****Universidade Federal Rural de Pernambuco  
Sistemas de Informação  
  
  
  
  
  
  
  
Segurança e Auditoria de Sistemas   
  
Lhaíslla Eduarda Cavalcanti Rodrigues da Silva  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
RECIFE-PE

2023

Ataque Applet

## **Requisitos**

Para esta atividade serão necessários o sistema operacional Kali linux para executar os ataques eo sistema operacional windows 7 o qual será monitorado os acessos à web dos sistema operacional.

* Kali linux
* social engineering toolkit(root)
* windows 7
* Java

## Configuração windows 7

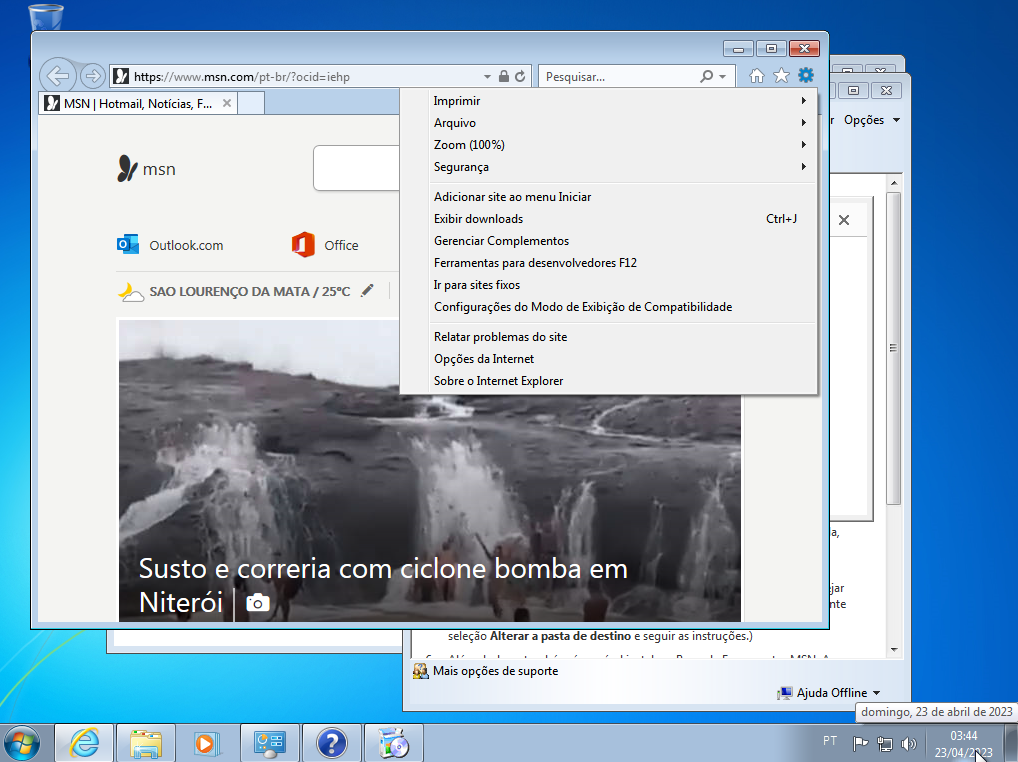
Acessar o painel de controle

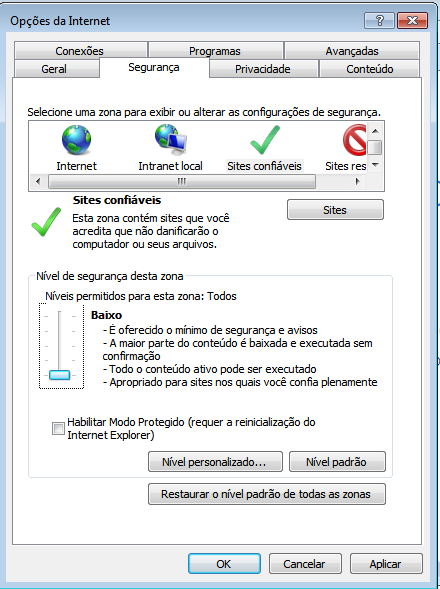
## 

* Inicializar o internet explorer
* Habilitar a regra de segurança do internet explorer: “Inicializar e executar scripts de controle activex não marcados como seguros”

