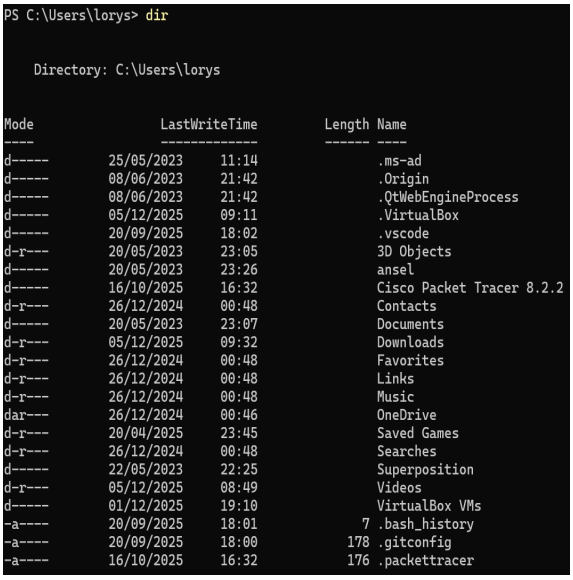
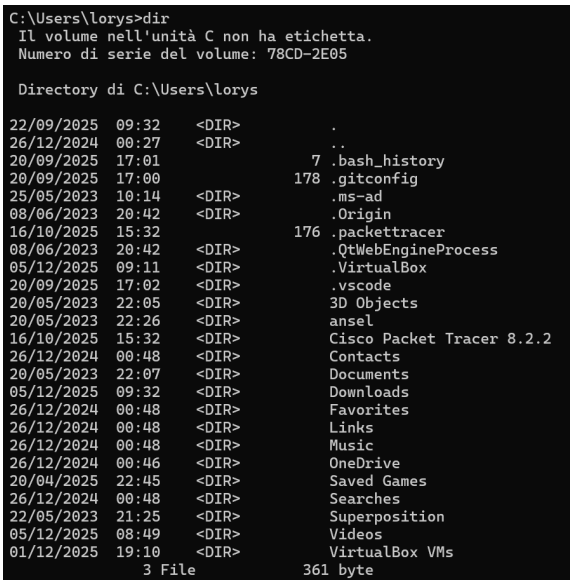
UNIT3 S11/L5 - Esercizi finali

- **Esplorare i comandi del Prompt dei Comandi e di PowerShell.** a. Inserisci dir al prompt in entrambe le finestre. Quali sono gli output del comando dir?



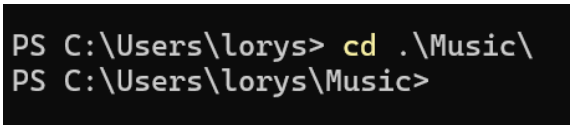
```
PS C:\Users\lorys> dir


    Directory: C:\Users\lorys


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        25/05/2023     11:14                .ms-ad
d-----        08/06/2023     21:42                .Origin
d-----        08/06/2023     21:42                .QtWebEngineProcess
d-----        05/12/2025     09:11                .VirtualBox
d-----        20/09/2025     18:02                .vscode
d-r---        20/05/2023     23:05                3D Objects
d-----        20/05/2023     23:26                ansel
d-----        16/10/2025     16:32                Cisco Packet Tracer 8.2.2
d-r---        26/12/2024     00:48                Contacts
d-----        20/05/2023     23:07                Documents
d-r---        05/12/2025     09:32                Downloads
d-r---        26/12/2024     00:48                Favorites
d-r---        26/12/2024     00:48                Links
d-r---        26/12/2024     00:48                Music
dar---        26/12/2024     00:46                OneDrive
d-r---        20/04/2025     23:45                Saved Games
d-r---        26/12/2024     00:48                Searches
d-----        22/05/2023     22:25                Superposition
d-r---        05/12/2025     08:49                Videos
d-----        01/12/2025     19:10                VirtualBox VMs
-a----        20/09/2025     18:01              7 .bash_history
-a----        20/09/2025     18:00            178 .gitconfig
-a----        16/10/2025     16:32            176 .packettracer
```



