

# LABORATORIO 21 FEBBRAIO 2025 S11-L5

## ESERCIZIO 1:

### Laboratorio - Utilizzo di Windows PowerShell

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

#### Objectives

---

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.**

#### Contesto / Scenario

---

PowerShell è un potente strumento di automazione. È sia una console di comando che un linguaggio di scripting. In questo lab si userà la console per eseguire alcuni dei comandi disponibili sia nel prompt dei comandi che in PowerShell. PowerShell dispone anche di funzioni in grado di creare script per automatizzare le attività e lavorare insieme al sistema operativo Windows.

#### Risorse necessarie

---

- 1 PC Windows con PowerShell installato e accesso a Internet

Scegliamo di svolgere il laboratorio su macchina reale.  
Procediamo con l'esercizio seguendo le linee guida. Apriamo  
come richiesto PowerShell e prompt dei comandi.  
Successivamente diamo il comando **dir** a entrambi.

## Disposizioni

### Parte 1: Accedere alla console di PowerShell.

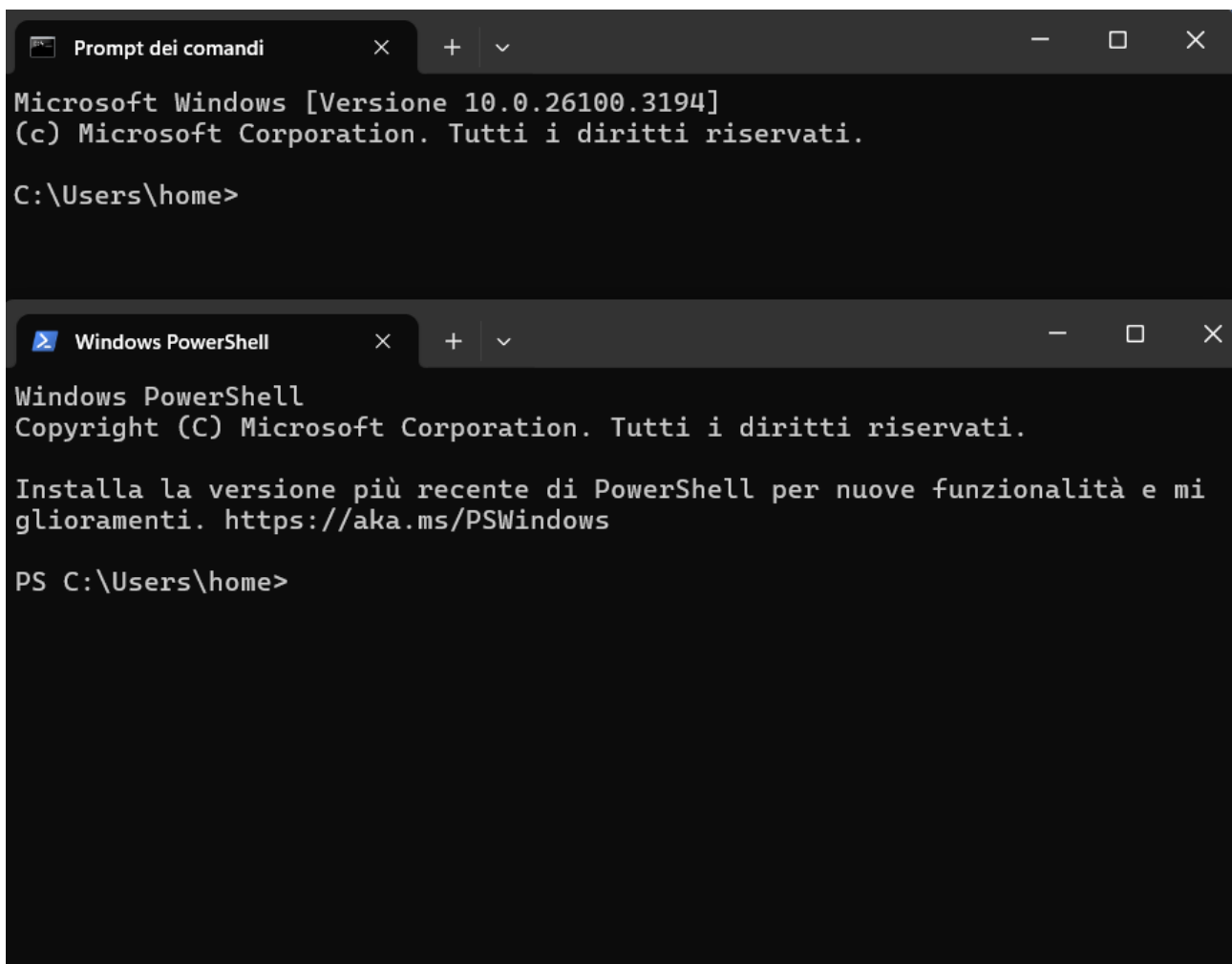
Fare clic su **Avvia**. Cerca e seleziona **PowerShell**.

b. Fare clic su **Start**. Cerca e seleziona **il prompt dei comandi**.

### Parte 2: Esplora il prompt dei comandi e i comandi di PowerShell.

un. Immettere **dir** al prompt in entrambe le finestre.

Quali sono gli output del comando? `dir`



```
Prompt dei comandi
Microsoft Windows [Versione 10.0.26100.3194]
(c) Microsoft Corporation. Tutti i diritti riservati.
C:\Users\home>

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

Installa la versione più recente di PowerShell per nuove funzionalità e mi
glioramenti. https://aka.ms/PSWindows
PS C:\Users\home>
```

```
Prompt dei comandi
C:\Users\home>dir
Il volume nell'unità C è Windows
Numero di serie del volume: 9A33-76A3

Directory di C:\Users\home

20/12/2024 18:20 <DIR> .
05/12/2024 12:12 <DIR> ..
20/02/2021 16:04 <DIR> .cache
25/11/2024 16:30 183 .gitconfig
29/06/2022 10:44 <DIR> .ms-ad
27/12/2024 12:20 174 .packettracer
20/02/2025 16:31 <DIR> .VirtualBox
17/12/2024 11:06 <DIR> .vscode
19/02/2021 08:13 <DIR> 3D Objects
27/12/2024 12:32 <DIR> Cisco Packet Tracer
06/12/2024 12:39 <DIR> Contacts
30/12/2021 16:20 <DIR> Documents
17/02/2025 15:07 <DIR> Downloads
06/12/2024 12:39 <DIR> Favorites
06/12/2024 12:39 <DIR> Links
06/12/2024 12:39 <DIR> Music
06/12/2024 12:31 <DIR> OneDrive
06/12/2024 12:39 <DIR> Saved Games

Windows PowerShell
Directory: C:\Users\home

Mode                LastWriteTime         Length Name
----                -
d-----         20/02/2021         16:04      .cache
d-----         29/06/2022         11:44      .ms-ad
d-----         20/02/2025         16:31      .VirtualBox
d-----         17/12/2024         11:06      .vscode
d-r---         19/02/2021          08:13      3D Objects
d-----         27/12/2024         12:32      Cisco Packet Tracer
d-r---         06/12/2024         12:39      Contacts
d-----         30/12/2021         16:20      Documents
d-r---         17/02/2025         15:07      Downloads
d-r---         06/12/2024         12:39      Favorites
d-r---         06/12/2024         12:39      Links
d-r---         06/12/2024         12:39      Music
d-r---         06/12/2024         12:39      OneDrive
d-----         22/03/2023         12:57      Saved Games
d-r---         06/12/2024         12:39      Saved Games
```

Come output avremo da entrambe gli elenchi delle sottodirectory e dei file e varie informazioni come data e ora dell'ultima modifica. In powershell abbiamo anche gli attributi.

b. Prova un altro comando che hai utilizzato nel prompt dei comandi, come **ping**, **cd** e **ipconfig**.

Quali sono i risultati?

