

# Report Esercizio 21/02/2025

## CyberOps Esercizi Leonardo Catalano

“La traccia di oggi ci chiede di effettuare degli esercizi di Cisco CyberOps”.

### 1\* Esercizio: “3.3.11 Lab- Using Windows PowerShell :

#### Obiettivi:

The objective of the lab is to explore some of the functions of PowerShell.

- Part 1: Access PowerShell console.
- Part 2: Explore Command Prompt and PowerShell commands.
- Part 3: Explore cmdlets.
- Part 4: Explore the netstat command using PowerShell.
- Part 5: Empty recycle bin using PowerShell.

#### -Background /Scenario:

In questo scenario andremo ad utilizzare PowerShell che è uno strumento potente di automazione.

E' sia un console di comandi che un linguaggio di scripting.

Useremo la console per eseguire alcuni comandi che sono disponibili sia nel cmd che nella PowerShell.

PowerShell ha inoltre la funzione di create script per eseguire task automatici e lavorare insieme al'OS Windows.

#### -PART 1: Access PowerShell console

- Cliccare Start e cercare powershell
- Cliccare Start e cercare cmd

Ricerca

App

Documenti

Web

Impostazioni

Cartelle

Foto



### Corrispondenza migliore

 **Windows PowerShell**  
Sistema


### App


 **Windows PowerShell ISE** >

 **Windows PowerShell (x86)** >


 **Windows PowerShell ISE (x86)** >


### Impostazioni

 **Impostazioni sviluppatore PowerShell** >

 **Consenti l'esecuzione di script PowerShell locali senza firma** >

### Cerca nel Web

 **powershell** - Visualizza altri risultati della ricerca >






 **powershell 7** >

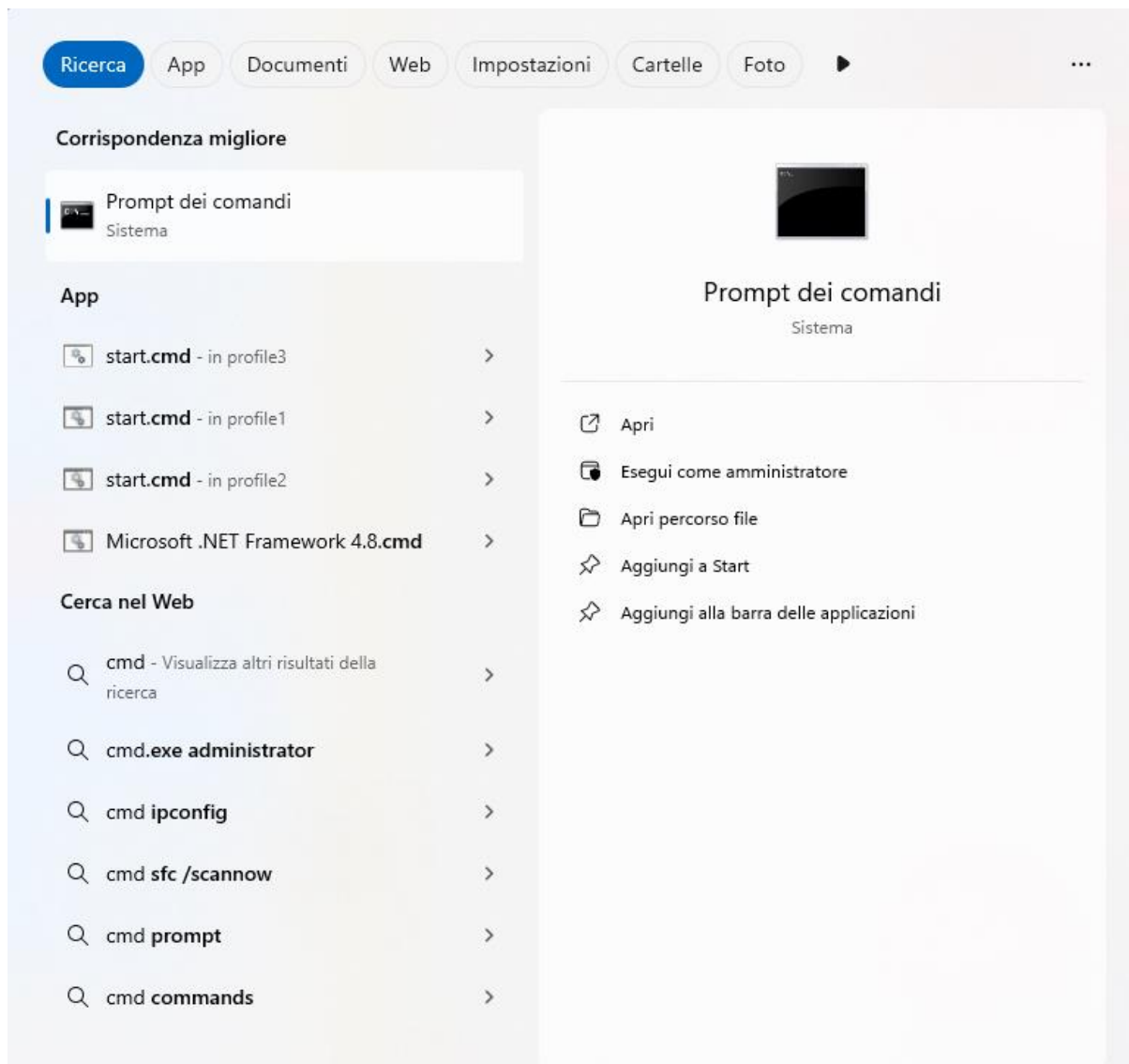
 **powershell amministratore** >



## Windows PowerShell

Sistema

-  **Apri**
-  **Esegui come amministratore**
-  **Apri percorso file**
-  **Aggiungi a Start**
-  **Aggiungi alla barra delle applicazioni**



## -PART 2: Explore Command Prompt and PowerShell commands

Scrivere “dir” ai prompt di entrambe le finestre.

Qual'è l'output?

“Entrambe le finestre forniscono un elenco di sottodirectory e file e informazioni associate come tipo, dimensione del file, data e ora dell'ultima scrittura. In PowerShell vengono visualizzati anche gli attributi/modalità. “

```
Prompt dei comandi
Microsoft Windows [Versione 10.0.26100.3194]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\leolo>dir
Il volume nell'unità C è Windows-SSD
Numero di serie del volume: 2E25-3FD1

Directory di C:\Users\leolo

18/02/2025  08:45  <DIR>      .
23/11/2024  10:29  <DIR>      ..
19/01/2025  17:49  <DIR>      .android
25/11/2024  17:25          198 .gitconfig
21/01/2025  12:04          176 .packettracer
18/02/2025  15:22  <DIR>      .VirtualBox
21/01/2025  12:05  <DIR>      Cisco Packet Tracer 8.2.2
23/11/2024  10:13  <DIR>      Contacts
21/02/2025  09:33  <DIR>      Desktop
17/02/2025  18:46  <DIR>      Documents
19/02/2025  09:26  <DIR>      Downloads
23/11/2024  10:13  <DIR>      Favorites
23/11/2024  10:13  <DIR>      Links
23/11/2024  10:13  <DIR>      Music
23/11/2024  10:16  <DIR>      OneDrive
20/02/2025  12:35  <DIR>      Pictures
23/11/2024  10:13  <DIR>      Saved Games
23/11/2024  10:29  <DIR>      Searches
04/12/2024  20:48  <DIR>      UrbanVPN
11/12/2024  09:46  <DIR>      Videos
18/02/2025  15:21  <DIR>      VirtualBox VMs

Windows PowerShell
PS C:\Users\leolo> dir

Directory: C:\Users\leolo

Mode                LastWriteTime         Length Name
----                -
d-----         19/01/2025         17:49          .android
d-----         18/02/2025         15:22          .VirtualBox
d-----         21/01/2025         12:05      Cisco Packet Tracer 8.2.2
d-r-----        23/11/2024         10:13          Contacts
d-r-----        21/02/2025         09:33          Desktop
d-r-----        17/02/2025         18:46          Documents
d-r-----        19/02/2025         09:26          Downloads
d-r-----        23/11/2024         10:13          Favorites
d-r-----        23/11/2024         10:13          Links
d-r-----        23/11/2024         10:13          Music
d-r-----        23/11/2024         10:16          OneDrive
d-r-----        20/02/2025         12:35          Pictures
d-r-----        23/11/2024         10:13          Saved Games
d-r-----        23/11/2024         10:29          Searches
d-----         04/12/2024         20:48          UrbanVPN
d-r-----        11/12/2024         09:46          Videos
d-----         18/02/2025         15:21      VirtualBox VMs
-a-----         25/11/2024          198          .gitconfig
-a-----         21/01/2025          176          .packettracer

PS C:\Users\leolo>
```

