

S11L5

UNIT 3

Marco Falchi

Esercizio 1

Quali sono gli output del comando dir?

Command Prompt

Microsoft Windows [Version 10.0.26100.6584]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Mimmo>dir
Volume in drive C has no label.
Volume Serial Number is 9834-1B2C

Directory of C:\Users\Mimmo

09/26/2025 01:13 AM <DIR> .
09/22/2025 06:08 AM <DIR> ..
09/22/2025 03:04 PM <DIR> Contacts
09/22/2025 03:04 PM <DIR> Desktop
09/22/2025 03:04 PM <DIR> Documents
09/22/2025 06:10 AM <DIR> Downloads
09/22/2025 03:04 PM <DIR> Favorites
09/22/2025 03:04 PM <DIR> Links
09/22/2025 03:04 PM <DIR> Music
09/22/2025 03:06 PM <DIR> OneDrive
09/22/2025 03:04 PM <DIR> Pictures
09/22/2025 03:04 PM <DIR> Saved Games
09/22/2025 06:08 AM <DIR> Searches
09/22/2025 06:36 AM <DIR> Videos
0 File(s) 0 bytes
14 Dir(s) 58,475,053,056 bytes fr

Windows PowerShell

Mode	LastWriteTime	Length	Name
d-r--	9/22/2025 3:04 PM		Contacts
d-r--	9/22/2025 3:04 PM		Desktop
d-r--	9/22/2025 3:04 PM		Documents
d-r--	9/22/2025 6:10 AM		Downloads
d-r--	9/22/2025 3:04 PM		Favorites
d-r--	9/22/2025 3:04 PM		Links
d-r--	9/22/2025 3:04 PM		Music
d-r--	9/22/2025 3:06 PM		OneDrive
d-r--	9/22/2025 3:04 PM		Saved Games
d-r--	9/22/2025 6:08 AM		Searches
d-r--	9/22/2025 6:36 AM		Videos

PS C:\Users\Mimmo>

Entrambe le schermate dopo il comando mostrano un elenco di directory e file, insieme ad altre informazioni come il LastWriteTime (ossia la data di ultima modifica), powershell in più ci mostra i permessi sotto la sezione Mode.

Quali sono i risultati?

```
Command Prompt
C:\Users\Mimmo>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : station
    IPv6 Address. . . . . : fd17:625c:f037:2:6711:83f1:325e:e8d
    Temporary IPv6 Address. . . . . : fd17:625c:f037:2:b1ea:214a:39b0:35f2
    Link-local IPv6 Address . . . . . : fe80::cd63:cb72:5b31:4ac2%14
    IPv4 Address. . . . . : 10.0.2.15
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::2%14
                                10.0.2.2

C:\Users\Mimmo>

Windows PowerShell
PS C:\Users\Mimmo> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : station
    IPv6 Address. . . . . : fd17:625c:f037:2:6711:83f1:325e:e8d
    Temporary IPv6 Address. . . . . : fd17:625c:f037:2:b1ea:214a:39b0:35f2
    Link-local IPv6 Address . . . . . : fe80::cd63:cb72:5b31:4ac2%14
    IPv4 Address. . . . . : 10.0.2.15
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::2%14
                                10.0.2.2

PS C:\Users\Mimmo>
```

Con il comando ipconfig sia il Command Prompt che Powershell mi danno gli stessi risultati

Qual è il comando PowerShell per dir?

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

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

PS C:\Users\Mimmo> get-ChildItem

Directory: C:\Users\Mimmo

Mode                LastWriteTime         Length Name
----                -
d-r---             9/22/2025   3:04 PM           Contacts
d-r---             9/22/2025   3:04 PM           Desktop
d-r---             9/22/2025   3:04 PM           Documents
d-r---             9/22/2025   6:10 AM           Downloads
d-r---             9/22/2025   3:04 PM           Favorites
d-r---             9/22/2025   3:04 PM           Links
d-r---             9/22/2025   3:04 PM           Music
d-r---             9/22/2025   3:06 PM           OneDrive
d-r---             9/22/2025   3:04 PM           Pictures
d-r---             9/22/2025   3:04 PM           Saved Games
d-r---             9/22/2025   6:08 AM           Searches
d-r---             9/22/2025   6:36 AM           Videos
```

Il comando Powershell per dir è “get-ChildItem” che otteniamo dopo il comando “Get-Alias dir” che ci dirà un comando alternativo

Qual è il gateway IPv4?

