S11L5

Esercizio 1: Usare Windows PowerShell

Obiettivi

L'obiettivo del laboratorio è esplorare alcune delle funzioni di PowerShell.

- Parte 1: Accedere alla console PowerShell.
- Parte 2: Esplorare i comandi del Prompt dei Comandi e di PowerShell.
- Parte 3: Esplorare i cmdlet.
- Parte 4: Esplorare il comando netstat usando PowerShell.
- Parte 5: Svuotare il cestino usando PowerShell.

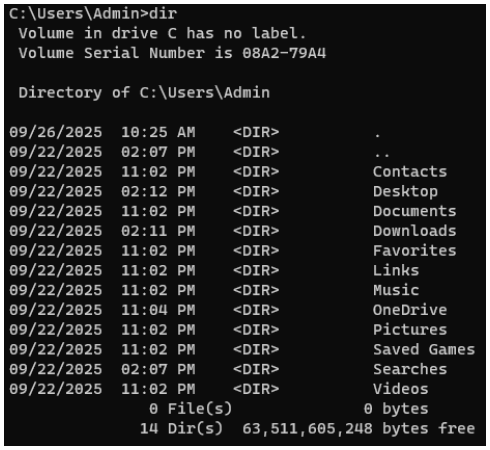
Contesto / Scenario

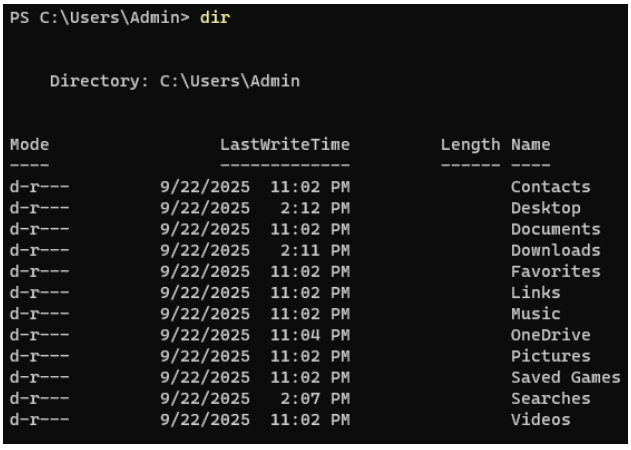
PowerShell è un potente strumento di automazione. È sia una console di comando che un linguaggio di scripting. In questo laboratorio, userai la console per eseguire alcuni dei comandi disponibili sia nel prompt dei comandi che in PowerShell. PowerShell ha anche funzioni che possono creare script per automatizzare compiti e lavorare insieme al Sistema Operativo Windows.

ESERCIZIO 1

Quali sono gli output del comando dir?

Il comando dir, in entrambe le shell, fornisce diverse informazioni su file e cartelle nella directory corrente o specificata. Il Command Prompt in fondo all'output, dopo l'elenco delle directory, mostra un riepilogo includendo numero cartelle e dimensione. PowerShell mostra anche i permessi relativi ai files e directories.





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

Il comando **ipconfig** ritorna un output perfettamente uguale in entrambe le shell

Qual è il comando PowerShell per dir?

Il comando PowerShell per dir è Get-ChildItem

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

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

Qual è il gateway IPv4?

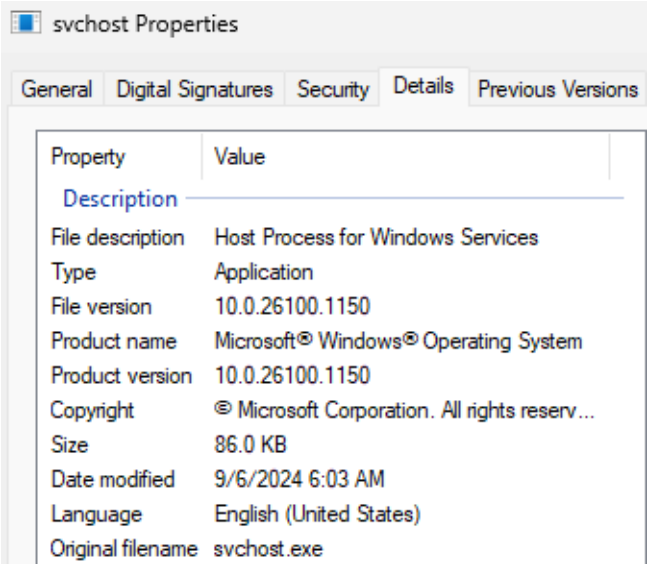
Il gateway IPv4 è 10.0.2.2

```
PS C:\Users\Admin> netstat -r
===========================================================================
Interface List
 12...08 00 27 50 3c ca ......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
```