Proviamo ad effettuare un ping per es. A Google “8.8.8.8”

```
Prompt dei comandi
Microsoft Windows [Versione 10.0.26100.3194]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\leolo>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=37ms TTL=115
Risposta da 8.8.8.8: byte=32 durata=32ms TTL=115
Risposta da 8.8.8.8: byte=32 durata=34ms TTL=115
Risposta da 8.8.8.8: byte=32 durata=37ms TTL=115

Statistiche Ping per 8.8.8.8:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 32ms, Massimo = 37ms, Medio = 35ms

C:\Users\leolo>

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

Installa la versione pi#u recente di PowerShell per nuove funzionalit#e e miglioramenti. https://aka.ms/PSWindows

PS C:\Users\leolo> 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=34ms TTL=115
Risposta da 8.8.8.8: byte=32 durata=31ms TTL=115
Risposta da 8.8.8.8: byte=32 durata=26ms TTL=115
Risposta da 8.8.8.8: byte=32 durata=33ms TTL=115

Statistiche Ping per 8.8.8.8:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 26ms, Massimo = 34ms, Medio = 31ms

PS C:\Users\leolo>
```

I risultati sono identici.

### -Part 3: Explore cmdlets.

-PoweShell commands, “cmdlets” sono costrutti sotto forma di verbo-nome stringa, che servono ad identificare i comandi PowerShell per identificare le sottodirectory e i file in una directory, immettere “Get-Alias dir” su 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:\Users\leolo> GET-Alias dir

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

PS C:\Users\leolo>
```

(L'alias di "dir" è Get-ChildItem).

#### -Part 4: Explore the netstat command using PowerShell

Nel PowerShell prompt, scrivere netstat -help per vedere il manuale del comando netstat.

```
Windows PowerShell

PS C:\Users\leolo> netstat -help

Mostra le statistiche del protocollo e le connessioni di rete TCP/IP correnti.

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

-a          Mostra tutte le connessioni e le porte di ascolto.
-b          Mostra l'eseguibile coinvolto nella creazione di ogni connessione o
             porta di ascolto. In alcuni casi, eseguibili noti ospitano
             più componenti indipendenti e in questi casi la
             sequenza dei componenti coinvolti nella creazione della connessione
             o della porta di ascolto viene visualizzata. In questo caso, il nome dell'eseguibile
             è in [] in basso, in alto si trova il componente chiamato,
             e così via fino al raggiungimento di TCP/IP. Tenere presente che questa opzione
             può essere dispendiosa in termini di tempo e non andrà a buon fine a meno che non si disponga delle
             autorizzazioni sufficienti.
-c          Visualizza un elenco di processi ordinati in base al numero di
TCP o UDP   porte attualmente utilizzate.
-d          Mostra il valore DSCP associato a ogni connessione.
-e          Mostra le statistiche Ethernet. Potrebbe essere in combinazione con l'opzione
             -s.
-f          Mostra Fully Qualified Domain Names (FQDN) per gli indirizzi
             stranieri.
-i          Mostra il tempo in cui una connessione TCP si trova nel suo stato corrente.
-n          Mostra i numeri di indirizzi e porte in formato numerico.
-o          Mostra l'ID processo di proprietà associato a ogni connessione.
-p proto    Mostra le connessioni per il protocollo specificato dal protocollo; il protocollo
             può essere: TCP, UDP, TCPv6 o UDPv6. Se usato con l'opzione -s
             per mostrare le statistiche per protocollo, il protocollo potrebbe essere:
             IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
-q          Mostra tutte le connessioni, le porte di ascolto e le porte
             TCP non di ascolto associate. Le porte non di ascolto associate potrebbero essere associate o meno
             a una connessione attiva.
-r          Mostra la tabella di routing.
```

Per visualizzare la tabella di routing si utilizza il comando "netstat -r":

```
Windows PowerShell
PS C:\Users\leolo> netstat -r

=====
Elenco interfacce
2...02 50 d3 60 f8 0c .....Famatech Radmin VPN Ethernet Adapter
14...00 ff 86 3c 7e 4b .....TAP-Windows Adapter V9
15...0a 00 27 00 00 0f .....VirtualBox Host-Only Ethernet Adapter
10...3e 0a f3 0a ed af .....Microsoft Wi-Fi Direct Virtual Adapter
7...3e 0a f3 0a fd bf .....Microsoft Wi-Fi Direct Virtual Adapter #2
21...3c 0a f3 0a cd 8f .....MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
1.....Software Loopback Interface 1
16...00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
=====

IPv4 Tabella route
=====
Route attive:
Indirizzo rete      Mask      Gateway    Interfaccia Metrica
0.0.0.0             0.0.0.0    192.168.1.1 192.168.1.42 35
0.0.0.0             0.0.0.0    26.0.0.1    26.175.132.63 9257
26.0.0.0            255.0.0.0  On-link     26.175.132.63 257
26.175.132.63       255.255.255.255 On-link     26.175.132.63 257
26.255.255.255      255.255.255.255 On-link     26.175.132.63 257
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     192.168.1.42 291
192.168.1.42        255.255.255.255 On-link     192.168.1.42 291
192.168.1.255       255.255.255.255 On-link     192.168.1.42 291
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     192.168.1.42 291
224.0.0.0           240.0.0.0  On-link     26.175.132.63 257
```

Cos'è l'indirizzo IPV4 Gateway?.

L'indirizzo Gateway che in questo caso è il 192.168.1.1 è l'indirizzo della porta di uscita ossia del Router.

Apriamo il PowerShell con i privilegi d'amministratore e scriviamo "netstat -abno".

