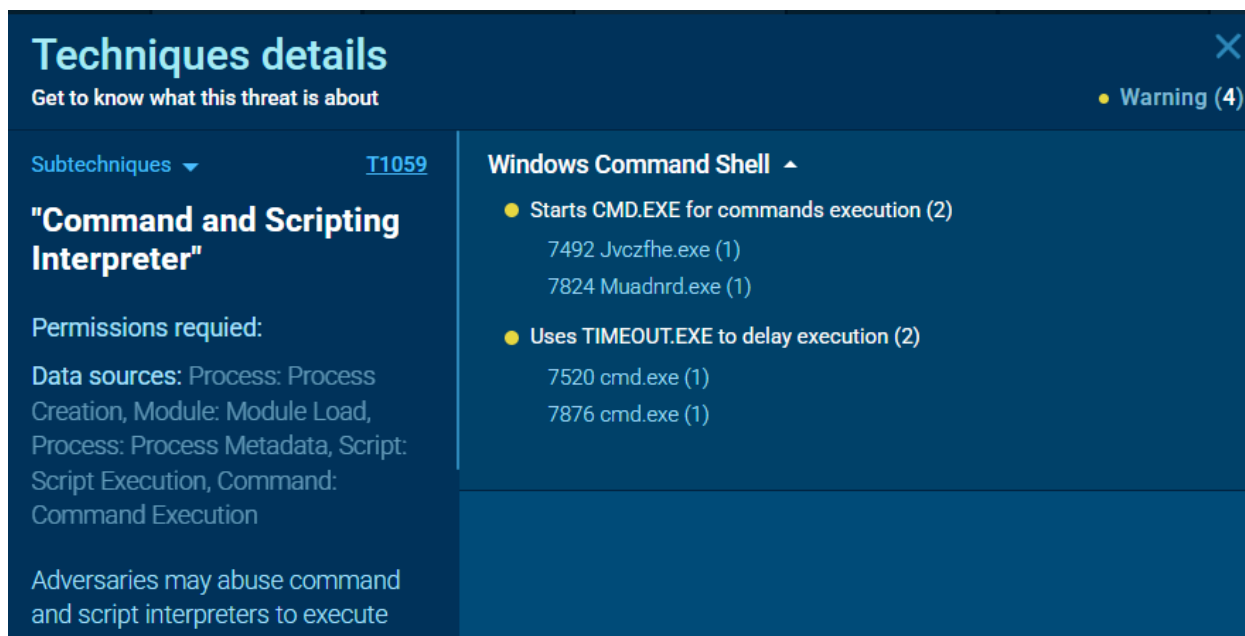
T1082 System Information Discovery (3)

- Reads the machine GUID from the registry
- Reads the computer name
- Checks supported languages

Muadnrd.exe dal canto suo sembra stia avviando delle ricerche come visto in precedenza nel punto 2 inerenti le nostre impostazioni di sicurezza del sistema



Inoltre **Anyrun** ci segnala con il simboletto del **'biohazard'** il fatto che si tratti di una possibile vulnerabilità nota.



All'ultimissimo stadio della nostra analisi possiamo vedere che le due cmd precedentemente aperte e oggetto di sospetto da parte nostra, vengono utilizzate per eseguire **TIMEOUT.EXE** che presumibilmente ha lo scopo

-
- o di ritardare l'esecuzione dei payload/malware al fine di eludere i controlli di sicurezza
 - oppure di ritardare l'esecuzione poichè l'attaccante desidera effettuare l'iniezione o l'esecuzione di codice malevolo in un secondo momento, e viste le numerose scansioni relative la sicurezza della macchina, propendo per la seconda ipotesi

3. CONCLUSIONI

Abbiamo concluso con la quasi totale certezza che si tratti di un malware automatizzato capace di

- downloadare applicazioni eseguibili malevole

-modificarne i nomi

-modificare alcune impostazioni di registro del nostro sistema e/o impostazioni di sicurezza di Windows e/o firefox(Mozzila)

-scansionare le impostazioni di sicurezza della macchina target e di Internet Explorer

-aprire diverse connessioni verso IP di dubbia provenienza

-eseguire due file eseguibili che stabiliscono un'unica connessione verso lo stesso indirizzo IP