Effettuando la prova di questi comandi abbiamo output simili.

```
C:\Users\home>ipconfig
Configurazione IP di Windows

Scheda Ethernet Ethernet 2:

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

Scheda Ethernet Ethernet 4:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::f9f8:cc8
9:fb80%14
    Indirizzo IPv4. . . . . : 192.168.56.1
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

Scheda LAN wireless Connessione alla rete locale (LAN)* 1:

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

PS C:\Users\home> ipconfig
Configurazione IP di Windows

Scheda Ethernet Ethernet 2:

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

Scheda Ethernet Ethernet 4:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::f9f8:cc8a:f329
:fb80%14
    Indirizzo IPv4. . . . . : 192.168.56.1
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

Scheda LAN wireless Connessione alla rete locale (LAN)* 1:

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

C:\Users\home>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=9ms TTL=120
Risposta da 8.8.8.8: byte=32 durata=10ms TTL=120
Risposta da 8.8.8.8: byte=32 durata=10ms TTL=120
Risposta da 8.8.8.8: byte=32 durata=10ms TTL=120

Statistiche Ping per 8.8.8.8:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 9ms, Massimo = 10ms, Medio = 9ms

C:\Users\home>

PS C:\Users\home> 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=10ms TTL=120
Risposta da 8.8.8.8: byte=32 durata=10ms TTL=120
Risposta da 8.8.8.8: byte=32 durata=11ms TTL=120
Risposta da 8.8.8.8: byte=32 durata=10ms TTL=120

Statistiche Ping per 8.8.8.8:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 10ms, Massimo = 11ms, Medio = 10ms

PS C:\Users\home>
```

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

```
PS C:\Users\home> cd Downloads
PS C:\Users\home\Downloads>
```

### Parte 3: Esplorare i cmdlet.

un. I comandi di PowerShell, i cmdlet, vengono costruiti sotto forma di stringa *verbo-sostantivo*. Per identificare il comando di PowerShell per elencare le sottodirectory e i file in una directory, immettere **Get-Alias dir** al prompt di PowerShell.

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

CommandType Name Version Source
-----
Aliasdir -> Get-ChildItem
```

Qual è il comando PowerShell per **dir**?

```
PS C:\Users\home> cd Downloads
PS C:\Users\home\Downloads> cd ..
PS C:\Users\home> Get-Alias dir

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

Version
-----
```

Il comando PowerShell per **dir** è **Get-ChildItem**.

### Parte 4: Esplorare il comando netstat usando PowerShell.

un. Al prompt di PowerShell, immettere per visualizzare le opzioni disponibili per il comando. **netstat -h netstat**

```
PS C:\Users\CyberOpsUser> netstat -h
```

Ci viene mostrata la lista dei comandi associabili a netstat.

```
PS C:\Users\home> 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
           IP.
```

Procediamo con **netstat -r** per la tabella di routing.

b. Per visualizzare la tabella di routing con i percorsi attivi, immettere al prompt. `netstat -r`

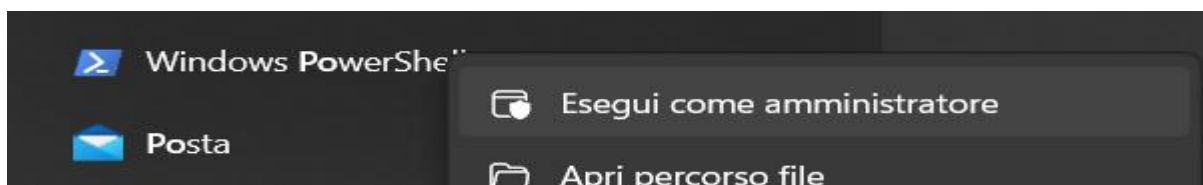
```
PS C:\Users\home> netstat -r
=====
Elenco interfacce
 5...00 ff 68 24 4d 69 .....ExpressVPN TAP Adapter
14...0a 00 27 00 00 0e .....VirtualBox Host-Only Ethernet Adapter
20...1a 47 3d e5 6e 37 .....Microsoft Wi-Fi Direct Virtual Adapter
12...9a 47 3d e5 6e 37 .....Microsoft Wi-Fi Direct Virtual Adapter #2
 9...6c 02 e0 cb c9 69 .....Realtek PCIe GbE Family Controller
 8...18 47 3d e5 6e 37 .....Realtek RTL8821CE 802.11ac PCIe Adapter
10...18 47 3d e5 6e 38 .....Bluetooth Device (Personal Area Network)
 1.....Software Loopback Interface 1
=====

IPv4 Tabella route
=====
Route attive:
  Indirizzo rete          Mask          Gateway       Interfaccia  Metrica
 0.0.0.0                  0.0.0.0       192.168.1.254 192.168.1.166 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       192.168.1.166 291
192.168.1.166            255.255.255.255 On-link       192.168.1.166 291
192.168.1.255            255.255.255.255 On-link       192.168.1.166 291
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       192.168.1.166 291
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       192.168.1.166 291
=====
Route permanenti:
Nessuna
```

Che cos'è il gateway IPv4?

Nel mio caso il gateway è **192.168.1.254**

c. Aprire ed eseguire un secondo PowerShell con privilegi elevati. Fare clic su **Avvia**. Cerca PowerShell e fai clic con il pulsante destro del mouse su **Windows PowerShell** e seleziona **Esegui come amministratore**. Fare clic su **Sì** per consentire all'app di apportare modifiche al dispositivo.



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

Installa la versione più recente di PowerShell per nuove funzioni.

PS C:\WINDOWS\system32>
```

d. Il comando netstat può anche visualizzare i processi associati alle connessioni TCP attive. Immettere il al prompt. `netstat -abno`

```
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  1420
RpcSs
[svchost.exe]
TCP    0.0.0.0:445             0.0.0.0:0            LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:5040            0.0.0.0:0            LISTENING  8744
CDPSvc
[svchost.exe]
TCP    0.0.0.0:5357            0.0.0.0:0            LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:7680            0.0.0.0:0            LISTENING  20012
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49664           0.0.0.0:0            LISTENING  1144
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49665           0.0.0.0:0            LISTENING  1060
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49666           0.0.0.0:0            LISTENING  2980
Schedule
```

e. Apri il Task Manager. Passare alla scheda **Dettagli**. Fare clic sull'intestazione **PID** in modo che i PID siano in ordine.

f. Selezionare uno dei PID dai risultati di netstat -abno. In questo esempio viene utilizzato il PID 756.

g. Individua il PID selezionato nel Task Manager. Fare clic con il pulsante destro del mouse sul PID selezionato in Gestione attività per aprire la finestra di dialogo **Proprietà** per ulteriori informazioni.

Apriamo il task manager e selezioniamo la voce **Dettagli**.  
 Clicchiamo sull'intestazione **PID** per ordinarli. Scegliamo un PID  
 dai risultati dell'output di powershell e individuiamolo sul task  
 manager. **Sceghieremo il PID numero 20048 relativo a Microsoft  
 Edge**. Apriamo la finestra **Proprietà** per altre informazioni.

Nome	Stato	CPU	Memoria	Disco	Rete
Firefox (37)	In esecuzione	6,8%	998,2 MB	0,1 MB/s	0 Mbps
Discord (6)	In esecuzione	4,6%	432,2 MB	0,1 MB/s	0,1 Mbps
Gestione finestre desktop	In esecuzione	3,3%	79,0 MB	0 MB/s	0 Mbps
Gestione attività	In esecuzione	2,4%	78,4 MB	0 MB/s	0 Mbps
System	In esecuzione	2,3%	0,1 MB	0,1 MB/s	0 Mbps
Microsoft Word	In esecuzione	1,8%	67,6 MB	0 MB/s	0 Mbps
Esplora risorse	In esecuzione	1,0%	60,5 MB	0 MB/s	0 Mbps
Isolamento grafico dispositivo...	In esecuzione	0,8%	5,3 MB	0 MB/s	0 Mbps