```
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

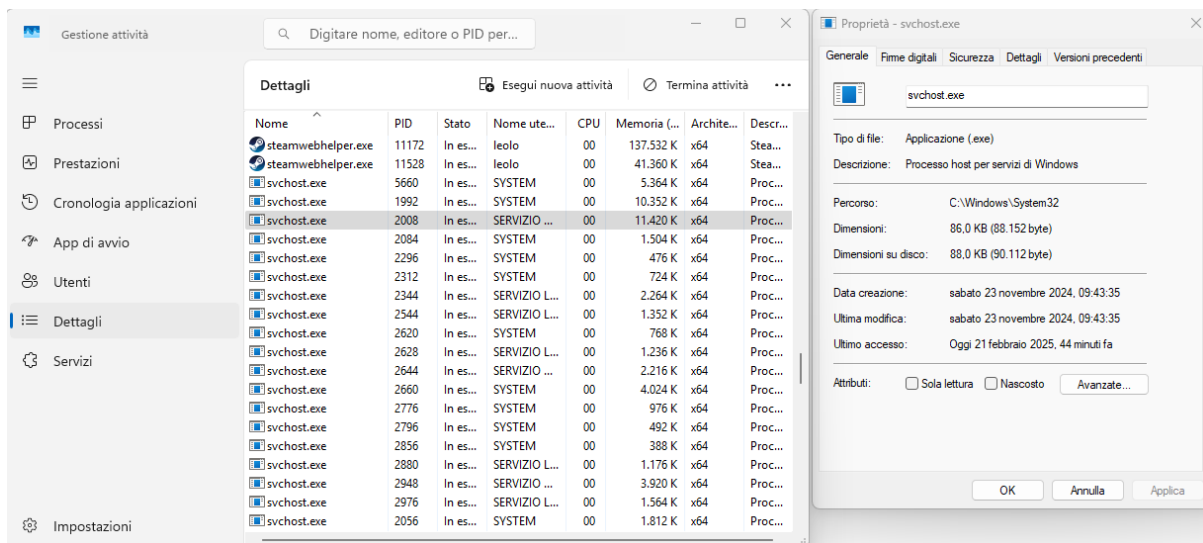
PS C:\Windows\system32> netstat -abno

Connessioni attive

Proto  Indirizzo locale      Indirizzo esterno      Stato      PID
TCP    0.0.0.0:135            0.0.0.0:0              LISTENING  2008
[svchost.exe]
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING  9088
[CDPSvc]
[svchost.exe]
TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING  14460
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:27036          0.0.0.0:0              LISTENING  11964
[steam.exe]
TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING  1856
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING  1672
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING  2660
[Schedule]
[svchost.exe]
TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING  3272
```

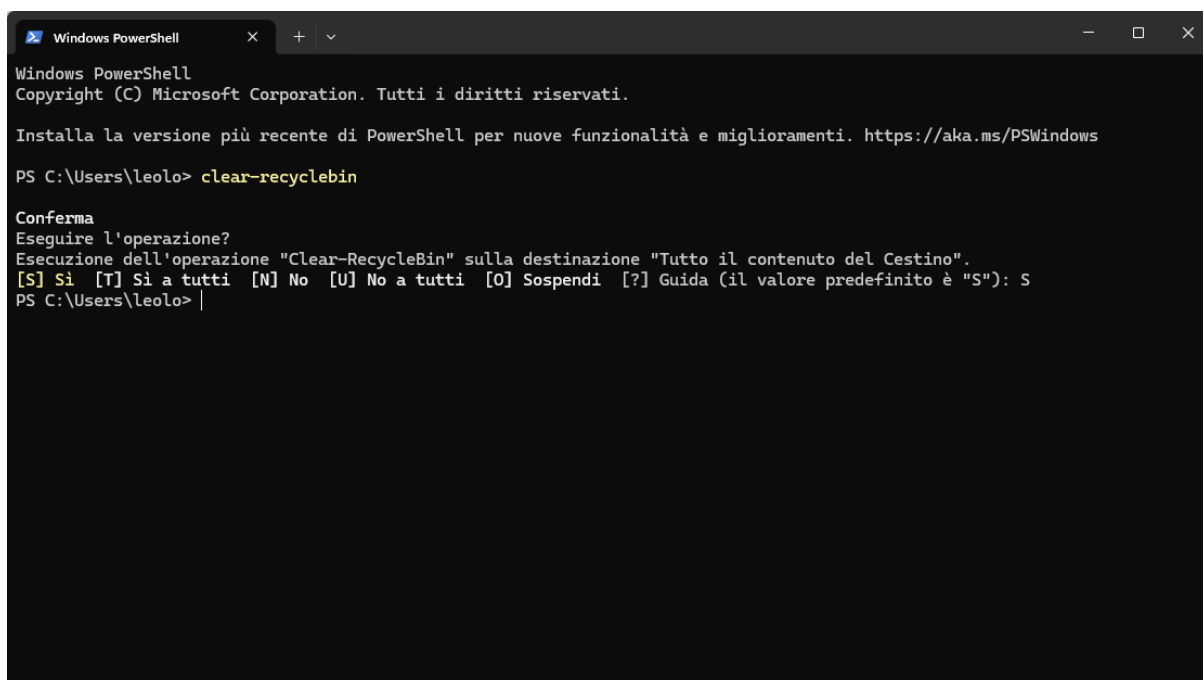
Andiamo su Gestione Attività, sezione Dettagli e cerchiamo i PID del sistema

svchost.exe:



-Part 5: Empty recycle bin using PowerShell.

Da Powershell possiamo inserire un comando per svuotare il cestino, il comando è il seguente “clear-recyclebin”:



Ora il cestino sarà vuoto e i file interni eliminati.

2\* Esercizio Analisi app.any.run:

Analizzare una scansione app.any.run :

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

L'utente ha scaricato da un github un eseguibile con nome “JVczfhe.exe”, andandolo ad eseguire è uscito il l'avviso che il file potrebbe non essere sicuro perchè non è verificato e l'utente ha scelto cmq di lanciarlo.



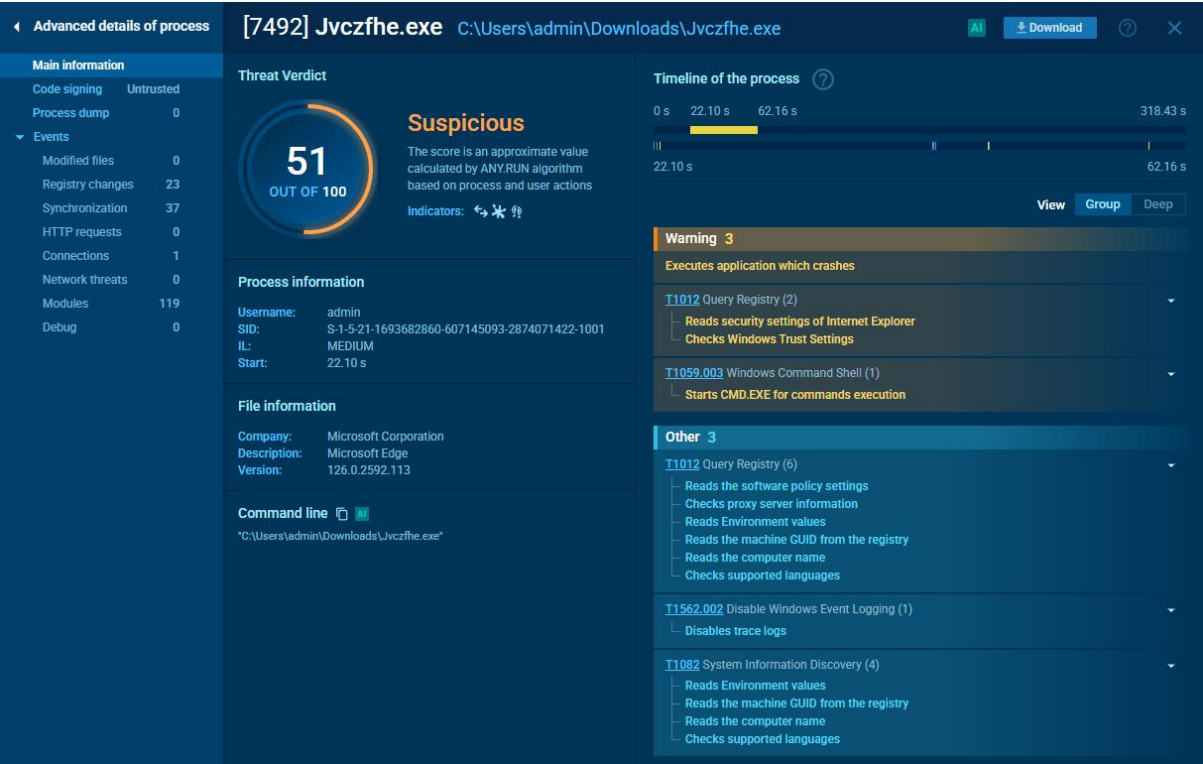
Successivamente dal browser edge ci apparirà un avviso che c'è stato un errore nell'aprire il documento, che il file è danneggiato e non può essere riparato.

L'utente allora cerca un altro file da github di nome "Muadnrd.exe" e lo scarica. Provandolo ad eseguire c'è lo stesso risultato precedente un errore dal browser edge.

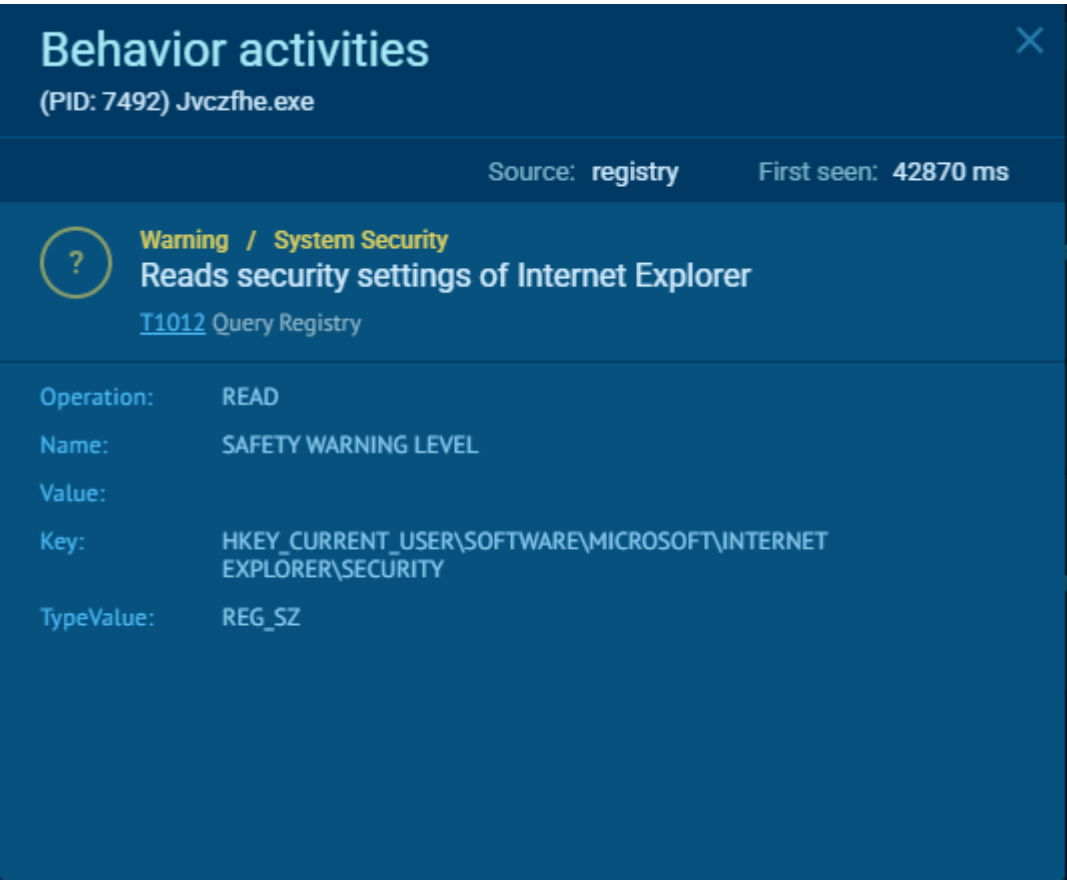


Analizzando il report grafico, possiamo notare ad occhio che i file .exe una volta scaricati hanno fatto qualcosa di nascosto (alla vista dell'utente) andando a modificare dei parametri di sistema.

Partendo con l'analisi di jvczfhe.exe:



Notiamo che va ad effettuare delle Query al registro di windows nello specifico ai settings di Internet Explorer\Security:



E i settaggi del Windows Trust Settings nel percorso  
CurrentVersion\WinTrust\TrustProviders\Software Publishing:

## Behavior activities

(PID: 7492) Jvczfhe.exe

Source: **registry**      First seen: **42870 ms**

?

**Warning / General**  
**Checks Windows Trust Settings**  
[T1012](#) Query Registry

Operation:	READ
Name:	STATE
Value:	146432
Key:	HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSIO N\WINTRUST\TRUST PROVIDERS\SOFTWARE PUBLISHING
TypeValue:	REG_DWORD

Successivamente starta una shell cmd per eseguire un comando:



Nella sezione Other, troviamo diverse letture nei registri interni di windows per informazioni sul sistema, e troviamo una modifica all'event logging di windows, andandolo a disabilitare:

# Behavior activities

(PID: 7492) Jvczfhe.exe

Source: registryFirst seen: 38736 ms

?

Other / Disables trace logs

T1562.002 Disable Windows Event Logging

Operation:

READ

Name:

ENABLEFILETRACING