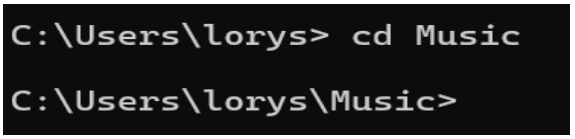
```
C:\Users\lorys>dir
 Il volume nell'unità C non ha etichetta.
 Numero di serie del volume: 78CD-2E05

 Directory di C:\Users\lorys

22/09/2025  09:32    <DIR>          .
26/12/2024  00:27    <DIR>          ..
20/09/2025  17:01                 7 .bash_history
20/09/2025  17:00               178 .gitconfig
25/05/2023  10:14    <DIR>          .ms-ad
08/06/2023  20:42    <DIR>          .Origin
16/10/2025  15:32               176 .packettracer
08/06/2023  20:42    <DIR>          .QtWebEngineProcess
05/12/2025  09:11    <DIR>          .VirtualBox
20/09/2025  17:02    <DIR>          .vscode
20/05/2023  22:05    <DIR>          3D Objects
20/05/2023  22:26    <DIR>          ansel
16/10/2025  15:32    <DIR>          Cisco Packet Tracer 8.2.2
26/12/2024  00:48    <DIR>          Contacts
20/05/2023  22:07    <DIR>          Documents
05/12/2025  09:32    <DIR>          Downloads
26/12/2024  00:48    <DIR>          Favorites
26/12/2024  00:48    <DIR>          Links
26/12/2024  00:48    <DIR>          Music
26/12/2024  00:46    <DIR>          OneDrive
20/04/2025  22:45    <DIR>          Saved Games
26/12/2024  00:48    <DIR>          Searches
22/05/2023  21:25    <DIR>          Superposition
05/12/2025  08:49    <DIR>          Videos
01/12/2025  19:10    <DIR>          VirtualBox VMs
               3 File            361 byte
```

A sinistra è possibile vedere l'output della powershell, in cui abbiamo la lista dei file presenti nella home del mio pc con i permessi relativi nella colonna di sinistra mentre a destra si può vedere l'output del prompt dei comandi, in cui è possibile distinguere le "directory" con la data e l'orario della creazione, mentre in tutti

- **b. Prova un altro comando che hai usato nel prompt dei comandi, come ping, cd e ipconfig.** Quali sono i risultati?



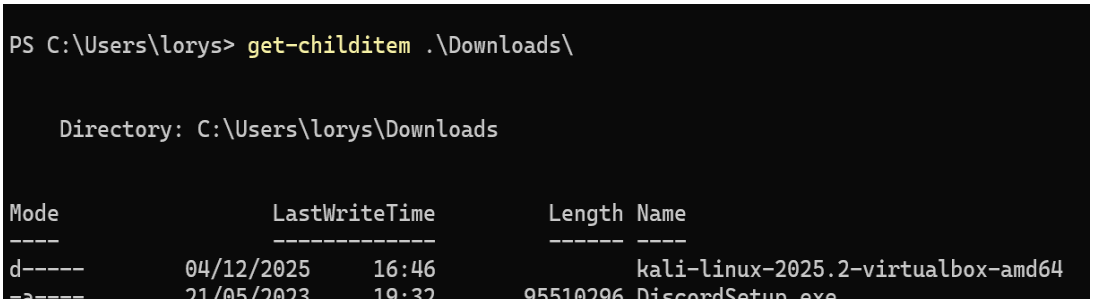
```
PS C:\Users\lorys> cd .\Music\
PS C:\Users\lorys\Music>
```



```
C:\Users\lorys> cd Music

C:\Users\lorys\Music>
```

per spostarsi in una delle directory basta utilizzare il comando cd e quando si inizia a scrivere, premendo Tab è possibile completare il suggerimento con la formattazione giusta.

- I comandi PowerShell, chiamati cmdlet, sono costruiti nella forma di una stringa verbo-nome. Per identificare il comando PowerShell per elencare le sottodirectory e i file in una directory, inserisci Get-Alias dir al prompt di PowerShell. **Qual è il comando PowerShell per dir?**



```
PS C:\Users\lorys> get-childitem .\Downloads\


    Directory: C:\Users\lorys\Downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         04/12/2025     16:46                kali-linux-2025.2-virtualbox-amd64
-a----         21/05/2023     19:32       95510296 DiscordSetup.exe
```

