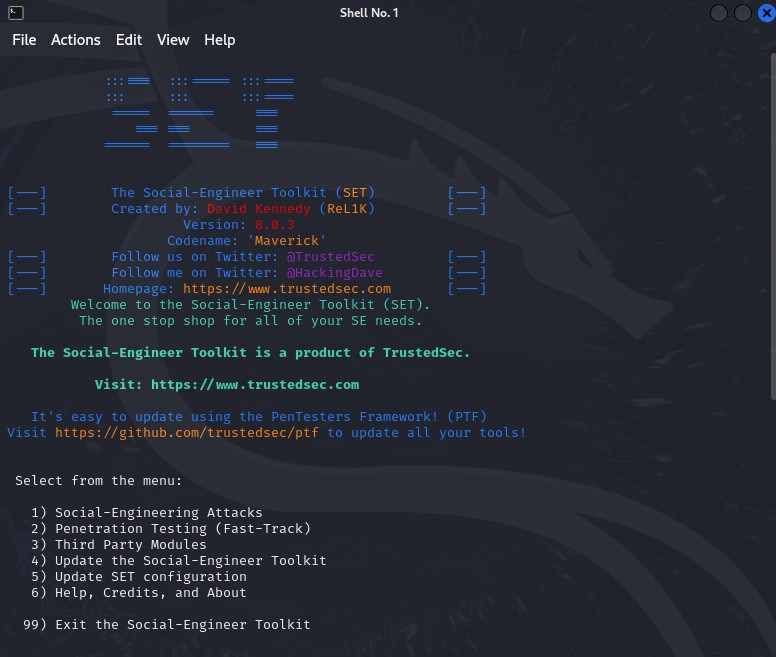
# Metodologia

Realizado através da utilização do software de virtualização Oracle VM VirtualBox 7.0, executando o sistema operacional Kali Linux 2024, uma distribuição Linux de código aberto baseada em Debian, para uso do *Social- Engineer Toolkit (SET)* versão 8.0.3, uma vez que a ferramenta já vem pré-instalada nesse sistema operacional. O objetivo principal foi avaliar e demonstrar a facilidade de utilização do *Social-Engineer Toolkit (SET)* para realização de ataques *phishing* e clonagem de sites.

O *Social-Engineer Toolkit (SET)* é uma ferramenta desenvolvida por David Kennedy, fundador da empresa *TrustedSec*. É um software de código aberto baseada em *Python* amplamente reconhecida e utilizada pela sua versatilidade e pela variedade de técnicas que oferece para simular ataques realistas. Ela é uma ferramenta muito utilizada por profissionais de segurança para avaliarem a segurança de sistemas, redes e indivíduos, explorando vulnerabilidades por meio de técnicas de manipulação psicológica e social, técnica conhecida como engenharia social. A engenharia social é um dos ataques mais difíceis de se proteger e um dos mais prevalentes na atualidade. O software possui mais de 2 milhões de *downloads* e é amplamente utilizado, possuindo forte suporte na comunidade de segurança. O programa é pré- instalado por padrão no Kali Linux, no entanto, também é possível fazer o *download* e instalá- lo diretamente caso não esteja instalado através do repositório do GitHub (TRUSTEDSEC, 2023). Observa-se na Figura 1 a tela inicial do software.

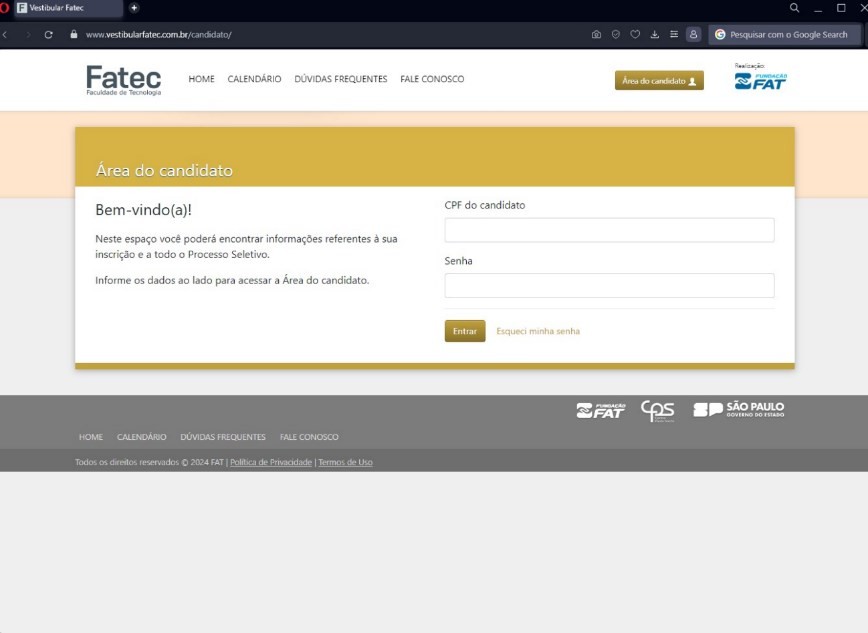
Figura 1. Apresentação do *Social-Engineer Toolkit (SET)*

