

Sommario

1. Esercizio 1 – Utilizzo di Windows PowerShell	3
1.1 Obiettivo	3
1.2 Esplorare i comandi del Prompt dei Comandi e di PowerShell	3
1.2.1 Accedere alla console PowerShell e al command prompt	3
1.2.2 Quali sono gli output del comando dir?	3
1.2.3 Quali sono i risultati provando altri comandi (ping, cd, ipconfig)?	3
1.3 Esplorare i cmdlet	4
1.3.1 Qual è il comando PowerShell per dir?	4
1.4 Esplorare il comando netstat usando PowerShell	5
1.4.1 Qual è il gateway IPv4?	5
1.4.2 Quali informazioni puoi ottenere dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID selezionato?	6
1.5 Svuotare il cestino usando Powershell	7
1.5.1 Cosa è successo ai file nel Cestino?	7
1.6 Domanda di Riflessione	7
2. Esercizio 2 – Studio Ioc	8
2.1 Report Analisi Malware	9
2.1.1 Introduzione	9
2.1.2 Attività principale: rilascio di un secondo eseguibile	9
2.1.3 Tecniche di evasione	10
2.1.4 Abuso di strumenti legittimi (LOLBin)	11
2.1.5 Offuscamento tramite .NET Reactor	11
2.1.6 Comunicazione esterna e canale C2	11
2.1.7 Persistenza e cancellazione delle tracce	12
2.1.8 Attività di ricognizione	12
2.1.9 Conclusione	13
3. Esercizio 3 – Esplorazione di Nmap	14
3.1 Obiettivi	14
3.2 Esplorazione di Nmap	14
3.2.1 Cos'è Nmap?	14
3.2.2 A cosa serve Nmap?	14
3.2.3 Nell'esempio 1 del manuale, qual è il comando nmap usato?	15
3.2.4 Nell'esempio 1 del manuale, cosa fa l'opzione -A??	15

3.2.5 Nell'esempio 1 del manuale, cosa fa l'opzione -T4?.....	15
3.2.6 Quali porte e servizi sono aperti sul tuo localhost?	16
3.2.7 A quale rete appartiene la tua VM?	17
3.2.8 Quanti host sono attivi sulla rete 192.168.1.0/24?	17
3.2.9 Qual è lo scopo di questo sito, <i>scanme.nmap.org</i> ?.....	17
3.2.10 Quali porte e servizi sono aperti?	18
3.2.11 Quali porte e servizi sono filtrati?	18
3.2.12 Qual è l'indirizzo IP del server?	18
3.2.13 Qual è il sistema operativo?	18
3.2.14 Domanda di Riflessione	18
4. Esercizio 4 – Attacco a un database MySQL.....	19
4.1 Obiettivi	19
4.2 Apertura del file .pcap e domande.....	19
4.2.1 Quali sono i due indirizzi IP coinvolti in questo attacco di SQL injection in base alle informazioni visualizzate?	19
4.2.2 Riassunto del procedimento riportato fino alla domanda successiva.	19
4.2.3 Qual è la versione?	19
4.2.4 Riassunto del procedimento riportato fino alla domanda successiva.	20
4.2.5 Quale utente ha l'hash della password di 8d3533d75ae2c3966d7e0d4fcc69216b?	20
4.2.6 Qual è la password in chiaro?	20
4.2.7 Domande di Riflessione	20

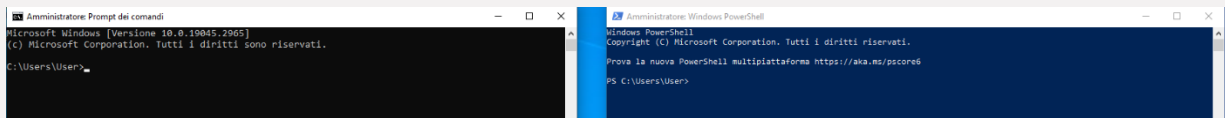
1. Esercizio 1 – Utilizzo di Windows PowerShell

1.1 Obiettivo

Esplorare alcune funzioni di Windows Powershell.

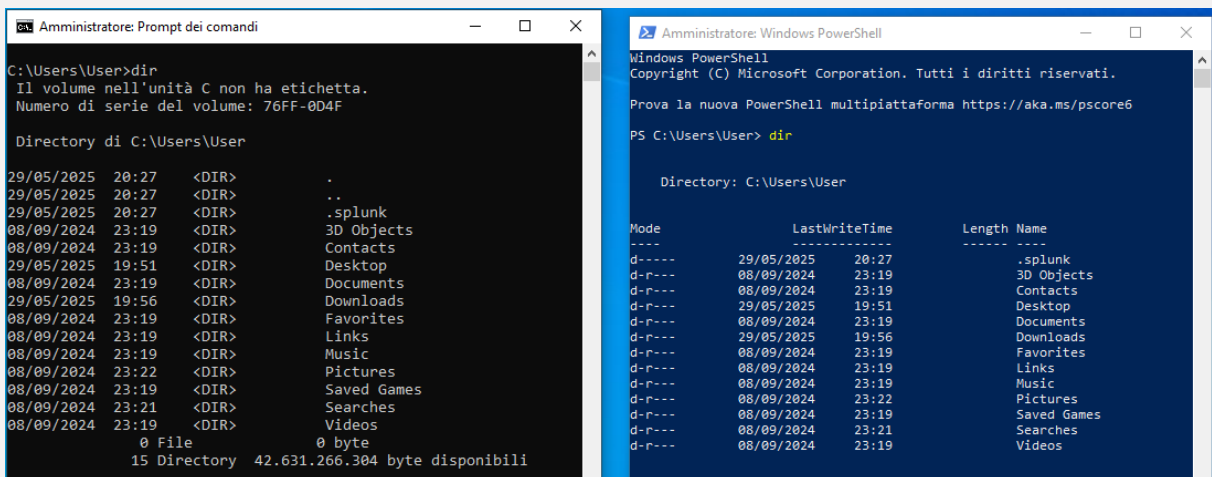
1.2 Esplorare i comandi del Prompt dei Comandi e di PowerShell.

