Matrix Hacker - Aula 4

O MAPA PRA SE TORNAR UM GUARDIÃO HACKER

MATRIX
HACKER

MATRIX HACKER

Teste de Intrusão de Site com Kali Linux

Aqui estão as instruções detalhadas sobre como usar o Nmap, Gobuster e SQLmap no Kali Linux para executar testes de segurança em um site.

1. Nmap

O Nmap é uma ferramenta poderosa para escanear redes e descobrir portas abertas, serviços e vulnerabilidades.

Passos para usar o Nmap

1. Escaneamento Básico
   sudo nmap example.com

2. Escaneamento de Portas Específicas
   sudo nmap -p 80,443 example.com

3. Escaneamento Completo (Todos os 65535 Portas)
   sudo nmap -p- example.com

4. Detecção de Sistema Operacional e Versão do Serviço
   sudo nmap -A example.com

5. Escaneamento de Vulnerabilidades
   sudo nmap --script vuln example.com

2. Gobuster

Gobuster é uma ferramenta para força bruta de URLs e descoberta de diretórios.

· Passos para usar o Gobuster

1. Diretórios com Lista de Palavras Padrão
gobuster dir -u http://example.com -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

2. Diretórios com uma Lista de Palavras Personalizada
gobuster dir -u http://example.com -w /caminho/para/sua/wordlist.txt

3. Especificando Extensões de Arquivos
gobuster dir -u http://example.com -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt

Exemplos de Uso do Gobuster

- Descobrir Subdomínios
gobuster dns -d example.com -w /usr/share/wordlists/dns/subdomains-top1million-5000.txt

- Diretórios em HTTPS
gobuster dir -u https://example.com -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

3. SQLmap

SQLmap é uma ferramenta para detectar e explorar vulnerabilidades de injeção SQL.

Passos para usar o SQLmap

1. Testar uma URL Específica para Vulnerabilidade SQL

```
sqlmap -u "http://example.com/page.php?id=1"
```

2. Verificar e Enumerar Bancos de Dados

```
sqlmap -u "http://example.com/page.php?id=1" --dbs
```

3. Selecionar um Banco de Dados e Verificar Tabelas

```
sqlmap -u "http://example.com/page.php?id=1" -D nome_do_banco --tables
```

4. Selecionar uma Tabela e Verificar Colunas

```
sqlmap -u "http://example.com/page.php?id=1" -D nome_do_banco -T nome_da_tabela --columns
```

5. Extrair Dados de uma Tabela Específica

```
sqlmap -u "http://example.com/page.php?id=1" -D nome_do_banco -T nome_da_tabela -C nome_da_coluna --dump
```

MATRIX HACKER

Considerações Finais

- Permissão e Ética: Certifique-se de ter permissão explícita para realizar esses testes no site em questão.
- Documentação: Mantenha um registro detalhado de todos os testes realizados, vulnerabilidades encontradas e recomendações de mitigação.

Essas ferramentas são extremamente poderosas e podem fornecer insights valiosos sobre a segurança de um site. Use-as com responsabilidade e sempre respeitando as leis e diretrizes éticas.

FAZER MINHA INSCRIÇÃO

⚠️ Liberamos mais um Lote de 15 vagas que receberão de bônus a Mentoria Profissional Hacker - com acompanhamento de 3 meses e encontros ao vivo quinzenais com o Professor Robson. De R$3.000 – Corre que já estão acabando [Últimas 5 Vagas da mentoria disponíveis]

Acesse o link abaixo e faça sua inscrição agora. 👇🏻

FAZER MINHA INSCRIÇÃO