

## #Exercício opcional

Credenciais de acesso no Kali Linux:

- Usuário: kali
- Senha: kali

[COPIAR CÓDIGO](#)

Nós conseguimos acessar a aplicação da Alura agora pelos endereços que configuramos no Route 53, porém ainda estamos fazendo o acesso somente com HTTP. Para verificarmos possíveis vulnerabilidades presentes na aplicação ao realizar o acesso com HTTP, vamos simular um segundo usuário que estará utilizando o Kali Linux e fará o ataque *Man in the middle* para ficar no meio da comunicação.

Para isso, abra o terminal no Kali Linux e faça o download do framework responsável por realizar tal ataque:

```
apt-get install mitmf
```

[COPIAR CÓDIGO](#)

Na sequência, realize o ataque colocando:

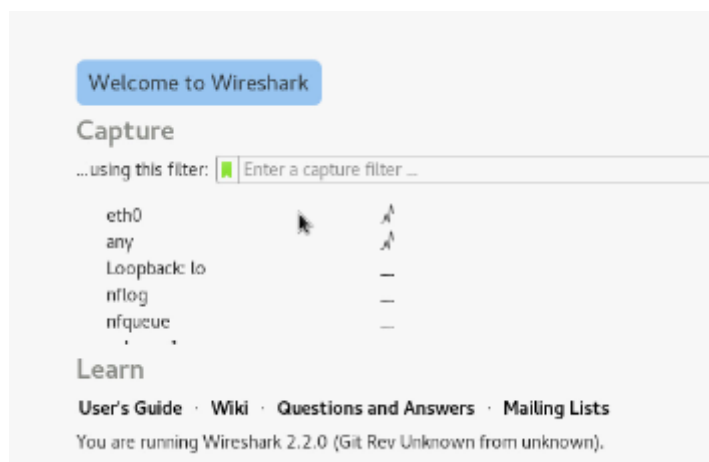
```
mitmf --arp --spoof --target [Endereço IP do computador local] --gate
```

[COPIAR CÓDIGO](#)

Feito isso, habilite o Wireshark para começar a capturar os protocolos que estão sendo tráfegados na rede:



Posteriormente, escolha o adaptador de rede utilizado pelo Kali Linux para começar a capturar os pacotes.



Na sequência, volte para seu computador local e acesse a aplicação pelo domínio que você registrou, vá até a aba de **Login**, insira o e-mail e a senha e clique no botão **Entrar**. Posteriormente volte até o Kali Linux e no Wireshark coloque o seguinte filtro:

```
http.request.method==POST
```

[COPIAR CÓDIGO](#)

Deveremos ter capturado o pacote referente a requisição **POST** do formulário de login, clique com o botão direito do mouse nesse pacote e selecione **Follow -> TCP Stream**.

Qual é o resultado? Você consegue visualizar o e-mail e senha que foram digitados no computador local?