1.2.1 Accedere alla console PowerShell e al command prompt



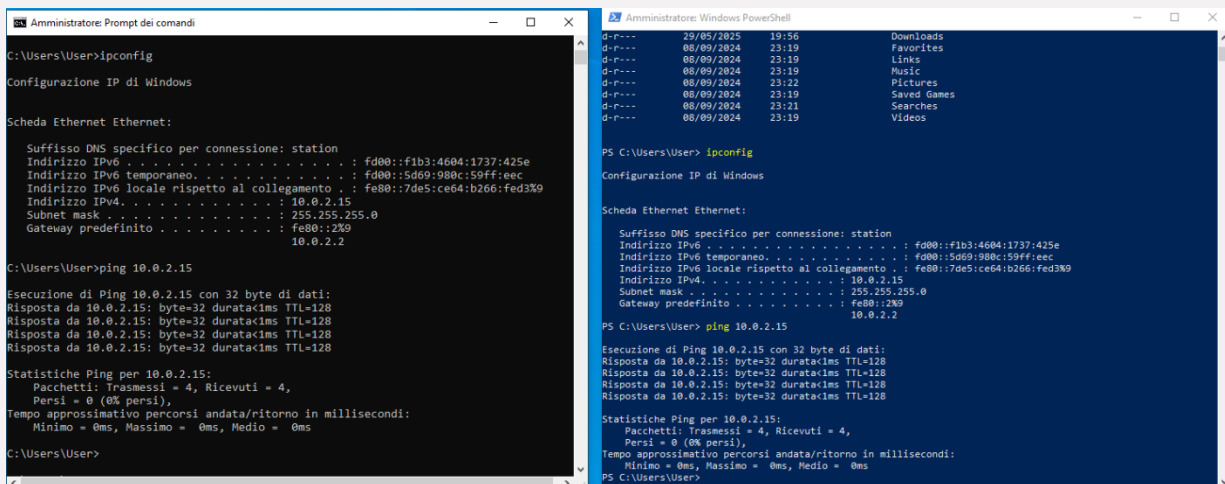
1.2.2 Quali sono gli output del comando dir?

Gli output sono i medesimi, sia su command prompt che su PowerShell.



1.2.3 Quali sono i risultati provando altri comandi (ping, cd, ipconfig)?

Come è possibile verificare nelle immagini riportate di seguito, i comandi eseguiti una volta con il command prompt e una volta con PowerShell restituiscono gli stessi output.



```
C:\Users\User>cd Desktop
C:\Users\User\Desktop>

PS C:\Users\User> cd Desktop
PS C:\Users\User\Desktop>
```

1.3 Esplorare i cmdlet

I cmdlet sono i comandi nativi di PowerShell, utilizzati per interagire con il sistema operativo e eseguire azioni specifiche. Sono, in sostanza, le "unità di base" dei comandi in PowerShell. I cmdlet seguono una convenzione di denominazione che inizia con un verbo (es. Get, Set, New, Stop) seguito da un sostantivo (es. Process, Service, File, Function). Questa convenzione aiuta a comprendere meglio l'azione che il comando compie.

1.3.1 Qual è il comando PowerShell per dir?

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

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

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

PS C:\Users\User> Get-Alias cd

CommandType      Name
-----
Alias             cd -> Set-Location
```

Altri *alias* utilizzabili in PowerShell.

```
PS C:\Users\User> Get-Command -CommandType Alias

CommandType      Name                                     Version      Source
-----
Alias             % -> ForEach-Object
Alias             ? -> Where-Object
Alias             ac -> Add-Content
Alias             Add-AppPackage                          2.0.1.0      Appx
Alias             Add-AppPackageVolume                   2.0.1.0      Appx
Alias             Add-AppProvisionedPackage              3.0          Dism
Alias             Add-ProvisionedAppPackage              3.0          Dism
Alias             Add-ProvisionedAppxPackage             3.0          Dism
Alias             Add-ProvisioningPackage                3.0          Provisioning
Alias             Add-TrustedProvisioningCertificate      3.0          Provisioning
Alias             algm ->
Alias             Apply-WindowsUnattend                 1.0.0.0      Microsoft.PowerShell.LocalAccounts
Alias             asnp -> Add-PSSnapin                   3.0          Dism
Alias             blsmba ->                              2.0.0.0      SmbShare
Alias             cat -> Get-Content
Alias             cd -> Set-Location
Alias             CFS -> ConvertFrom-String              3.1.0.0      Microsoft.PowerShell.Utility
Alias             chdir -> Set-Location
Alias             clc -> Clear-Content
Alias             clear -> Clear-Host
```

1.4 Esplorare il comando netstat usando PowerShell

Il comando netstat in PowerShell è uno strumento da riga di comando utilizzato per visualizzare le informazioni relative alle connessioni di rete, le tabelle di routing, le interfacce di rete e le statistiche della rete. In sostanza, netstat permette di monitorare e analizzare l'attività di rete del sistema.

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

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

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

-a Visualizza tutte le connessioni e le porte di ascolto.
-b Visualizza l'eseguibile coinvolto nella creazione di ogni connessione o
  porta di ascolto. In alcuni casi, host di eseguibili noti
  più componenti indipendenti e in questi casi il
  sequenza di componenti coinvolti nella creazione della connessione
  o la porta in ascolto. In questo caso, l'eseguibile
  il nome è in [] nella parte inferiore, in alto è il componente che ha chiamato,
  e così via fino al raggiungimento di TCP/IP. Si noti che questa opzione
  può richiedere molto tempo e avrà esito negativo, a meno che non siano sufficienti
  autorizzazioni.
-e visualizza le statistiche Ethernet. È possibile combinare
  opzioni.
-f Visualizza nomi di dominio completi (FQDN) per stranieri
  indirizzi.
-n Visualizza indirizzi e numeri di porta in formato numerico.
-o Visualizza l'ID del processo proprietario associato a ogni connessione.
-p proto Mostra le connessioni per il protocollo specificato da proto; proto
  può essere qualsiasi: TCP, UDP, TCPv6 o UDPv6. Se usato con -s
  opzione per la visualizzazione delle statistiche per protocollo, Proto può essere qualsiasi:
  IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
-q Visualizza tutte le connessioni, le porte di ascolto e i binding
  non in ascolto di porte TCP. Le porte di nonlistening associate possono o meno essere
  essere associato a una connessione attiva.
-r Visualizza la tabella di routing.
-s Visualizza le statistiche per protocollo. Per impostazione predefinita, le statistiche vengono
  visualizzate per IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6;
  l'opzione -p può essere utilizzata per specificare un sottoinsieme del valore predefinito.
-t Visualizza lo stato corrente di offload della connessione.
-x Visualizza connessioni NetworkDirect, listener e condivisi
  endpoint.
-y Visualizza il modello di connessione TCP per tutte le connessioni.
  Non può essere combinato con le altre opzioni.
intervallo Rivisualizza le statistiche selezionate, la sospensione dell'intervallo di secondi
  tra ogni schermo. Premere CTRL+C per interrompere la rivisualizzazione
  Statistiche. Se viene omissa, netstat stamperà il
  informazioni di configurazione una volta.
```