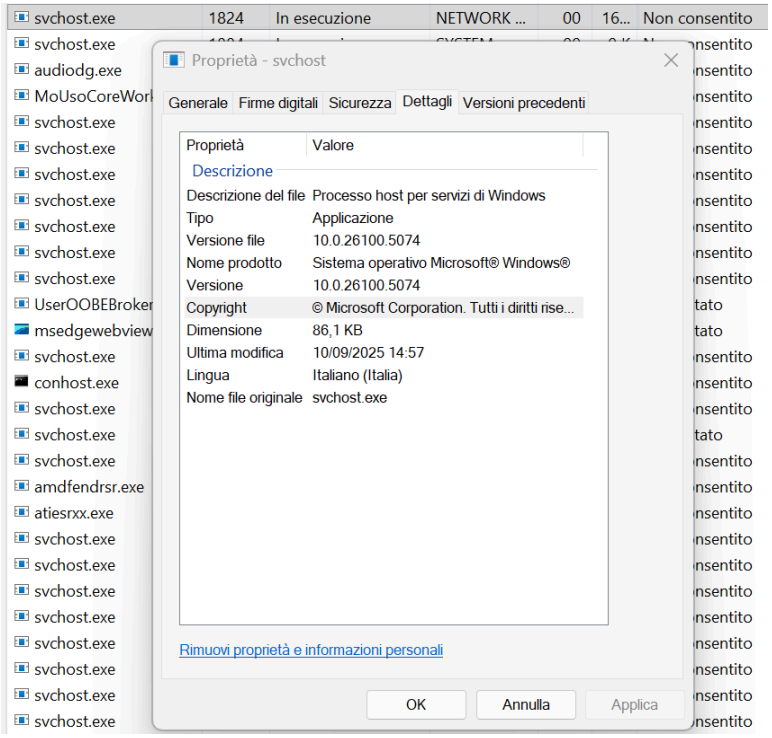
il comando è "get-childitem dir"

- Per visualizzare la tabella di routing con le rotte attive, inserisci netstat -r al prompt. **Qual è il gateway IPv4?**

```
IPv4 Tabella route
===========================================================================
Route attive:
     Indirizzo rete               Mask          Gateway       Interfaccia Metrica
          0.0.0.0          0.0.0.0      192.168.1.1     192.168.1.48     25
```

Il gateway è l'ip presente sotto la colonna gateway, in questo caso 192.168.1.1

- Apri ed esegui una seconda PowerShell con privilegi elevati. Inserisci netstat -abno al prompt. Apri Gestione Attività Task Manager). Naviga alla scheda Dettagli Details). Fai clic sull'intestazione PID in modo che i PID siano in ordine. Seleziona uno dei PID. Individua il PID selezionato in Gestione Attività. Fai clic con il pulsante destro sul PID selezionato in Gestione Attività per aprire la finestra di dialogo Proprietà Properties) per maggiori informazioni. **Quali informazioni puoi ottenere dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID selezionato?**



La scheda "Dettagli" elenca tutti i processi attivi e le relative metriche. Una volta individuato il PID selezionato dall'output di netstat, si ottengono le seguenti informazioni immediate sul processo: il nome, il pid, lo stato, nome utente, la CPU, delta working set (memoria), virtualizzazione controllo dell'account utente. Nella scheda dettaglio è possibile invece avere informazioni generali, eventuali firme digitali, i permessi relativi (nella sezione "sicurezza"), i dettagli del processo e le versioni precedenti,

- Svuotare il cestino usando PowerShell. In una console PowerShell, inserisci clear-recyclebin al prompt. **Cosa è successo ai file nel Cestino?**

