**S11/L5**

Parte 2: Esplorare i comandi del Prompt dei Comandi e di PowerShell.

Confronto output dei comandi: dir, ping, cd e ipconfig

**Dir (Prompt)**: elenca file e cartelle della directory attuale, mostrando data e ora di modifica, se si tratta di una directory (<DIR>) o un file (con relativa dimensione). In fondo, riassume numero di file, directory e spazio libero.

**Dir (PowerShell)**: Anche qui dir mostra file e cartelle, ma in formato tabellare. Indica tipo (es. d per directory), ultima modifica, dimensione e nome. È più dettagliato e basato su oggetti, tipico di PowerShell

**ping**: Serve a verificare se un host è raggiungibile in rete. Mostra pacchetti inviati/ricevuti/persi e i tempi di risposta. Output simile sia in Prompt dei comandi che in PowerShell.

**cd**: Cambia la directory corrente. Funziona allo stesso modo in entrambi gli ambienti, con identica sintassi e risultato.

**ipconfig**: Visualizza la configurazione di rete (IP, subnet, gateway, DNS). L’output è lo stesso in entrambi, poiché viene eseguito lo stesso eseguibile (ipconfig.exe).

Parte 3: esplorare i cmdIet

Il comando per dir è: Get-ChildItem

Parte 4: esplorare netstat

Il comando netstat ci permette di visualizzare le statistiche del protocllo e le connessioni di rete TCP/IP correnti.

Qual è il gateway IPv4?

Utilizzando netstat -r si identifica il gateway: 10.0.2.2

Parte 4:

**Informazioni dal PID in Gestione Attività**

Queste info aiutano a capire quale programma è legato al PID, chi lo esegue, dove si trova, quanto consuma e se è sicuro o aggiornato. Utile per analizzare o risolvere problemi legati ai processi.

* **Scheda *Dettagli***: Se selezioni un PID (es. 756), qui trovi info tecniche sul processo in esecuzione, come:
  + Nome del file eseguibile (es. chrome.exe)
  + PID, stato (es. in esecuzione), utente
  + Uso di CPU e memoria (sia privata che totale)
  + Descrizione, azienda, versione
  + Percorso del file e riga di comando usata per avviarlo
* **Finestra *Proprietà*** (clic destro > Proprietà):
  + **Generale**: tipo, dimensione, date, percorso
  + **Sicurezza**: permessi file (lettura, scrittura, esecuzione)
  + **Dettagli**: versione software, lingua, copyright
  + **Compatibilità**: opzioni per eseguirlo su vecchie versioni di Windows
  + **Versioni precedenti**: permette il ripristino, se disponibile

Immagine che contiene testo, schermata, software, numero

Il contenuto generato dall'IA potrebbe non essere corretto.

Parte 5: Svuotare il cestino usando PowerShell.

I file si cancella definitivamente, elimina il procedimento da interfaccia grafica.

PowerShell è molto utile per l’automazione delle attività ripetitive e il monitoraggio del sistema, specialmente nel campo della **cybersecurity**. Ecco alcuni comandi che un analista di sicurezza può usare per semplificare il proprio lavoro:

* **Get-Process**  
  Elenca tutti i processi in esecuzione. Utile per individuare attività sospette o non autorizzate.
* **Get-Service**  
  Mostra lo stato dei servizi Windows, incluso se sono attivi o disabilitati.
* **Get-EventLog**  
  Consente di leggere i log di sistema, applicazioni o sicurezza. Utile per tracciare accessi non autorizzati o errori.
* **Get-LocalUser / Get-LocalGroup**  
  Elenca utenti e gruppi locali. Aiuta a controllare la presenza di account sconosciuti o privilegiati.
* **Test-Connection**  
  Simile a ping, verifica la raggiungibilità di altri host nella rete.
* **Get-Command / Get-Help**  
  Ricerca di comandi disponibili e guida per ciascuno. Ideale per imparare velocemente nuove funzioni.
* **Get-FileHash**  
  Calcola l'hash di un file (es. SHA256) per verificare l'integrità o identificare malware.
* **Invoke-WebRequest**  
  Scarica contenuti da URL. Può essere usato anche per analizzare attività sospette in rete.
* **Set-ExecutionPolicy**  
  Gestisce i criteri di esecuzione degli script, importante per sicurezza e controllo degli script automatizzati.