Nota: Su Windows 11 il comando è `netstat /?`

1.4.1 Qual è il gateway IPv4?

Il gateway IPv4 è 192.168.1.1

```
PS C:\Users\User> netstat -n

=====
Elenco interfacce
  9...08 00 27 96 c2 10 .....Intel(R) PRO/1000 MT Desktop Adapter
  1.....Software Loopback Interface 1
=====

IPv4 Tabella route
=====
Route attive:
  Indirizzo rete      Mask      Gateway      Interfaccia  Metrica
  0.0.0.0             0.0.0.0   192.168.1.1  192.168.1.13  25
  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      192.168.1.13  281
  192.168.1.13        255.255.255.255 On-link      192.168.1.13  281
  192.168.1.255       255.255.255.255 On-link      192.168.1.13  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      192.168.1.13  281
  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      192.168.1.13  281
=====
Route permanenti:
  Nessuna

IPv6 Tabella route
=====
Route attive:
  Interf Metrica Rete Destinazione Gateway
  1 331 ::1/128 On-link
  9 281 fe80::/64 On-link
  9 281 fe80::7de5:ce64:b266:fed3/128 On-link
  1 331 ff00::/8 On-link
  9 281 ff00::/8 On-link
=====
Route permanenti:
  Nessuna
```

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

Possiamo ottenere informazioni relative a:

Nome processo: svchost.exe;

Stato: In esecuzione;

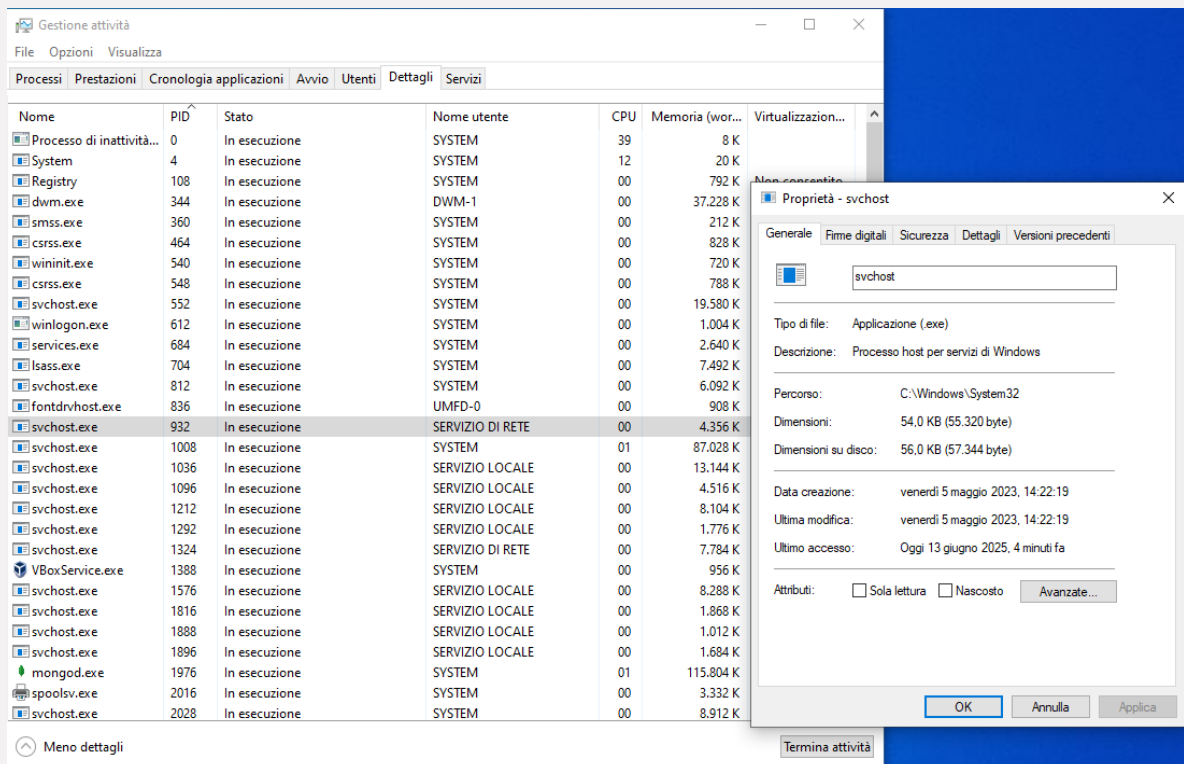
Nome utente (Servizio): SERVIZIO DI RETE

Memoria utilizzata: 4.356 K.

```
PS C:\Users\User> netstat -abno

Connessioni attive

Proto Indirizzo locale      Indirizzo esterno    Stato      PID
TCP    0.0.0.0:135              0.0.0.0:0            LISTENING  932
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  1212
CDPSvc
[svchost.exe]
```



