Consegna S11-L5

Consegna: Windows PowerShell, Wireshark, Nmap, MySQL

⚜️ **Tag:** #powershell #wireshark #nmap #mysql #cybersecurity

Progetto S11/L5

Laboratorio 1: Utilizzo di Windows PowerShell

- In questo laboratorio, esplorerai alcune delle principali funzioni offerte da Windows PowerShell.
- **Obiettivi:**
  - Comprendere le funzionalità base e avanzate di PowerShell.

Guida e link: Windows PowerShell Lab Answers

Laboratorio 2: Analisi del traffico HTTP e HTTPS con Wireshark

- Utilizzerai Wireshark per catturare e analizzare il traffico di rete, distinguendo i protocolli HTTP e HTTPS.

Obiettivi:

- Catturare e visualizzare il traffico HTTP.
- Catturare e visualizzare il traffico HTTPS.

Guida e link: Wireshark HTTP and HTTPS Traffic Analysis

Bonus 1: Esplorazione di Nmap

- Scansione delle porte come parte di attività di riconoscimento.
- Analisi dei metodi principali di scansione offerti da Nmap.

Guida e link: Exploring Nmap Answers

Bonus 2: Attacco a un Database MySQL

- Visualizzazione di un file PCAP relativo a un attacco SQL su un database MySQL.

Obiettivi:

- Analizzare i file PCAP per comprendere le modalità di attacco contro database MySQL.

Guida e link: MySQL Database Attack Analysis

🔑 **Chiavi:** [powershell, wireshark, nmap, mysql, cybersecurity]