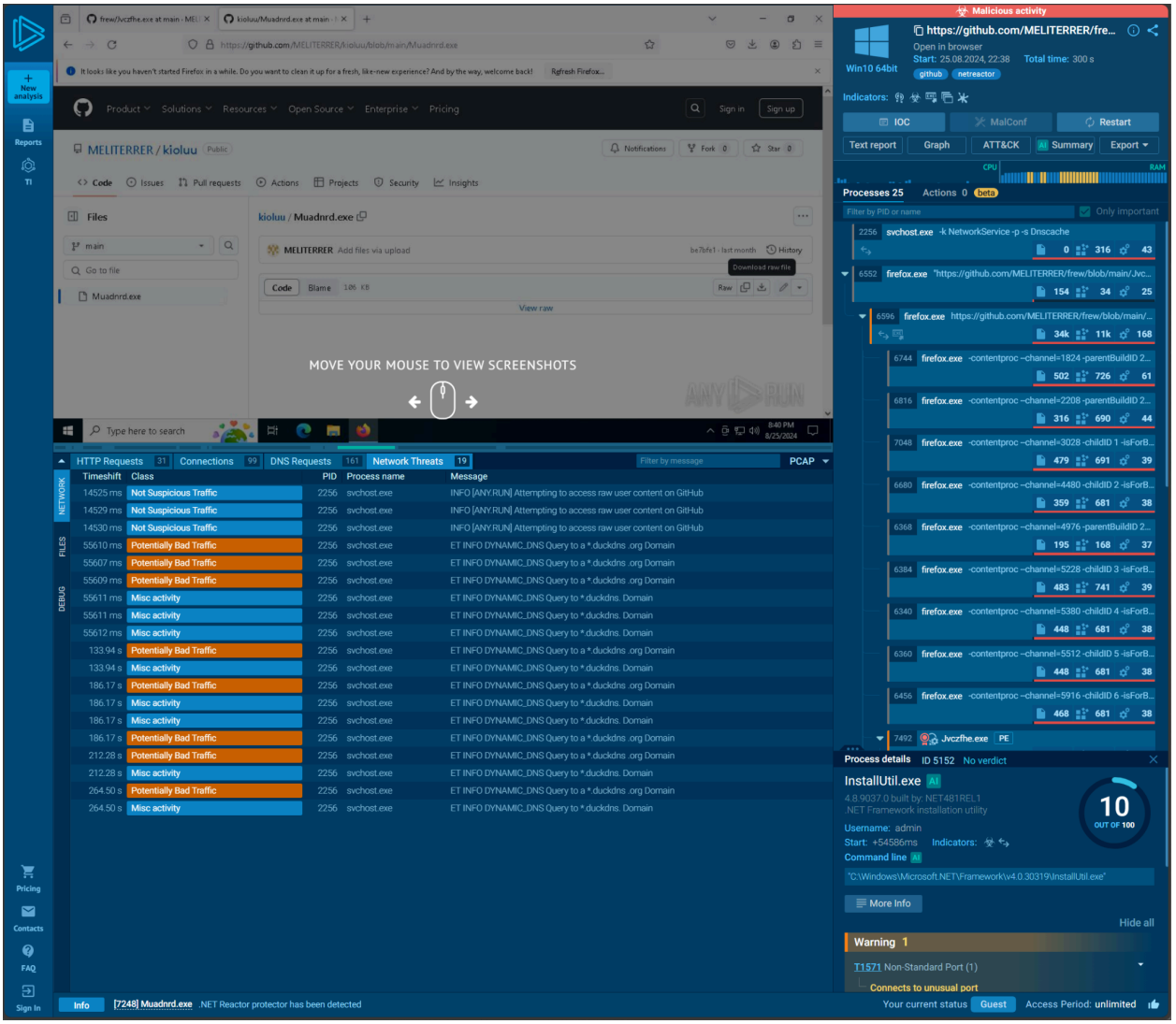
I file sono stati eliminati dalla memoria

- **Ricerca comandi che potresti usare per semplificare i tuoi compiti come analista di sicurezza. Registra le tue scoperte.**
- Get-Process: Elenca tutti i processi in esecuzione. Può essere filtrato per risorse, utente o ora di avvio per rilevare processi anomali o nascosti.
- Get-NetTCPConnection: L'equivalente nativo di PowerShell di netstat -ano. Mostra tutte le connessioni TCP attive (inclusi gli stati LISTENING, ESTABLISHED) e le correla direttamente al PID (Process ID).
- Get-EventLog (o Get-WinEvent): Permette di filtrare e cercare eventi specifici nei registri di Windows (Sicurezza, Sistema, Applicazione). Essenziale per trovare tentativi di accesso falliti (Event ID 4625), modifiche ai criteri o installazioni di software sospetto.
- Get-Service: Elenca tutti i servizi Windows. Può essere usato per identificare servizi non necessari o servizi auto-avviati da percorsi non standard (un vettore comune per la persistenza del malware).
- Get-ItemProperty: Utilizzato per leggere le chiavi e i valori nel Registro di sistema (HKLM:, HKCU:), cercando meccanismi di persistenza come le chiavi Run o le associazioni di estensioni file modificate.
- Get-NetFirewallRule: Elenca tutte le regole del Firewall di Windows. Essenziale per identificare eccezioni che potrebbero permettere a un malware di comunicare o a un utente malintenzionato di accedere a servizi inaspettati.
- Get-Acl: Ottiene le liste di controllo accessi (ACL) per file o directory. Utile per verificare se le autorizzazioni di un file critico sono state indebolite.
- Stop-Process -Id [PID]: Termina immediatamente un processo sospetto, isolando la minaccia. Si usa il PID ottenuto da Get-NetTCPConnection o Get-Process.
- Measure-Object -HashAlgorithm SHA256: Calcola l'hash crittografico (es. SHA256) di un file sospetto. L'hash può essere confrontato con database di Threat Intelligence online (es. VirusTotal) per confermare se si tratta di un malware noto.