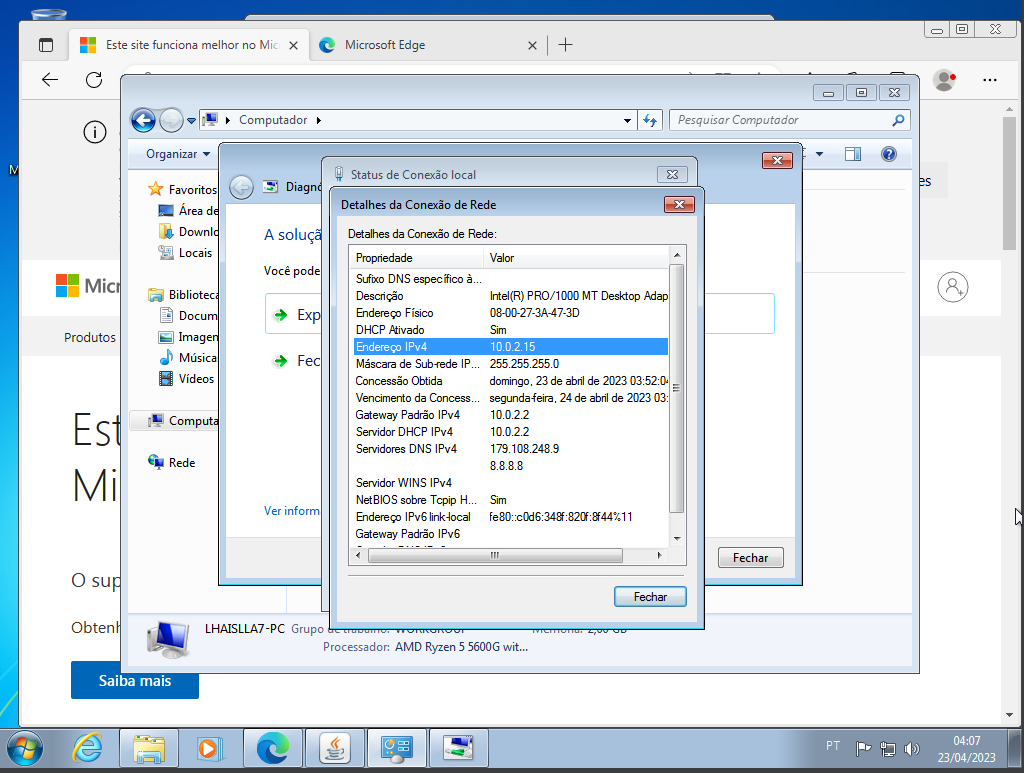
##### **Internet Explorer**

* + - Clique em **Ferramentas** e, em seguida, em **Opções de Internet**
    - Selecione a guia **Segurança** e clique no botão **Nível Personalizado**
    - Percorra a lista até **Scripts Java**
    - Verifique se o botão de opção **Ativar** está selecionado
    - Clique em **OK** para salvar sua preferência

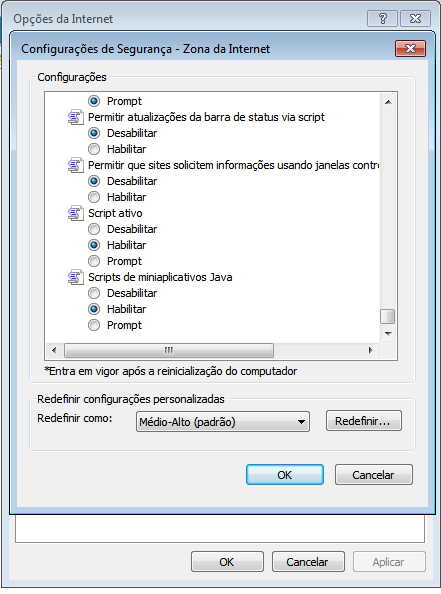




Verificar endereço IP da máquina:

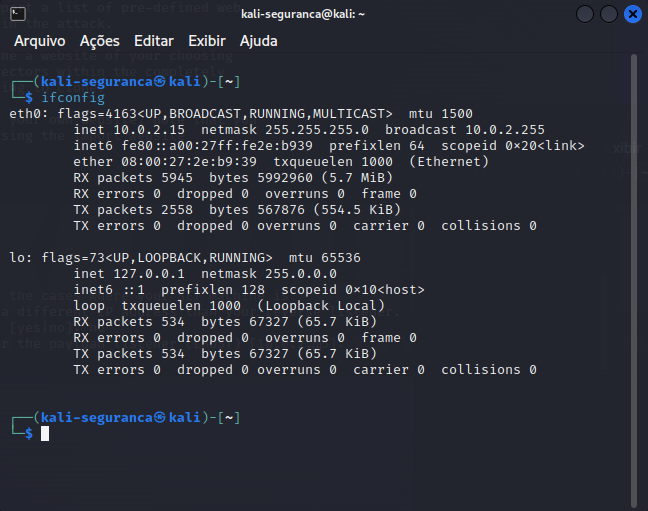


Ir na aba de segurança do Java e adicionar o IP da máquina e confirmar.

