1 - Vulnerabilidades: As Portas Abertas

Vulnerabilidades são falhas em sistemas, processos ou pessoas que podem ser exploradas por invasores. Elas são o ponto de partida de qualquer ataque cibernético.

Principais tipos:

- **Software:** Erros de programação ou falhas em validações, como *SQL Injection* e *buffer overflow*.
- **Configuração:** Configurações inseguras, como senhas padrão ou portas abertas sem necessidade.
- **Humana:** Falhas causadas por descuido ou falta de treinamento, como clicar em links falsos ou usar a mesma senha em vários sistemas.

2. Tipos e Técnicas de Ataque

Ataques exploram vulnerabilidades para obter acesso, roubar dados ou causar danos.

- Engenharia Social

- **Phishing:** E-mails ou mensagens falsas que se passam por empresas legítimas para roubar senhas e dados, basicamente explora o erro humano por meio da manipulação psicológica.

Malware (Software Malicioso)
Programas criados para invadir ou danificar sistemas.

- **Ransomware:** Bloqueia arquivos e exige pagamento para liberá-los.
- **Spyware:** Espiona o usuário, capturando senhas, teclas digitadas e histórico de navegação.

Ataques a Aplicações Web
Exploram falhas em sites e sistemas online.

- **SQL Injection:** Inserção de comandos maliciosos em formulários para acessar ou alterar bancos de dados.

Ataques de Rede
Afetam servidores e conexões.

- **DDoS:** Inunda um servidor com tráfego falso, derrubando o serviço.

3. A Motivação do Cracker

Diferente do *hacker ético*, o *cracker* age com intenções maliciosas. Suas principais motivações são:

- **Financeira:** Roubo de dinheiro, venda de dados ou extorsão com ransomware.
- **Espionagem:** Busca por segredos corporativos, políticos ou militares.
- **Hacktivismo:** Ataques por razões ideológicas ou de protesto.
- **Desafio ou vingança:** Motivação pessoal, busca por fama ou retaliação contra empresas e ex-empregadores.