```
PS C:\Users\Mimmo> netstat -r
=====
Interface List
 14...08 00 27 d0 08 b0 .....Intel(R) PRO/1000 MT Desktop Adapter
 1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          10.0.2.2         10.0.2.15         25
10.0.2.0                  255.255.255.0    On-link          10.0.2.15         281
10.0.2.15                  255.255.255.255  On-link          10.0.2.15         281
10.0.2.255                 255.255.255.255  On-link          10.0.2.15         281
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
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          10.0.2.15         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          10.0.2.15         281
=====
Persistent Routes:
None
```

Il gateway è 10.0.2.2

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

Property	Value
Description	
File description	Windows Start-Up Application
Type	Application
File version	10.0.26100.5074
Product name	Microsoft® Windows® Operating System
Product version	10.0.26100.5074
Copyright	© Microsoft Corporation. All rights reserv...
Size	772 KB
Date modified	9/22/2025 5:27 AM
Language	English (United States)
Original filename	WinInit.exe

Ottingo diverse informazioni come:

File Description: Windows Start-Up Application. Indica la funzione primaria del file.

Type: Application. Indica che si tratta di un file eseguibile (.exe).

File version: 10.0.26100.5074. Questo è il numero di versione specifico del file.

Product name: Microsoft® Windows® Operating System. Conferma che il file è un componente ufficiale del sistema operativo Windows.

Product version: 10.0.26100.5074. Indica la versione del sistema operativo a cui appartiene il file, generalmente correlata alla versione di Windows 10 o 11 (in questo caso, un numero di build specifico).

Copyright: © Microsoft Corporation. All rights reserved. Conferma che il file è di proprietà e protetto da copyright di Microsoft.

Size: 772 KB. La dimensione del file in kilobyte.

Date modified: 9/22/2025 5:27 AM. La data e l'ora in cui il file è stato modificato l'ultima volta.

Language: English (United States). La lingua del codice binario o delle risorse incorporate nel file.

Original filename: WinInit.exe. Il nome del file così come era stato originariamente compilato, essenziale per la verifica dei file di sistema.

Cosa è successo ai file nel Cestino?