Esercizio 2: Studio Ioc

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

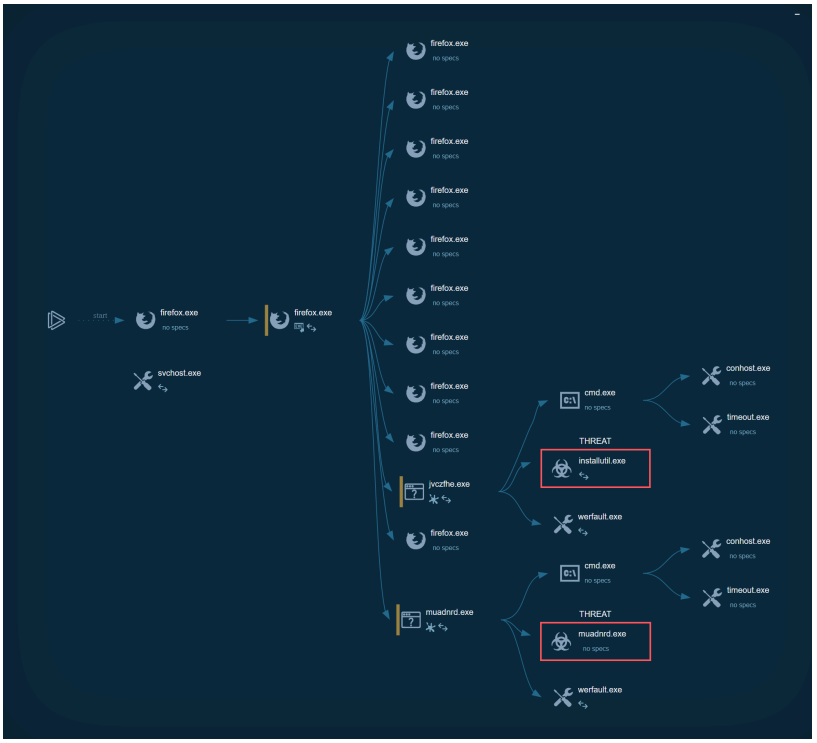
Cliccando sul link presente sulle slide la pagina che ci si apre è la seguente:



In alto c'è una carrellata di foto di un pc che ha eseguito due download di due file eseguibili da una pagina di Github, **Jvczfhe.exe** e **Muadnrd.exe** che risultano come file danneggiati e irreparabili. Nel menù in basso a destra ci sono un insieme di informazioni sulla rete, come le richieste HTTP, le connessioni, le richieste DNS, e le potenziali minacce Network segnalate da Suricata.

Nel Menù a destra invece c'è una lista di processi che si sono attivati e cliccando sulle schede viene già data una prima distinzione tra processi sospetti o meno.

In alto a destra poi è possibile ricavare ulteriori informazioni per analizzare il malware, quale è stato il suo percorso e che metodi ha utilizzato per l'exploit cliccando su **graph**.



Dal grafico è possibile vedere i processi e i passaggi del malware, e cliccando sui singoli indici poi le tecniche e i comportamenti messi in atto una volta che sono stati scaricati gli eseguibili.
Dalla schermata iniziale invece, cliccando su **ATT&CK** è possibile leggere le tattiche e tecniche eseguite dal malware proposte dal Mitre.