Secondo la mia personale opinione,

credo che il malware serva principalmente ad effettuare una scansione delle impostazioni di sicurezza della macchina e dei suoi browser, in particolare internet explorer, e poi ad effettuare alcune eventuali modifiche ed esportare questi dati tramite una connessione TCP.

tutto il resto delle operazioni potrebbero essere volte a mascherare questo comportamento, al fine di lanciare un futuro attacco sulla macchina avendo già preparato un payload adatto a quanto riscontrato nella prima analisi.

ad ogni modo è evidente come la minaccia non sia da sottovalutare e va indicato al cliente che ha fornito l'analisi, come evitare che operazioni del genere succedano e soprattutto come mitigare questo e altri possibili simili attacchi alla sua macchina, in relazione alle vulnerabilità evidenziate in questo report.

BONUS 1

Objectives

- Part 1: Exploring Nmap
- Part 2: Scanning for Open Ports

Background / Scenario

Port scanning is usually part of a reconnaissance attack. There are a variety of port scanning methods that can be used. We will explore how to use the Nmap utility. Nmap is a powerful network utility that is used for network discovery and security auditing.

Required Resources

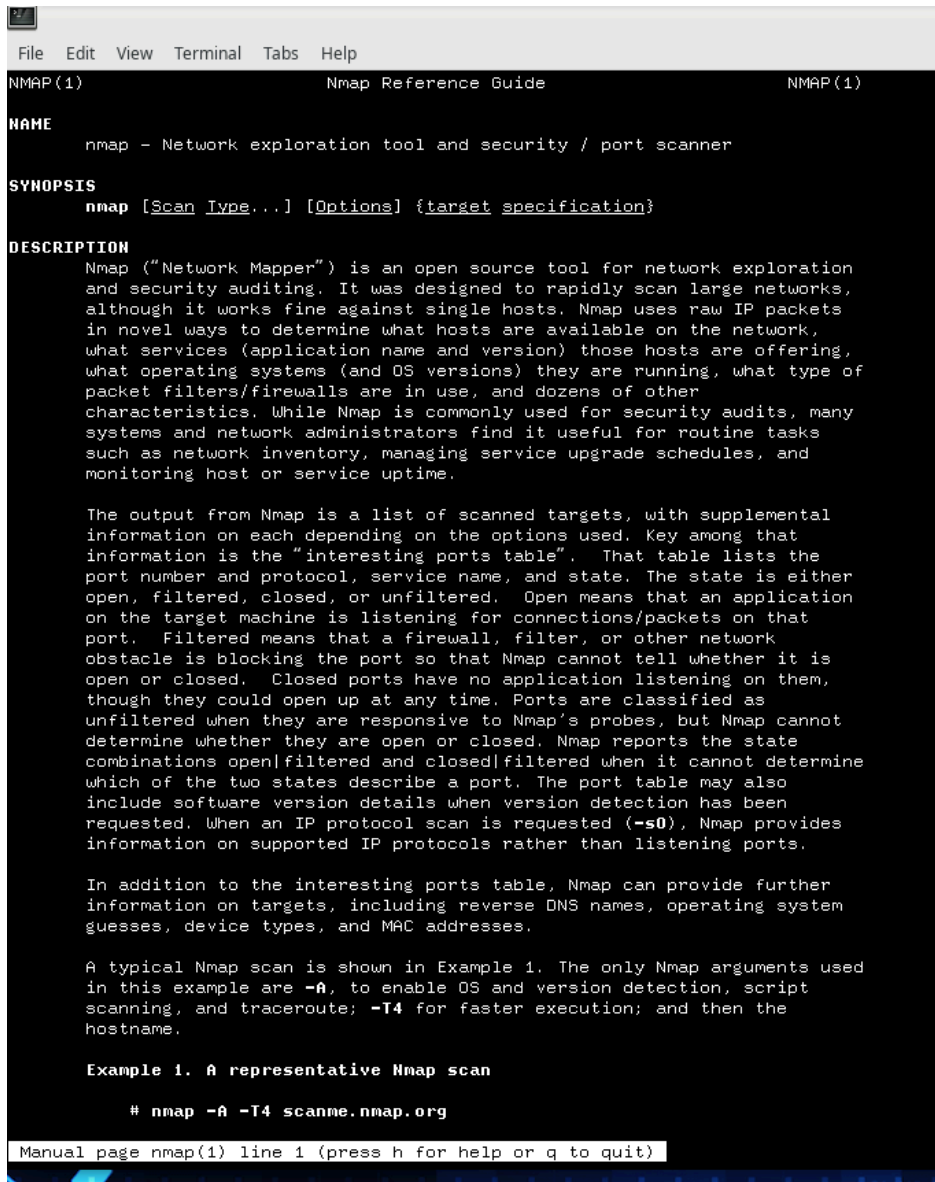
- CyberOps Workstation virtual machine
- Internet access

Part 1: Exploring Nmap

In this part, you will use manual pages (or man pages for short) to learn more about Nmap.