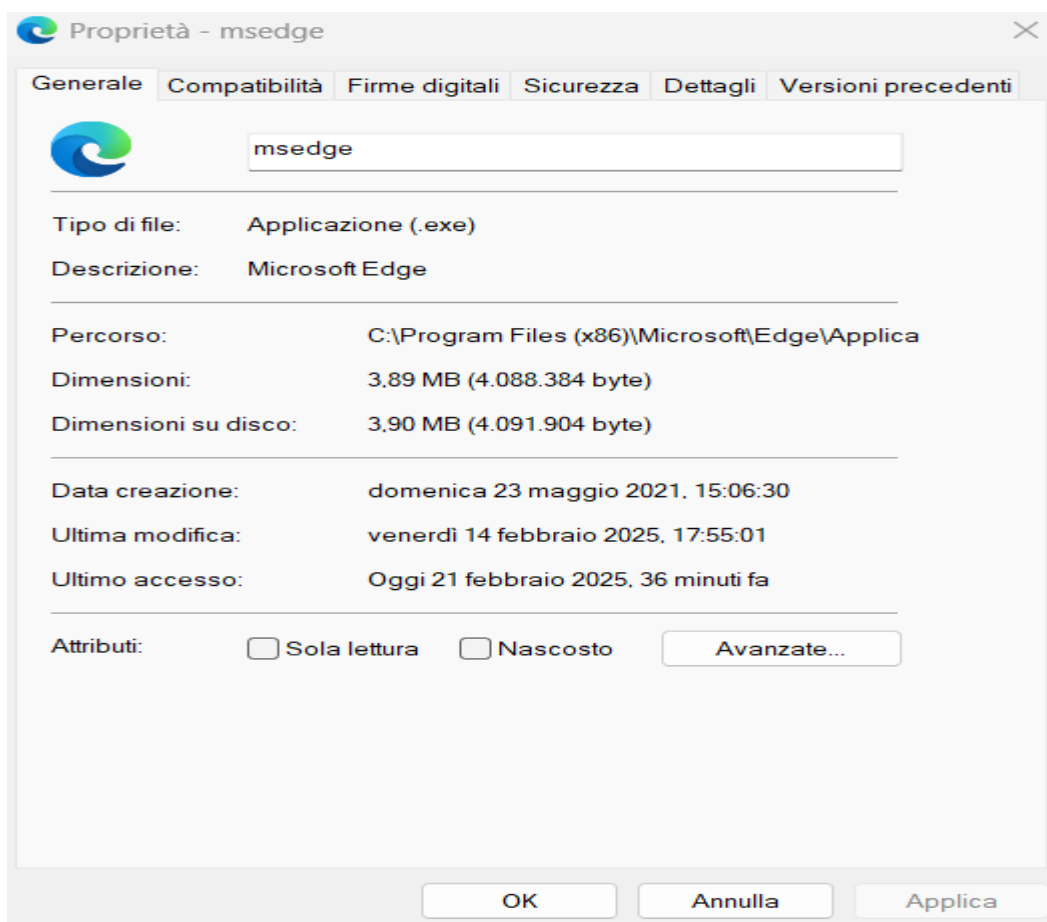
Nome	PID	Stato	Nome utente	CPU	Memoria (...)	Architet...	Descrizione
Interrupt sistema	-	In esecuzione	SYSTEM	01	0 K		Chiamate di proce...
Processo di inattività ...	0	In esecuzione	SYSTEM	88	8 K		Percentuale di tem...
System	4	In esecuzione	SYSTEM	01	12 K		NT Kernel & System
csrss.exe	8	In esecuzione	SYSTEM	00	904 K		Processo runtime cl...
Registry	176	In esecuzione	SYSTEM	00	2.432 K		NT Kernel & System
svchost.exe	392	In esecuzione	SERVIZIO L...	00	1.272 K	x64	Processo host per s...
smss.exe	660	In esecuzione	SYSTEM	00	8 K		Gestione sessioni d...
svchost.exe	1004	In esecuzione	SERVIZIO L...	00	2.344 K	x64	Processo host per s...
explorer.exe	1052	In esecuzione	home	01	62.084 K	x64	Esplora risorse
wininit.exe	1060	In esecuzione	SYSTEM	00	404 K		Applicazione di av...
services.exe	1132	In esecuzione	SYSTEM	00	4.936 K		App Servizi e Contr...
lsass.exe	1144	In esecuzione	SYSTEM	00	8.748 K		Local Security Auth...
svchost.exe	1284	In esecuzione	SYSTEM	00	19.432 K	x64	Processo host per s...
fontdrvhost.exe	1316	In esecuzione	UMFD-0	00	212 K	x64	Usermode Font Dri...
WUDFHost.exe	1360	In esecuzione	SERVIZIO L...	00	1.580 K	x64	Windows Driver Fo...
svchost.exe	1420	In esecuzione	SERVIZIO D...	00	16.096 K	x64	Processo host per s...
svchost.exe	1464	In esecuzione	SYSTEM	00	1.544 K	x64	Processo host per s...
WUDFHost.exe	1512	In esecuzione	SERVIZIO L...	00	552 K	x64	Windows Driver Fo...
VBBoxSVC.exe	1708	In esecuzione	home	00	3.976 K	x64	VirtualBox Interface
svchost.exe	1724	In esecuzione	SERVIZIO L...	00	852 K	x64	Processo host per s...
svchost.exe	1732	In esecuzione	SERVIZIO L...	00	1.676 K	x64	Processo host per s...
svchost.exe	1752	In esecuzione	SERVIZIO L...	00	1.980 K	x64	Processo host per s...
msedge.exe	20048	In esecuzione	home	00	24.192 K	x64	Microsoft Edge



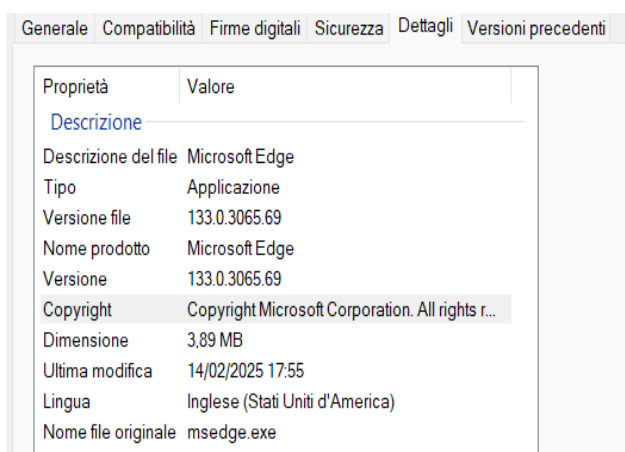
```

TCP [2a01:e11:9:4c90:338d:80df:3bf5:f5e7]:52450 [2606:4700:20::ac43:4670]:443 ESTABLISHED 20048
[msedge.exe]
TCP [2a01:e11:9:4c90:338d:80df:3bf5:f5e7]:52452 [2606:4700:10::ac43:147f]:443 ESTABLISHED 20048
[msedge.exe]
TCP [2a01:e11:9:4c90:338d:80df:3bf5:f5e7]:52453 [2606:4700:20::ac43:4513]:443 ESTABLISHED 20048
[msedge.exe]
TCP [2a01:e11:9:4c90:338d:80df:3bf5:f5e7]:52456 [2a04:4e42:4f::820]:443 ESTABLISHED 20048
[msedge.exe]

```



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



**Possiamo vedere che il Pid è associato a Microsoft Edge, ha una dimensione di 3,89 MB e che è di tipo Applicazione. Ci vengono fornite anche la versione e data e ora dell'ultima modifica.**



## Parte 5: Svuotare il cestino utilizzando PowerShell.

I comandi di PowerShell possono semplificare la gestione di una rete di computer di grandi dimensioni. Ad esempio, se si desidera implementare una nuova soluzione di sicurezza in tutti i server della rete, è possibile utilizzare un comando o uno script di PowerShell per implementare e verificare che i servizi siano in esecuzione. È anche possibile eseguire comandi di PowerShell per semplificare le azioni che richiederebbero più passaggi per l'esecuzione utilizzando gli strumenti desktop grafici di Windows.

- un. Apri il Cestino. Verifica che siano presenti elementi che possono essere eliminati definitivamente dal tuo PC. In caso contrario, ripristina quei file.
- b. Se non sono presenti file nel Cestino, creare alcuni file, ad esempio un file di testo utilizzando Blocco note, e inserirli nel Cestino.
- c. In una console di PowerShell, immettere al prompt. `clear-recyclebin`