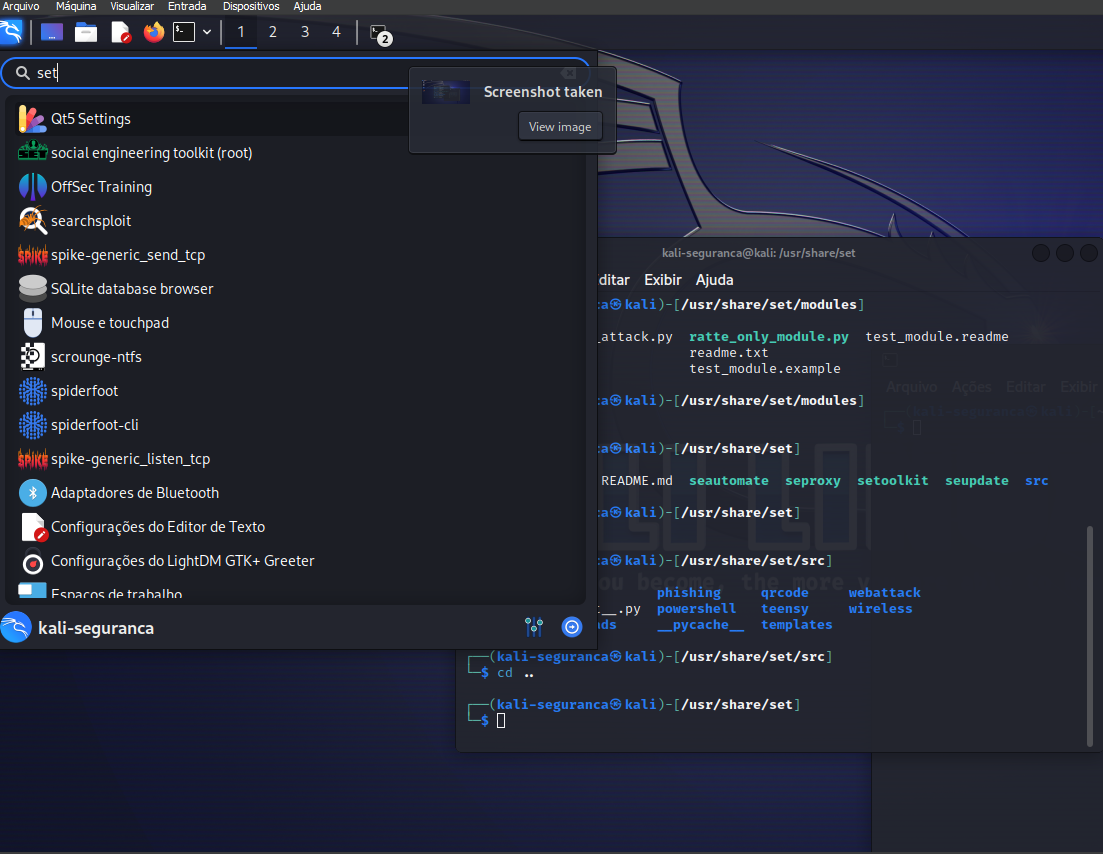


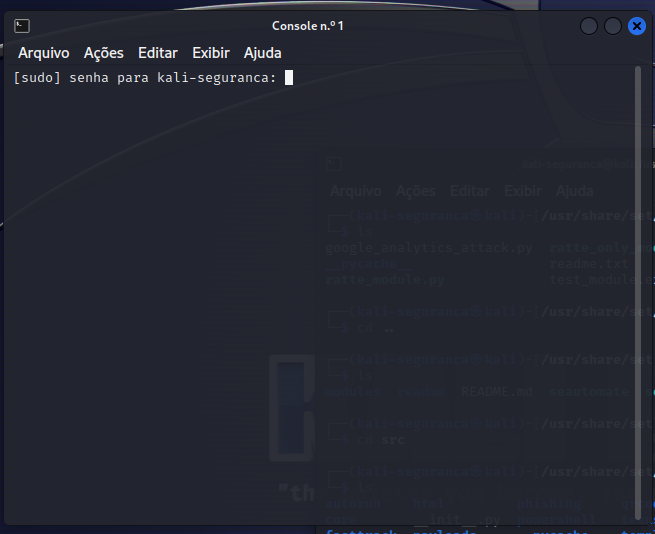
## **Execução do ataque**

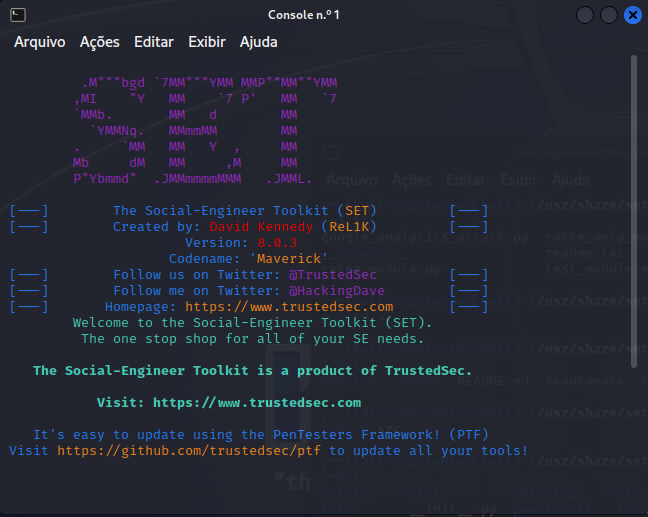