```
PS C:\WINDOWS\system32> clear-recyclebin

Confirm
Are you sure you want to perform this action?
Performing the operation "Clear-RecycleBin" on target "All of the contents of the
Recycle Bin".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):y
```



Dopo l'esecuzione del comando il cestino si svuoterà dandoci un'alternativa tramite riga di comando per eliminare i dati dentro di esso.

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.

1. Risposta agli Incidenti (Incident Response)

Cmdlet	Descrizione	Utilità per la Sicurezza
Get-Process	Elenca tutti i processi in esecuzione.	Identificare processi sospetti per nome, utilizzo CPU o anomalie di parentela.
Get-NetTCPConnection	Visualizza tutte le connessioni di rete TCP attive (equivalente a netstat -ano).	Rilevare comunicazioni C2 (Command and Control) o esfiltrazioni di dati.
Stop-Process	Termina un processo in base a nome o ID (PID).	Contenere rapidamente una minaccia terminando il processo del malware.
Get-Service	Elenca i servizi di sistema installati.	Individuare servizi anomali o nuovi creati per la persistenza.
Restart-Service	Riavvia un servizio specificato.	Ripristinare servizi critici di sicurezza compromessi o bloccati.

2. Analisi Forense e Threat Hunting

Questi comandi aiutano a raccogliere indicatori di compromissione (IoC) e a scandagliare i registri.

Cmdlet	Descrizione	Utilità per la Sicurezza
Get-WinEvent	Analizza i registri eventi di Windows (Log di Sicurezza, Applicazione, ecc.).	Filtrare i log per ID evento specifici (es. accessi falliti 4625 o creazione processi 4688).

Cmdlet	Descrizione	Utilità per la Sicurezza
Get-ChildItem - Recurse	Cerca file e directory in modo ricorsivo. (Alias: dir -r o ls -r).	Eseguire una ricerca rapida di file con estensioni o nomi sospetti su tutto il disco.
Get-FileHash	Calcola l'hash crittografico (SHA256, MD5) di un file.	Verificare l'integrità dei file o confrontare l'hash di un file sospetto con database di IoC noti.
Select-String	Cerca pattern di testo all'interno di file (equivalente a grep).	Eseguire ricerche ad alta velocità di indirizzi IP, URL o stringhe di codice in file di log o script.
Get-ScheduledTask	Elenca le attività pianificate.	Rilevare la persistenza degli attaccanti, che spesso creano attività pianificate.
Get-Content	Visualizza il contenuto di un file. (Alias: cat o type).	Esaminare rapidamente il contenuto di file di log, script o configurazione.

3. Gestione e Audit di Sicurezza

Questi comandi sono utilizzati per valutare e rafforzare la configurazione di sicurezza del sistema.

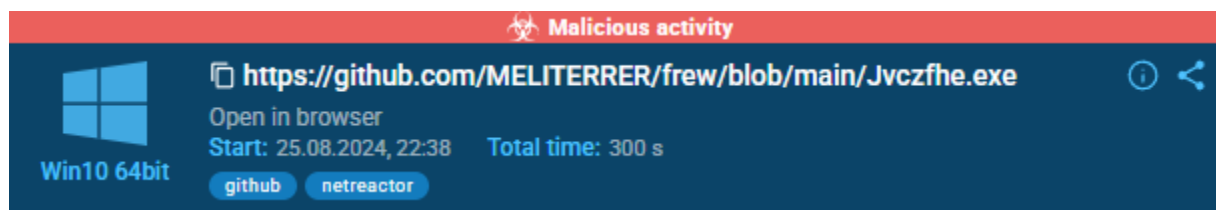
Cmdlet	Descrizione	Utilità per la Sicurezza
Get-ExecutionPolicy	Visualizza la politica di esecuzione degli script PowerShell.	Verificare che la politica non sia impostata su Unrestricted, che è un rischio per la sicurezza.
Set-ExecutionPolicy	Imposta la politica di esecuzione per limitare il codice eseguibile.	Impostare su RemoteSigned per bloccare script scaricati non firmati.
Start-Transcript / Stop-Transcript	Avvia e interrompe la registrazione di tutti i comandi e l'output della sessione.	Creare una traccia forense affidabile delle attività di indagine.
Get-Acl	Recupera i permessi (ACL) di un file o cartella.	Audit e verifica dei permessi per individuare modifiche anomale o escalation di privilegi.

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/>

Possiamo subito notare che il software ci avverte che è stata rilevata attività malevola durante l'esecuzione.



tutto inizia probabilmente dal PID 6596 firefox.exe

Processes 25Actions 0beta

Filter by PID or name

☒ Only important

2256	svchost.exe	-k NetworkService -p -s Dnscache		0	316	43
6552	firefox.exe	"https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe"		154	34	25
6596	firefox.exe	https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe		34k	11k	168
6744	firefox.exe	-contentproc -channel=1824 -parentBuildID 20240213221259 -prefsHandle 1752 -pre...		502	726	61
6816	firefox.exe	-contentproc -channel=2208 -parentBuildID 20240213221259 -prefsHandle 2192 -pre...		316	690	44
7048	firefox.exe	-contentproc -channel=3028 -childID 1 -isForBrowser -prefsHandle 2880 -prefMapHa...		479	691	39
6680	firefox.exe	-contentproc -channel=4480 -childID 2 -isForBrowser -prefsHandle 4472 -prefMapHa...		359	681	38
6368	firefox.exe	-contentproc -channel=4976 -parentBuildID 20240213221259 -sandboxingKind 0 -pre...		195	168	37
6384	firefox.exe	-contentproc -channel=5228 -childID 3 -isForBrowser -prefsHandle 5224 -prefMapHa...		483	741	39
6340	firefox.exe	-contentproc -channel=5380 -childID 4 -isForBrowser -prefsHandle 5516 -prefMapHa...		448	681	38
6360	firefox.exe	-contentproc -channel=5512 -childID 5 -isForBrowser -prefsHandle 5668 -prefMapHa...		448	681	38
6456	firefox.exe	-contentproc -channel=5916 -childID 6 -isForBrowser -prefsHandle 5908 -prefMapHa...		468	681	38

Defense Evasion

Possiamo evincere che il PID maschera il proprio comportamento per apparire come un file legittimo dalla sezione MITRE ATT&CK.

Le nostre tesi vengono confermate dalla sezione "Process drops legitimate windows executable (1)" (Il processo rilascia un eseguibile Windows legittimo)

Questo significa che è stata rilevata un'attività in cui un processo sta scaricando o creando un file che è un eseguibile legittimo di Windows.

Notiamo sotto il PID "**6596 firefox.exe (1)**" questo conferma ulteriormente le nostre tesi sul file che ha fatto iniziare tutto (il *dropper* o il *parent process*) è quindi l'istanza con ID **6596** del browser **firefox.exe**.

Techniques details

Get to know what this threat is about

Warning (1)

Subtechniques [T1036.003](#)

"Rename Legitimate Utilities"

Permissions required:

Data sources: File: File Modification, Process: Process Metadata, Command: Command Execution, File: File Metadata

Adversaries may rename legitimate / system utilities to try to evade security mechanisms concerning the usage of those utilities. Security monitoring and control mechanisms may be in place for legitimate utilities adversaries are capable of abusing, including both built-in binaries and tools such as PSEXec, AutoHotKey, and IronPython.

Process drops legitimate windows executable (1)

6596 firefox.exe (1)

Filename:	C:\Users\admin\Downloads\OOD5yt-b.exe.part
Md5:	5ec4256e6a2367502a8058f4bc8f4ecc
Sha1:	c6f996570b6f34cb813028c601b9d27bf8df0550
Sha256:	e6a7aaff54eb6d06acfc6f1dfa21a85b767dbf7ff3e9bdfd2ddbdeced86aa9b2