**

# Resultados e Discussões

Para a realização da parte prática, iniciou-se com a etapa de clonagem de um site alvo. O site escolhido como alvo para demonstrar a técnica de clonagem foi o site do vestibular da própria instituição de ensino da FATEC, disponível no link "https://[www.vestibularfatec.com.br/candidato/](http://www.vestibularfatec.com.br/candidato/)".

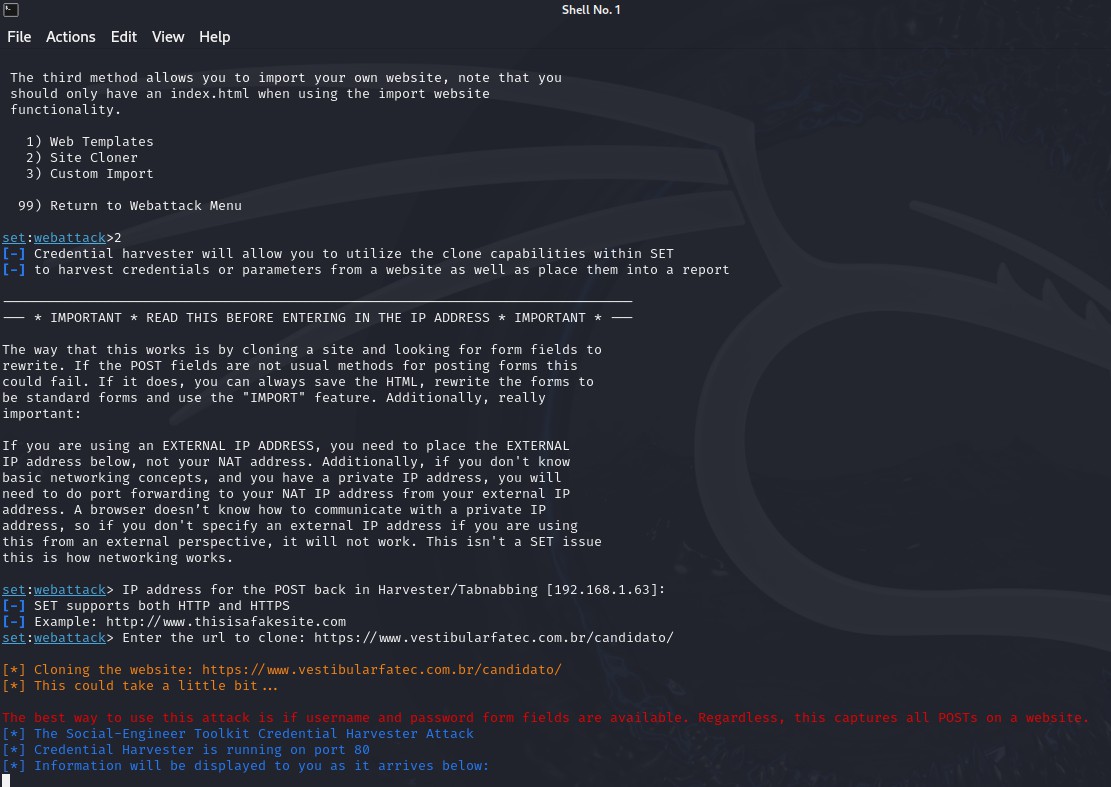
Figura 2. Site Alvo



Conforme demonstrado na Figura 2, é possível confirmar a autenticidade do site em questão ao analisar detalhes cruciais, tais como a URL (*Uniform Resource Locator*) e a presença de um certificado digital, que tem por objetivo autenticar o proprietário do site e assegurar uma comunicação segura, confiável e criptografada entre o navegador do usuário e o servidor, garantindo uma confiabilidade do processo de comunicação e troca de informação.