Nome	PID	Stato	Nome utente	CPU	Memoria (wor...)	Virtualizzazion...
Processo di inattività...	0	In esecuzione	SYSTEM	39	8 K	
System	4	In esecuzione	SYSTEM	12	20 K	
Registry	108	In esecuzione	SYSTEM	00	792 K	
dwm.exe	344	In esecuzione	DWM-1	00	37.228 K	
smss.exe	360	In esecuzione	SYSTEM	00	212 K	
csrss.exe	464	In esecuzione	SYSTEM	00	828 K	
wininit.exe	540	In esecuzione	SYSTEM	00	720 K	
csrss.exe	548	In esecuzione	SYSTEM	00	788 K	
svchost.exe	552	In esecuzione	SYSTEM	00	19.580 K	
winlogon.exe	612	In esecuzione	SYSTEM	00	1.004 K	
services.exe	684	In esecuzione	SYSTEM	00	2.640 K	
lsass.exe	704	In esecuzione	SYSTEM	00	7.492 K	
svchost.exe	812	In esecuzione	SYSTEM	00	6.092 K	
fontdrvhost.exe	836	In esecuzione	UMFD-0	00	908 K	
svchost.exe	932	In esecuzione	SERVIZIO DI RETE	00	4.356 K	
svchost.exe	1008	In esecuzione	SYSTEM	01	87.028 K	
svchost.exe	1036	In esecuzione	SERVIZIO LOCALE	00	13.144 K	
svchost.exe	1096	In esecuzione	SERVIZIO LOCALE	00	4.516 K	
svchost.exe	1212	In esecuzione	SERVIZIO LOCALE	00	8.104 K	
svchost.exe	1292	In esecuzione	SERVIZIO LOCALE	00	1.776 K	
svchost.exe	1324	In esecuzione	SERVIZIO DI RETE	00	7.784 K	
VBoxService.exe	1388	In esecuzione	SYSTEM	00	956 K	
svchost.exe	1576	In esecuzione	SERVIZIO LOCALE	00	8.288 K	
svchost.exe	1816	In esecuzione	SERVIZIO LOCALE	00	1.868 K	
svchost.exe	1888	In esecuzione	SERVIZIO LOCALE	00	1.012 K	
svchost.exe	1896	In esecuzione	SERVIZIO LOCALE	00	1.684 K	
mongod.exe	1976	In esecuzione	SYSTEM	01	115.804 K	
spoolsv.exe	2016	In esecuzione	SYSTEM	00	3.332 K	
svchost.exe	2028	In esecuzione	SYSTEM	00	8.912 K	

Proprietà - svchost

Generale Fime digitali Sicurezza Dettagli Versioni precedenti

svchost

Tipo di file: Applicazione (.exe)

Descrizione: Processo host per servizi di Windows

Percorso: C:\Windows\System32

Dimensioni: 54,0 KB (55.320 byte)

Dimensioni su disco: 56,0 KB (57.344 byte)

Data creazione: venerdì 5 maggio 2023, 14:22:19

Ultima modifica: venerdì 5 maggio 2023, 14:22:19

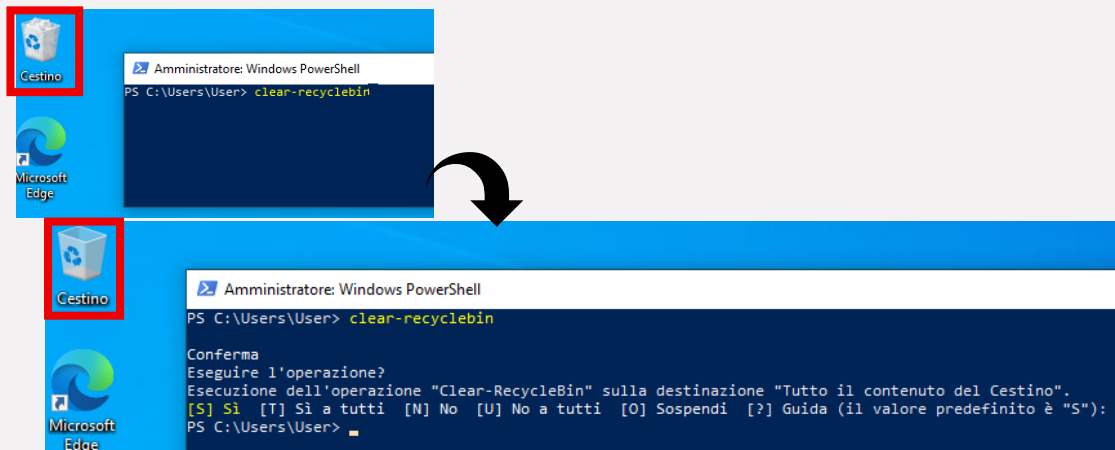
Ultimo accesso: Oggi 13 giugno 2025, 4 minuti fa

Attributi: ☐ Sola lettura ☐ Nascosto

1.5 Svuotare il cestino usando Powershell

1.5.1 Cosa è successo ai file nel Cestino?

Come è possibile notare dalle immagini sotto, usando il comando **clear-recyclebin** è stato svuotato il cestino.



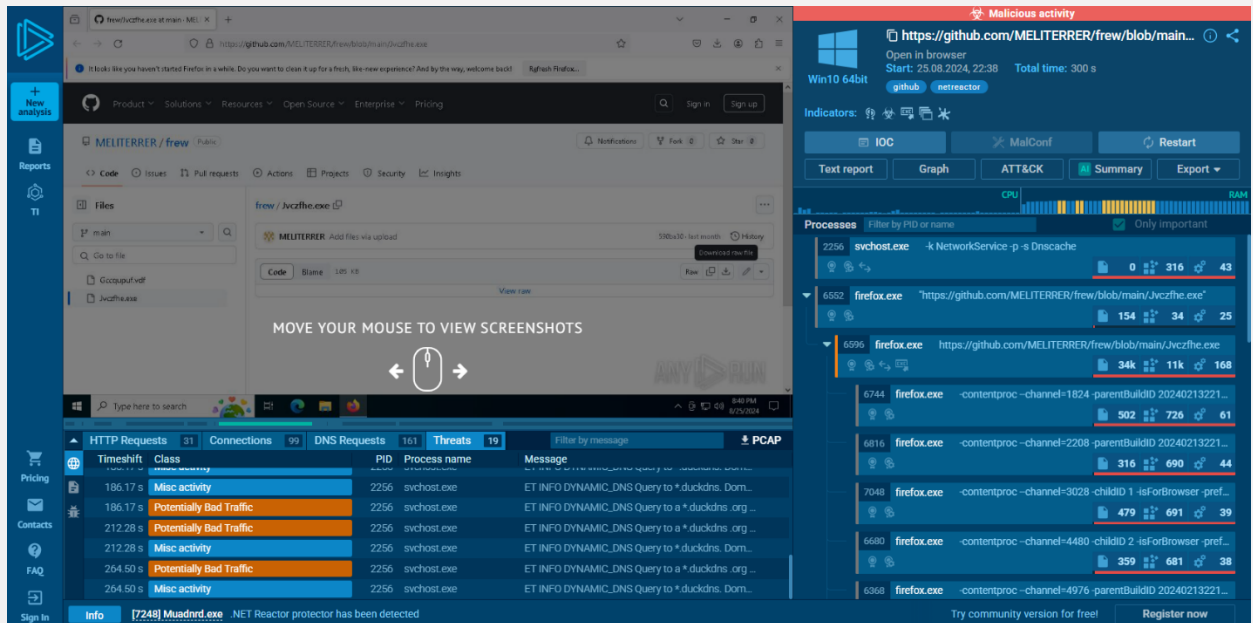
1.6 Domanda di Riflessione

PowerShell è stato sviluppato per l'automazione delle attività e la gestione della configurazione. Usando internet, ricerca comandi che potresti usare per semplificare i tuoi compiti come analista di sicurezza. Registra le tue scoperte.