1 of 1

Execution

I due file eseguibili Jvczfhe.exe e Muadnrd.exe avviano il cmd e eseguono il timeout come tecnica di elusione per evitare di farsi rilevare dal sistema come software malevolo ritardando l'esecuzione dei comandi

Nello specifico, l'attaccante sta utilizzando l'utilità di sistema **timeout.exe** per ritardare l'esecuzione di 21 secondi. Questo ritardo è una tattica comune per eludere i sandbox (ambienti di analisi automatica) e altri sistemi di sicurezza.

The screenshot shows a 'Techniques details' window with a dark blue header. The title is 'Techniques details' and the subtitle is 'Get to know what this threat is about'. There is a 'Warning (4)' icon in the top right corner. The main content is divided into two columns. The left column contains the following information: 'Subtechniques' with a dropdown arrow and the ID 'T1059.003', the title '"Windows Command Shell"', 'Permissions required: User', 'Data sources: Command: Command Execution, Process: Process Creation', and a note: 'Adversaries may abuse the Windows command shell for execution. The Windows command'. The right column contains two bullet points: 'Uses TIMEOUT.EXE to delay execution (2)' with sub-points '7520 cmd.exe (1)' and '7876 cmd.exe (1)', and 'Starts CMD.EXE for commands execution (2)' with sub-points '7492 Jvczfhe.exe (1)' and '7824 Muadnrd.exe (1)'. At the bottom right, there is a section with 'Image: C:\Windows\SysWOW64\timeout.exe' and 'Cmdline: timeout 21'.

Techniques details	
Get to know what this threat is about	
Warning (4)	
Subtechniques ▼ T1059.003	
"Windows Command Shell"	
Permissions required: User	
Data sources: Command: Command Execution, Process: Process Creation	
Adversaries may abuse the Windows command shell for execution. The Windows command	
	<ul style="list-style-type: none">● Uses TIMEOUT.EXE to delay execution (2)<ul style="list-style-type: none">7520 cmd.exe (1)7876 cmd.exe (1)● Starts CMD.EXE for commands execution (2)<ul style="list-style-type: none">7492 Jvczfhe.exe (1)7824 Muadnrd.exe (1)
	Image: C:\Windows\SysWOW64\timeout.exe Cmdline: timeout 21

Technique details

Dalla sezione Technique details possiamo inoltre vedere tutto quello che ha fatto il software malevolo.

Tra le cose più pericolose troviamo che questo ha visionato i Windows Trust Settings e ha letto i security Settings del browser Internet Explorer

The screenshot shows a list of actions performed by the malware. It contains two bullet points: 'Checks Windows Trust Settings (2)' with sub-points '7492 Jvczfhe.exe (1)' and '7824 Muadnrd.exe (1)', and 'Reads security settings of Internet Explorer (2)' with sub-points '7492 Jvczfhe.exe (1)' and '7824 Muadnrd.exe (1)'.

<ul style="list-style-type: none">● Checks Windows Trust Settings (2)<ul style="list-style-type: none">7492 Jvczfhe.exe (1)7824 Muadnrd.exe (1)● Reads security settings of Internet Explorer (2)<ul style="list-style-type: none">7492 Jvczfhe.exe (1)7824 Muadnrd.exe (1)
--

Troviamo anche altre cose meno rilevanti come:

- Reads the software policy settings
- Checks proxy server information
- Reads the machine GUID from the registry
- Reads the computer name
- Checks supported languages
- Reads Environment values
- Reads Microsoft Office registry keys

C&C

Il software malevolo usare su una porta insolita (7702) e si connette tramite protocollo tcp

Techniques details

Get to know what this threat is about

Warning (1)

[T1571](#)

"Non-Standard Port"

Permissions required:

Data sources: Network Traffic: Network Traffic Flow, Network Traffic: Network Traffic Content

Adversaries may communicate using a protocol and port pairing that are typically not associated. For example, HTTPS over port 8088(Citation: Symantec Elfin Mar 2019) or port 587(Citation: Fortinet Agent Tesla April 2018) as opposed to the traditional port 443.



Connects to unusual port (1)

5152 InstallUtil.exe (1)

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

HTTP Request

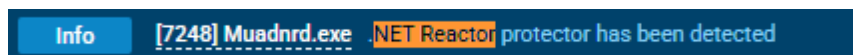
Continuando l'analisi si può vedere che sono presenti numerose richieste HTTP verso diversi domini, di cui alcuni sembrano essere legittimi mentre altri risultano sospetti (ad esempio <http://r10.o.lencr.org>, <http://o.pki.goog/wr2>). Le richieste POST verso questi domini possono indicare che il malware sta inviando dati raccolti o eseguendo azioni remote.

15629 ms	POST 200: OK	?	6596	firefox.exe		http://o.pki.goog/wr2	83 b ↑ binary
15630 ms	POST 200: OK	?	6596	firefox.exe		http://o.pki.goog/wr2	471 b ↓ binary

Verso alcuni di questi domini sospetti sono attive diverse connessioni TCP che potrebbero essere utilizzate per la comunicazione con server C&C o per l'esfiltrazione dei dati

ULTERIORI ANALISI

Viene inoltre rilevato il NET Reactor Protector, confermando che il malware sta cercando di proteggere il proprio codice da decompilazione o analisi.



Esercizio 3 BONUS

Cos'è Nima?

Per cosa viene usato nmap?

Nmap (acronimo di "Network Mapper") è uno strumento open source fondamentale per l'esplorazione di rete e l'audit di sicurezza.

Nmap opera inviando pacchetti IP "grezzi" (raw IP packets) ai target e analizzando le risposte per raccogliere informazioni. Le sue funzioni principali includono:

Scansione delle Porte (Port Scanning): È la funzione più nota. Determina lo **stato delle porte TCP e UDP** su un host di destinazione, indicando se sono **aperte** (c'è un servizio in ascolto), **chiuse** o **filtrate** (probabilmente bloccate da un firewall).

Individuazione degli Host (Host Discovery): Identifica quali dispositivi sono **attivi e raggiungibili** su una rete.

Rilevamento del Servizio e della Versione (Service/Version Detection): Non si limita a dire che una porta è aperta, ma indaga per identificare il **nome e la versione** esatta del servizio in esecuzione su quella porta (es. Apache 2.4.41, OpenSSH 7.4).

Fingerprinting del Sistema Operativo (OS Fingerprinting): Tenta di determinare il **sistema operativo** in esecuzione sull'host di destinazione (es. Linux 4.x, Windows Server 2019) analizzando sottili differenze nello stack TCP/IP.

Nmap Scripting Engine (NSE): Un potente motore di scripting che estende le funzionalità di Nmap, consentendo di eseguire attività avanzate come la rilevazione di specifiche vulnerabilità, l'enumerazione avanzata, e l'interazione con i servizi di rete.

Qual è il comando nmap usato?

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