Value:

0

Key:

HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\TRACING\VCZFHE\_RASAPI32

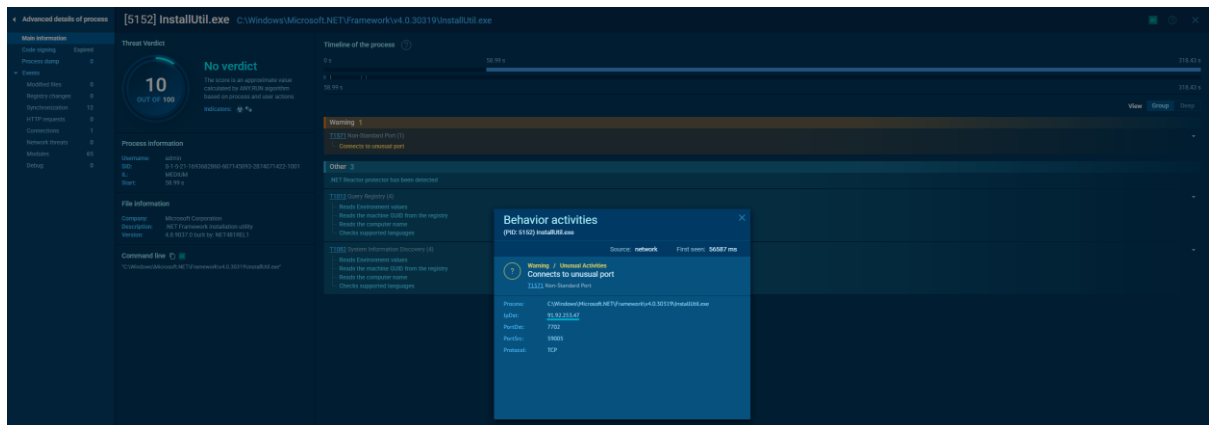
TypeValue:

REG\_DWORD

Nella sezione Registry changes, notiamo che il processo ha effettuato 23 modifiche ai registri di windows:

Advanced details of process [7492] Jvczfhe.exe			
Put the value in the desired position or select the desired segment by yourself			
22.165 s			
+21.04 s			
62.164 s			
Main information			
Code signing: Untrusted			
Process dump: 0			
Events			
Modified files: 0			
Registry changes: 23			
System operations: 17			
HTTP requests: 0			
Connections: 1			
Network events: 0			
Modules: 119			
Tracing: 0			
Time			
Operation			
Name			
Key and value			
+21040 ms	Winlog	EnableConsoleTracing	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing
			0
+21040 ms	Winlog	EnableFileTracing	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
			0
+21040 ms	Winlog	EnableAutoFileTracing	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
			0
+21040 ms	Winlog	EnableConsoleTracing	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
			0
+21040 ms	Winlog	FileTracingBlock	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
			(value not set)
+21040 ms	Winlog	ConsoleTracingBlock	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
			(value not set)
+21040 ms	Winlog	MailFolder	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
			1046576
+21040 ms	Winlog	FileDirectory	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
			SwampTracing
+21040 ms	Winlog	EnableFileTracing	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAMANC
			0
+21040 ms	Winlog	EnableAutoFileTracing	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAMANC
			0
+21040 ms	Winlog	EnableConsoleTracing	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAMANC
			0
+21040 ms	Winlog	FileTracingBlock	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAMANC
			(value not set)
+21040 ms	Winlog	ConsoleTracingBlock	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAMANC
			(value not set)
+21040 ms	Winlog	MailFolder	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAMANC
			1046576
+21040 ms	Winlog	FileDirectory	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAMANC
			SwampTracing
+25237 ms	Winlog	ProxyBypass	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
			1
+25237 ms	Winlog	IntranetName	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
			1
+25237 ms	Winlog	UNCAnnoyance	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
			1
+26217 ms	Winlog	Anonymous	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
			1

Il programma Crea altri processi e thread, quello che viene classificato come anomalo è installutil.exe:

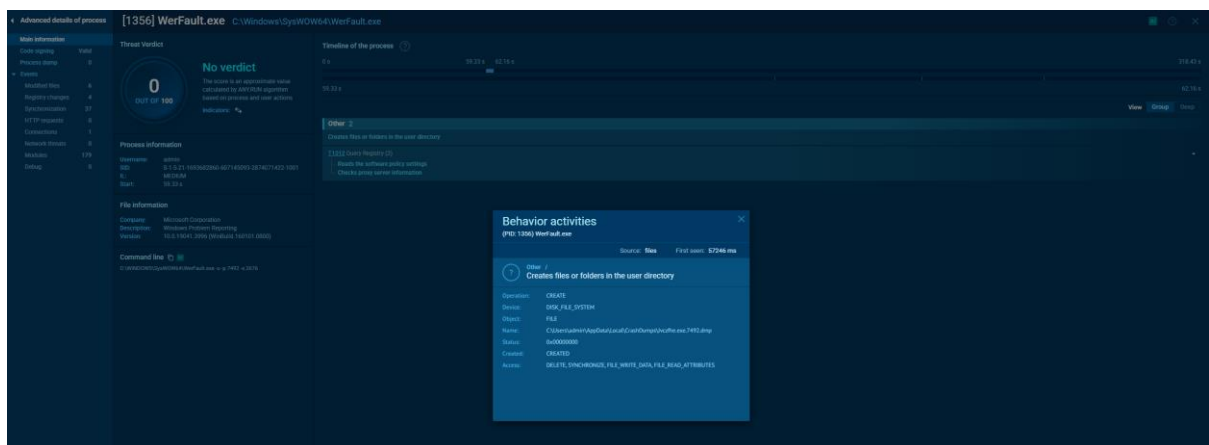


Oltre a varie Query di lettura nel registro di windows, vediamo che va a stabilire una connessione ad un socket sconosciuto della Bulgaria: "91.92.253.47 7702" (IndirizzoIp + Porta).

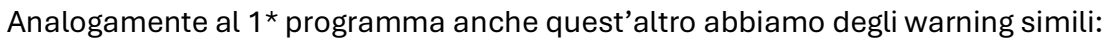
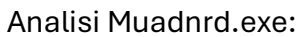
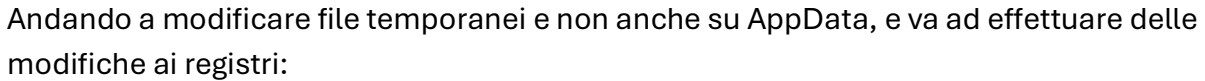
Sui dettagli delle Connessioni, vediamo anche il dominio di questo indirizzo ip duckdns.org:

Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
31946 ms	UDP	?	6596	firefox.exe		35.190.72.216	443	location.services.mozilla.com	-	2 Kb ↓ 4 Kb