Comando / Cmdlet	Utilizzo	Esempio
Get-EventLog / Get-WinEvent	Visualizza i log di sistema, sicurezza, applicazioni	Get-EventLog -LogName Security -Newest 50
Get-Process	Elenca i processi attivi	`Get-Process
Get-Service	Visualizza lo stato dei servizi	`Get-Service
Get-LocalUser	Elenca gli utenti locali del sistema	`Get-LocalUser
Get-LocalGroupMember	Verifica i membri di un gruppo (es. Amministratori)	Get-LocalGroupMember -Group "Administrators"
Get-Content	Legge file di testo o log (utile per cercare IOCs)	`Get-Content C:\Logs\eventi.txt
Set-ExecutionPolicy	Modifica la policy di esecuzione degli script	Set-ExecutionPolicy RemoteSigned -Scope CurrentUser
Invoke-Command	Esegue comandi su un computer remoto	Invoke-Command -ComputerName PC1 -ScriptBlock { Get-Process }
Start-Transcript	Registra tutto ciò che avviene nella sessione	Start-Transcript -Path "C:\LogAudit\sessione.txt"

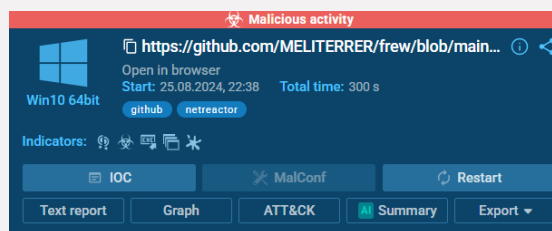
2. Esercizio 2 – Studio Ioc

Il secondo esercizio richiede di studiare un link di anyrun e discutere le minacce. Accedendo al link si ottiene la seguente schermata:

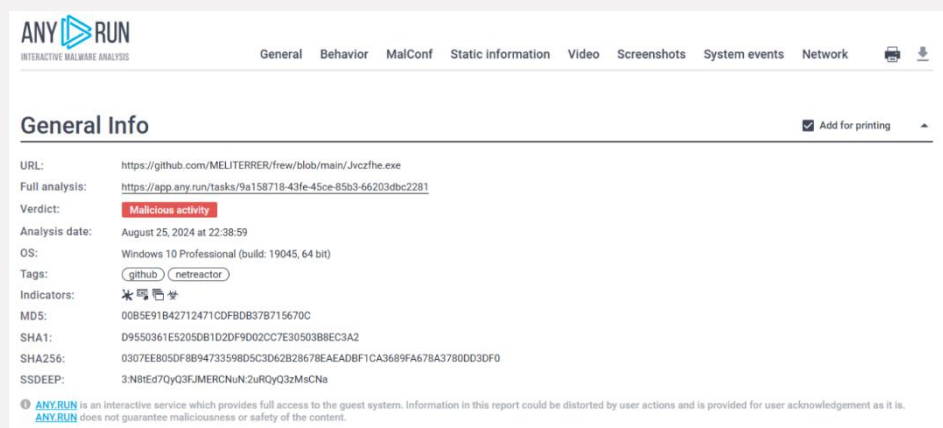


Si può notare, dalle immagini in successione che l'utente cerca di scaricare da un repository GitHub degli eseguibili ma gli viene restituito un messaggio di errore.

È possibile ottenere un report cliccando su **Text report**.



Il report consente di avere delle informazioni meno frammentare e più strutturate. Di seguito viene riportata un'analisi delle evidenze individuate e un'ipotesi sul funzionamento del malware.



- La sezione **Behavior Activities** riporta esplicitamente la voce:
Executable content was dropped or overwritten, suggerendo che il file principale ha sganciato contenuti eseguibili.

Executable content was dropped or overwritten
• firefox.exe (PID: 6596)

Entrambi i file presentano come descrizione interna **Microsoft Edge**, un chiaro **tentativo di 'impersonificazione'** volto a rendere i processi meno sospetti.

Questi elementi suggeriscono con buona probabilità che Jvczfhe.exe sia un **dropper**, la cui funzione è installare o eseguire componenti aggiuntivi – in questo caso **Muadnrd.exe**.

2.1.3 Tecniche di evasione

Diversi processi avviati da Jvczfhe.exe e Muadnrd.exe eseguono il comando: **cmd /c timeout 21**.
Rilevato nei processi PID 7520, 7572, 7876, 7968.

7520	"cmd" /c timeout 21 & exit	C:\Windows\SysWOW64\cmd.exe	—	Jvczfhe.exe
Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	Windows Command Processor	
Exit code:	0	Version:	10.0.19041.3636 (WinBuild.160101.0800)	

7572	timeout 21	C:\Windows\SysWOW64\timeout.exe	—	cmd.exe
Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	timeout - pauses command processing	
Exit code:	0	Version:	10.0.19041.1 (WinBuild.160101.0800)	

7876	"cmd" /c timeout 21 & exit	C:\Windows\SysWOW64\cmd.exe	—	Muadnrd.exe
Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	Windows Command Processor	
Exit code:	0	Version:	10.0.19041.3636 (WinBuild.160101.0800)	

7968	timeout 21	C:\Windows\SysWOW64\timeout.exe	—	cmd.exe
Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	timeout - pauses command processing	
Exit code:	0	Version:	10.0.19041.1 (WinBuild.160101.0800)	

Questa tecnica è comunemente usata per **ritardare l'esecuzione del malware e eludere i limiti temporali delle sandbox**, che spesso analizzano i processi solo per brevi intervalli.

2.1.4 Abuso di strumenti legittimi (LOLBin)

Jvczfhe.exe avvia anche il processo **InstallUtil.exe** (PID 5152), un tool legittimo del framework .NET.

- Questo comportamento è tipico delle tecniche **LOLBin (Living off the Land Binary)**, dove strumenti firmati Microsoft vengono utilizzati per eseguire codice malevolo, riducendo la **probabilità di rilevamento** da parte degli antivirus.