The `man [program | utility | function]` command displays the manual pages associated with the arguments. The manual pages are the reference manuals found on Unix and Linux OSs. These pages can include these sections: Name, Synopsis, Descriptions, Examples, and See Also.

- a. Start CyberOps Workstation VM.
- b. Open a terminal.
- c. At the terminal prompt, enter `man nmap`.



```
NMAP(1) Nmap Reference Guide NMAP(1)

NAME
    nmap - Network exploration tool and security / port scanner

SYNOPSIS
    nmap [Scan Type...] [Options] {target specification}

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

    The output from Nmap is a list of scanned targets, with supplemental
    information on each depending on the options used. Key among that
    information is the "interesting ports table". That table lists the
    port number and protocol, service name, and state. The state is either
    open, filtered, closed, or unfiltered. Open means that an application
    on the target machine is listening for connections/packets on that
    port. Filtered means that a firewall, filter, or other network
    obstacle is blocking the port so that Nmap cannot tell whether it is
    open or closed. Closed ports have no application listening on them,
    though they could open up at any time. Ports are classified as
    unfiltered when they are responsive to Nmap's probes, but Nmap cannot
    determine whether they are open or closed. Nmap reports the state
    combinations open|filtered and closed|filtered when it cannot determine
    which of the two states describe a port. The port table may also
    include software version details when version detection has been
    requested. When an IP protocol scan is requested (-s0), Nmap provides
    information on supported IP protocols rather than listening ports.

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

    A typical Nmap scan is shown in Example 1. The only Nmap arguments used
    in this example are -A, to enable OS and version detection, script
    scanning, and traceroute; -T4 for faster execution; and then the
    hostname.

    Example 1. A representative Nmap scan

    # nmap -A -T4 scanme.nmap.org

Manual page nmap(1) line 1 (press h for help or q to quit)
```

What is Nmap?

Nmap is a network exploration tool and security / port scanner.

What is nmap used for?

Nmap is used to scan a network and determine the available hosts and services offered in the network. Some of the nmap features include host discovery, port scanning and operating system detection. Nmap can be commonly used for security audits, to identify open ports, network inventory, and find vulnerabilities in the network.

d. While in the man page, you can use the up and down arrow keys to scroll through the pages. You can also press the space bar to forward one page at a time.

```
File Edit View Terminal Tabs Help
-sn: Ping Scan - disable port scan
-Pn: Treat all hosts as online -- skip host discovery
-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given port
-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
-PO[protocol list]: IP Protocol Ping
-n/-R: Never do DNS resolution/Always resolve [default: sometimes]
--dns-servers <serv1[,serv2],...>: Specify custom DNS servers
--system-dns: Use OS's DNS resolver
--traceroute: Trace hop path to each host
SCAN TECHNIQUES:
-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/window/Maimon scans
-sU: UDP Scan
-sN/sF/sX: TCP Null, FIN, and Xmas scans
--scanflags <flags>: Customize TCP scan flags
-sI <zombie host[:probeport]>: Idle scan
-sV/sZ: SCTP INIT/COOKIE-ECHO scans
-sO: IP protocol scan
-b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
-p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
--exclude-ports <port ranges>: Exclude the specified ports from scanning
-F: Fast mode - Scan fewer ports than the default scan
-r: Scan ports consecutively - don't randomize
--top-ports <number>: Scan <number> most common ports
--port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
-sV: Probe open ports to determine service/version info
--version-intensity <level>: Set from 0 (light) to 9 (try all probes)
--version-light: Limit to most likely probes (intensity 2)
--version-all: Try every single probe (intensity 9)
--version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
-sC: equivalent to --script=default
--script=<Lua scripts>: <Lua scripts> is a comma separated list of
  directories, script-files or script-categories
--script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
--script-args-file=filename: provide NSE script args in a file
--script-trace: Show all data sent and received
--script-updatedb: Update the script database.
--script-help=<Lua scripts>: Show help about scripts.
  <Lua scripts> is a comma-separated list of script-files or
  script-categories.
OS DETECTION:
-O: Enable OS detection
--osscan-limit: Limit OS detection to promising targets
--osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
Options which take <time> are in seconds, or append 'ms' (milliseconds)
's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
-T<0-5>: Set timing template (higher is faster)
--min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
```