Verificando o Ip da máquina

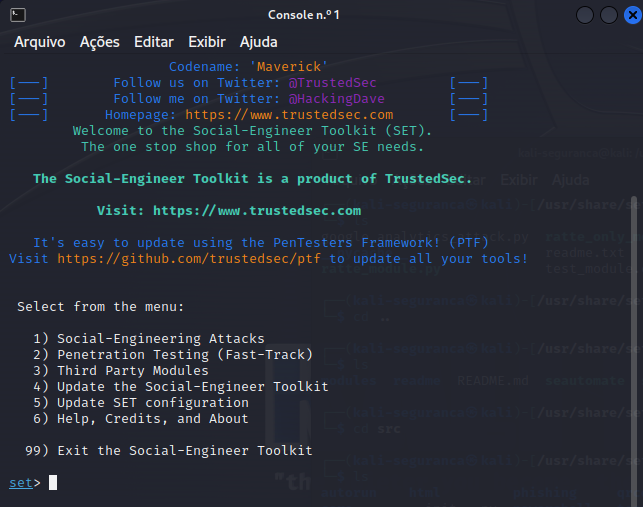


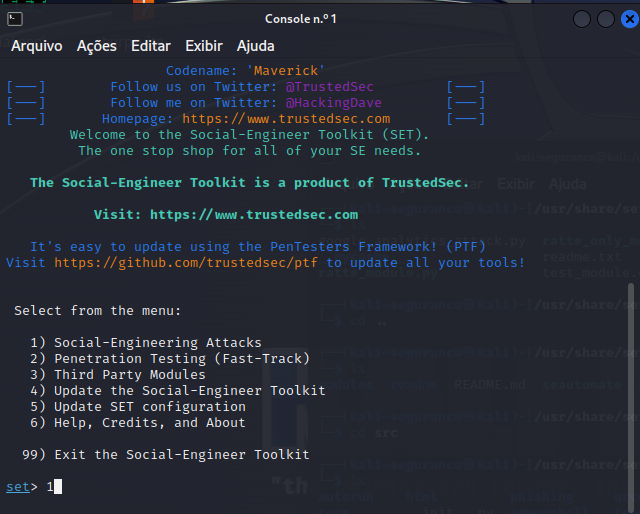
Acessando a aplicação do kali linux para realizar o ataque