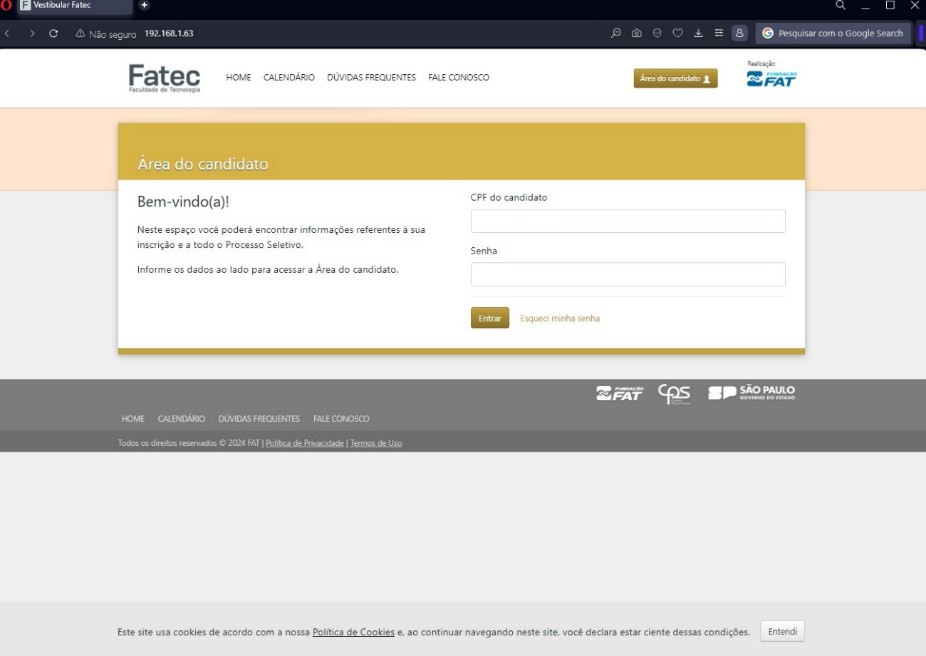
Escolhendo a opção *“Social-Engineering Attacks”* disponível no *Social-Engineer Toolkit (SET)*, procedeu-se à clonagem do site alvo, utilizando a opção *“Website Attack Vectors*”, seguida da opção *“Credential Harbester Attack Method*” e selecionando o *“Site Cloner*”*,* conforme ilustrado na Figura 3. Os parâmetros passados foram o endereço IP para o *POST Back* e a URL do site alvo.

Figura 3. Processo de Clonagem do Site-Alvo



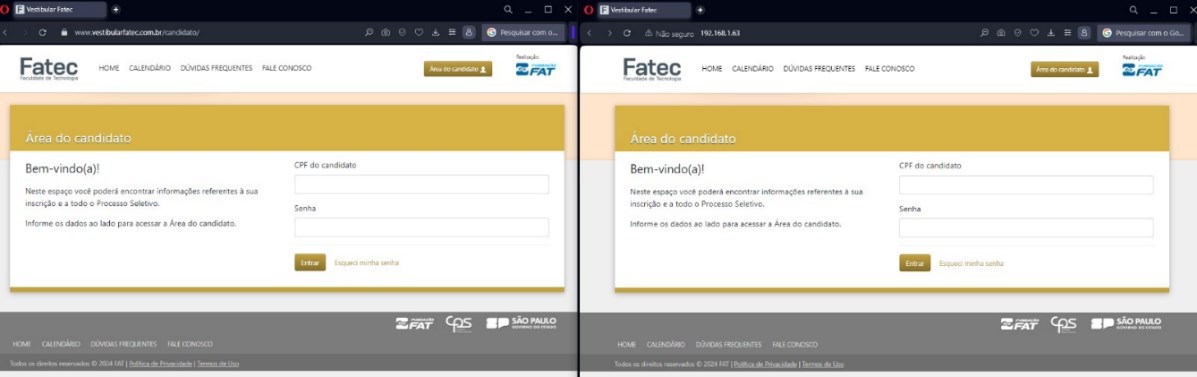
O acesso à página falsa foi feito através do IP da Máquina Kali, 192.168.1.63, conforme a Figura 4, devido ao teste ter sido conduzido internamente na rede, sem exposição à Internet. Em um ambiente real, caso um invasor tenha acesso à rede interna de uma organização, técnicas como manipulação de arquivos DNS poderiam redirecionar um usuário para o site falso utilizando o próprio domínio ou poderia configurar a ferramenta para redirecionar o tráfego para um servidor externo, permitindo assim a obtenção de credenciais e tornando o ataque mais sofisticado, no entanto, este último exemplo requer uma configuração mais complexa.

Figura 4. Réplica do site-alvo



A Figura 5 apresenta um comparativo dos sites onde o lado esquerdo representa o site original do Vestibular da FATEC e o lado direito representa o site clonado pela ferramenta.

Figura 5. Comparação site Original e Falso



É evidente que há uma alta semelhança entre o site original e sua versão clonada, sendo a URL e a ausência de um certificado digital os únicos elementos distintos entre os dois. Ao acessar o site falso e tentar fazer login com uma credencial falsa para fins de teste, a ferramenta SET capturou tanto o nome de usuário, no caso, um CPF gerado aleatoriamente, quanto a senha, como ilustrado na Figura 6. Os dados capturados foram mostrados diretamente no terminal da ferramenta.

Figura 6. Sucesso na obtenção as credenciais