To search for a specific term or phrase use enter a forward slash (/) or question mark (?) followed by the term or phrase. The forward slash searches forward through the document, and the question mark searches backward through the document. The key n moves to the next match.

Type /example and press ENTER. This will search for the word example forward through the man page.

e. In the first instance of example, you see three matches. To move to the next match, press n.

```

File Edit View Terminal Tabs Help

--sn: Ping Scan - disable port scan
--Pn: Treat all hosts as online -- skip host discovery
--PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given port
--PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
--PO[protocol list]: IP Protocol Ping
--n/-R: Never do DNS resolution/Always resolve [default: sometimes]
--dns-servers <serv1[,serv2],...>: Specify custom DNS servers
--system-dns: Use OS's DNS resolver
--traceroute: Trace hop path to each host

SCAN TECHNIQUES:
-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
-sU: UDP Scan
-sN/sF/sX: TCP Null, FIN, and Xmas scans
--scanflags <flags>: Customize TCP scan flags
-sI <zombie host[:probeport]>: Idle scan
-sV/sZ: SCTP INIT/COOKIE-ECHO scans
-sO: IP protocol scan
-b <FTP relay host>: FTP bounce scan

PORT SPECIFICATION AND SCAN ORDER:
-p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
--exclude-ports <port ranges>: Exclude the specified ports from scanning
-F: Fast mode - Scan fewer ports than the default scan
-r: Scan ports consecutively - don't randomize
--top-ports <number>: Scan <number> most common ports
--port-ratio <ratio>: Scan ports more common than <ratio>

SERVICE/VERSION DETECTION:
-sV: Probe open ports to determine service/version info
--version-intensity <level>: Set from 0 (light) to 9 (try all probes)
--version-light: Limit to most likely probes (intensity 2)
--version-all: Try every single probe (intensity 9)
--version-trace: Show detailed version scan activity (for debugging)

SCRIPT SCAN:
-sC: equivalent to --script-default
--script=<Lua scripts>: <Lua scripts> is a comma separated list of
  directories, script-files or script-categories
--script-args=<n1=v1[,n2=v2,...]>: provide arguments to scripts
--script-args-file=filename: provide NSE script args in a file
--script-trace: Show all data sent and received
--script-updatedb: Update the script database.
--script-help=<Lua scripts>: Show help about scripts.
  <Lua scripts> is a comma-separated list of script-files or
  script-categories.

OS DETECTION:
-O: Enable OS detection
--osscan-limit: Limit OS detection to promising targets
--osscan-guess: Guess OS more aggressively

TIMING AND PERFORMANCE:
Options which take <time> are in seconds, or append 'ms' (milliseconds)
's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
-T<0-5>: Set timing template (higher is faster)
--min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes

```

```

File Edit View Terminal Tabs Help

list of numbers or ranges for each octet. For example,
192.168.0-255.1-254 will skip all addresses in the range that end in .0
or .255, and 192.168.3-5.7.1 will scan the four addresses 192.168.3.1,
192.168.4.1, 192.168.5.1, and 192.168.7.1. Either side of a range may
be omitted; the default values are 0 on the left and 255 on the right.
Using - by itself is the same as 0-255, but remember to use 0- in the
first octet so the target specification doesn't look like a
command-line option. Ranges need not be limited to the final octets:
the specifier 0-255.0-255.13.37 will perform an Internet-wide scan for
all IP addresses ending in 13.37. This sort of broad sampling can be
useful for Internet surveys and research.

IPv6 addresses can be specified by their fully qualified IPv6 address
or hostname or with CIDR notation for subnets. Octet ranges aren't yet
supported for IPv6.

IPv6 addresses with non-global scope need to have a zone ID suffix. On
Unix systems, this is a percent sign followed by an interface name; a
complete address might be fe80::a8bb:ccff:fedd:eeff%eth0. On Windows,
use an interface index number in place of an interface name:
fe80::a8bb:ccff:fedd:eeff%1. You can see a list of interface indexes by
running the command netsh.exe interface ipv6 show interface.

Nmap accepts multiple host specifications on the command line, and they
don't need to be the same type. The command nmap scanme.nmap.org
192.168.0.0/8 10.0.0.1,3-7.- does what you would expect.

While targets are usually specified on the command lines, the following
options are also available to control target selection:

-il inputfilename (Input from list)
  Reads target specifications from inputfilename. Passing a huge list
  of hosts is often awkward on the command line, yet it is a common
  desire. For example, your DHCP server might export a list of 10,000
  current leases that you wish to scan. Or maybe you want to scan all
  IP addresses except for those to locate hosts using unauthorized
  static IP addresses. Simply generate the list of hosts to scan and
  pass that filename to Nmap as an argument to the -il option.
  Entries can be in any of the formats accepted by Nmap on the
  command line (IP address, hostname, CIDR, IPv6, or octet ranges).
  Each entry must be separated by one or more spaces, tabs, or
  newlines. You can specify a hyphen (-) as the filename if you want
  Nmap to read hosts from standard input rather than an actual file.

  The input file may contain comments that start with # and extend to
  the end of the line.

```

Look at Example 1.

What is the nmap command used?

```
Example 1. A representative Nmap scan
```

```
# nmap -A -T4 scanme.nmap.org
```

What does the switch -A do?

-A: Enable OS detection, version detection, script scanning, and traceroute

What does the switch -T4 do?

-T4 for faster execution by prohibiting the dynamic scan delay from exceeding 10 ms for TCP ports. -T4 is recommended for a decent broadband or ethernet connection.

Part 2: Scanning for Open Ports

In this part, you will use the switches from the example in the Nmap man pages to scan your localhost, your local network, and a remote server at scanme.nmap.org.

Step 1: Scan your localhost.

a. If necessary, open a terminal on the VM. At the prompt, enter **nmap -A -T4 localhost**.

Depending on your local network and devices, the scan will take anywhere from a few seconds to a few minutes.

```

analyst@sec0ps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-02-21 08:01 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000088s 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 11.96 seconds
analyst@sec0ps ~]$

```

b. Review the results and answer the following questions.

Which ports and services are opened?

21/tcp: ftp, 22/tcp: ssh

For each of the open ports, record the software that is providing the services.

ftp: vsftpd,

ssh: OpenSSH

Step 2: Scan your network.

Warning: Before using Nmap on any network, please gain the permission of the network owners before proceeding.

a. At the terminal command prompt, enter `ip address` to determine the IP address and subnet mask for this host. For this example, the IP address for this VM is 10.0.2.15 and the subnet mask is 255.255.255.0.

```

[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: ovs-system: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether e6:12:e2:8e:cc:e5 brd ff:ff:ff:ff:ff:ff
3: s1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether b2:3d:ea:27:b1:44 brd ff:ff:ff:ff:ff:ff
4: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 0a:00:27:ff:fe:af:de:b5 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 85652sec preferred_lft 85652sec
    inet6 fd00::a00:27ff:feaf:deb5/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86097sec preferred_lft 14097sec
    inet6 fe80::a00:27ff:feaf:deb5/64 scope link
        valid_lft forever preferred_lft forever

```

Record the IP address and subnet mask for your VM.

Which network does your VM belong to?

Answers will vary. This VM has an IP address of 10.0.0.15/24 and it is part of the 10.0.2.0/24 network.

b. To locate other hosts on this LAN, enter `nmap -A -T4 network address/prefix`. The last octet of the IP address should be replaced with a zero. For example, in the IP address 10.0.2.15, the .15 is the last octet. Therefore, the network address is 10.0.2.0. The /24 is called the prefix and is a shorthand for the netmask 255.255.255.0. If your VM has a different netmask, search the internet for a “CIDR conversion table” to find your prefix. For example, 255.255.0.0 would be /16. The network address 10.0.2.0/24 is used in this example