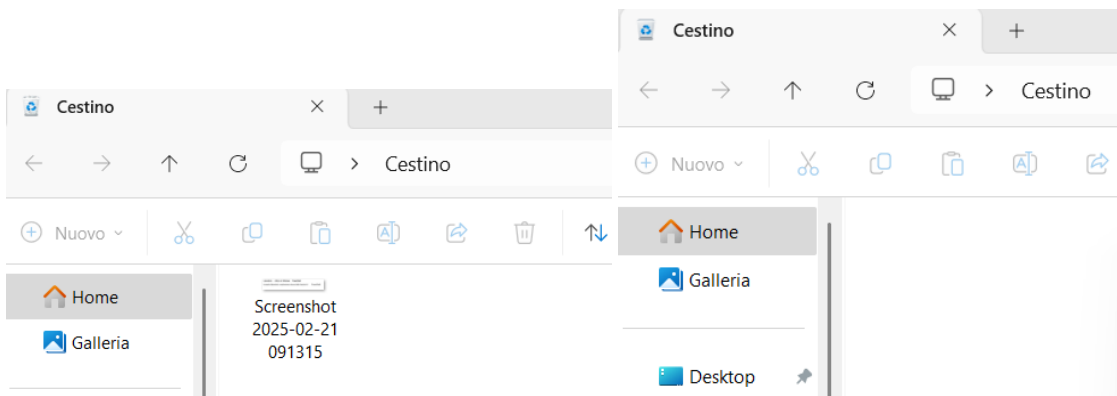
Apriamo il cestino da GUI e verifichiamo che ci siano elementi al suo interno. A questo punto su PowerShell immettiamo il comando **clear-recyclebin** e noteremo che si svuoterà in automatico.

```
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\home> clear-recyclebin

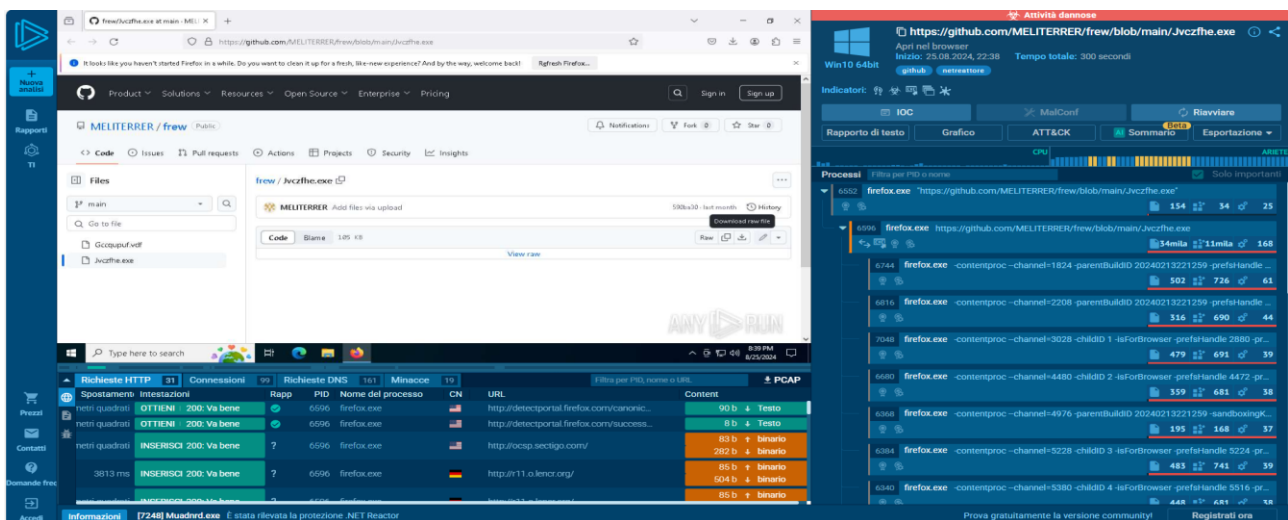
Conferma
Eseguire l'operazione?
Esecuzione dell'operazione "Clear-RecycleBin" sulla destinazione "Tutto il contenuto del Cestino".
[S] Sì [T] Sì a tutti [N] No [U] No a tutti [O] Sospendi [?] Guida (il valore predefinito è "S"): S
```



## ESERCIZIO 2:

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

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



Da una prima occhiata si può notare che si tratta di un link che riporta ad una pagina GitHub. Ci spostiamo nella parte relativa al rapporto di testo che ci fornisce una panoramica completa.



INTERACTIVE MALWARE ANALYSIS

Generale Comportamento MalConf Informazioni statiche Video Schermate Eventi di sistema Rete

### Informazioni generali

Aggiungi per la stampa

URL: <https://github.com/MELTERRER/frew/blob/main/Jvczfhe.exe>  
Analisi completa: <https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281>  
Verdetto: **Attività dannose**  
Data dell'analisi: 25 agosto 2024 alle 22:38:59  
Sistema operativo: Windows 10 Professional (versione: 19045, 64 bit)  
Tag: [github](#) [netreattore](#)  
Indicatori: [🌐](#) [📄](#) [🔍](#)  
MD5: 00B5E91B42712471CDFBDB37B715670C  
SHA1: D9550361E5205DB1D2DF9D02CC7E30503B8EC3A2  
SHA256: 0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0  
SSDEEP: 3:N8tEd7QyQ3FJMERCNuN:2uRQyQ3zMsCNa

**QUALUNQUE CORRERE** è un servizio interattivo che fornisce l'accesso completo al sistema ospite. Le informazioni contenute in questo rapporto potrebbero essere distorte dalle azioni dell'utente e vengono fornite per il riconoscimento dell'utente così com'è. **QUALUNQUE CORRERE** non garantisce la malizia o la sicurezza del contenuto.

## MALIGNO

Nessun indicatore dannoso.

## SOSPETTOSO

Il processo elimina l'eseguibile legittimo di Windows

- firefox.exe (PID: 6596)

Avvia CMD.EXE per l'esecuzione dei comandi

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

Utilizza TIMEOUT.EXE per ritardare l'esecuzione

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

Legge le impostazioni di sicurezza di Internet Explorer

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

Controlla le impostazioni di attendibilità di Windows

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

Esegue l'applicazione che si arresta in modo anomalo

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

Si collega a una porta insolita

- InstallUtil.exe (PID: 5152)

L'applicazione è stata avviata da sola

- Muadnrd.exe (PID: 7824)

## INFORMAZIONI

Disabilita i log di traccia

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

L'applicazione è stata avviata da sola

- firefox.exe (PID: 6552)
- firefox.exe (PID: 6596)

Controlla le lingue supportate

- Jvczfhe.exe (PID: 7492)
- InstallUtil.exe (PID: 5152)
- Muadnrd.exe (PID: 7824)
- Muadnrd.exe (PID: 7248)

Controlla le informazioni sul server proxy

- Jvczfhe.exe (PID: 7492)
- WerFault.exe (PID: 1356)
- Muadnrd.exe (PID: 7824)
- WerFault.exe (PID: 7584)

Legge le chiavi del Registro di sistema di Microsoft Office

- firefox.exe (PID: 6596)

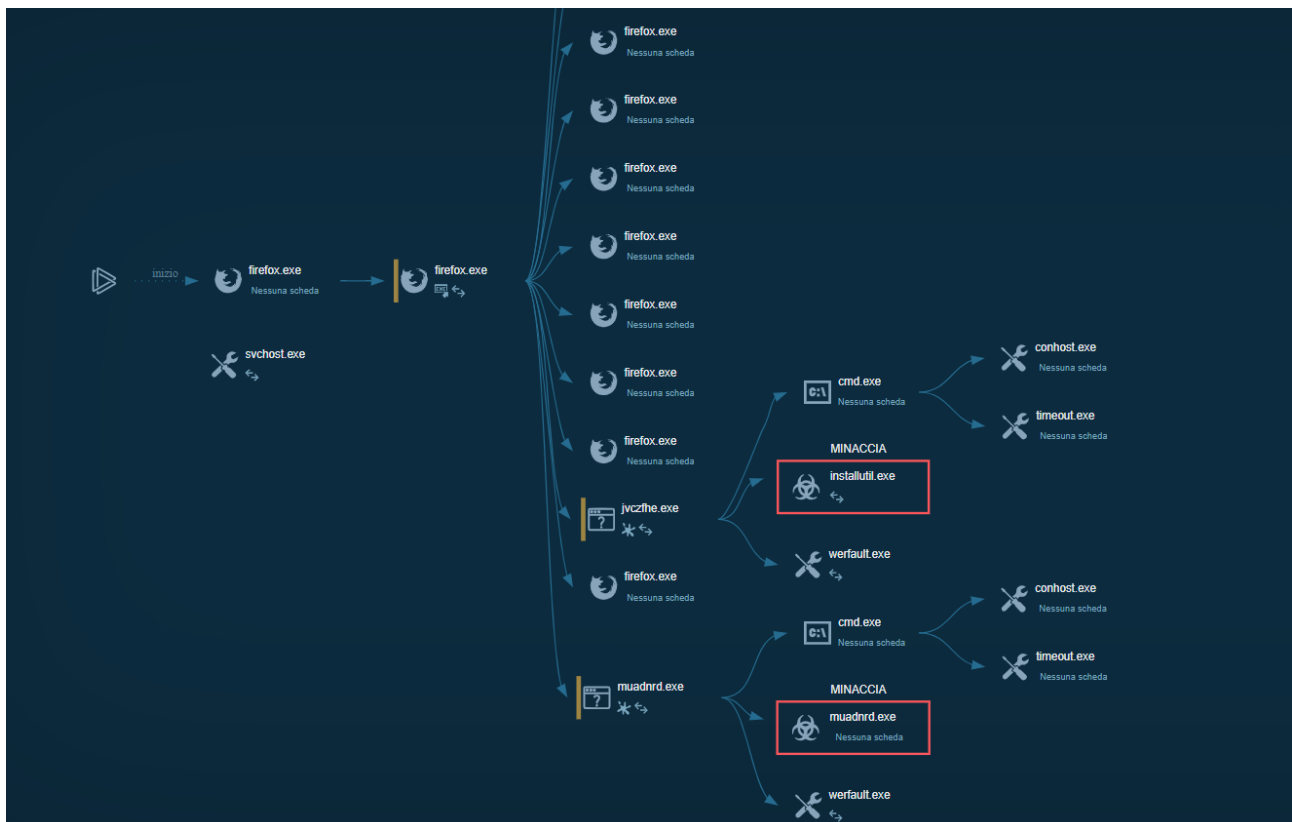
Legge i valori dell'ambiente

- Jvczfhe.exe (PID: 7492)
- InstallUtil.exe (PID: 5152)
- Muadnrd.exe (PID: 7824)

