05

Mãos à obra: Testando acesso HTTPS

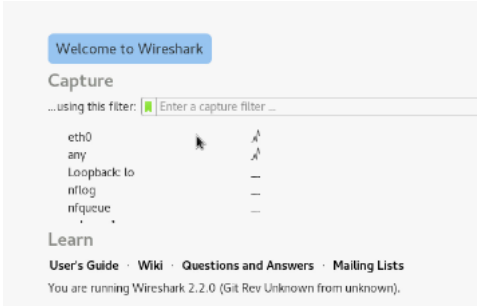
Agora que criamos o certificado e fizemos a devida associação com o CloudFront, vamos confirmar que de fato o acesso da aplicação está sendo realizado de forma segura. Para isso, vá até o browser e coloque **seu endereço de acesso**, nesse momento, devemos ser capazes de realizar o acesso de nossa aplicação de uma forma segura:

Uma vez que o acesso está sendo realizado de forma segura, vamos realizar o mesmo teste que fizémos nas etapas anteriores com o Kali Linux utilizando o ataque **man in the middle** para que possamos assim confirmar as diferenças nos resultados obtidos.

Volte até o Kali Linux, abra o terminal e inicialize o ataque **man in the middle**:

```
mitmf --arp --spoof --target [Endereço IP máquina local] --gateway [Endereço IP do roteador] -i [ada
```

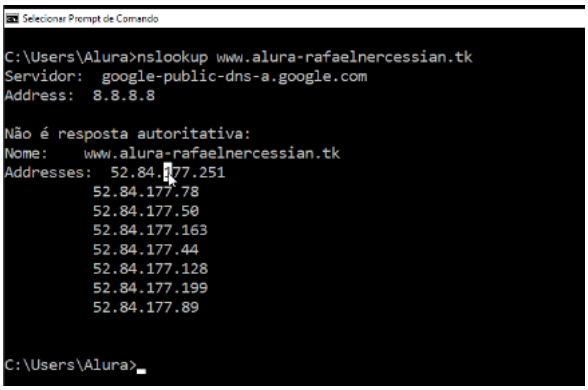
Na sequência, abra o Wireshark e escolha o adaptador de rede para realizar o processo de captura de pacotes:



Volte para o computador local e vá até a parte de login, coloque um e-mail e senha de sua preferência e clique no botão **Entrar**. Devemos analisar o resultado obtido no Wireshark, porém agora não estamos trabalhando com o HTTP e sim com o HTTPS, dessa forma, o filtro que utilizamos no Wireshark na etapa anterior não irá funcionar. Para isso, vamos agora realizar o filtro da comunicação estabelecida entre nosso computador e o CloudFront da Amazon, abra o prompt no Windows ou o terminal no Linux ou no Mac e coloque:

```
nslookup [Endereço acesso aplicação]
```

Devemos ter uma lista de endereços IP:



Como nós temos os 3 primeiros intervalos iguais para todos os endereços IP, vamos realizar um filtro no Wireshark para que tenhamos o resultado da comunicação entre nosso computador local e o CloudFront:

```
ip.addr==[endereço IP]/24
```

Ao realizarmos esse filtro, devemos ter uma lista com os pacotes que foram transmitidos e recebidos durante a comunicação com o CloudFront. Selecione o primeiro pacote, clique com o botão direito do mouse e posteriormente selecione **Follow -> TCP Stream**. Qual é o resultado? Você consegue descobrir o e-mail e senha digitado pelo usuário que estava no computador local?