```
# 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
```

Cosa fa l'opzione -A?

L'opzione -A abilita una serie di funzionalità avanzate e invasive, raggruppandole in un'unica bandiera:

Rilevamento del Sistema Operativo (-O): Tenta di determinare il sistema operativo in esecuzione sull'host di destinazione tramite l'analisi del fingerprint dello stack TCP/IP.

Rilevamento del Servizio/Versione (-sV): Esegue un'analisi più approfondita sulle porte aperte per identificare l'**applicazione esatta** e la sua **versione** in esecuzione.

Scansione con Script di Default (-sC): Esegue gli script NSE (Nmap Scripting Engine) di default. Questi script eseguono test per vulnerabilità comuni, enumerazione e altre funzioni avanzate.

Traceroute: Esegue un traceroute per visualizzare il percorso di rete (gli hop) che i pacchetti impiegano per raggiungere l'obiettivo.

Cosa fa l'opzione -T4?

L'opzione -T (Timing) imposta la velocità dello scan.

Nmap ha sei modelli di temporizzazione, da T0 (Paranoid, estremamente lento e furtivo) a T5 (Insane, estremamente veloce e rumoroso).

Quali porte e servizi sono aperti?

Dopo la scansione col comando **nmap -A -T4 localhost** ho trovato la porta 21 e 22 aperta con i servizi ftp e ssh