Command and Scripting Interpreter: Tramite la Windows Command Shell il malware esegue comandi di sistema. Nella descrizione si specifica che “Gli avversari possono anche eseguire comandi tramite terminali/shell interattivi, nonché utilizzare vari servizi remoti per ottenere l'esecuzione remota.”
Defense evasion - Masquerading: il malware rinomina o utilizza binari legittimi per confondersi. Lo stesso Mitre definisce questa tecnica come “Gli avversari possono rinominare le utility legittime/di sistema per cercare di eludere i meccanismi di sicurezza relativi all'utilizzo di tali utility.”
Mentre per quanto riguarda l’impair defenses: vengono disabilitati i windows event logging per limitare i dati che possono essere utilizzati per rilevamenti e controlli.
Nella sezione Discovery - Query Registry il Mitre spiega come il malware cerchi di interagire con Windows Registry per raccogliere informazioni su configurazioni di sistema (installazioni software il sistema, le configurazioni) e più nello specifico nel System

Information Discovery si raccolgono info più specifiche come versione OS, architettura, utenti, hotfixes.
C&C - Non-Standard Port suggerisce invece una comunicazione verso server di comando e controllo usando porte non convenzionali.

Dall'insieme di tutte le informazioni raccolte possiamo ipotizzare che il malware quindi si nasconde dietro un download di un file (quindi è nella categoria dei trojan), esegue esfiltrazioni dati dal pc e tramite una comunicazione su una porta non standard, contatta un server esterno.

Esercizio bonus 1: Esplorazione di Nmap

- Cos'è Nmap? Per cosa viene usato nmap?

Nmap è primariamente uno strumento di ricognizione (reconnaissance) e discovery. Utilizza pacchetti IP grezzi (raw IP packets) in modi non convenzionali per determinare: Quali host sono disponibili sulla rete, quali servizi (nome dell'applicazione e versione) stanno offrendo quegli host, quale sistema operativo (OS) è in esecuzione (compresa la versione) sul target.

- Guarda l'Esempio 1. Qual è il comando nmap usato? Usa la funzione di ricerca per rispondere alle seguenti domande. Cosa fa l'opzione -A? Cosa fa l'opzione -T4?

Nell'esempio viene eseguito uno scan sul sito scanme.nmap.org. Le opzioni che sono state richieste per lo scan permettendo di eseguire uno scan di tutte le porte in maniera estremamente veloce (-T4) e di fare un'analisi completa dei protocolli, i servizi e le loro relative versioni attive(-A).

- Scansiona il tuo localhost. Quali porte e servizi sono aperti?

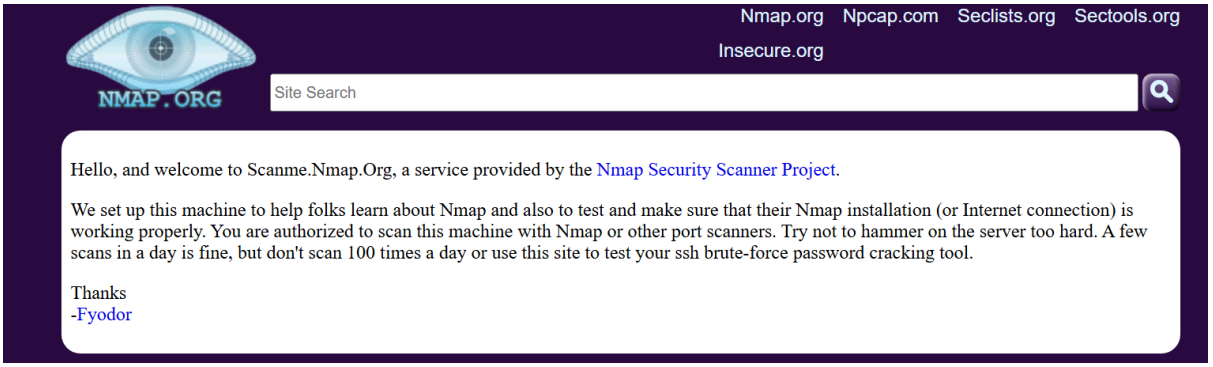
Dallo scan è possibile vedere aperte le porte 21 e 22 con i servizi attivi FTP e SSH

- A quale rete appartiene la tua VM? Quanti host sono attivi? Dai risultati di Nmap, elenca gli indirizzi IP degli host che si trovano sulla stessa LAN della tua VM.