Bonus 1: Esplorazione di Nmap

**Cos'è Nmap e a cosa serve**

**Nmap** (abbreviazione di *Network Mapper*) è uno strumento open source usato per la **scansione e l’analisi delle reti**. È ampiamente impiegato da amministratori di sistema e analisti di sicurezza per ottenere informazioni dettagliate su host e servizi presenti in una rete.

**A cosa serve Nmap:**

* **Scoprire host attivi**: identifica i dispositivi connessi e attivi su una rete.
* **Scansione delle porte**: individua quali porte sono aperte su un host e quali servizi stanno rispondendo.
* **Identificazione dei servizi**: determina il tipo e la versione dei servizi in esecuzione (es. server web, FTP, SSH).
* **Rilevamento del sistema operativo**: cerca di identificare il sistema operativo utilizzato su un determinato host.
* **Audit di sicurezza**: consente di trovare potenziali vulnerabilità, configurazioni errate o servizi non autorizzati.

**In sintesi**, Nmap è uno strumento potente e versatile per la **ricognizione, l’analisi di rete e la valutazione della sicurezza**, molto usato nel campo della cybersecurity.

Guarda l'Esempio 1.

1. Qual è il comando nmap usato?
2. Cosa fa l'opzione -A?
3. Cosa fa l'opzione -T4?

Comando usato: nmap -A -T4 [target]

Opzione -A: Aggressive scan

Attiva una serie di rilevamenti avanzati:

* **OS Detection** → prova a identificare il sistema operativo dell’host
* **Version Detection** → rileva la versione dei servizi attivi sulle porte
* **Script Scanning** → esegue alcuni script Nmap predefiniti (NSE) per raccogliere più info
* **Traceroute** → traccia il percorso di rete fino all’host

**(Timing template 4)**

Imposta la **velocità della scansione** su un livello "Aggressivo":

* **T4** è più veloce di default (T3) e più adatto su reti stabili o LAN
* Aiuta a completare le scansioni più rapidamente
* Ma potrebbe **generare più traffico** e far scattare allarmi su reti sensibili

Parte 2: Scansione delle Porte Aperte

Quali porte e servizi sono aperti?

Per ognuna delle porte aperte, registra il software che fornisce i servizi.

Output:

• Porta 21/tcp:

o Stato: open o Servizio: ftp

o Versione: vsftpd 2.0.8 or later

o Dettagli aggiuntivi: Permesso l'accesso FTP anonimo (Anonymous FTP login allowed).

• Altre porte: L'output mostra "Not shown: 996 closed ports", indicando che, oltre alla porta 21, non ci sono altre porte aperte visibili nell'output fornito

A quale rete appartiene la tua VM?

Utilizzando il comando ip address si trova che:

la VM appartiene alla rete 10.0.2.0/24

Subnet Mask: 255.255.255.0

Quanti host sono attivi?

Verificare quanti host sono attivi nella rete 10.0.2.0/24 e raccogliere informazioni dettagliate su di essi.

**Risultati**

* Sono stati analizzati **256 indirizzi IP** della subnet.
* È stato rilevato **1 host attivo** all’indirizzo IP **10.0.2.15**.

**Dettagli sull’host 10.0.2.15**

* **Porte aperte:**
  + Porta 21/tcp (FTP) con server vsftpd 2.0.8 o successivo
  + Porta 22/tcp (SSH) con OpenSSH 7.7
* **Servizi identificati:**
  + FTP con accesso anonimo consentito
  + SSH con protocolli di sicurezza aggiornati
* **Tempi di risposta:** molto rapidi (latency 0.000032s)
* **Passo 3 – Scansione di un server remoto**
* **a. Navigazione su scanme.nmap.org**
* Aprendo un browser e visitando il sito **scanme.nmap.org**, si trova un messaggio che spiega lo scopo del sito.
* **Scopo del sito:**  
  Scanme.nmap.org è un server messo a disposizione dagli sviluppatori di Nmap per consentire agli utenti di provare e testare legalmente lo strumento di scansione Nmap. È un ambiente pubblico dedicato alla pratica e all’apprendimento delle funzionalità di Nmap, senza rischi legali o di sicurezza.
* In sostanza, il sito offre un target sicuro e autorizzato per effettuare scansioni di rete e sperimentare i comandi Nmap