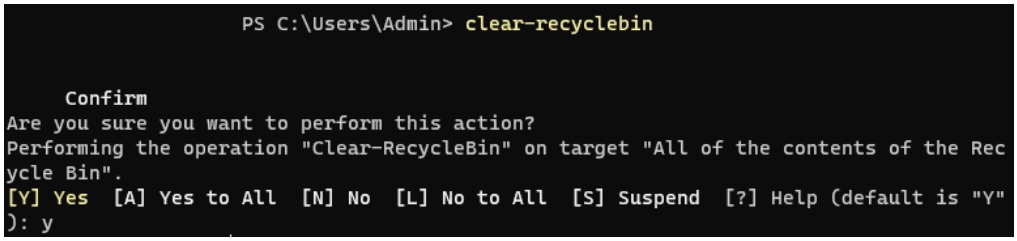
Quali informazioni puoi ottenere dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID selezionato?

Tramite la scheda Dettagli della finestra Proprietà del PID selezionato possiamo ottenere informazioni come la descrizione del file, il tipo di file, versione, dimensione, lingua e ultima modifica. In questo caso le informazioni indicano che il file è il processo **Host Process for Windows Services** (**svchost.exe**), il file ha la versione **10.0.26100.1150** ed è stato modificato il **9 giugno 2024**.



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

Tramite il comando clear-recyclebin è possibile svuotare il cestino. Pertanto il cestino è stato svuotato dopo aver dato conferma su PowerShell



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.

Comandi per l'Analisi	
Get-EventLog / Get-WinEvent	**Analisi dei Log:** Permettono di interrogare i registri eventi di Windows (Sicurezza, Applicazione, Sistema) per cercare attività sospette, tentativi di accesso falliti o esecuzioni di codice. Get-WinEvent è il cmdlet più moderno e potente.

Get-Service	**Audit dei Servizi:** Elenca tutti i servizi in esecuzione o installati sul sistema. Utilissimo per identificare servizi non necessari o non autorizzati che potrebbero rappresentare una superficie di attacco.
Get-Process	**Monitoraggio dei Processi:** Visualizza tutti i processi in esecuzione. È fondamentale per la ricerca di malware o processi anomali (es. un processo figlio inaspettato). Può essere combinato con -IncludeUserName per vedere l'utente che ha avviato il processo.
Get-Content	**Lettura di File:** Legge il contenuto di file di testo. Essenziale per analizzare file di configurazione, file di log specifici o per esaminare lo *script block* in memoria per la *threat hunting*.
Select-String	**Ricerca Pattern:** Cerca pattern di testo specifici (come indirizzi IP, nomi utente o stringhe sospette) all'interno di file o output di altri comandi, in modo simile a grep in Linux.

Comandi per la Gestione della Rete	
Test-NetConnection	**Connettività di Rete:** Verifica la connettività di rete verso un host specifico (simile a ping o tracert, ma più versatile) e può testare una porta TCP. Fondamentale durante la risposta agli incidenti per verificare la comunicazione con i Command and Control (C2) o l'accesso a risorse di rete.
Get-NetIPConfiguration	**Configurazione di Rete:** Visualizza la configurazione IP, le interfacce di rete e i server DNS. Utile per identificare indirizzi IP "rogue" o per la diagnostica di rete.

Invoke-WebRequest	**Richieste Web:** Consente di effettuare richieste HTTP/HTTPS. Spesso utilizzato per scaricare file sospetti o per simulare le azioni di un attaccante.