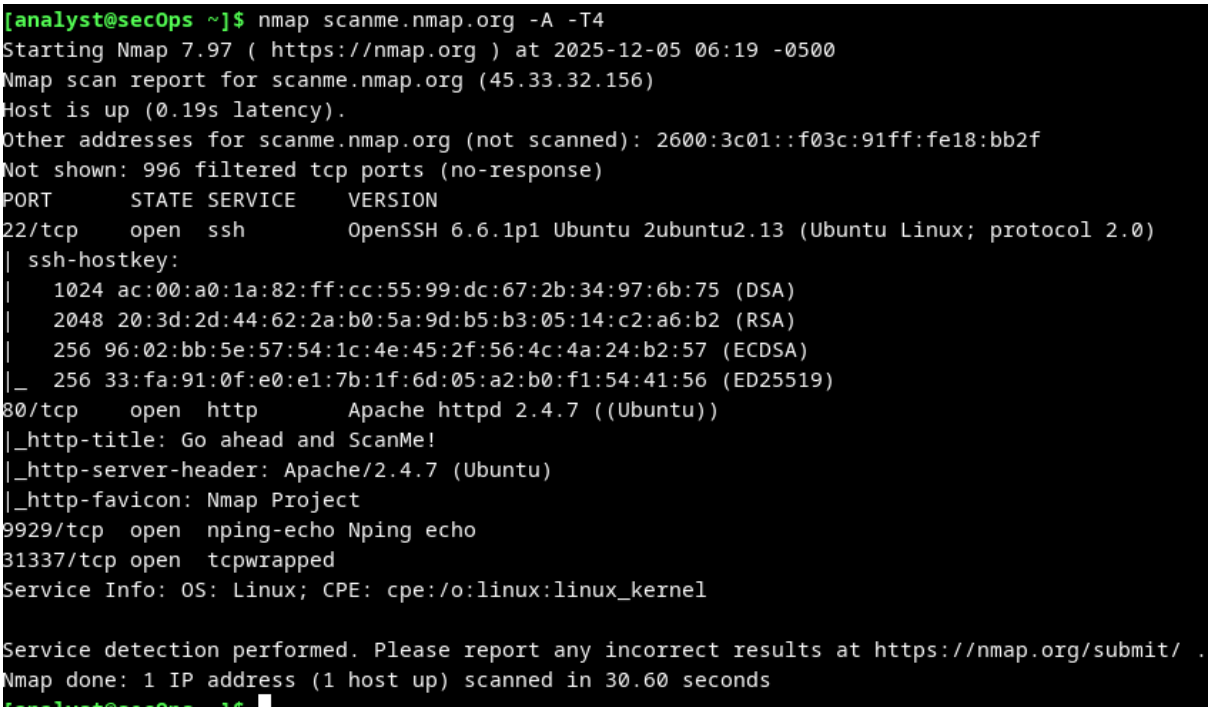
La VM è connessa tramite Rete con NAT, quindi ho acceso una seconda VM per avere una seconda macchina visibile sulla stessa rete della Cyberops. L'unica altro host attivo risultante infatti è il 192.168.50.3 (in questo caso la Kali)

```
[analyst@secOps ~]$ nmap -A -T4 192.168.50.0/24
Starting Nmap 7.97 ( https://nmap.org ) at 2025-12-05 06:08 -0500
Nmap scan report for 192.168.50.2
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.50.2 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.50.3
Host is up (0.0015s latency).
All 1000 scanned ports on 192.168.50.3 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.50.14
Host is up (0.0011s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.50.14
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0               0 Mar 26  2018 ftp_test
22/tcp open  ssh     OpenSSH 10.0 (protocol 2.0)
Service Info: Host: Welcome
```

- Scansiona un server remoto. a. Apri un browser web e naviga su scanme.nmap.org. Leggi il messaggio pubblicato. Quali porte e servizi sono aperti? Quali porte e servizi sono filtrati? Qual è l'indirizzo IP del server? Qual è il sistema operativo?



Questa è la pagina del sito



Questo invece è lo scan con le porte aperte 22, 80, 9929, 31337. L'indirizzo ip è 45.33.32.156 è il sistema operativo del server è un LINUX.

Esercizio bonus 2: Attacco SQL injection

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

Gli indirizzi IP coinvolti sono 10.0.2.4 e 10.0.2.15

- Qual è la versione ?

5.7.12- ubuntu 1.1

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

riceverebbe in output il nome delle colonne dalla table "Users"

- Quale utente ha l'hash della password di 8d3533d75ae2c3966d7e0d4fcc69216b? c. Usando un sito web come https://crackstation.net/, copia l'hash della password nel cracker di hash di password e inizia a decifrare. Qual è la password in chiaro?

L'hash appartiene all'user "**1337**", come tipologia è un md5 e la password in chiaro risulta essere "**charley**"