```
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
```

A quale rete appartiene la tua VM?

```
inet 10.0.2.15/24
```

La mia rete appartiene alla rete **10.0.2.15/24**

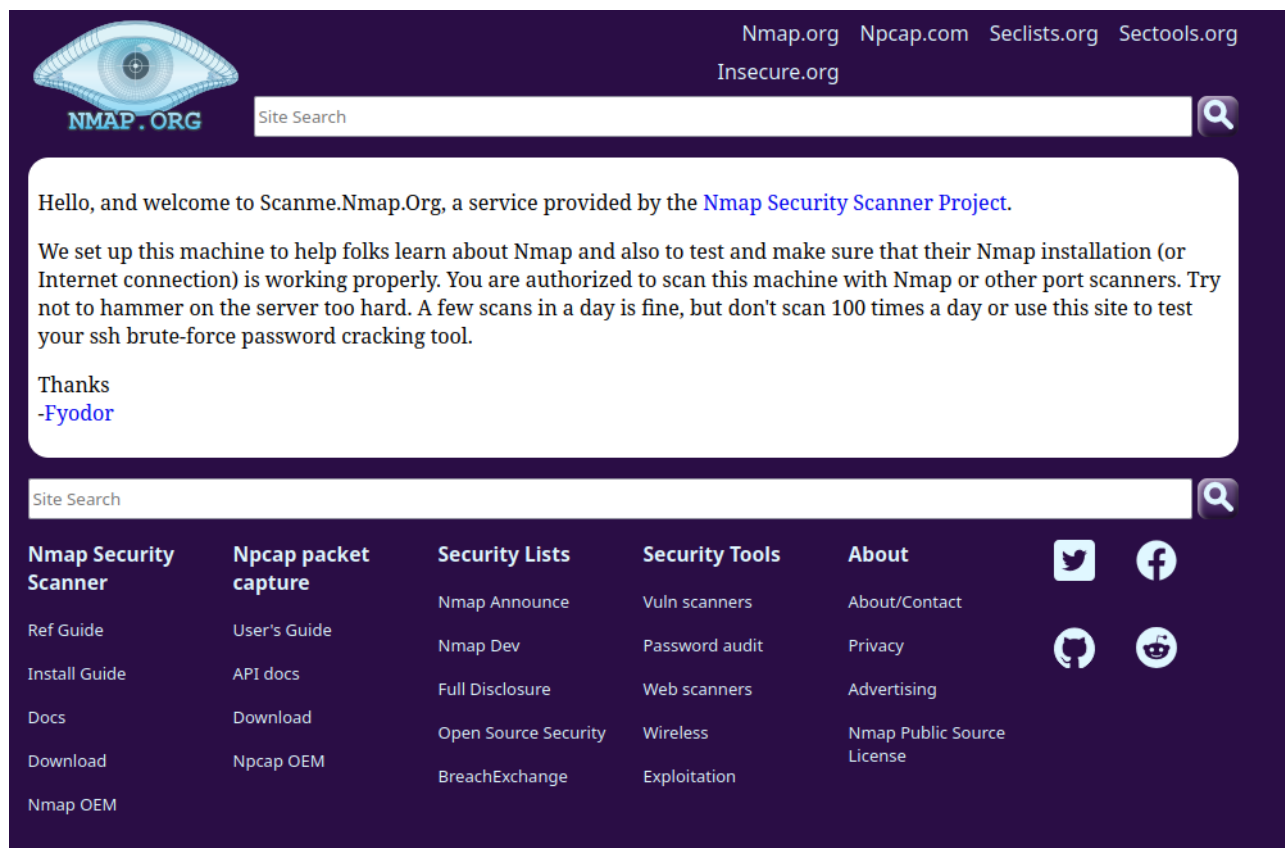
Quanti host sono attivi?

Dopo il comando “**nmap -A -T4 10.0.2.0/24**” trovo che l’host attivo è solo uno.

```
Nmap done: 256 IP addresses (1 host up)
```


Qual è lo scopo di questo sito?

Aiuta a comprendere meglio nmap e garantisce la corretta installazione di nmap



The screenshot shows the Nmap.org website with a dark purple header. The header contains the NMAP.ORG logo (an eye with a target) on the left, and links to Nmap.org, Npcap.com, Seclists.org, Sectools.org, and Insecure.org on the right. Below the header is a white search bar with the text "Site Search" and a magnifying glass icon. The main content area is white and contains a welcome message: "Hello, and welcome to Scanme.Nmap.Org, a service provided by the Nmap Security Scanner Project." followed by a paragraph explaining the site's purpose and a "Thanks -Fyodor" signature. Below this is another "Site Search" bar. At the bottom, there is a dark purple footer with a grid of links organized into five columns: "Nmap Security Scanner" (Ref Guide, Install Guide, Docs, Download, Nmap OEM), "Npcap packet capture" (User's Guide, API docs, Download, Npcap OEM), "Security Lists" (Nmap Announce, Nmap Dev, Full Disclosure, Open Source Security, BreachExchange), "Security Tools" (Vuln scanners, Password audit, Web scanners, Wireless, Exploitation), and "About" (About/Contact, Privacy, Advertising, Nmap Public Source License). Social media icons for Twitter, Facebook, GitHub, and Reddit are also present.

Quali porte e servizi sono aperti?

Le porte aperte sono 4:

22/tcp: ssh

80/tcp: http

9929/tcp: nping-echo

31337/tcp: tcpwrappedtcpwrapped

Quali porte e servizi sono filtrati?

996 porte sono filtrate

-Not shown: 996 filtered tcp ports (no-response) (Nmap ha inviato i probe ma non ha ricevuto risposta, indicando la presenza di un firewall o filtro).

Qual è l'indirizzo IP del server?

L'indirizzo IPv4 del server è: 45.33.32.156

Qual è il sistema operativo?

Il sistema operativo rilevato è: Linux (Specificato anche come Ubuntu per i servizi aperti).

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.97 ( https://nmap.org ) at 2025-09-23 11:10 -0400
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
Not shown: 996 filtered tcp ports (no-response)
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-title: Go ahead and ScanMe!
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-favicon: Nmap Project
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 32.45 seconds
```

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 per la Sicurezza (Ruolo Difensivo/Etico)

Gli amministratori di sistema e i professionisti della sicurezza (hacker etici) usano Nmap per rafforzare le difese della rete, in quanto offre la stessa visibilità che un attaccante cercherebbe.

