Criação de um Plano de Invasão:

1. Encontrar Falhas no Site do Detran MA:

- **Ferramenta: NMAP**
  - ✓ Use o NMAP para realizar um scan no site para identificar portas abertas e serviços rodando. Exemplo de comando:

```
nmap -sV -T4 detran.ma.gov.br
```

- **Ferramenta: NIKTO**
  - ✓ Utilize o NIKTO para identificar vulnerabilidades web específicas. Comando:

```
nikto -h detran.ma.gov.br
```

2. Elaborar um Plano de Invasão:

- Categorize as vulnerabilidades encontradas com NMAP e NIKTO, determinando quais são exploráveis para acesso ou extração de dados.

Primeiro Tipo de Ataque (Engenharia Social):

1. Metodologia dos Antivírus para E-mails:

- Discuta como os antivírus identificam e categorizam e-mails como spam com base em assinaturas de malware, URLs suspeitas e análise de comportamento.

2. Coletar E-mails Expostos no Site do Detran MA:

- **Ferramenta: GOBUSTER**
  - ✓ Use GOBUSTER para descobrir diretórios e arquivos que possam conter informações de contato. Comando:

```
gobuster dir -u http://detran.ma.gov.br -w /usr/share/wordlist/dirbuster/directory-list-2.3-medium.txt
```

3. Elaborar uma Engenharia Social sob Medida:

- Crie um e-mail ou página web falsa com HTML e CSS que imite comunicações legítimas do Detran, mas contendo links que direcionem para um site controlado por você usando setoolkit.

Segundo Tipo de Ataque (Exploração de Vulnerabilidade):

1. Scan no Site:

- **Ferramenta: SSLYZE**
  - ✓ Verifique a configuração SSL/TLS do site para identificar falhas usando SSLYZE:

```
sslyze --regular detran.ma.gov.br
```

2. Identificação de Subdomínios e Diretórios:

1. Identificação de Subdomínios:

- **Ferramenta: Sublist3r**

Sublist3r é uma ferramenta de reconhecimento popular usada para encontrar subdomínios de um domínio principal. Ela combina várias fontes, incluindo motores de busca e serviços como VirusTotal e DNSdumpster.

Exemplo de Comando:

```
sublist3r -d detran.ma.gov.br
```

Este comando executa a ferramenta Sublist3r para descobrir subdomínios associados ao domínio principal **detran.ma.gov.br**.

- **Ferramenta: Amass**

Amass é outra ferramenta poderosa para mapeamento de rede que realiza enumeração de DNS para identificar subdomínios.

Exemplo de Comando:

```
amass enum -d detran.ma.gov.br
```

Este comando irá procurar subdomínios ativos associados ao domínio principal usando várias técnicas, incluindo scraping de DNS e consultas a bancos de dados públicos.

2. Identificação de Diretórios:

- **Ferramenta: DirBuster**

DirBuster é uma ferramenta multi-threaded de aplicação web que usa uma lista de palavras para encontrar diretórios e arquivos existentes em um servidor web.

Exemplo de Comando:

```
java -jar DirBuster-1.0-RC1.jar -u http://detran.ma.gov.br -l /path/to/wordlist.txt -t 100
```

Este comando inicia a ferramenta DirBuster, apontando para o site alvo e utilizando uma lista de palavras específica para tentar descobrir diretórios e arquivos. O parâmetro **-t** define o número de threads para acelerar o processo.

- **Ferramenta: GOBUSTER**

GOBUSTER é uma ferramenta escrita em Go que utiliza "bruteforce" para encontrar diretórios e arquivos escondidos em um servidor web, além de ser capaz de descobrir subdomínios.

Exemplo de Comando para Diretórios:

```
gobuster dir -u http://detran.ma.gov.br -w /path/to/dir-list.txt -x php,html,txt -t 50
```

Este comando configura o GOBUSTER para buscar diretórios no site **http://detran.ma.gov.br** usando uma lista de palavras e especificando extensões de arquivo (**-x**) para buscar. O parâmetro **-t** controla o número de threads.

3. Identificação de Vulnerabilidades:

- Use scripts de vulnerabilidade do NMAP para identificar falhas específicas:

```
nmap --script vuln detran.ma.gov.br
```

Confecção da Documentação:

1. Elaborar o Plano de Invasão:

- Documente todas as etapas, desde a pesquisa inicial até os métodos de ataque propostos, categorizando-os por tipo de vulnerabilidade e potencial impacto.

2. Organizar o Documento por Etapas e Categorias:

- Separe a documentação em duas grandes seções: Engenharia Social e Exploração de Vulnerabilidades, detalhando os métodos, ferramentas usadas e resultados esperados.