5152	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe"	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe	Jvczfhe.exe
Information			
User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	.NET Framework installation utility
Version:	4.8.9037.0 built by: NET481REL1		

2.1.5 Offuscamento tramite .NET Reactor

Nella sezione Behavior Activities è riportata l'identificazione del protector:

.NET Reactor protector has been detected

- .NET Reactor protector has been detected
- InstallUtil.exe (PID: 5152)
- Muadnrd.exe (PID: 7248)

.NET Reactor è un tool commerciale utilizzato per offuscare applicazioni .NET, rendendo difficile la decompilazione e l'analisi del codice. La sua presenza conferma l'intento di proteggere il payload da reverse engineering.

2.1.6 Comunicazione esterna e canale C2

Uno dei comportamenti più critici rilevati è l'instaurazione di una comunicazione con un **server esterno di comando e controllo (C2)**.

- Il processo InstallUtil.exe effettua una connessione verso il dominio:

egehgdhejbhjt.re.duckdns.org

che risolve nell'IP pubblico: **91.92.253.47**, sulla porta **7702** (Sezione Connections).

5152	InstallUtil.exe	91.92.253.47:7702	egehgdhejbhjt.re.duckdns.org
------	-----------------	-------------------	------------------------------

Il dominio utilizza **DuckDNS**, un servizio **DNS dinamico gratuito**, spesso impiegato per mantenere l'**infrastruttura C2** (Command and Control - C2 o C&C) **elusiva e temporanea** ovvero l'insieme di server e servizi usati dagli attaccanti per comunicare con i dispositivi infetti.

L'uso della porta non standard **7702** può servire a bypassare i firewall o i sistemi di rilevamento basati su porte.

Il traffico viene classificato da ANY.RUN come: **Potentially Bad Traffic**

2.1.7 Persistenza e cancellazione delle tracce

Sono stati osservati tentativi di manipolare il registro di sistema, in particolare: **HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing** dove vengono scritte chiavi come:

- EnableFileTracing
- EnableConsoleTracing
- MaxFileSize

Queste modifiche sono compatibili con un tentativo di disabilitare il tracciamento di Windows, riducendo l'evidenza delle operazioni svolte.

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation:	write	Name:	EnableFileTracing
Value:	0		

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation:	write	Name:	EnableConsoleTracing
Value:	0		

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation:	write	Name:	MaxFileSize
Value:	1048576		

Inoltre, WerFault.exe (PID 1356 e 7584) – il componente di Windows per la gestione degli errori – potrebbe essere utilizzata per simulare crash e eludere strumenti forensi che operano in memoria.

(PID) Process:	(1356) WerFault.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Property
Operation:	write	Name:	00180010F429971D
Value:	0100000001000000D08C9DDF0115D1118C7A00C04FC297EB0100000042CB6C300049C042863C8A748EF9A2B20000000020000000001066000000010000200000000CCC6B875C440CBAEA58C5BED8611E39AA9829013E4B8AC51D0D9F7163EADF00000000000E800000000200002000000000BE26AF426085AF609742DB1A14612244C8BCC3E0EDE09C59A27330B31E6E2E9800000003BE1583AE43F56559EF36DEAFC074326B67E4667C7B38DFDF2D00FEFB0DAFFB6ED08C7C33F7A635133822E53A45D88F87E2E838C0E75D68C7ABE181C36822668FEEA0C6662B412EA28B9FBBAC304069F4755109ABD70078DB56B41A9E3D50ACDF8312B7407568A8EB09E45CD710B4CFB2B5804DE8C31792DF1D88EDD9A04FA40000000BFEEA620CE76ADB5C5AB194CB9B71310F2C4899DC791B2152EE28D52ABE9B061C9591BBB2EE89C5DC5ED9BD34A1D5EE58C76A4B2B4A909FE6CD0AA7A113C97B		

(PID) Process:	(1356) WerFault.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Token\{67082621-8D18-4333-9C64-10DE93676363}
Operation:	write	Name:	DeviceTicket
Value:	0100000001000000D08C9DDF0115D1118C7A00C04FC297EB0100000042CB6C300049C042863C8A748EF9A2B200000000200000000010660000000100002000000001DA1D6B12A5EC90F4F9706980DE59F73C4560375D4FCB70C2320F70F2BC4C6C6000000000E800000000200002000000007FB8CEDD17CB5141B2B0ADB40F9A7502AA36C37603876555ECDAA09F3C20551CD200800044D2B2E46D6008C27AF67936328535D6B0B492601DE7F4CB111286C54A126EB6E2E501C833930775A205AB65F6AEDA8ED2D78FA5A121722DEB8668C3EDCCE49C7D5AE173D74D788		

7584	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Muadnrd.exe_dd9d47dfcaa2177d1190b55ee6f3574cf671f90_4600b98d_c0351b42-4a4c-4b9d-bdbe-a700399d2592\Report.wer	MD5: —	SHA256: —
7584	WerFault.exe	C:\Users\admin\AppData\Local\CrashDumps\Muadnrd.exe.7824.dmp	MD5: —	SHA256: —

2.1.8 Attività di ricognizione

Il malware effettua anche operazioni mirate alla raccolta di informazioni sull'ambiente:

- Lettura della GUID del sistema
- Accesso a chiavi di registro relative a Microsoft Office
- Raccolta dati su:
 - configurazione proxy
 - impostazioni lingua
 - ambiente di sistema



Queste azioni sono coerenti con una fase di ricognizione, probabilmente volta a profilare il sistema bersaglio e selezionare azioni successive in base al contesto.

Reads the machine GUID from the registry

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

Reads the software policy settings

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

Reads Environment values

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

2.1.9 Conclusione

Il file Jvczfhe.exe si configura come un **dropper trojan multistadio avanzato**, dotato di:

- capacità di evasione temporale (timeout)
- utilizzo di LOLBin (InstallUtil.exe)
- offuscamento tramite .NET Reactor
- connessioni C2 verso dominio dinamico
- tecniche di antiforensics e disabilitazione logging

La sua finalità principale è il rilascio di un secondo eseguibile (Muadnrd.exe), in un contesto di compromissione modulare. Tutti gli elementi osservati indicano un malware progettato con attenzione per passare inosservato, persistere nel sistema e comunicare con un'infrastruttura remota controllata da attori malevoli.

3 Esercizio 3 – Esplorazione di Nmap

3.1 Obiettivi

- Esplorazione di Nmap
- Scansione delle Porte Aperte

3.2 Esplorazione di Nmap

L' esercizio richiede di lanciare diversi comandi relativi al tool *nmap* sulla macchina *CyberOps Workstation* e rispondere ad alcune domande.