31947 ms	TCP	?	6596	firefox.exe		34.160.144.191	443	prod.content-signature-chains.prod.webservices.mozilla.com	GOOGLE	8 Kb ↓ 226 Kb
39652 ms	TCP	?	7492	javzthe.exe		185.199.110.133	443	raw.githubusercontent.com	FASTLY	417 b ↓ 5 Mb
39656 ms	UDP	?	3888	svchost.exe		239.255.255.250	1900	-	-	411 b ↓ -
44558 ms	TCP	?	2268	svchost.exe		20.190.159.0	443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	5 Kb ↓ 14 Kb
44563 ms	TCP	?	1920	svchost.exe		40.127.240.158	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	2 Kb ↓ 4 Kb
51472 ms	TCP	?	6596	firefox.exe		34.160.144.191	443	prod.content-signature-chains.prod.webservices.mozilla.com	GOOGLE	983 b ↓ 9 Kb
51498 ms	TCP	?	6596	firefox.exe		23.53.40.162	80	st19.dsccg10.akamai.net	Akamai International B.V.	305 b ↓ 480 Kb
55663 ms	TCP	?	5152	installutil.exe		91.92.253.47	7702	eeghdehjhjtre.duckdns.org	-	No Data
56761 ms	TCP	?	2268	svchost.exe		20.190.159.0	443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	5 Kb ↓ 15 Kb
56763 ms	TCP	?	1356	WerFault.exe		104.208.16.94	443	watson.events.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	6 Kb ↓ 5 Kb
63865 ms	TCP	?	6596	firefox.exe		34.107.221.82	80	detectportal.firefox.com	GOOGLE	303 b ↓ 298 b
63869 ms	TCP	?	6596	firefox.exe		34.107.221.82	80	detectportal.firefox.com	GOOGLE	305 b ↓ 216 b
100.80 s	TCP	?	6596	firefox.exe		34.36.165.17	443	tiles.cdn.prod.ads.prod.webservices.mozilla.com	GOOGLE-CLOUD-PLATFORM	2 Kb ↓ 29 Kb
102.70 s	TCP	?	6596	firefox.exe		140.82.121.3	443	github.com	GITHUB	3 Kb ↓ 115 Kb
102.71 s	TCP	?	6596	firefox.exe		140.82.112.21	443	collector.github.com	GITHUB	10 Kb ↓ 8 Kb

Un altro processo WerFault.exe va a creare una directory nel file system appdata dell'utente.



Va ad effettuare delle modifiche a dei file di windows:



Il processo va ad effettuare 2 Query ai registri di Windows, dove va a vedere i settings per i providers sicuri, ed un'altra dove va a leggere le impostazioni di sicurezza di Internet Explorer.

## Behavior activities



(PID: 7824) Muadnrd.exe

Source: registry

First seen: 132.37 s



**Warning / General**

### Checks Windows Trust Settings

[T1012](#) Query Registry

Operation: READ  
Name: STATE  
Value: 146432  
Key: HKEY\_CURRENT\_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSIO  
N\WINTRUST\TRUST PROVIDERS\SOFTWARE PUBLISHING  
TypeValue: REG\_DWORD

## Behavior activities



(PID: 7824) Muadnrd.exe

Source: registry

First seen: 132.37 s



**Warning / System Security**

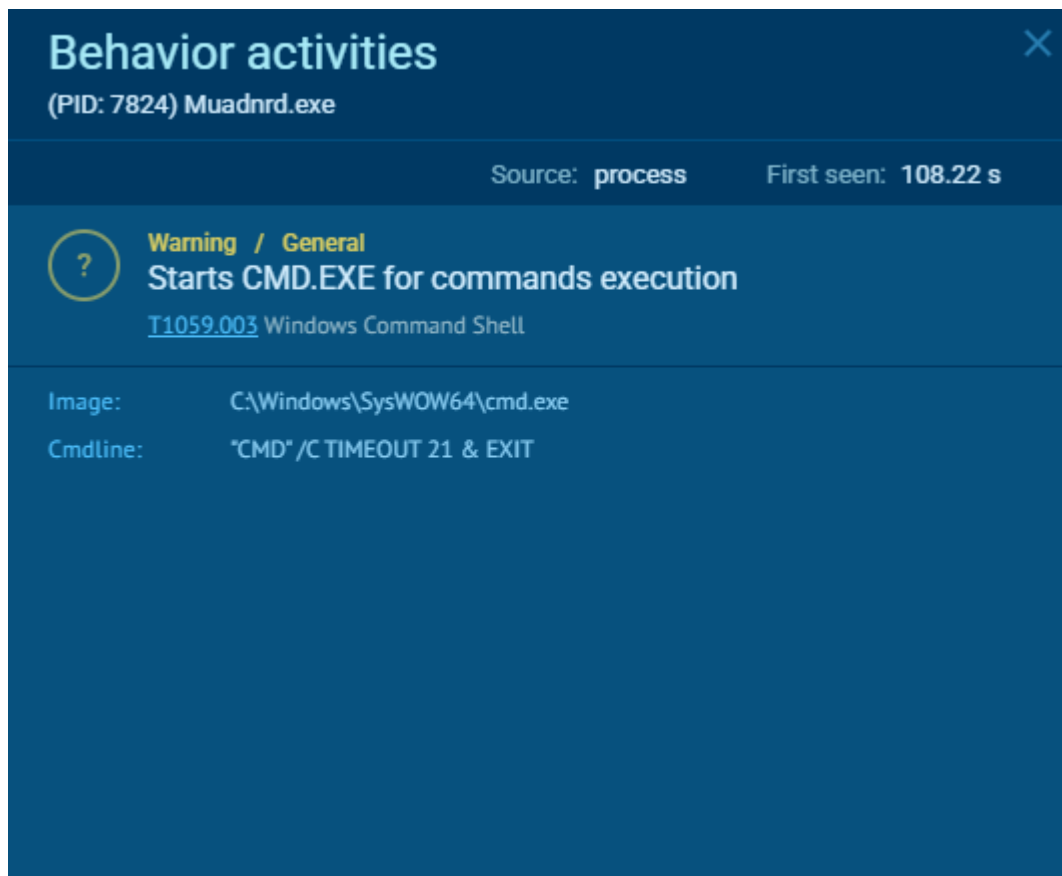
### Reads security settings of Internet Explorer

[T1012](#) Query Registry

Operation: READ  
Name: SAFETY WARNING LEVEL  
Value:  
Key: HKEY\_CURRENT\_USER\SOFTWARE\MICROSOFT\INTERNET  
EXPLORER\SECURITY  
TypeValue: REG\_SZ



Successivamente va ad eseguire una shell ed ad eseguire il timeout per la chiusura del processo:



Nella sezione Other vediamo diverse Query di lettura ai registri di windows e anche qui la modifica dell'event Logging di windows, disabilitandola mettendo il valore a 0:

# Behavior activities

(PID: 7824) Muadnrd.exe

Source: registry
First seen: 128.52 s

?

Other /

Disables trace logs

T1562.002 Disable Windows Event Logging

Operation:

WRITE

Name:

ENABLEFILETRACING

Value:

0

Key:

HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\TRACING\MUADNRD\_RASAPI32

TypeValue:

REG\_NONE

Anche qui si vanno a modificare i registri interni di windows:

Advanced details of process

7824 Muadnrd.exe

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

112.367 s

+128.52 s

181.704 s

Main information

Code integrity

Untrusted

Process dump

0

Events

Modified files

0

Registry changes

22

System events

27

HTTP requests

0

Connections

1

Network events

0

Modules

116

Dring

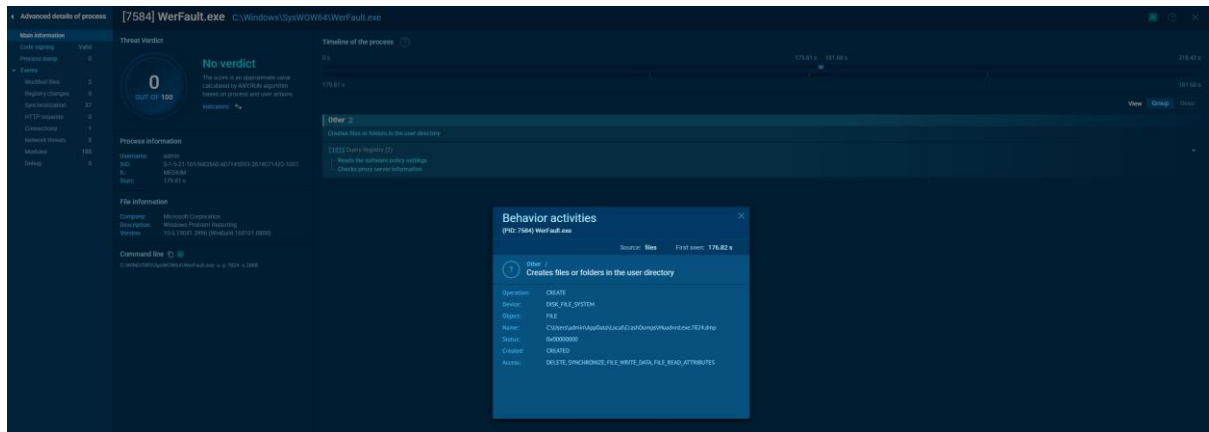
0

Time	Operation	Name	Key and value
+2363 ms	Write	Enabled file tracing	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32 0
+2363 ms	Write	Enabled Auto file tracing	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32 0
+2363 ms	Write	Enabled Console tracing	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32 0
+2363 ms	Write	File Tracing book	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32 (value not set)
+2363 ms	Write	Console Tracing book	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32 (value not set)
+2363 ms	Write	Host file trace	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32 1048576
+2363 ms	Write	File directory	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32 1048576
+2363 ms	Write	Enabled file tracing	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32 0
+2363 ms	Write	Enabled Auto file tracing	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32 0
+2363 ms	Write	Enabled Console tracing	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32 0
+2363 ms	Write	File Tracing book	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32 (value not set)
+2363 ms	Write	Console Tracing book	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32 (value not set)
+2363 ms	Write	Host file trace	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32 1048576
+2363 ms	Write	File directory	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32 1048576
+24294 ms	Write	Proxy options	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1
+24294 ms	Write	Internet home	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1
+24294 ms	Write	UNC Address	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1
+24294 ms	Write	Auto detect	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 0
+24294 ms	Write	Proxy options	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1

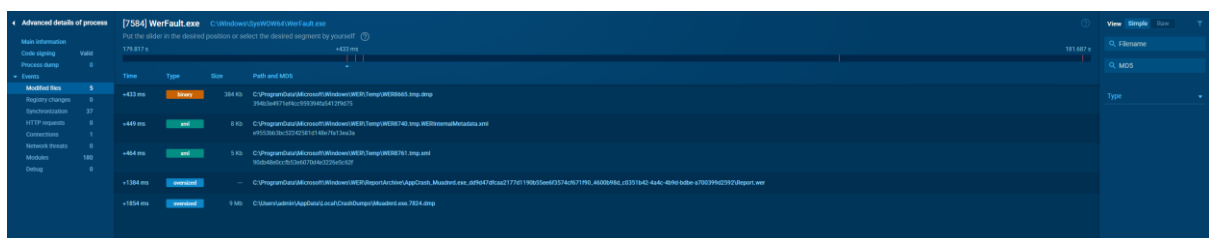
Nel thread Muadnrd.exe, vediamo che va ad effettuare delle Query di lettura sui registri per acquisire informazioni sul sistema:



Il sottoprocesso WerFault.exe svolge la stessa funzione precedente, va a creare un file.dmp all'interno di Appdata:



E va a modificare dei file:



Come ultimo processo ci appare svchost.exe:



Andando nella sezione Network Threats, vediamo i vari spostamenti di query che sono visualizzate come potenziale bad traffic verso il domain .duckdns.org che è apparso prima con la connessione verso l'indirizzo bulgaro "91.92.253.47".

Advanced details of process

svchost.exe

C:\Windows\System32\svchost.exe

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

318.437 s

Main information

Code signing

Valid

Process dump

0

Events

0

Modified files

0

Registry changes

0

Synchronization

0

HTTP requests

0

Connections

0

Network threads