Note: This operation can take some time, especially if you have many devices attached to the network. In one test environment, the scan took about 4 minutes.

```

[analyst@secops ~]$ nmap -A -T4 network 10.0.2.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2025-02-21 08:22 EST
Failed to resolve "network".
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 10.06% done; ETC: 08:23 (0:00:09 remaining)
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 56.35% done; ETC: 08:23 (0:00:04 remaining)
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 67.09% done; ETC: 08:23 (0:00:03 remaining)
Stats: 0:00:27 elapsed; 256 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 08:23 (0:00:11 remaining)
Nmap scan report for 10.0.2.15
Host is up (0.000097s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_  _rw-r--r--  1 0      0      0 Mar 26 2018 ftp_test
|_ ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 10.0.2.15
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 5
|     vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 7.7 (protocol 2.0)
|_ ssh-hostkey:
|   2048 b4:91:f9:f9:d6:79:25:86:44:c7:9e:f8:e0:a7:5b:bb (RSA)
|   256 06:12:75:fe:b3:89:29:4f:8d:f3:9e:9a:d7:c6:03:52 (ECDSA)
|_  256 34:5d:f2:d3:5b:9f:b4:b6:08:96:a7:30:52:8c:96:06 (ED25519)
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 256 IP addresses (1 host up) scanned in 27.55 seconds

```


How many hosts are up?

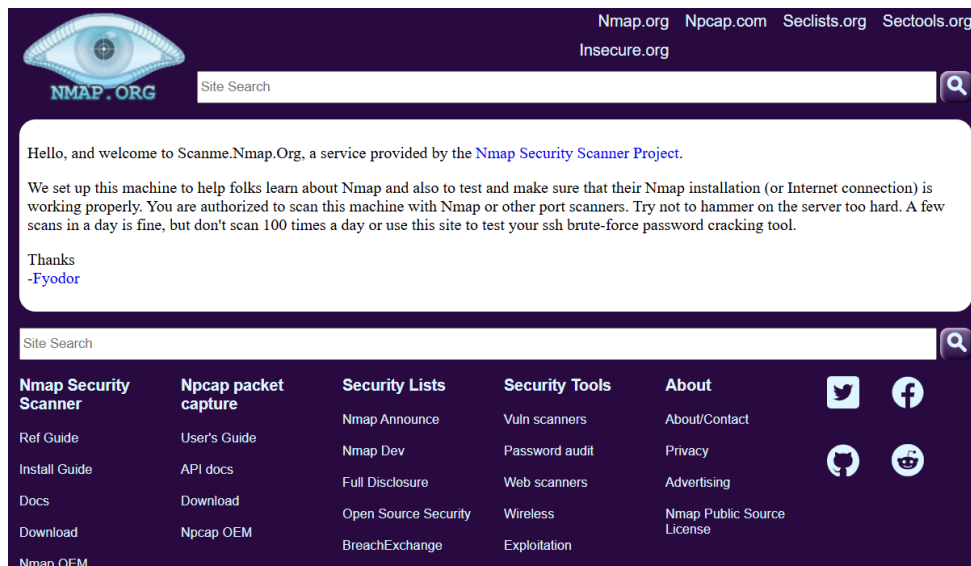
1

From your Nmap results, list the IP addresses of the hosts that are on the same LAN as your VM. List some of the services that are available on the detected hosts.

ftp e ssh

Step 3: Scan a remote server.

a. Open a web browser and navigate to scanme.nmap.org. Please read the message posted.



What is the purpose of this site?

This site allows users to learn about Nmap and test their Nmap installation.

b. At the terminal prompt, enter `nmap -A -T4 scanme.nmap.org`.

```
analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org.
Starting Nmap 7.70 ( https://nmap.org ) at 2025-02-21 08:29 EST
Nmap scan report for scanme.nmap.org. (45.33.32.156)
Host is up (0.28s latency).
Other addresses for scanme.nmap.org. (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
DNS record for 45.33.32.156: scanme.nmap.org
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 50.25 seconds
analyst@secOps ~]$
```

c. Review the results and answer the following questions.

Which ports and services are opened?

22/tcp: ssh, 9929/tcp: n ping-echo, 31337/tcp: tcpwrapped, 80/tcp: http

Which ports and services are filtered?

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

What is the IP address of the server?

IPv4 address: 45.33.32.156 IPv6 address: 2600:3c01::f03c:91ff:fe18:bb2f

What is the operating system?

Ubuntu Linux

DANIELE BALANI