3.2.1 Cos'è Nmap?

Inviando nel **prompt dei comandi** il comando **man nmap** possiamo ottenere la risposta.

Nmap (Network Mapper) è uno **strumento open source** per l'esplorazione della rete e il controllo della sicurezza.

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

NAME
    nmap - Network exploration tool and security / port scanner

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

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

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

3.2.2 A cosa serve Nmap?

Secondo il manuale (man nmap), Nmap può essere utilizzato per:

- Scoprire host attivi su una rete (host discovery)
- Eseguire port scanning per identificare porte aperte, chiuse o filtrate
- Identificare i servizi (nome, versione) in esecuzione su quelle porte
- Determinare il sistema operativo e le sue caratteristiche (OS detection)
- Rilevare firewall, router o altri dispositivi di filtraggio pacchetti
- Effettuare audit di sicurezza e penetration test su reti e host
- Creare inventari di rete automatici

3.2.3 Nell'esempio 1 del manuale, qual è il comando nmap usato?

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

```
Example 1. A representative Nmap scan
# nmap -A -T4 scanme.nmap.org
```

3.2.4 Nell'esempio 1 del manuale, cosa fa l'opzione -A??

Il flag `-A` in `nmap` abilita una scansione avanzata, e secondo quanto mostrato nell'immagine (man nmap), esegue automaticamente:

In dettaglio:

- **OS detection**
Cerca di identificare il sistema operativo dell'host (es. Windows, Linux, ecc.).
- **Version detection**
Rileva le versioni precise dei servizi in esecuzione su porte aperte (es: Apache 2.4.41).
- **Script scanning (NSE)**
Lancia script di sicurezza predefiniti dell'Nmap Scripting Engine per cercare vulnerabilità note, backdoor, malware, ecc.
- **Traceroute**
Ricostruisce il percorso di rete tra il tuo host e quello di destinazione.

```
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
```

3.2.5 Nell'esempio 1 del manuale, cosa fa l'opzione -T4?

Il flag `-T4` in `nmap` imposta un *timing template* (modello di temporizzazione) per la scansione.

`-T4` è un profilo di scansione veloce, ottimizzato per reti affidabili e stabili (Aggressive). Viene spesso usato in ambienti LAN o test locali, dove:

- La latenza è bassa
- I pacchetti non si perdono
- La scansione può essere aggressiva senza falsi positivi

```
TIMING AND PERFORMANCE:
Options which take <time> are in seconds, or append 'ms' (milliseconds),
's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
-T<0-5>: Set timing template (higher is faster)
--min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
--min-parallelism/max-parallelism <numprobes>: Probe parallelization
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
probe round trip time.
--max-retries <tries>: Caps number of port scan probe retransmissions.
--host-timeout <time>: Give up on target after this long
--scan-delay/--max-scan-delay <time>: Adjust delay between probes
--min-rate <number>: Send packets no slower than <number> per second
--max-rate <number>: Send packets no faster than <number> per second
```


È possibile sostituire il valore 4 con valori da 0 a 5 in relazione ai diversi casi.

Valore	Nome	Descrizione
-T0	Paranoid	Estremamente lento, evita rilevamento (per IDS evasion)
-T1	Sneaky	Molto lento, evasivo
-T2	Polite	Rallenta per ridurre il carico sulla rete
-T3	Normal	Impostazione di default
-T4	Aggressive	Più veloce, ma meno stealth
-T5	Insane	Estremamente veloce, rischia perdita dati o falsi positivi

3.2.6 Quali porte e servizi sono aperti sul tuo localhost?

Porta 21/tcp

- **Servizio:** FTP (File Transfer Protocol)
- **Software identificato:** vsftpd 3.0.3 (secure, fast, stable)

Porta 22/tcp

- **Servizio:** SSH (Secure Shell)
- **Software identificato:** OpenSSH 7.7 (protocollo 2.0)

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 07:07 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000043s 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 12.55 seconds
```

3.2.7 A quale rete appartiene la tua VM?

La VM appartiene alla rete 192.168.1.0/24.

```
[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:fa:c7:18 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.14/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 83681sec preferred_lft 83681sec
    inet6 fe80::a00:27ff:fefa:c718/64 scope link
        valid_lft forever preferred_lft forever
```

3.2.8 Quanti host sono attivi sulla rete 192.168.1.0/24?

Host attivi sulla LAN:

1. 192.168.1.1
2. 192.168.1.14
3. 192.168.1.16
4. 192.168.1.17
5. 192.168.1.18

Servizi disponibili sui vari host:

192.168.1.1 (router/gateway):

- HTTPS (porta 443)

192.168.1.14 (CyberOps Workstation):

- SSH (porta 22)

192.168.1.16:

- Porta 8009 – Apache JServ Protocol (AJP)

192.168.1.17:

- Porta 8008 – HTTP API

192.168.1.18:

- Porta 2049 – NFS (Network File System)

3.2.9 Qual è lo scopo di questo sito, *scanme.nmap.org*?

Il sito è stato creato come ambiente di test per l'apprendimento e la verifica dell'uso di Nmap, permettendo agli utenti di eseguire alcune scansioni moderate in modo lecito, senza abusarne o usarlo per attacchi reali.

3.2.10 Quali porte e servizi sono aperti?

Per rispondere a queste domande eseguiamo il comando `nmap -A -T4 scanme.nmap.org`.

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 07:54 EDT
Nmap scan report for scanme.nmap.org. (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org. (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: scanme.nmap.org
Not shown: 996 closed 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 18.12 seconds
```

Le seguenti porte risultano **aperte** (open):

- **22/tcp** – Servizio: ssh; Versione: OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13
- **80/tcp** – Servizio: http; Versione: Apache httpd 2.4.7 (Ubuntu)
- **9929/tcp** – Servizio: nping-echo; Versione: Nping echo
- **31337/tcp** – Servizio: tcpwrapped

3.2.11 Quali porte e servizi sono filtrati?

Nessuna porta filtrata è rilevata (Not shown: 996 closed ports)

Non ci sono porte **filtrate** indicate esplicitamente, ma solo **chiuse** (closed).