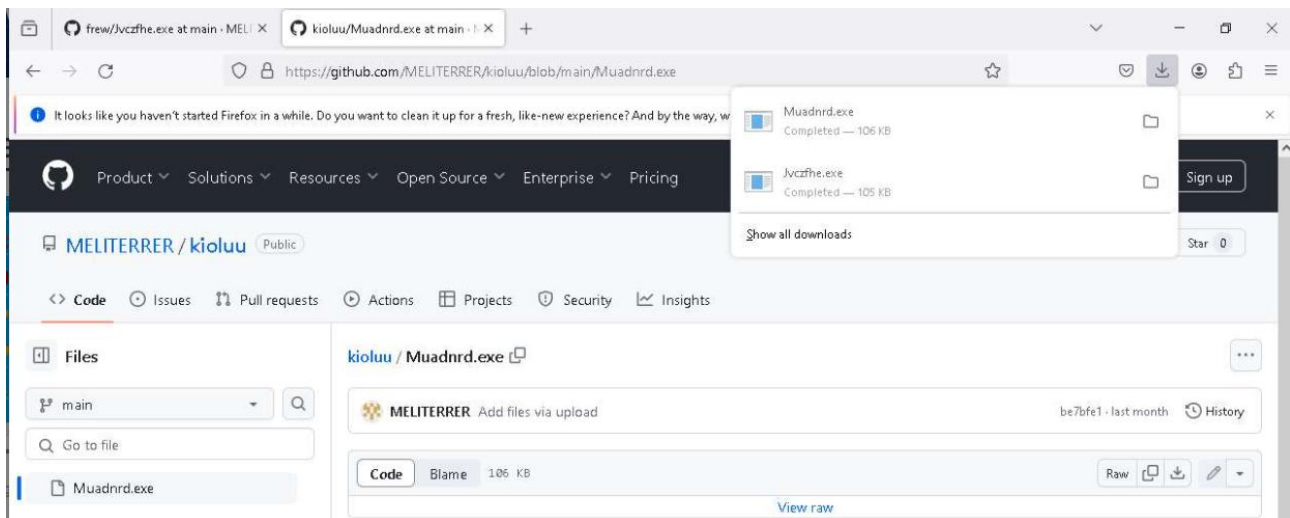
Legge il nome del computer

- Jvczfhe.exe (PID: 7492)
- InstallUtil.exe (PID: 5152)

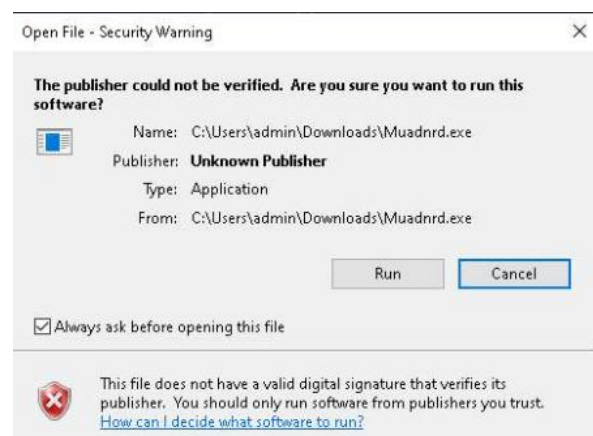
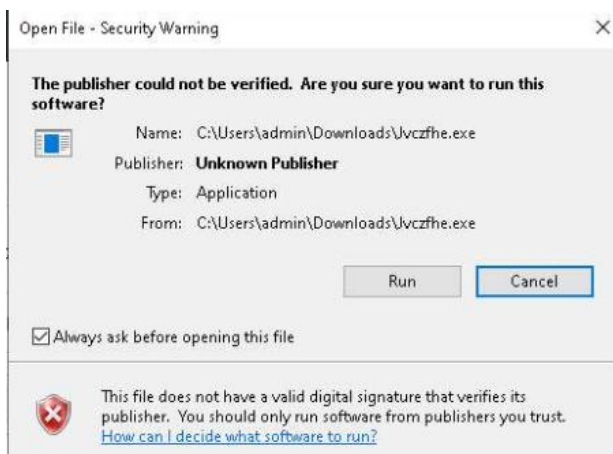
Possiamo vedere anche il grafico che ci mostra l'andamento degli eventi e il comportamento del file.



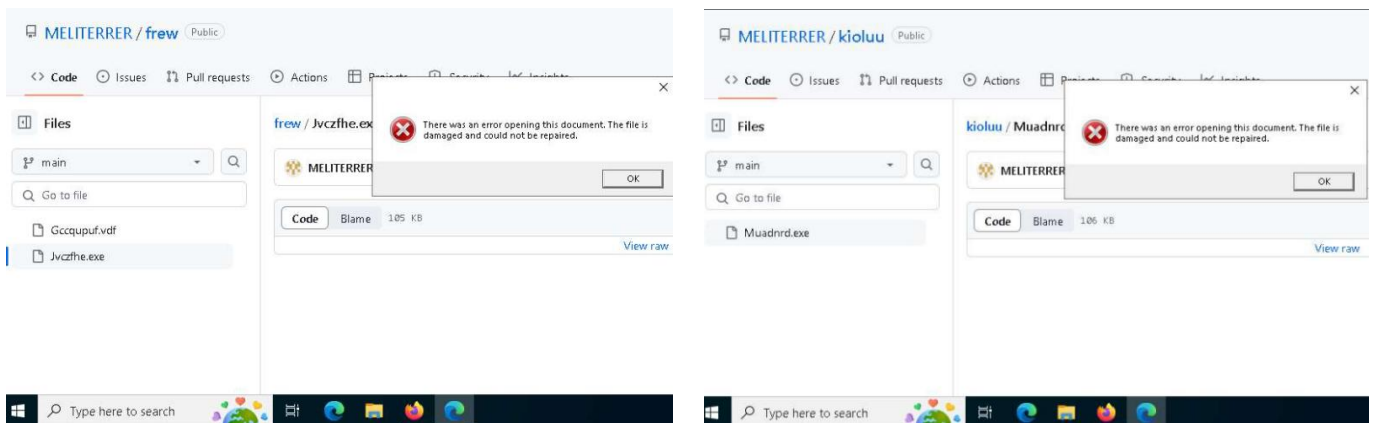
Possiamo notare anche dagli screenshot forniti che l'utente utilizzando il web browser Firefox ha copiato e incollato dei link che riportano a GitHub ed ha scaricato due file .exe chiamati rispettivamente **Jvczfhe.exe** e **Muadnrd.exe**



