# Dia 2 – Conceitos Web e Nmap

## Objetivos do Dia

- Compreender HTTP e HTTPS

- Entender métodos GET e POST

- Conhecer headers e cookies

- Aprender o ciclo do pentest

- Executar Nmap para reconhecimento de portas e serviços

---

## 1️⃣ Conceitos Web

- \*\*HTTP / HTTPS\*\*

- HTTP: protocolo sem criptografia

- HTTPS: protocolo com SSL/TLS, protege dados

- \*\*Métodos HTTP\*\*

- GET: solicita dados do servidor (não altera)

- POST: envia dados para o servidor (formulários, login)

- \*\*Headers HTTP\*\*

- Ex.: User-Agent, Authorization, Cookie

- Útil para identificar vulnerabilidades e manipulação de sessões

- \*\*Cookies\*\*

- Armazenam informações de sessão

- Teste: alterar cookies para verificar controle de acesso

---

## 2️⃣ Ciclo do Pentest

1. Planejamento – definir escopo e objetivos

2. Reconhecimento – descobrir portas, serviços, URLs

3. Enumeração – coletar informações detalhadas do alvo

4. Exploração – testar vulnerabilidades

5. Pós-exploração – consolidar acesso e coletar dados

6. Relatório – documentar tudo

> Hoje focamos em \*\*reconhecimento e enumeração com Nmap\*\*

---

## 3️⃣ Ferramenta Nmap

\*\*Comandos utilizados:\*\*

```bash

nmap -F <IP\_da\_VM> # Scan rápido das portas mais comuns

nmap -p- <IP\_da\_VM> # Scan completo de todas as portas

nmap -sV -p22,80 <IP\_da\_VM> # Descobre versão dos serviços