

Categorias de Vulnerabilidades:

- **Tecnológicas:** Deficiências em softwares, como:
 - Injeção de comandos (SQL Injection)
 - Estouro de memória (Buffer Overflow)
- **Operacionais:** Configurações inadequadas, como:
 - Uso de senhas padrão
 - Portas de rede abertas sem necessidade
- **Comportamentais:** Erros humanos, como:
- Clicar em links suspeitos
- Reutilizar senhas em diferentes plataformas

2. Estratégias de Invasão Digital

Os ataques cibernéticos utilizam essas falhas para invadir sistemas, extrair informações ou causar prejuízos.

Manipulação Psicológica

- **Phishing:** Mensagens fraudulentas que simulam comunicações legítimas para enganar usuários e obter dados confidenciais.

Programas Maliciosos (Malware)

- **Ransomware:** Criptografa arquivos e exige pagamento para desbloqueio.
- **Spyware:** Monitora atividades do usuário e coleta informações como senhas e histórico de navegação.

Exploração de Sistemas Web

- **Injeção SQL:** Inserção de comandos maliciosos em campos de entrada para manipular bancos de dados.

Ataques à Infraestrutura de Rede

- **DDoS (Negação de Serviço Distribuída):** Sobrecarrega servidores com tráfego falso, tornando o serviço indisponível.

3. O Que Move o Cracker

Ao contrário do hacker ético, o cracker atua com intenções prejudiciais. Suas motivações incluem:

Motivações Comuns:

- **Lucro Financeiro:** Roubo de valores, venda de dados ou extorsão digital.
- **Espionagem:** Obtenção de informações sigilosas de empresas, governos ou instituições militares.
- **Ativismo Digital (Hacktivismo):** Ataques motivados por causas ideológicas ou sociais.
- **Desafios Pessoais ou Vingança:** Busca por notoriedade ou retaliação contra organizações ou indivíduos.

Se quiser, posso transformar esse conteúdo em slides, um guia visual ou até um quiz interativo para facilitar o aprendizado.