Como solicitado, foi criado um phising para captura de senha do Facebook

Foi usado o software Kali Linux, na máquina virtual VirtualBox.

Obs.: algumas dificuldades foram encontradas no caminho pois a configuração de yrede que o professor ensinou não funcionou para mim, daí fui testando outras configurações e deu certo.

Passo 1

Foi usado o comando sudo su para permissões de admin: **sudo**: Dá permissões temporárias de administrador para executar um único comando como superusuário. **su**: inicia uma sessão como outro usuário, por padrão o usuário root.

Tela de computador com fundo azul

Descrição gerada automaticamente com confiança média

Senha da máquina, solicitado ao usar o comando acima;

Tela de computador com fundo azul

Descrição gerada automaticamente

* O comando **setoolkit**: usado para iniciar o **Social-Engineer Toolkit (SET)**, uma ferramenta poderosa de engenharia social projetada para criar ataques simulados. Ela é muito utilizada em testes de segurança para identificar vulnerabilidades relacionadas ao fator humano em sistemas e redes.

1. Nessa parte é mostrado alguns números de menu para selecionar a função qual vai ser utilizada.   
   O primeiro foi o número 1; já que estamos trabalhando com Engenharia Social.

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

* **Social-Engineering Attacks**. um conjunto de técnicas e ferramentas projetadas para explorar vulnerabilidades humanas, simulando ataques de engenharia social. Esse menu é usado para realizar testes de penetração e treinar organizações contra ameaças baseadas no fator humano.

Passo 2 – **Website Attack Vectors**

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

. uma coleção de ataques voltados para a exploração de vulnerabilidades em sites ou para a realização de ataques baseados na web. É amplamente usado em simulações de segurança e testes de penetração (pentest). Ele permite que os atacantes éticos realizem vários tipos de ataques para avaliar a segurança de sistemas e treinamentos contra phishing. Explora fraquezas em navegadores, criando sites falsos ou maliciosos para coletar informações ou executar exploits.

Objetivo: Realizar phishing ou ataques baseados na web.

Exemplo: Clonar uma página de login para capturar credenciais.

Passo 3 - **Credential Harvest Attack Method/ Método de Coleta de Credenciais**

**Clonagem do site.** O SET clona um site real, como uma página de login, para criar uma cópia idêntica.

**Captura de dados**: Quando a vítima insere informações (como usuário e senha), essas credenciais são capturadas e armazenadas pelo SET.

**Redirecionamento opcional**: Após a captura, a vítima pode ser redirecionada para o site real para minimizar suspeitas.

Obs.: Capturar credenciais sem permissão é ilegal e pode acarretar sérias consequências legais.

Logo depois vem uma explicação sobre como funciona a Credendial. Em seguida, no menu disponível, vem opções para selecionar qual tipo de origem da página falsa vai ser clonado.

Terá três opções:

1. **Web Templates**: Use modelos de sites pré-configurados no SET.
2. **Site Cloner**: Clona um site real, como Gmail, Facebook etc.
3. **Custom Import**: Permite importar um arquivo HTML personalizado.

Foi usado a opção 2 – site clonerTela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

1. Em seguida é solicitado o endereço de IP do servidor, qual vai ser hospedado a página
2. Digite a URL https://www.facebook.com quando solicitado.
3. Após configurar, o SET iniciará um servidor HTTP e exibirá logs em tempo real das credenciais capturadas, essa exibição a

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

Tela de computador

Descrição gerada automaticamente com confiança média