Comandi per il Controllo e l'Esecuzione	
Get-ExecutionPolicy	**Politica di Esecuzione:** Mostra l'attuale politica di esecuzione degli script di PowerShell. È il primo controllo di sicurezza, poiché politiche troppo permissive (es. Unrestricted) possono consentire l'esecuzione di script dannosi.
Set-ExecutionPolicy	**Imposta Politica di Esecuzione:** Consente di modificare la politica (es. RemoteSigned è un buon compromesso per la sicurezza). **Importante:** Usare con cautela.
Stop-Process	**Terminazione di Processi:** Termina uno o più processi, specificandone il nome o l'ID (PID). Cruciale nella fase di **contenimento** di un incidente per fermare l'esecuzione di malware.
Get-AuthenticodeSignature	**Verifica Firma Digitale:** Controlla la firma digitale di un file eseguibile. Molto utile per verificare se un file binario di sistema è stato manomesso.

Comandi per l'Automazione e il Remoto

Comando	Funzione per la Sicurezza
Export-Csv / ConvertTo-Json	**Gestione Dati:** Comandi per esportare i dati raccolti (es. l'elenco dei processi o i log filtrati) in formati strutturati come CSV o JSON per l'analisi successiva.
Enter-PSSession / Invoke-Command	**Gestione Remota:** Permettono di eseguire comandi o script su computer remoti. Essenziali per la **risposta agli incidenti su larga scala** per investigare o contenere rapidamente più macchine sulla rete.

ESERCIZIO 2

Esercizio 2: Studio Ioc

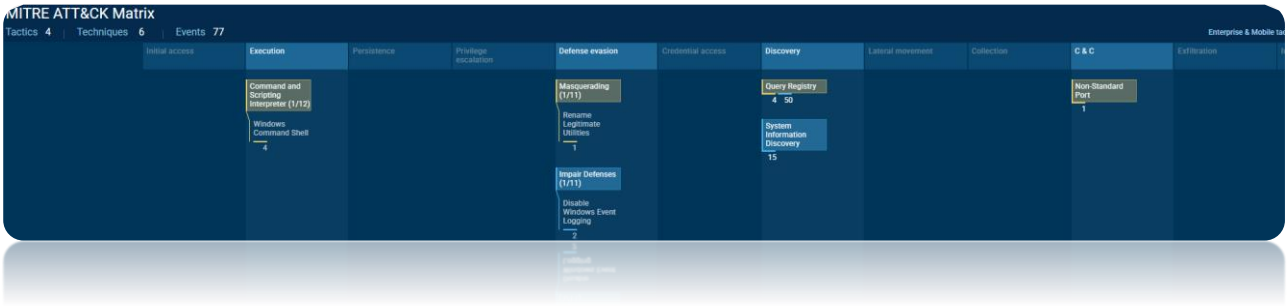
Studiare questo link di anyrun e spiegare queste minacce in un piccolo report.

https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/

L'analisi dinamica ha rilevato una catena di attacco complessa e altamente evasiva, progettata per eludere i sistemi di sandboxing e le difese basate su firma. La minaccia si è manifestata attraverso il **mascheramento di processi legittimi** e l'abuso di strumenti di sistema per l'esecuzione, il ritardo e la comunicazione con il dispositivo attaccante (**server di Command and Control**).

Il comportamento è coerente con un attaccante che cerca di stabilire una **persistenza furtiva** e di eseguire una ricognizione locale prima di procedere al download del payload finale.

Mappatura delle Tattiche e Tecniche di attacco (MITRE ATT&CK)



Execution
La minaccia ha ottenuto l'esecuzione abusando dei meccanismi di sistema
Windows Command Shell
L'entità malevola ha avviato **CMD.EXE** (PID 7520, 7876) per eseguire comandi in modo nativo sul sistema operativo. Questa azione è spesso il precursore del lancio di un payload di secondo stadio, di modifiche al registro o di un'iniezione di codice.
Esecuzione Binaria
L'entità ha abusato di un binario legittimo di Windows, **InstallUtil.exe** (PID 5152), per stabilire una connessione di rete e mascherare il traffico dannoso come traffico di un processo fidato.

