Bypass de Firewall

+ As vezes, quando vamos fazer um mapeamendo em um host, o firewall existente pode estar mal configurado ao ponto de permitir o acesso a partir de algumas portas de origem

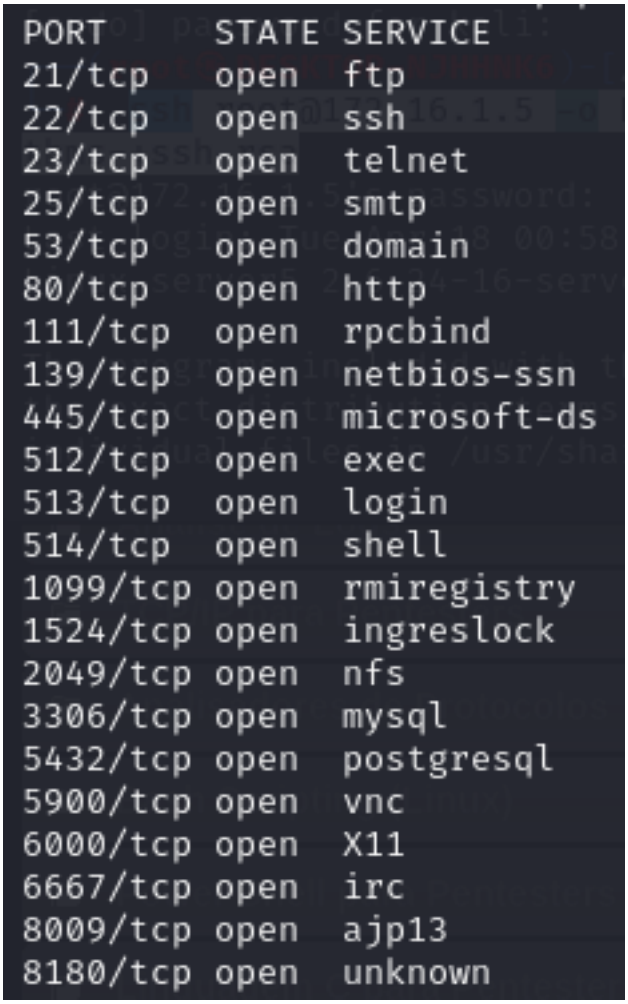
+ Para verificar isso na prática, acessamos o 172.16.1.5 da rede interna por meio do comando

```
ssh root@172.16.1.5 -o HostKeyAlgorithms=+ssh-dss -o PubkeyAcceptedAlgorithms=+ssh-rsa
```

usando root como USER e PASSWORD.

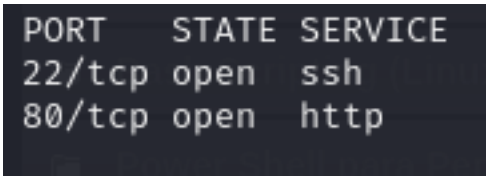
+ Antes de ativar a ./rules4.sh em /home/msfadmin/firewall fizemos a varredura de portas com o kali

```
nmap -v -sS -Pn 53 172.16.1.5
```



+ Em seguida, ativamos a ./rules4.sh e a mesma varredura mostrou-se ineficiente

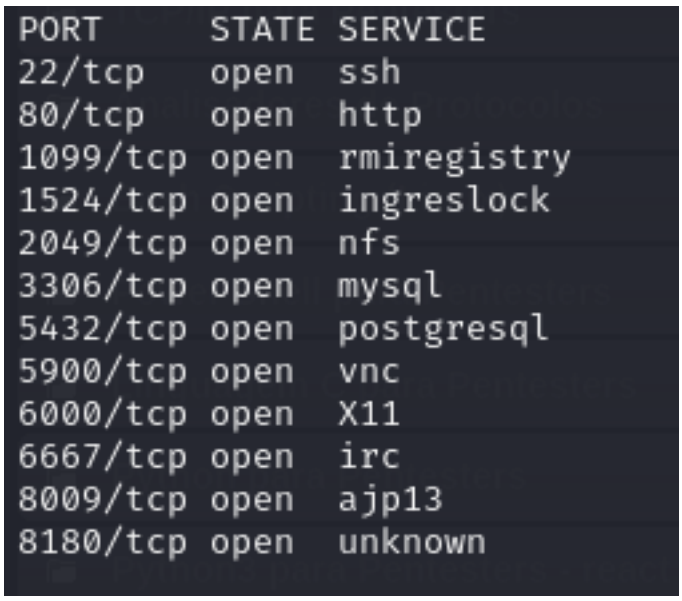
```
nmap -v -sS -Pn 172.16.1.5
```



+ Para dar o bypass nesse firewall, usamos como porta de origem a 53, que ele deixava passar

```
nmap -v -sS -Pn -g 53 172.16.1.5
```

-g indica a porta de origem



+ Para conseguir conectar ao serviço, fizemos uma conexão via netcat especificando a porta de origem e mandando o resultado da interação para a mesma pasta do apache em um arquivo chamado recon.html

```
nc -vn -p 53 172.16.1.5 > var/www/html/recon.html
```

o qual pudemos acessar depois de fazer uma requisição GET (GET / HTTP/1.0) com nosso endereço de ip no navegador: 192.168.1.138/recon.html

OBS: Acesso ao ssh

Comando SSH:
ssh root@172.16.1.5 -o HostKeyAlgorithms=+ssh-dss -o PubkeyAcceptedAlgorithms=+ssh-rsa

Credenciais:
- user: root
- pass: root