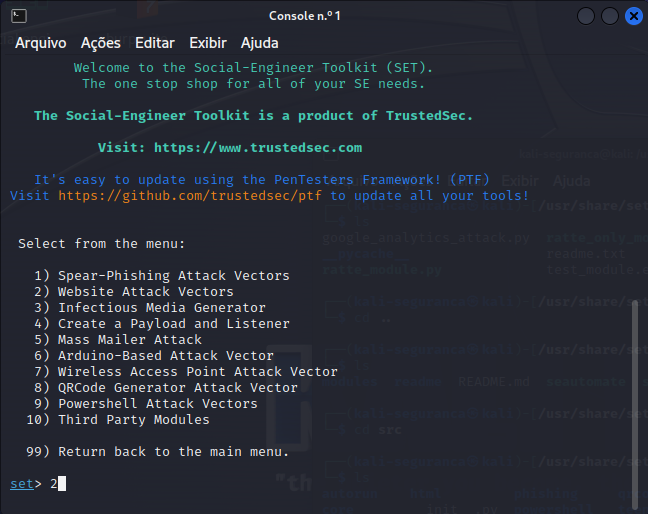


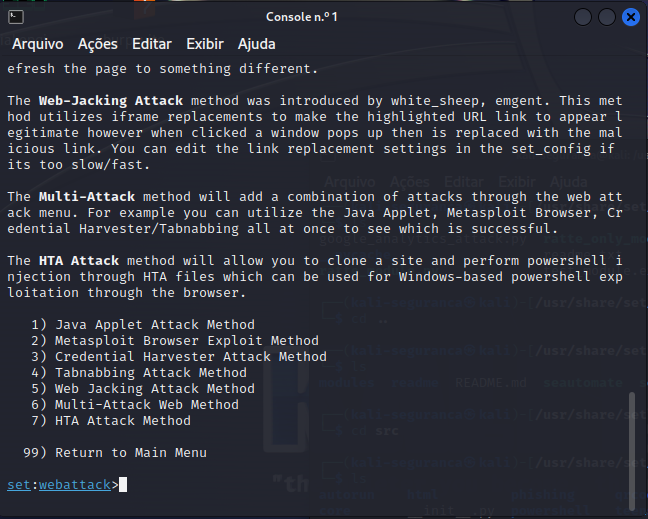


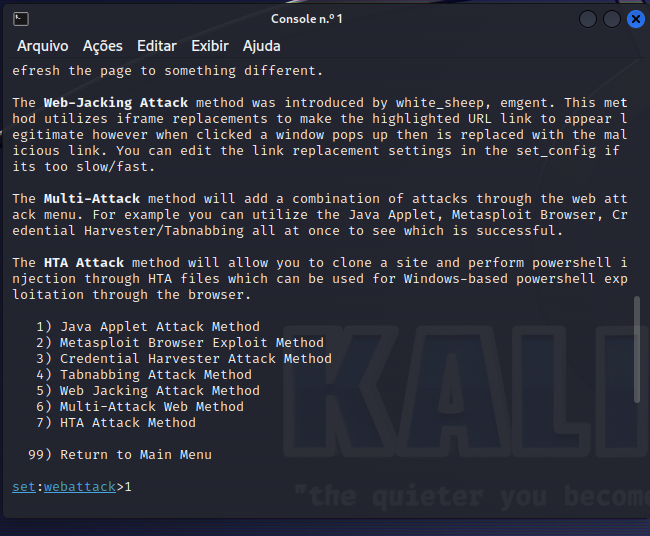












Selecionando attack Applet

O módulo Web Attack é uma maneira única de utilizar vários ataques baseados na Web para comprometer a vítima pretendida.

O método Java Applet Attack falsificará um certificado Java e fornecerá uma carga útil baseada em metasploit. Usa um applet java personalizado criado por Thomas Werth para entregar a carga útil.

O método Metasploit Browser Exploit utilizará exploits de navegador Metasploit selecionados por meio de um iframe e fornecerá uma carga útil do Metasploit.

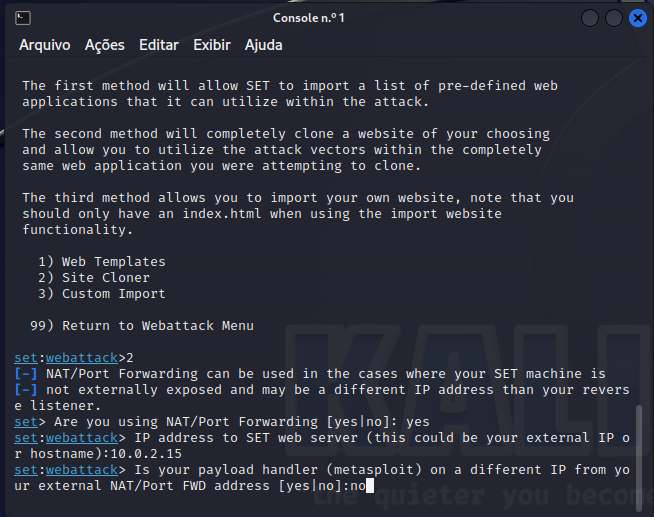
O método Credential Harvester utilizará a clonagem da Web de um site que possui um campo de nome de usuário e senha e colherá todas as informações postadas no site.