Defense Evasion
La tattica più evidente è stata l'elusione delle difese e degli ambienti di analisi
Mascheramento
Il malware ha rilasciato e abusato dell'eseguibile legittimo **firefox.exe** (PID 6596) per mascherare la propria attività. Inoltre, i nomi dei file dannosi (Jvczfhe.exe, Muadnrd.exe) sono stati scelti casualmente per renderli difficilmente tracciabili con analisi basate su nome.
Ritardo nell'Esecuzione
L'utilizzo di **TIMEOUT.EXE** da parte di **cmd.exe** è una classica tecnica anti-sandbox. L'obiettivo è ritardare l'esecuzione del codice critico per superare il limite di tempo di esecuzione di un ambiente virtuale (sandbox), terminando così la sessione di analisi prima che venga eseguito il vero attacco.

Discovery
Il malware ha tentato di raccogliere informazioni sull'ambiente prima di procedere
Individuazione del Browser Web e Impostazioni di Fiducia
I processi Jvczfhe.exe e Muadnrd.exe hanno letto le impostazioni di sicurezza di Internet Explorer e verificato le Windows Trust Settings. Questo indica un tentativo di comprendere le policy di sicurezza in vigore per adattare i suoi moduli o per bypassare specifici controlli di sicurezza del browser.

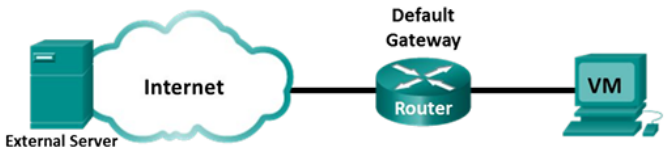
Command and Control
Il processo mascherato InstallUtil.exe ha avviato una connessione su una porta insolita. Questa connessione rappresenta molto probabilmente una backdoor utilizzata per ricevere ulteriori istruzioni o un payload di secondo stadio.

Indicatori di Compromissione
Nomi dei Processi Sospetti: Jvczfhe.exe, Muadnrd.exe.
Abuso di Binari Legittimi: firefox.exe, cmd.exe, TIMEOUT.EXE, InstallUtil.exe.
Attività Chiave: Connessione di rete da parte di InstallUtil.exe.
Comportamento: Auto-lancio di Muadnrd.exe (potenziale meccanismo di persistenza o tentativo di ripristino).

BONUS 1

Bonus 1: Esplorazione di Nmap

Topologia



Obiettivi

- **Parte 1: Esplorazione di Nmap**
- **Parte 2: Scansione delle Porte Aperte**

Contesto / Scenario

La scansione delle porte fa solitamente parte di un attacco di ricognizione. Esistono diversi metodi di scansione delle porte utilizzabili. Esploreremo come usare l'utility Nmap. Nmap è una potente utility di rete usata per la scoperta della rete e l'audit di sicurezza.

Risorse Richieste

- Macchina virtuale CyberOps Workstation
- Accesso a Internet

Cos'è Nmap?