3.2.12 Qual è l'indirizzo IP del server?

45.33.32.156

3.2.13 Qual è il sistema operativo?

Ubuntu Linux

3.2.14 Domanda di Riflessione

Nmap è uno strumento potente per l'esplorazione e la gestione della rete. Come può Nmap aiutare con la sicurezza della rete? Come può Nmap essere usato da un attore malevolo come strumento nefasto?

Nmap è uno strumento molto utile per gli amministratori di sistema e gli analisti di sicurezza perché permette di effettuare la **ricognizione di rete** in modo dettagliato. Con una scansione Nmap posso identificare:

- quali host sono attivi su una rete,
- quali porte TCP/UDP sono aperte,
- quali servizi stanno girando e le loro versioni,
- e a volte anche il sistema operativo del dispositivo.

Tutte queste informazioni sono fondamentali per fare una **valutazione delle vulnerabilità**: ad esempio, sapere che un server espone una vecchia versione di SSH o Apache può aiutare a prevenire possibili exploit aggiornando o disattivando quel servizio.

Dal punto di vista offensivo, un attaccante può usare Nmap nello stesso modo per eseguire una **fase di ricognizione (footprinting e scanning)**. Prima di attaccare un sistema, è fondamentale sapere quali porte e servizi sono accessibili. Nmap permette quindi di costruire una vera e propria **mappa della rete target**, identificare punti deboli, e decidere dove concentrare l'attacco.

4 Esercizio 4 – Attacco a un database MySQL

4.1 Obiettivi

In questo laboratorio, visualizzerai un file PCAP di un attacco precedente contro un database SQL.

4.2 Apertura del file .pcap e domande

Apriamo il file .pcap fornito in Wireshark.

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

Gli indirizzi IP coinvolti sono:

- 10.0.2.4
- 10.0.2.15

No.	Time	Source	Destination
1	0.000000	10.0.2.4	10.0.2.15
2	0.000315	10.0.2.15	10.0.2.4
3	0.000349	10.0.2.4	10.0.2.15
4	0.000681	10.0.2.4	10.0.2.15
5	0.002149	10.0.2.15	10.0.2.4
6	0.005700	10.0.2.15	10.0.2.4
7	0.005700	10.0.2.4	10.0.2.15
8	0.014383	10.0.2.4	10.0.2.15

4.2.2 Riassunto del procedimento riportato fino alla domanda successiva.

- Si è analizzata la riga **13** della cattura in Wireshark, seguendo il **flusso HTTP** per una richiesta **GET** verso l'host **10.0.2.15**.
- L'attaccante ha inserito nel campo **UserID** la stringa **1' or 1=1**, una tipica **SQL Injection test**, per verificare se il campo è vulnerabile.
- L'applicazione ha risposto mostrando un record dal database, confermando la vulnerabilità.
- Si è esaminata la riga **19** con un'altra richiesta GET.
- L'attaccante ha usato la stringa **1' or 1=1 union select database(), user()#** per ottenere:
 - Il nome del database → dvwa
 - L'utente del database → root@localhost
- Questo mostra che l'attaccante può già eseguire query arbitrarie e leggere dati sensibili.
- Si è analizzata la riga **22** per vedere la continuazione dell'attacco.
- L'attaccante ha usato la stringa **1' or 1=1 union select null, version()#** per scoprire la versione del sistema.
- Nell'output restituito dal server, **la versione si trova alla fine della risposta**, subito prima del tag HTML di chiusura **</pre>**.

4.2.3 Qual è la versione?

La versione è **5.7.12-0ubuntu1.1**.

4.2.4 Riassunto del procedimento riportato fino alla domanda successiva.

- L'aggressore continua l'esplorazione del database analizzando la riga **25** in Wireshark.
- Tramite il flusso HTTP, si nota che l'attaccante ha inviato la query:

1' or 1=1 union select null, table_name from information_schema.tables#

- Questa query serve a elencare **tutti i nomi delle tabelle** presenti nel database, attingendo da **information_schema.tables**.
- Nell'output viene visualizzata una grande quantità di dati perché la richiesta non è filtrata.
- Una versione ottimizzata della query:

*1' or 1=1 union select null, column_name from information_schema.columns
where table_name='users'#*

permetterebbe di **recuperare solo i nomi delle colonne** dalla tabella users, restringendo così il campo di ricerca.

- L'attaccante passa alla fase finale analizzando la riga **28**, sempre tramite **Segui > Flusso HTTP**.
 - La query inviata è:
- 1' or 1=1 union select user, password from users#*
- Lo scopo è ottenere **nomi utente e password** direttamente dalla tabella users.
 - La risposta del server mostra diverse coppie utente/password.

4.2.5 Quale utente ha l'hash della password di 8d3533d75ae2c3966d7e0d4fcc69216b?

Il nome dell'utente è **1337**.

4.2.6 Qual è la password in chiaro?

La password in chiaro è **charley**.

Hash	Type	Result
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

4.2.7 Domande di Riflessione

Qual è il rischio che le piattaforme utilizzino il linguaggio SQL? Quali sono 2 metodi o passaggi che possono essere adottati per prevenire gli attacchi di SQL injection?

L'uso di SQL nei siti web è molto diffuso tuttavia, se un'applicazione non controlla adeguatamente i dati inseriti, può diventare vulnerabile agli **attacchi di SQL Injection**.

Con questo tipo di attacco, un aggressore può accedere a dati riservati (come nomi utente e password), modificare o cancellare informazioni o in casi più gravi, ottenere il controllo del server o eseguire comandi a livello di sistema. Il rischio principale è quindi che un'applicazione vulnerabile esponga **tutto il database** e quindi anche **i dati degli utenti** a potenziali abusi o furti.

Ci sono diverse tecniche per proteggersi dagli attacchi SQLi. Le due più fondamentali sono:

- **Controllo dell'input dell'utente**
È importante **filtrare e validare** ogni dato inserito dagli utenti, evitando caratteri sospetti come **'**, **--**, **;**, ecc. Questo riduce la possibilità che vengano eseguite istruzioni SQL indesiderate.
- **Uso di query parametrizzate**
Invece di creare le query unendo manualmente testo e input dell'utente, si usano **parametri predefiniti**, che separano i dati dal codice SQL. Questo approccio impedisce che l'input venga interpretato come parte della query.

Questi esempi mostrano quanto sia facile per un attaccante ottenere dati critici se il codice non è scritto in modo sicuro. Un'adeguata validazione degli input e l'uso di query sicure rappresentano la base per prevenire gravi falle nei sistemi basati su database.