Obiettivo	Come Nmap aiuta
Valutazione della Superficie di Attacco	Identifica tutti gli host attivi e le porte aperte (open) che un attaccante potrebbe sfruttare. Se una porta non necessaria è aperta (es. una porta di gestione), è un rischio.
Verifica delle Firewall	Esegue scansioni per determinare se le porte sono filtered (filtrate) o closed (chiuse). Questo verifica che le regole del firewall stiano funzionando come previsto e bloccando correttamente il traffico indesiderato.
Inventario degli Asset (Asset Inventory)	Rileva il Sistema Operativo (OS) e la versione del servizio in esecuzione su ciascun dispositivo. Questa informazione è vitale per la gestione delle patch e l'identificazione di software obsoleto o vulnerabile.
Rilevamento di Vulnerabilità	Tramite l' Nmap Scripting Engine (NSE) , Nmap può eseguire automaticamente script predefiniti per testare la presenza di vulnerabilità comuni (es. configurazioni SSL deboli o servizi con credenziali predefinite).
Rilevamento di Dispositivi Non Autorizzati (Shadow IT)	Aiuta a scoprire rapidamente server, access point wireless o dispositivi IoT (Internet of Things) non autorizzati collegati alla rete che potrebbero essere privi di patch o configurazioni di sicurezza adeguate.

Nmap come Strumento Nefasto (Ruolo Offensivo/Malevolo)

Gli hacker malevoli usano Nmap come strumento di **ricognizione (reconnaissance)** nella prima fase di un attacco. Il loro obiettivo è raccogliere quante più informazioni possibili prima di lanciare l'attacco vero e proprio.

Obiettivo dell'Attaccante	Come Nmap viene usato
Ricognizione e Mappatura	Mappa l'intera topologia della rete, identificando gli host target attivi che meritano attenzione.
Identificazione del Punto Debole	L'attaccante usa le scansioni di rilevamento della versione (-sV) e del sistema operativo (-O) per trovare software o sistemi operativi specifici che hanno vulnerabilità pubbliche note (CVE, <i>Common Vulnerabilities and Exposures</i>).
Evasione dei Sistemi di Difesa	Utilizza tecniche di scansione "furtive" (stealth) come la scansione SYN a mezzo aperto (-sS) per tentare di bypassare i sistemi di rilevamento delle intrusioni (IDS) o i log del sistema che registrano le connessioni complete.
Analisi dei Firewall	Usa la scansione ACK (-sA) per determinare la presenza e le regole dei firewall (<i>stateful vs stateless</i>) e pianificare come aggirarle (proprio come faceva l'analisi nel tuo esempio con le porte filtered).

Esercizio 4 BONUS

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

-Indirizzo IP dell'Attaccante/Client (Sorgente): 10.0.2.4

-Indirizzo IP del Server Web Target (Destinazione): 10.0.2.15

1	0.000000	10.0.2.4	10.0.2.15	TCP	74	35614 → 80 [SYN] Seq=0 Win=29200
2	0.000315	10.0.2.15	10.0.2.4	TCP	74	80 → 35614 [SYN, ACK] Seq=0 Ack=1
3	0.000349	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1 Ack=1 Win=2
4	0.000681	10.0.2.4	10.0.2.15	HTTP	654	POST /dvwa/login.php HTTP/1.1 (ap
5	0.002149	10.0.2.15	10.0.2.4	TCP	66	80 → 35614 [ACK] Seq=1 Ack=589 Wir
6	0.005700	10.0.2.15	10.0.2.4	HTTP	430	HTTP/1.1 302 Found
7	0.005700	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=589 Ack=365 W
8	0.014383	10.0.2.4	10.0.2.15	HTTP	496	GET /dvwa/index.php HTTP/1.1
9	0.015485	10.0.2.15	10.0.2.4	HTTP	3107	HTTP/1.1 200 OK (text/html)
10	0.015485	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1019 Ack=3406
11	0.068625	10.0.2.4	10.0.2.15	HTTP	429	GET /dvwa/dvwa/css/main.css HTTP/1
12	0.070400	10.0.2.15	10.0.2.4	HTTP	1511	HTTP/1.1 200 OK (text/css)
13	174.254430	10.0.2.4	10.0.2.15	HTTP	536	GET /dvwa/vulnerabilities/sqli/?ic
14	174.254581	10.0.2.15	10.0.2.4	TCP	66	80 → 35638 [ACK] Seq=1 Ack=471 Wir
15	174.257989	10.0.2.15	10.0.2.4	HTTP	1861	HTTP/1.1 200 OK (text/html)
16	220.490531	10.0.2.4	10.0.2.15	HTTP	577	GET /dvwa/vulnerabilities/sqli/?ic
17	220.490637	10.0.2.15	10.0.2.4	TCP	66	80 → 35640 [ACK] Seq=1 Ack=512 Wir
18	220.493085	10.0.2.15	10.0.2.4	HTTP	1918	HTTP/1.1 200 OK (text/html)
19	277.727722	10.0.2.4	10.0.2.15	HTTP	630	GET /dvwa/vulnerabilities/sqli/?ic
20	277.727871	10.0.2.15	10.0.2.4	TCP	66	80 → 35642 [ACK] Seq=1 Ack=565 Wir
21	277.732200	10.0.2.15	10.0.2.4	HTTP	1955	HTTP/1.1 200 OK (text/html)
22	313.710129	10.0.2.4	10.0.2.15	HTTP	659	GET /dvwa/vulnerabilities/sqli/?ic
23	313.710277	10.0.2.15	10.0.2.4	TCP	66	80 → 35644 [ACK] Seq=1 Ack=594 Wir
24	313.712414	10.0.2.15	10.0.2.4	HTTP	1954	HTTP/1.1 200 OK (text/html)
25	383.277032	10.0.2.4	10.0.2.15	HTTP	680	GET /dvwa/vulnerabilities/sqli/?ic
26	383.277811	10.0.2.15	10.0.2.4	TCP	66	80 → 35666 [ACK] Seq=1 Ack=615 Wir
27	383.284289	10.0.2.15	10.0.2.4	HTTP	4068	HTTP/1.1 200 OK (text/html)
28	441.804070	10.0.2.4	10.0.2.15	HTTP	685	GET /dvwa/vulnerabilities/sqli/?ic