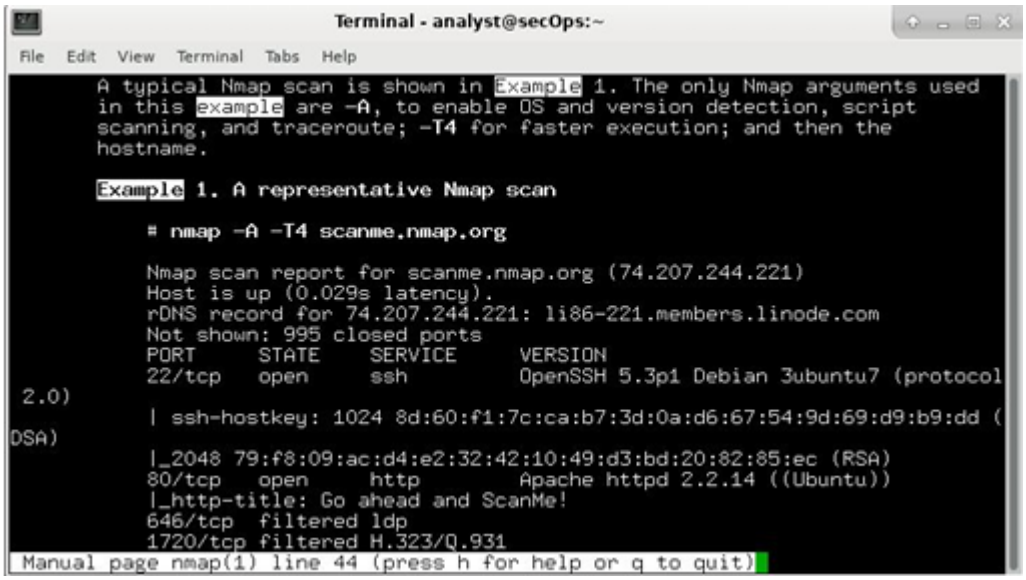
Nmap è uno strumento open source per l'esplorazione della rete e il controllo della sicurezza. Utilizza pacchetti IP grezzi in modi innovativi per determinare quali host sono disponibili sulla rete, quali servizi (nome e versione dell'applicazione) offrono tali host, quali sistemi operativi (e versioni del sistema operativo) stanno eseguendo, che tipo di filtri di pacchetti/firewall sono in uso, e decine di altre caratteristiche.

Per cosa viene usato nmap?

Nmap è comunemente usato per gli audit di sicurezza, molti sistemi e amministratori di rete lo trovano utile per attività di routine come l'inventario di rete, la gestione dei programmi di aggiornamento dei servizi e il monitoraggio del tempo di attività di host o servizi.

Qual è il comando nmap usato? (Vedi immagine)

Nmap -A -T4 scanme.nmap.org



Cosa fa l'opzione -A?

L'opzione -A abilità il rilevamento del sistema operativo con corrispettiva versione, la scansione degli script e il tracerout

Cosa fa l'opzione -T4?

L'opzione -T4 determina il **timing template**. Imposta automaticamente una serie di parametri temporali per rendere la scansione più o meno veloce e aggressiva. (Il suo valore di base è T3)

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

Le porte aperte sono la **21** e la **22**. I servizi aperti sono corrispettivamente **ftp** con versione **vsftpd 2.0.8** e **ssh** con versione **OpenSHH 10.0**

```
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 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
```

A quale rete appartiene la tua VM?

La rete appartenente alla mia Virtual Machine è 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 84762sec preferred_lft 84762sec
    inet6 fd17:625c:f037:2:a00:27ff:fe2f:87a7/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86372sec preferred_lft 14372sec
    inet6 fe80::a00:27ff:fe2f:87a7/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

Quanti host sono attivi?

La scansione rivela un solo un host attivo sulla rete

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.97 ( https://nmap.org ) at 2025-09-26 07:22 -0400
Service detection performed. Please report any incorrect results a
Nmap done: 256 IP addresses (1 host up) scanned in 84.91 seconds
```

Scansiona un server remoto. Quali porte e servizi sono aperti?

Le porte aperte sono 22, 80, 9929, 31337.

I servizi sono rispettivamente SSH, http, nping-echo e tcpwrapper