19

Modules

42

Debug

0

Time

Type

Src

Src IP

Port

Dest IP

Port

+18934 ms

INFO [ANY/URL] Attempting to access new user content on GitHub

Not Suspicious Traffic

8001935

192.168.100.139

53

192.168.100.2

53

+18938 ms

INFO [ANY/URL] Attempting to access new user content on GitHub

Not Suspicious Traffic

8001935

192.168.100.139

53

192.168.100.2

53

+18929 ms

INFO [ANY/URL] Attempting to access new user content on GitHub

Not Suspicious Traffic

8001935

192.168.100.139

53

192.168.100.2

53

+40014 ms

ET INFO DYNAMIC DNS Query to a \*.duckdns. org Domain

Potentially Bad Traffic

2042936

192.168.100.139

53

192.168.100.2

53

+40018 ms

ET INFO DYNAMIC DNS Query to a \*.duckdns. org Domain

Potentially Bad Traffic

2042936

192.168.100.139

53

192.168.100.2

53

+40019 ms

ET INFO DYNAMIC DNS Query to a \*.duckdns. org Domain

Potentially Bad Traffic

2042936

192.168.100.139

53

192.168.100.2

53

+40020 ms

ET INFO DYNAMIC DNS Query to a \*.duckdns. Domain

Mal activity

2022918

192.168.100.139

53

192.168.100.2

53

+40020 ms

ET INFO DYNAMIC DNS Query to a \*.duckdns. Domain

Mal activity

2022918

192.168.100.139

53

192.168.100.2

53

+40021 ms

ET INFO DYNAMIC DNS Query to a \*.duckdns. Domain

Mal activity

2022918

192.168.100.139

53

192.168.100.2

53

+138352 ms

ET INFO DYNAMIC DNS Query to a \*.duckdns. org Domain

Potentially Bad Traffic

2042936

192.168.100.139

53

192.168.100.2

53

+138353 ms

ET INFO DYNAMIC DNS Query to a \*.duckdns. Domain

Mal activity

2022918

192.168.100.139

53

192.168.100.2

53

+190576 ms

ET INFO DYNAMIC DNS Query to a \*.duckdns. org Domain

Potentially Bad Traffic

2042936

192.168.100.139

53

192.168.100.2

53

+190577 ms

ET INFO DYNAMIC DNS Query to a \*.duckdns. org Domain

Potentially Bad Traffic

2042936

192.168.100.139

53

192.168.100.2

53

+190578 ms

ET INFO DYNAMIC DNS Query to a \*.duckdns. Domain

Mal activity

2022918

192.168.100.139

53

192.168.100.2

53

+190579 ms

ET INFO DYNAMIC DNS Query to a \*.duckdns. Domain

Mal activity

2022918

192.168.100.139

53

192.168.100.2

53

+190687 ms

ET INFO DYNAMIC DNS Query to a \*.duckdns. org Domain

Potentially Bad Traffic

2042936

192.168.100.139

53

192.168.100.2

53

+190688 ms

ET INFO DYNAMIC DNS Query to a \*.duckdns. Domain

Mal activity

2022918

192.168.100.139

53

192.168.100.2

53

77258 Cmd.exe

77296 Cmdhost.exe

77570 Timeout.exe

78100 lsicall.exe

78100 lsicall.exe

77568 Firefox.exe

77626 Msadvt.exe

78176 Cmd.exe

77668 Cmdhost.exe

77968 Timeout.exe

77188 Msadvt.exe

77954 lsicall.exe

77256 svchost.exe

-Part 1: Exploring Nmap

-Part 2: Scanning for Open Ports

### -Background /Scenario:

La scansione delle porte è solitamente parte di un attacco di ricognizione.

E' possibile utilizzare diversi metodi di scansione delle porte.

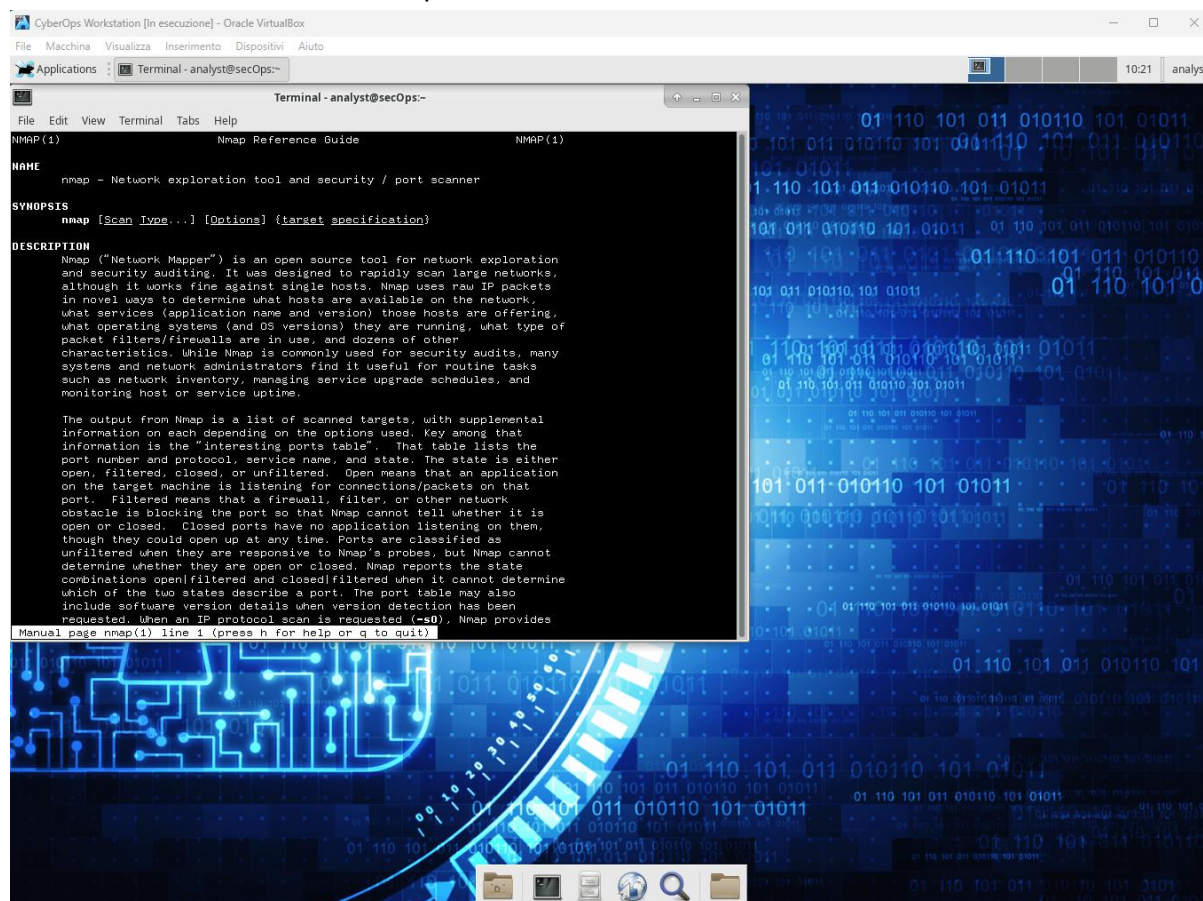
Andremo ad illustrare come utilizzare lo strumento "Nmap".

Nmap è una potente utility di rete utilizzata per effettuare scansioni di porte e servizi su un determinato host.

Per l'esercizio è richiesto l'utilizzo della VM CyberOps Workstation

### -Part 1: Exploring Nmap

Per prima cosa per vedere le opzioni di nmap usiamo il comando "man nmap" da cli per visualizzare il manuale di nmap:



