

Cenário:

Você, aluno, deverá ter o seu container inicial-LOGIN (Ubuntu – Xenial – AMD64) em operação. As atividades abaixo devem ser realizadas nesse container.

Objetivo:

*Identificar os parâmetros básicos de reade do seu container (IP, hostname, etc)
Compreender as operações básicas sobre containers
Testar o login ao servidor SSH usando certificados
Compreender o tunelamento usando SSH*

Atividades:

- 1) Qual o IP da sua máquina? Ele é estático ou dinâmico?

- 2) Mude o *hostname* da sua máquina para `host-LOGIN`, onde *LOGIN* é o seu *login* no servidor ASA. Por exemplo, se o seu login é `ricardo45`, o nome da máquina do seu container deve ser `host-ricardo45`. Confirme se o nome da máquina realmente mudou. Reinicie o seu container. O nome se manteve como o novo nome?

- 3) Configure o servidor de *SSH*. Escute na porta cujo valor é *NN* (os dois últimos números do nome do seu *LOGIN* no servidor ASA). Caso essa porta esteja sendo usada por um serviço padrão, some 100 a esse valor. Inicie o servidor com essa configuração e teste fazendo um login no container a partir do servidor ASA.

- 4) Permita acesso à conta `root` através do *SSH*. Faça um acesso e confirme se logrou êxito. Agora desabilite o acesso à conta de "root" e teste.

- 5) Crie um usuário no seu container com o login `usuarioNN` – *NN* tem o mesmo significado do item 3. Crie um par de chave pública/privada para este usuário. Observe o resultado em `~usuario/.ssh`

- 6) Passe o arquivo `id_rsa.pub` (referente ao usuário criado no passo 5) para o seu vizinho e peça a ele que autorize o seu login no container dele, partindo do seu `usuarioNN` para o `usuarioYY` dele. Faça o login no container dele a partir do seu. Pediu senha? Por que?

- 7) Gere um novo par de chaves para `usuarioNN` da sua máquina. Não passe ao seu vizinho. Tente fazer o login no *container* do vizinho, como no passo 6. Pediu senha? Por que?

- 8) Instale um cliente de *telnet* no seu *container* (`apt-get install telnet`). Faça uma conexão *HTTP* para www.asdfg.com.br. Funcionou?

```
telnet www.asdfg.com.br 80
get / HTTP/1.1
Host: www.asdfg.com.br
```

9) Agora bloqueie qualquer conexão de sua máquina para a porta 80 de qualquer outra

```
iptables -A OUTPUT -p tcp --dport 80 -j REJECT
```

10) Repita o exercício 8. Funcionou?

11) Agora crie na sua máquina um tunel *SSH* entre a porta 4444 da sua máquina e a máquina do seu vizinho de modo que qualquer conexão à sua porta 4444 seja redirecionada para www.asdfg.com.br:80. Feita a configuração, teste usando o comando abaixo. Qual o resultado? Explique o que está acontecendo.

```
telnet localhost 4444
get / HTTP/1.1
Host: www.asdfg.com.br
```

12) Peça para o vizinho bloquear o acesso dele a conexões a qualquer máquina na porta 80. Repita o exercício 11. Funcionou.

13) Libere o acesso a conexão para a porta 80:

```
iptables -D OUTPUT -p tcp --dport 80 -j REJECT
```