Qual è la versione?

La versione è **5.7.12-0ubuntu14.1**

5.7.12-0ubuntu1.1</pre>



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

L'utente che ha l'hash 8d3533d75ae2c3966d7e0d4fcc69216b è l'utente **1337**

```
First name: 1337<br />Surname: 8d3533d75ae2c3966d7e0d4fcc69216b<br />Password from users#<br />First name: pablo<br />Surname: 0d107d0<br />or 1=1 union select user, password from users#<br />First name:
```

Qual è la password in chiaro?

La password in chiaro è **charley**

Hash	Type	Result
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley

Qual è il rischio che le piattaforme utilizzino il linguaggio SQL?

Il rischio principale nell'uso di SQL da parte delle piattaforme web risiede nella sua funzione stessa: SQL è il linguaggio che permette a un'applicazione di interagire, manipolare e accedere a tutti i dati contenuti nel database (ad esempio, informazioni sugli utenti, transazioni, contenuti del sito).

Il rischio specifico è rappresentato dalla vulnerabilità chiamata SQL Injection (SQLi).

Il Problema: Se l'input dell'utente (come il testo in un campo di login o di ricerca) non viene gestito e pulito correttamente dall'applicazione, un aggressore può inserire comandi SQL dannosi direttamente nella query.

La Gravità: Un attacco SQLi ben riuscito permette all'aggressore di bypassare l'autenticazione, visualizzare, modificare o eliminare l'intero contenuto del database, inclusi dati sensibili di tutti gli utenti, con conseguenze che vanno dalla violazione della privacy al totale controllo del server.

Naviga in internet ed esegui una ricerca per “prevenire attacchi di SQL injection”. Quali sono 2 metodi o passaggi che possono essere adottati per prevenire gli attacchi di SQL injection?

A. Utilizzare Istruzioni Prepare (Prepared Statements) con Parametri

Questo è il metodo di difesa più efficace e raccomandato. Invece di costruire la query SQL concatenando le stringhe di input dell'utente, l'applicazione invia al database prima il modello della query (il *prepared statement*) e poi i dati dell'utente come parametri separati.

- **Come funziona:** Il database distingue chiaramente tra il codice SQL vero e proprio e i dati che devono essere trattati solo come valori. Se un utente inserisce codice SQL dannoso, il database lo interpreta come una semplice stringa di testo da cercare, non come un comando da eseguire.

B. Filtrare e Validare Rigorosamente l'Input dell'Utente

Implementare un filtro di validazione (Input Validation) su ogni dato ricevuto dall'esterno:

- **Principio di Fiducia Zero:** Non fidarsi mai di nessun dato proveniente dall'utente o da fonti esterne.
- **Validazione della whitelist:** L'applicazione dovrebbe accettare solo i caratteri, i formati e i tipi di dati specificamente previsti (ad esempio, accettare solo numeri interi per un campo ID e non il carattere apostrofo ' utilizzato nelle iniezioni SQL).
- **Sanitizzazione:** Rimuovere o sostituire (escape) i caratteri speciali che hanno un significato in SQL (come l'apostrofo ', il doppio trattino --, o il punto e virgola ;) prima che la query venga inviata, impedendo così l'iniezione di codice malevolo.