O método TabNabbing aguardará que um usuário vá para uma guia diferente e, em seguida, atualize a página para algo diferente.

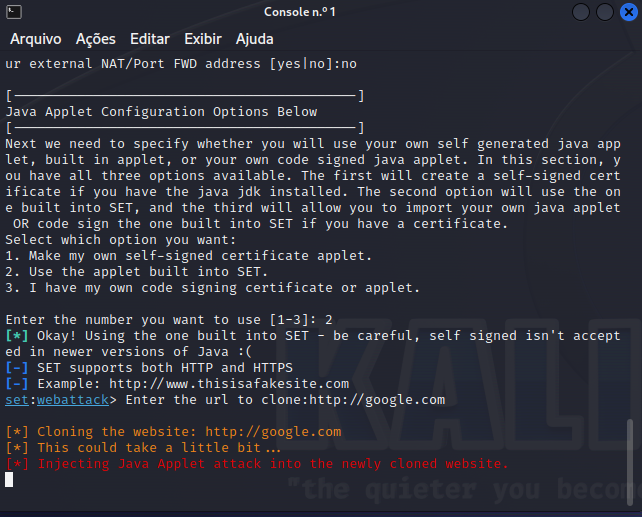
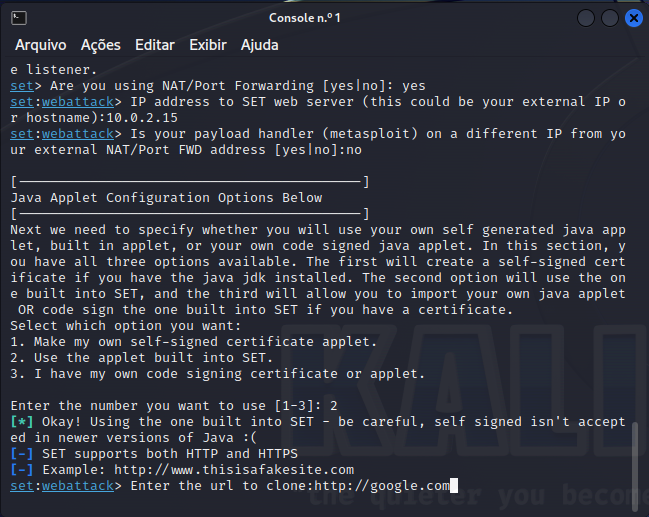
O método Web-Jacking Attack foi introduzido por white\_sheep, emgent. Este método utiliza substituições de iframe para fazer com que o link de URL realçado pareça legítimo. No entanto, quando clicado, uma janela aparece e é substituída pelo link malicioso. Você pode editar as configurações de substituição do link no set\_config se for muito lento/rápido.

O método Multi-Attack adicionará uma combinação de ataques através do menu de ataque da web. Por exemplo, você pode utilizar o Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing de uma só vez para ver qual é bem-sucedido.

O método de ataque HTA permitirá que você clone um site e execute injeção de powershell por meio de arquivos HTA, que podem ser usados ​​para exploração de powershell baseada em Windows por meio do navegador.