```
[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
```

Quali porte e servizi sono filtrati?

In questo caso nessuna porta è filtrata. Sono tutte aperte; lo possiamo notare seguendo l'indice "STATE"

Qual è l'indirizzo IP del server?

L'indirizzo IP del server è 45.33.32.156

Qual è il sistema operativo?

Il sistema operativo è Linux.

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 lo strumento fondamentale per la **ricognizione e la gestione della rete** dal punto di vista difensivo. Aiuta gli amministratori e i professionisti della sicurezza ad avere un quadro generale di cosa vedono gli attaccanti sulla rete interessata.

Per un **attore malevolo** (hacker, criminale informatico), Nmap è la prima fase di quasi ogni attacco informatico mirato. L'obiettivo è la **ricognizione attiva** per raccogliere informazioni dettagliate sul bersaglio. E' lo strumento perfetto per la ricognizione. Permette all'attaccante di avere una **"piantina" completa** e dettagliata (indirizzi IP, porte, servizi e versioni) dell'ambiente target, trasformando un obiettivo sconosciuto in un bersaglio con vulnerabilità note e sfruttabili.

BONUS 2

Bonus 2: Attacco a un database MySQL

Obiettivi

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

- **Parte 1:** Aprire Wireshark e caricare il file PCAP.
- **Parte 2:** Visualizzare l'attacco di SQL Injection.
- **Parte 3:** L'attacco di SQL Injection continua...
- **Parte 4:** L'attacco di SQL Injection fornisce informazioni di sistema.
- **Parte 5:** L'attacco di SQL Injection e le informazioni sulle tabelle
- **Parte 6:** L'attacco di SQL Injection si conclude.

Contesto / Scenario

Gli attacchi di SQL injection consentono agli hacker malintenzionati di digitare istruzioni SQL in un sito web e ricevere una risposta dal database. Ciò permette agli aggressori di manomettere i dati correnti nel database, falsificare identità e compiere varie azioni dannose.

È stato creato un file PCAP per consentirti di visualizzare un attacco precedente contro un database SQL. In questo laboratorio, visualizzerai gli attacchi al database SQL e risponderai alle domande.

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

I due IP coinvolti in questo attacco SQL injection sono 10.0.2.15 (vittima) e 10.0.2.4 (attaccante)

Qual è la versione?

La versione è 5.7.12-0 Ubuntu 1.1

```
                    </form>
                    <pre>ID: 1' or 1=1 union select null, version ()#<br />First name: admin<br />Surname: a
dmin</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' o
r 1=1 union select null, version ()#<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1 un
ion select null, version ()#<br />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select n
ull, version ()#<br />First name: <br />Surname: 5.7.12-0ubuntu1.1</pre>
            </div>
```

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

L'utente che ha l'hash della password è 1337

```
nion 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: 8d3533d75ae2c3966d7e0d4fcc69216b</pre><pre>ID: 1' or 1=1 union select u
ser, password from users#<br />First name: pablo<br />Surname: 0d107d09f5bbe40cade3de5c71e9e9b7</pre><pre>ID: 1' or 1=1 union select user, pa
ssword from users#<br />First name: smithy<br />Surname: 5f4dcc3b5aa765d61d8327deb882cf99</pre>
```

Qual è la password in chiaro?

La password in chiaro è **charley**

Domande di Riflessione

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

Il rischio principale dell'uso del linguaggio SQL nelle piattaforme è la **SQL Injection**, una tecnica di attacco che sfrutta le vulnerabilità nel codice dell'applicazione per iniettare istruzioni SQL malevole. Questo può portare a conseguenze disastrose per la sicurezza dei dati.

Le conseguenze di un attacco SQL Injection comprendono:

L'accesso non autorizzato ai dati

La modifica o cancellazione dei dati

Bypass autenticazione e compromissione dell'amministratore

In alcuni casi esecuzione di comandi sul sistema operativo

Quali sono 2 metodi o passaggi che possono essere adottati per prevenire gli attacchi di SQL injection?

Per prevenire la SQL Injection, non è sufficiente evitare il linguaggio SQL, ma è cruciale usare pratiche di codifica sicure.

- **Query parametrizzate (Prepared Statements):** Le query parametrizzate separano le istruzioni SQL dai dati di input, impedendo all'interprete del database di trattare l'input come codice SQL.
- **Validazione e Sanitizzazione dell'Input:** Rimuovere o neutralizzare i caratteri speciali prima che vengano passati a una query.
- **Principio del minimo privilegio:** Utilizzare account di database con privilegi limitati, in modo che un attacco riuscito non possa compromettere l'intero sistema o l'intero database.
- **Implementazione WAF:** Grazie all'aggiunta di un WAF sarà possibile ispezionare il contenuto del traffico HTTP/HTTPS e analizzare le richieste che arrivano all'applicazione web.