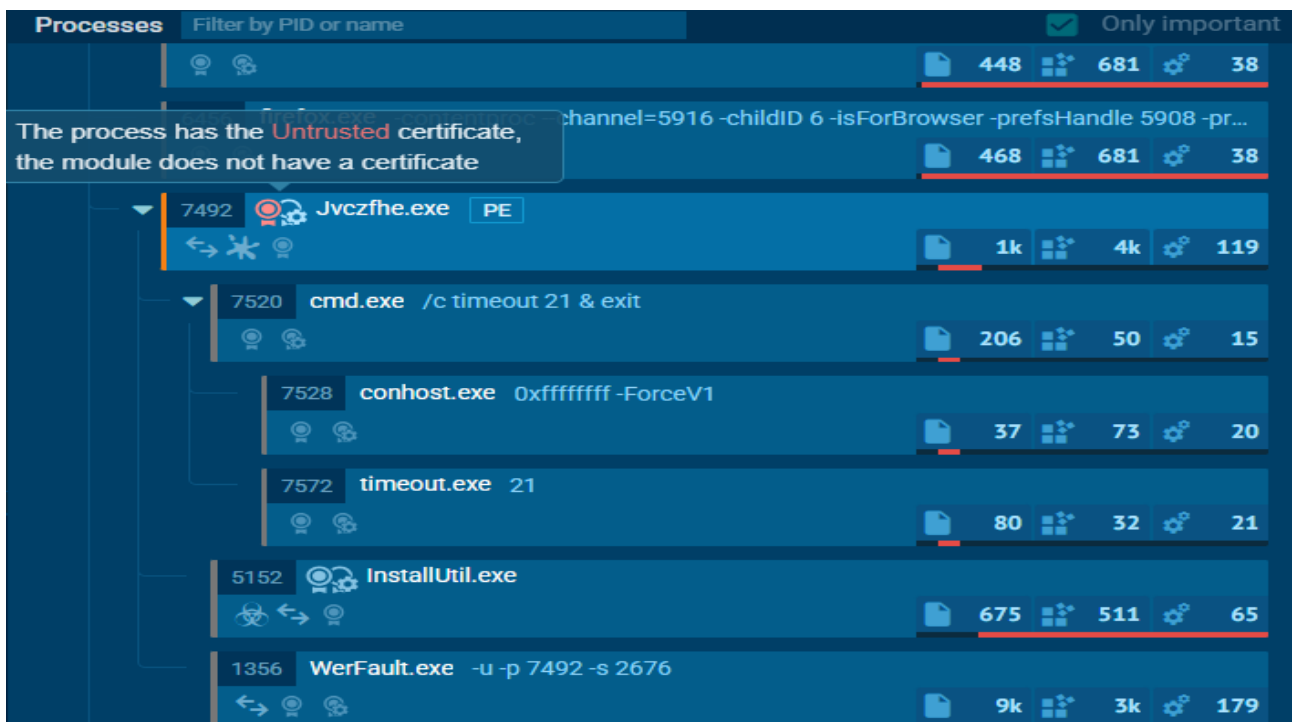
Ha poi eseguito entrambi i file nonostante il Security Warning lo informasse sulla impossibilità di verificarne l'autore. Specifica appunto che questi file non hanno una valida firma digitale e che bisognerebbe eseguire solo i file dei quali si conosce l'autore.



In entrambi i casi si apre un popup di Microsoft Edge che avverte sulla presenza di un errore nell'apertura dei documenti, i quali sono danneggiati in modo irreparabile. Ciò rende ineseguibili i file.

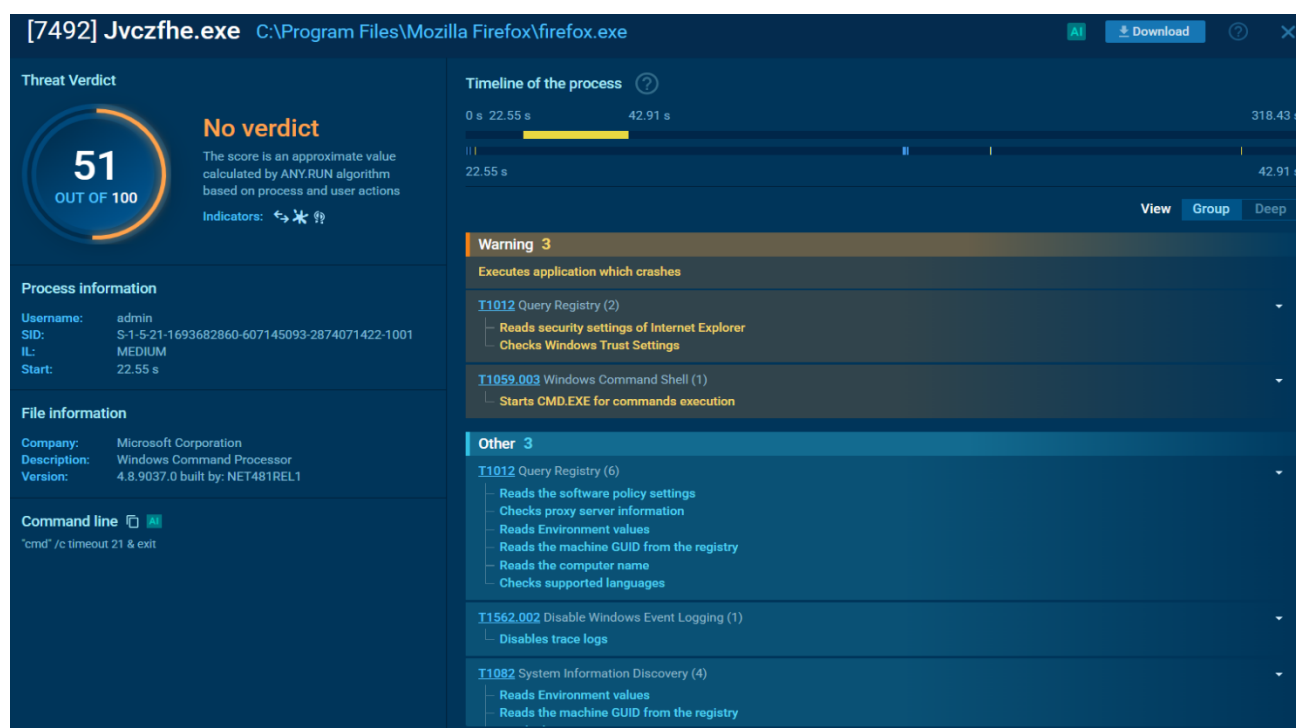


Procediamo esaminando nel dettaglio i due file per capire cosa facciano esattamente. Iniziamo con il file Jvczfhe.exe



Analizziamo i dettagli avanzati del processo per capirne le funzioni. Notiamo che ha un punteggio di 51 su 100 il che lo rende sospetto ma non necessariamente malevolo. Gli indicatori sospetti sono:

- **Chiusura con errore**
- **Connessione alla rete**
- **Certificato non valido**



Dai warning possiamo notare che questo file mostra comportamenti sospetti:

- **Stop anomalo dell'applicazione.**
- **Apre il command prompt per eseguire comandi**
- **Controlla le impostazioni di Windows e di Internet Explorer dalle query di registro**

- Disabilita i log di traccia presumibilmente per non essere rilevato nei registri di sistema.
- Ha accesso alle informazioni di sistema
- Recupera informazioni su proxy, variabili d'ambiente, GUID del computer, nome host e lingue supportate.

Continuiamo ad analizzare i file controllando la parte relativa al cmd.exe

[7520] cmd.exe C:\Programmi\Mozilla Firefox\firefox.exe

Verdetto di minaccia

**15**

SU 100

**Nessun verdetto**

Il punteggio è un valore approssimativo calcolato da ANY. Algoritmo RUN basato sul processo e sulle azioni dell'utente

Indicatori:

Informazioni sul processo

Nome utente: Admin  
SID: S-1-5-21-1693682860-607145093-2874071422-1001  
IL: MEDIO  
Inizio: 22,55 secondi

Informazioni sul file

Società: Società Microsoft  
Descrizione: Processore dei comandi di Windows  
Versione: 4.8.9037.0 costruito da: NET481REL1

Riga di comando

"cmd" /c timeout 21 ed uscita

Cronologia del processo

0 secondi 22,55 secondi 42,91 secondi

22,55 secondi

**Avvertimento 1**

**T1059.003** Shell dei comandi di Windows (1)

Utilizza TIMEOUT.EXE per ritardare l'esecuzione

Notiamo che utilizza il comando **cmd /c timeout 21**. Questo potrebbe indicare un tentativo di ritardare l'esecuzione o nascondere attività sospette.

Un altro warning ci avverte che effettua il collegamento ad una porta non standard.

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

Verdetto di minaccia

**10**

SU 100

**Nessun verdetto**

Il punteggio è un valore approssimativo calcolato da ANY. Algoritmo RUN basato sul processo e sulle azioni dell'utente

Indicatori:

Informazioni sul processo

Cronologia del processo

0 secondi 58,99 secondi

58,99 secondi

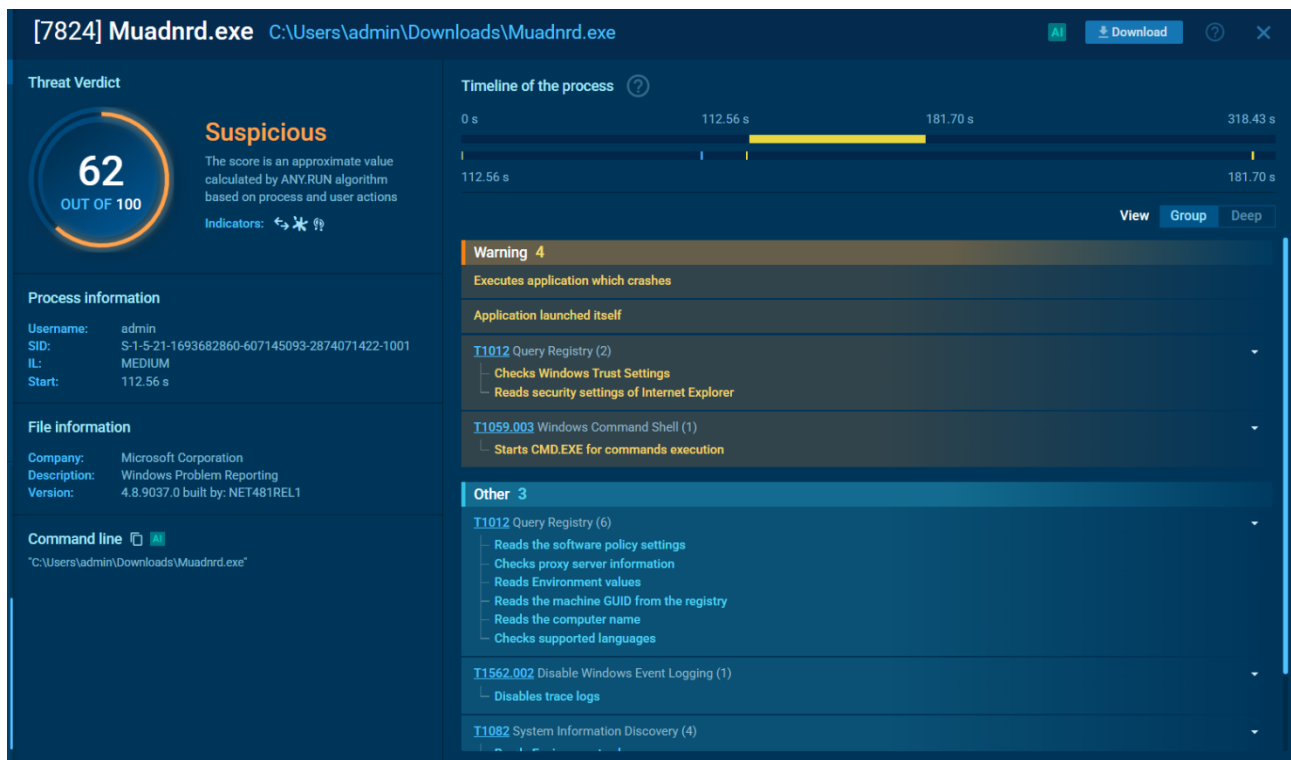
**Avvertimento 1**

**T1571** Porta non standard (1)

Si collega a una porta insolita



Procediamo ora con l'analisi del secondo file: **Muadnrd.exe**



In questo caso il verdetto di minaccia ha un punteggio di 62 su 100 ed il file è considerato sospetto. Gli indicatori corrispondono a quelli dell'altro file ovvero:

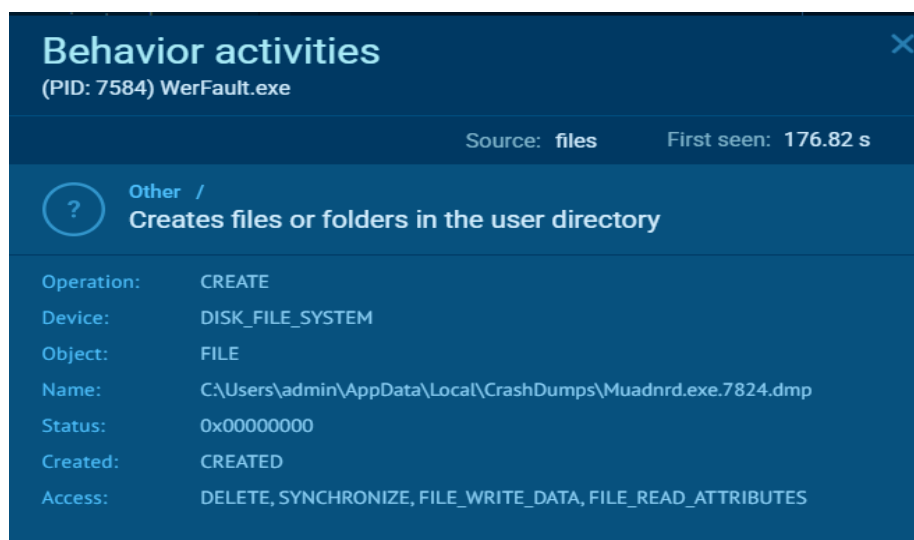
- **Connessione alla rete**
- **Certificato non valido**
- **Chiusura con errore**

I comportamenti sospetti in questo caso sono i seguenti:

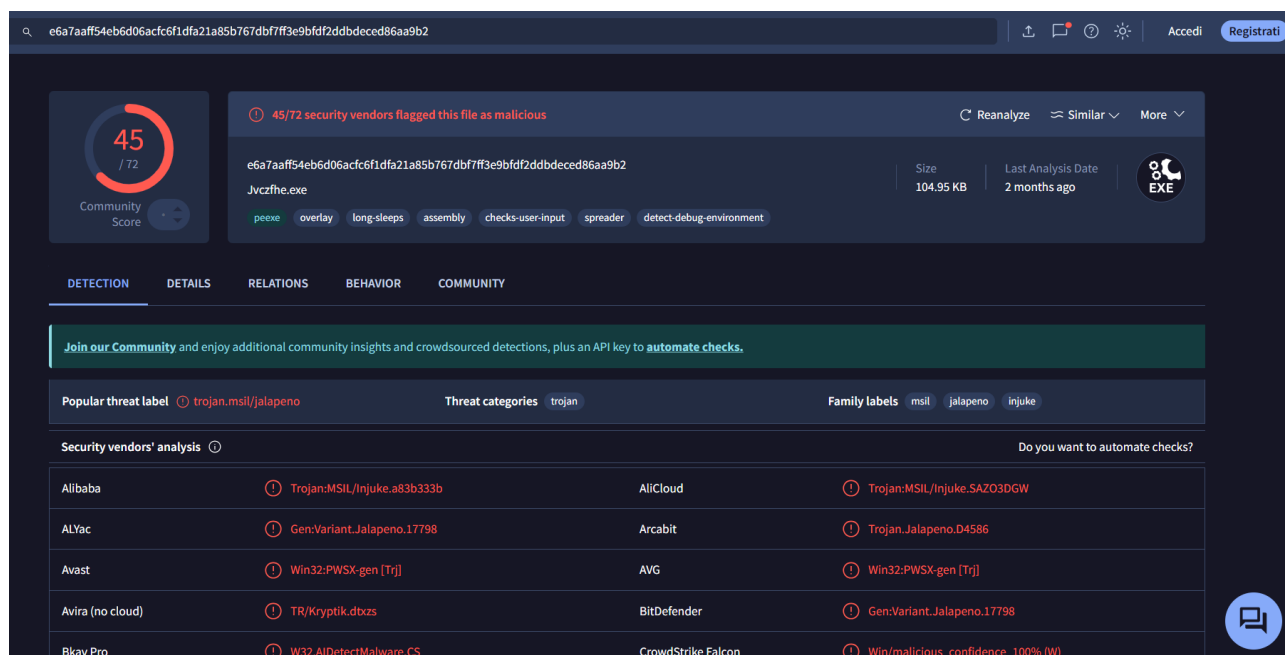
- **Si avvia da solo**
- **Interroga il registro di sistema controllando impostazioni di sicurezza e attendibilità di Windows e Internet Explorer**
- **Recupera informazioni di sistema, incluse variabili d'ambiente, nome host e GUID del computer**

- Avvia cmd.exe per eseguire comandi
- Disabilita la registrazione eventi di Windows
- Arresto in modo anomalo dell'applicazione

Possiamo inoltre notare che tra le altre funzioni ha anche quella di creare file o cartelle nella directory **user**.

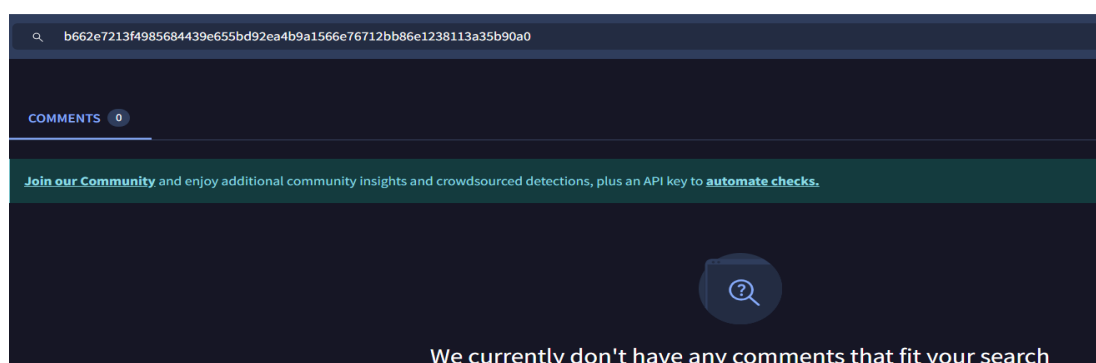


A questo punto per un'ulteriore verifica controlliamo i file utilizzando virusTotal.