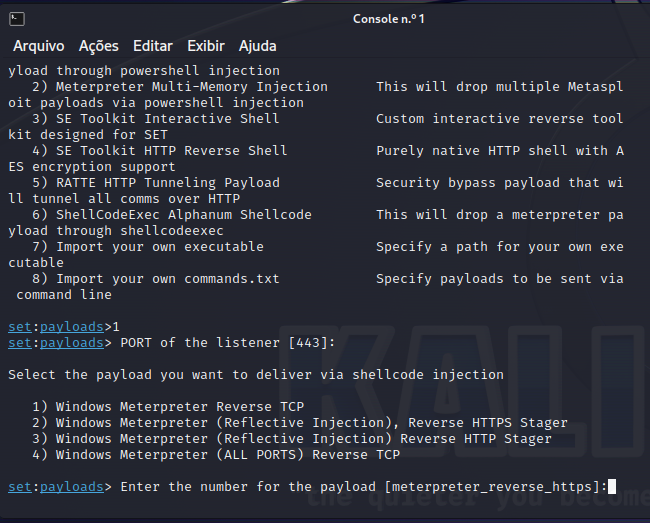


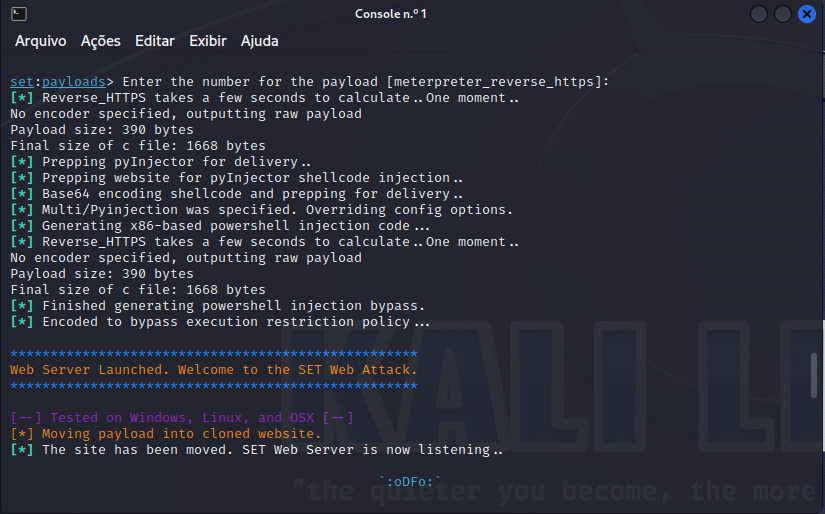
Clonando o site do google

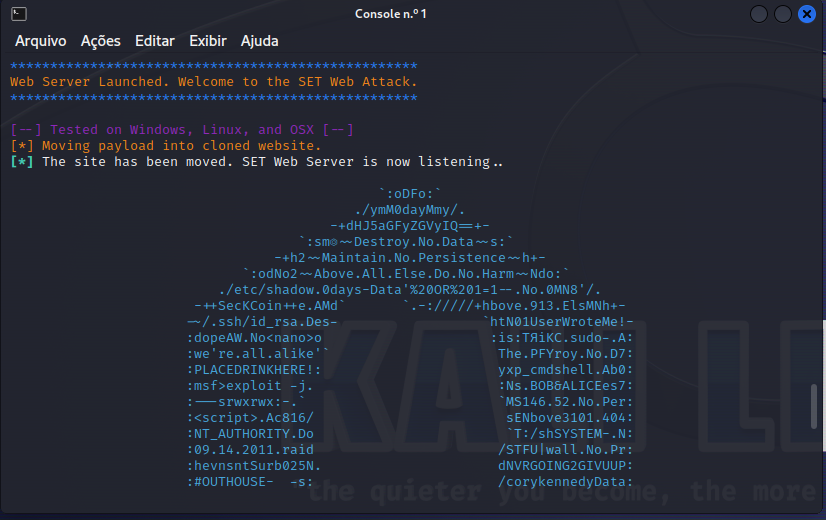


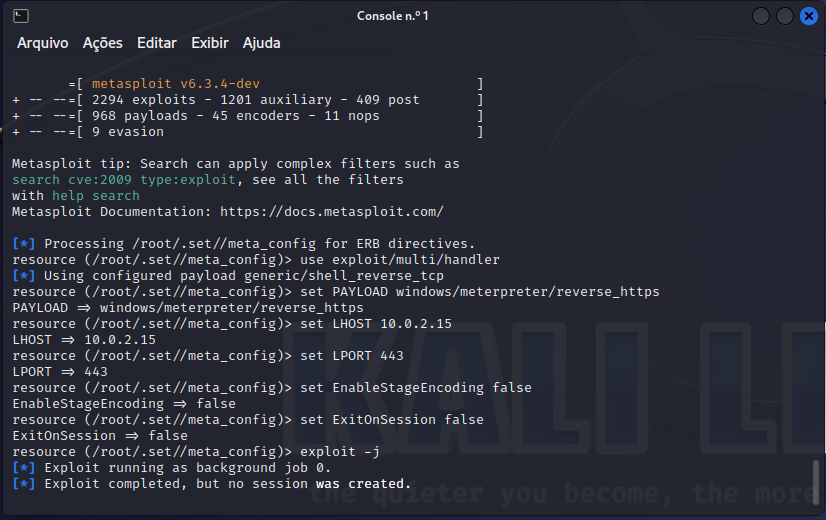


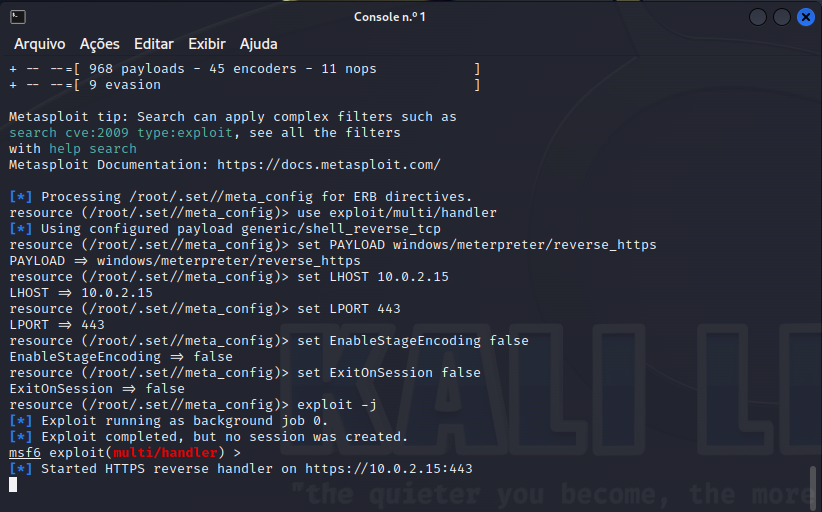
Selecionar o payload e a porta que deseja escutar:



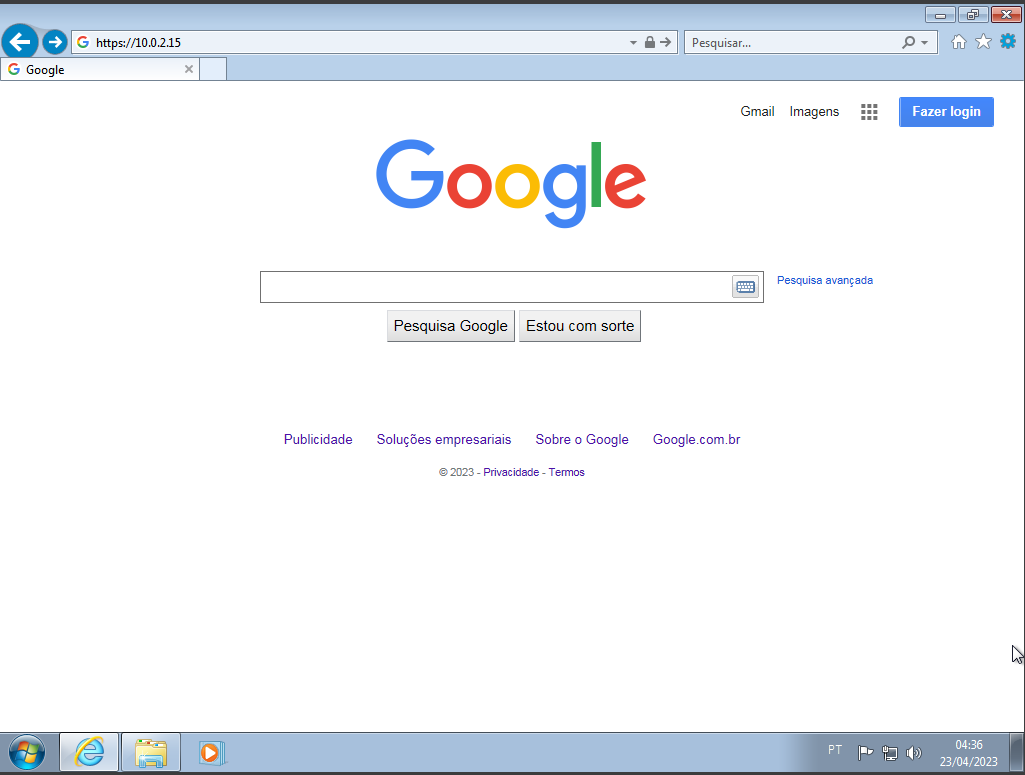








Acessar a VM do windows e digital o endereço IP, a resposta da página será o site que foi clonado



Depois disso é exibido um Security Warning perguntando se tem certeza se deseja executar a aplicação.

O que acontece após a permissão é uma porta de entrada para que esse tipo de warning possibilite ao hacker visualizar as informações acessadas.

Vídeo de referência: <https://youtu.be/6V8J47foKzA>