**Scansione Nmap su scanme.nmap.org**  
**Comando eseguito:** nmap -A -T4 scanme.nmap.org

**1. Indirizzo IP del server**

* **45.33.32.156**

**2. Porte e servizi aperti**

| **Porta** | **Stato** | **Servizio** | **Versione** | **Note** |
| --- | --- | --- | --- | --- |
| 22/tcp | Aperta | SSH | OpenSSH 6.6.1p1 Ubuntu | Protocollo 2.0 |
| 53/tcp | Aperta | DNS | dnsmasq 2.84rc2 |  |
| 80/tcp | Aperta | HTTP | Apache httpd 2.4.7 (Ubuntu) |  |
| 31337/tcp | Aperta | tcpwrapped | Servizio mascherato o personalizzato |  |

**3. Porte filtrate**

* 996 porte risultano **filtrate**, probabilmente bloccate da firewall o filtri di rete e quindi non rispondono alla scansione.

**4. Sistema operativo rilevato**

* **Linux** (kernel Linux)

**5. Analisi e riflessioni**

**Utilizzo di Nmap per la sicurezza della rete:**  
Nmap permette agli amministratori di rete di identificare dispositivi attivi, porte aperte e servizi in esecuzione, aiutando a individuare potenziali vulnerabilità e migliorare la sicurezza chiudendo porte non necessarie e aggiornando i software esposti.

**Uso malevolo di Nmap:**  
Nmap può essere utilizzato da attaccanti per mappare la rete, scoprire sistemi vulnerabili e preparare attacchi mirati. Per questo motivo, la sua scansione può essere considerata un’attività sospetta se effettuata senza autorizzazione.

Immagine che contiene testo, schermata, Carattere

Il contenuto generato dall'IA potrebbe non essere corretto.

BONUS 2:

Attacco a un database MySQL

Quali sono i due indirizzi ip:

10.0.2.4 (Destinatario)

10.0.2.15 (Attaccante)

Qual è la versione?

5.7.12-Oubuntu1.1

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

L’utente è: 1337



Qual è la password in chiaro?

La password in chiaro utilizzando CrackStation è: charley.

**Domande di Riflessione su SQL Injection**

**1. Qual è il rischio che le piattaforme utilizzino il linguaggio SQL?**  
Molti siti web e applicazioni si basano su database che utilizzano il linguaggio SQL per gestire dati e informazioni. Questo rende le piattaforme vulnerabili ad attacchi di SQL injection, in cui un aggressore può manipolare le query SQL per ottenere accesso non autorizzato, modificare dati o eseguire comandi dannosi. La gravità di questi attacchi dipende dalle capacità e dall’intento dell’aggressore, potendo portare a violazioni di dati, perdita di integrità o controllo del sistema.

**2. Metodi per prevenire attacchi di SQL injection**  
Dalla ricerca su Internet, i seguenti due metodi risultano tra i più efficaci per prevenire attacchi di SQL injection:

* **Filtrare e validare l’input dell’utente:** Assicurarsi che tutti i dati inseriti dall’utente siano controllati e puliti da caratteri o comandi potenzialmente dannosi prima di essere utilizzati nelle query SQL.
* **Utilizzare query parametrizzate o stored procedure:** Evitare di concatenare direttamente input dell’utente nelle query SQL. Invece, utilizzare parametri o stored procedure che separano il codice SQL dai dati, riducendo la possibilità di esecuzione di comandi malevoli.

Altri metodi utili includono:

* Implementare un firewall per applicazioni web (WAF) per bloccare richieste sospette.
* Disabilitare funzionalità non necessarie del database che possono essere sfruttate.
* Monitorare continuamente le istruzioni SQL per rilevare attività anomale.