```
CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
Applications  Terminal - analyst@secOps:~

Terminal - analyst@secOps:~
File  Edit  View  Terminal  Tabs  Help

NMAP(1)                                Nmap Reference Guide                                NMAP(1)

NAME
  nmap - Network exploration tool and security / port scanner

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

DESCRIPTION
  Nmap ("Network Mapper") is an open source tool for network exploration
  and security auditing. It was designed to rapidly scan large networks,
  although it works fine against single hosts. Nmap uses raw IP packets
  in novel ways to determine what hosts are available on the network,
  what services (application name and version) those hosts are offering,
  what operating systems (and OS versions) they are running, what 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

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

Come Sinossi abbiamo:

"nmap [Scan Type] [Options] {target specification}"

Che cos'è Nmap?

Nmap è uno strumento utilizzato in ambito security per effettuare scansioni di porte e servizi su un determinato host.

Per cosa si utilizza Nmap ?

Nmap viene utilizzato per scansionare una rete e determinare gli host disponibili e i servizi offerti nella rete. Alcune delle funzionalità di nmap includono il rilevamento dell'host, la scansione delle porte e il rilevamento del sistema operativo. Nmap può essere comunemente utilizzato per controlli di sicurezza, per identificare porte aperte, inventario di rete e trovare vulnerabilità nella rete.

Nel manuale per cercare nello specifico una parola chiave possiamo usare lo slash "/" oppure il "?" seguito dalla parola chiave.

Se inseriamo come parola chiave /example avremo in output un esempio di nmap:

“/example”

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

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

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
|_ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:86:ec (RSA)
80/tcp    open  http         Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
646/tcp   filtered ldp
1720/tcp  filtered H.323/Q.931
9929/tcp  open  nping-echo   Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
[Cut first 10 hops for brevity]
11  17.65 ms li86-221.members.linode.com (74.207.244.221)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds

The newest version of Nmap can be obtained from https://nmap.org. The newest version of this
man page is available at https://nmap.org/book/man.html. It is also included as a chapter
Manual page nmap(1) line 37 (press h for help or q to quit)
```

Il comando utilizzato è "Nmap -A -T4 scanme.nmap.org"

Lo switch -A a cosa serve?

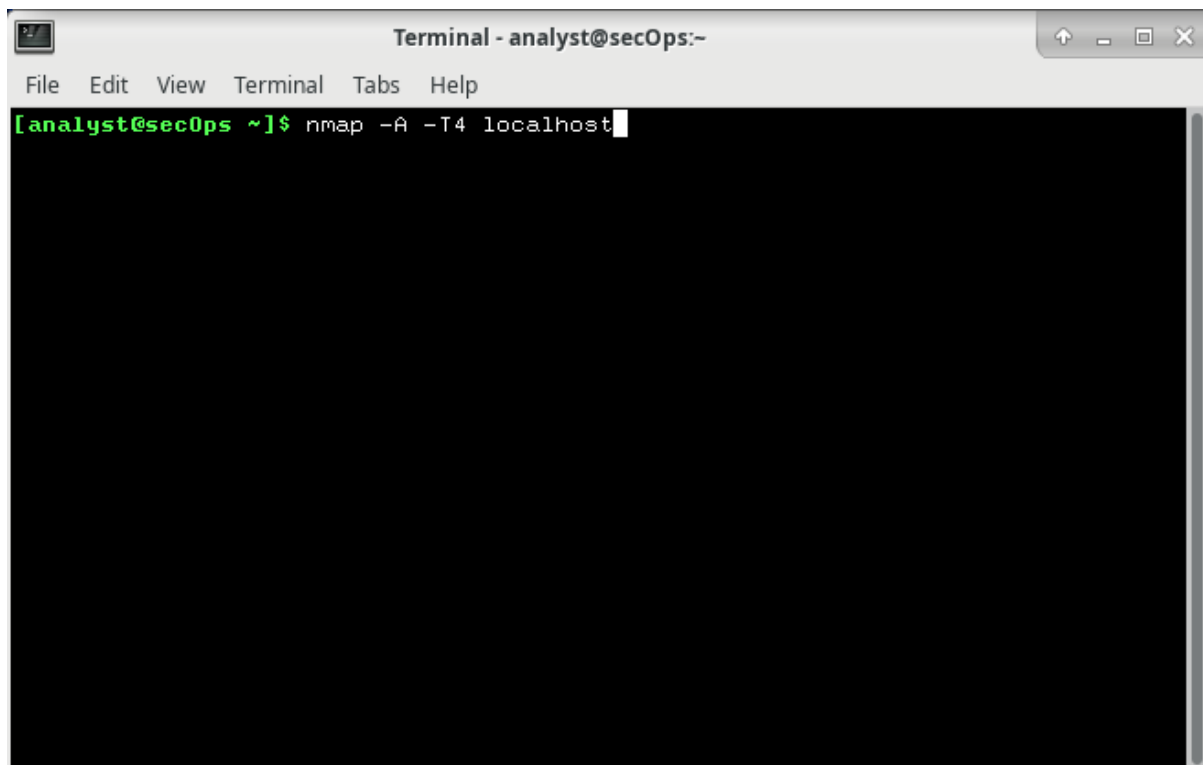
-A: Enable OS detection, version detection, script scanning, and traceroute.

Lo switch -T4 a cosa serve?

-T4: è lo switch che limita la scansione a velocità 4.

-Part 2: Scanning for Open Ports

Ora faremo una prova scansionando il nostro localhost ed utilizzando gli switch, successivamente andremo ad effettuare l'nmap a [scanme.nmap.org](https://scanme.nmap.org).

A screenshot of a terminal window titled "Terminal - analyst@secOps:~". The window has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The terminal content shows the prompt "[analyst@secOps ~]" in green, followed by the command "nmap -A -T4 localhost" in white, with a cursor at the end. The rest of the terminal area is black.

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ nmap -A -T4 localhost
```

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-02-21 10:52 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000033s 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 11.53 seconds
[analyst@secOps ~]$
```

Possiamo notare che ci sono 2 porte e servizi aperti:

Porta 21/tcp FTP

Porta 22/tcp SSH OpenSSH

Step 2: Scan your network

Da terminale usiamo il comando ip address per determinare che indirizzo ip e subnet mask abbiamo nel nostro host.

In questo caso avremo come indirizzo della VM 10.0.2.15/24 indirizzo predefinito del



NAT.

```
[analyst@sec0ps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default ql
en 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 ql
en 1000
    link/ether 2e:6c:34:f0:cd:63 brd ff:ff:ff:ff:ff:ff
3: s1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 5e:45:3a:6f:8f:40 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 08:00:27:e8:fa:a0 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 79791sec preferred_lft 79791sec
    inet6 fd00::a00:27ff:fee8:faa0/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 85843sec preferred_lft 13843sec
    inet6 fe80::a00:27ff:fee8:faa0/64 scope link
        valid_lft forever preferred_lft forever
[analyst@sec0ps ~]$
```

Ora andremo a provare ad effettuare l'nmap al dns "scanme.nmap.org":

```
[analyst@sec0ps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-02-21 11:05 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protoco
l 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 69.04 seconds
[analyst@sec0ps ~]$
```

Possiamo notare che ci sono varie porte aperte e servizi:

Porta 22/tcp SSH OpenSSH Ubuntu

Porta 80/tcp HTTP Server Apache

Porta 9929/tcp Nping-echo

Porta 31337/tcp TcpWrapped

Qual'è il sistema operativo del server?

Ubuntu Linux