Per quanto riguarda **Jvczfhe.exe**, viene contrassegnato come file malevolo da 45 antivirus su 72. Si tratta di un malware già conosciuto, più esattamente un trojan chiamato Jalapeno. Questo malware ha quindi funzionalità dannose atte a rubare informazioni, eseguire comandi remoti e persistenza nel sistema. Ha facoltà di scaricare ed eseguire altri file dannosi e avviare processi nascosti come ad esempio cmd.exe per eseguire comandi all'insaputa dell'utente. Inoltre può modificare le impostazioni di sistema tramite le query al registro di sistema per ottenere informazioni su Internet Explorer e Windows Security così da poter eventualmente identificare e sfruttare vulnerabilità e disabilitare protezioni. In ultimo ha la facoltà di disabilitare i log di sistema per evitare di essere rilevato da antivirus e firewall.

Passiamo al secondo malware ovvero **Muadrnd.exe** ma in questo caso la ricerca su virusTotal non porta nessun risultato.



A differenza dell'altro malware questo sembra più sospetto a causa della sua esecuzione automatica, per il resto ha più o meno le stesse caratteristiche del primo. Si può supporre che si tratti anche in questo caso di un trojan per rubare dati sensibili ed aprire possibilmente una backdoor.

## BONUS 1:

### Laboratorio - Esplorazione di Nmap

La scansione delle porte è solitamente parte di un attacco di ricognizione. Esistono diversi metodi di scansione delle porte che possono essere utilizzati.

<https://itexamanswers.net/9-3-8-lab-exploring-nmap-answers.html>

## 9.3.8 Lab – Exploring Nmap

### 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

Prepariamo lo scenario per l'esercizio avviando la VM CyberOps Workstation in Nat.



## 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.

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

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

What is Nmap?

In questa fase apriamo il terminale e diamo il comando **man nmap** per visualizzare il manuale di nmap.

```
[analyst@secOps ~]$ 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.
```

Ci viene chiesto cosa sia Nmap e a cosa serve.

Nmap è lo strumento che utilizziamo per esplorare le reti e scannerizzare le porte. Serve a determinare gli host all'interno delle reti, scansionare le porte e rilevare il sistema operativo.

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.

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.

Una volta nella pagina del manuale possiamo utilizzare vari comandi per muoverci all'interno dello stesso.

Digitiamo **/example** e premiamo invio per cercare la parola example.

```
/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:20:82:85:ec (RSA)
80/tcp    open      http         Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
646/tcp   filtered  ldap
1720/tcp  filtered  H.323/Q.931

Manual page nmap(1) line 44 (press h for help or q to quit)
```

Look at Example 1.

What is the nmap command used?

Il comando è **nmap -A -T4 scanme.nmap.org**

Use the search function to answer the following questions.

What does the switch -A do?

What does the switch -T4 do?

Il comando -A serve per abilitare il rilevamento del sistema operativo, la versione, la scansione degli script e il traceroute.

Il comando -T4 serve per un'esecuzione più rapida della scansione.

## PARTE 2:

### 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.



Effettuiamo ora una scansione sul nostro localhost con il comando **nmap -A -T4 localhost**.

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-02-21 10:20 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000065s 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 2
|   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
```

b. Review the results and answer the following questions.

Which ports and services are opened?

**Le porte aperte sono la porta TCP 21 ftp e la TCP 22 ssh.**

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

**Il software che fornisce il servizio ftp è vsftpd. Quello che fornisce il servizio ssh è invece 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.

Procediamo con una scansione sulla nostra rete con **ip address**.

```
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:7a:c3:bb brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 83805sec preferred_lft 83805sec
    inet6 fd00::a00:27ff:fe7a:c3bb/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86084sec preferred_lft 14084sec
    inet6 fe80::a00:27ff:fe7a:c3bb/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

Record the IP address and subnet mask for your VM.

Which network does your VM belong to?

**Indirizzo IP 10.0.2.15; subnet mask 255.255.255.0 (/24).**

**Appartiene alla rete enp0s3.**

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

Cerchiamo altri eventuali host su questa LAN con il comando

**nmap -A -T4 10.0.2.0/24**

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2025-02-21 10:33 EST
Nmap scan report for 10.0.2.15
Host is up (0.00023s 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 2
|_     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: 256 IP addresses (1 host up) scanned in 20.87 seconds
```

## How many hosts are up?

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.

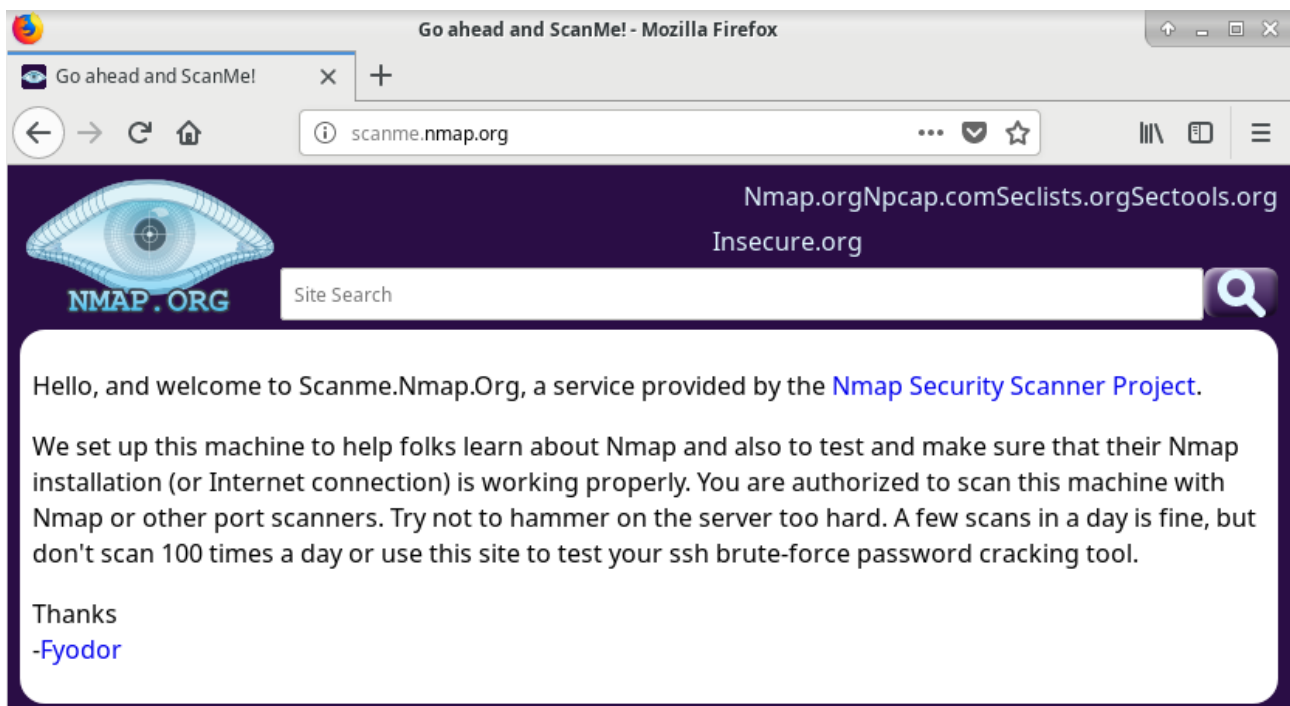
**È attivo solo un host, quello della VM in uso ovvero il local host.**

### 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?

Apriamo un web browser e raggiungiamo il sito **scanme.map.org**



Lo scopo di questo sito è conoscere e testare Nmap. Si ha la possibilità di scannerizzarlo, senza esagerare con i tentativi.

Procediamo dunque con la scansione del sito.

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

```
[analyst@sec0ps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-02-21 10:45 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.17s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|_ 2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|_ 256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_ 256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo   Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.85 seconds
[analyst@sec0ps ~]$
```

c. Review the results and answer the following questions.

Which ports and services are opened?

**Le porte aperte sono la 22: SSH, la 80: HTTP, la 9929: N ping-echo e la 31337: TCPwrapped.**

Which ports and services are filtered?

**996 porte sono filtrate.**

What is the IP address of the server?

**L'indirizzo IP del server è 45.33.32.156.**

What is the operating system?

**Il sistema operativo è Linux Ubuntu.**

