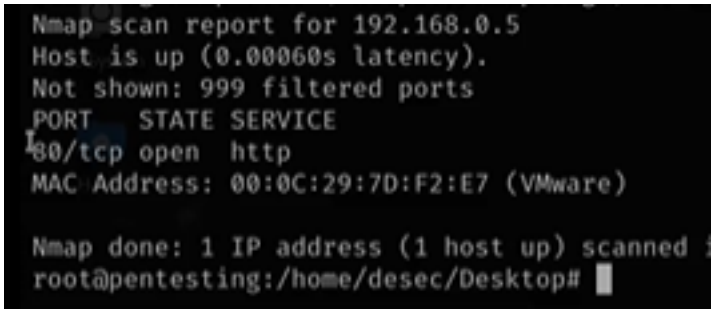
Estudando o Software

+ Iniciamos o mapeamento com o nmap no ip do host para identifia
qual porta está aberta:

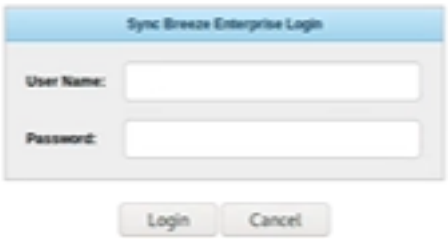
```
nmap -sS -Pn 192.168.0.5
```



→ A porta 80 estava aberta. Vamos iniciar agora a enumeração
+ Ao acessar o endereço na rede seguido da porta, entraremos na
página que mostra o software e a versão dele, o que é importante para que
possamos montar nosso ambiente (controlado) individual de teste.
+ Objetivo: entender como a aplicação funciona, se é por meio de um socket,
de algum protocolo conhecido (ftp, smtp, etc), mas principalmente qual a maneira
que temos de **ENVIAR DADOS**. [as vezes um ambiente de login já é uma resposta
pra essa pergunta]

+ Fizemos o processo de dar um attach na aplicação pra termos uma ideia do seu
comportamento conforme nossa interação.

+ O primeiro ambiente que nos deparamos ao acessar o programa na porta prevista
é um ambiente de login



→ Estudaremos de início o que acontece quando enviamos dados errados ou muitos
caracteres: De início, nada que o Immunity Debugger acuse.
→ Porém, quando mandamos uns 100A+100B (AAA..AABB..BB), o que podemos notar
é que a página só reconhece alguns A's, ou seja, tem um limitador
→ Esse agente limitante é encontrado no código fonte da aplicação e pode ser removido

```
>
=0 cellspacing=0 width=100% class='login_data'>
 name='username' maxlength=64></td></tr>
rd' name='password' maxlength=64></td></tr>
```

→ Esse maxlength é o limitador de caracteres
→ Removeremos ele com o auxílio do "inspect element" → botão esquerdo do mouse
→ Controle client side