

# Bypass de Firewall

+ As vezes, quando vamos fazer um mapeamento 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
```

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
111/tcp	open	rpcbind
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
1099/tcp	open	rmiregistry
1524/tcp	open	ingreslock
2049/tcp	open	nfs
3306/tcp	open	mysql
5432/tcp	open	postgresql
5900/tcp	open	vnc
6000/tcp	open	X11
6667/tcp	open	irc
8009/tcp	open	ajp13
8180/tcp	open	unknown

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

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

PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http

+ 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

PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
1099/tcp	open	rmiregistry
1524/tcp	open	ingreslock
2049/tcp	open	nfs
3306/tcp	open	mysql
5432/tcp	open	postgresql
5900/tcp	open	vnc
6000/tcp	open	X11
6667/tcp	open	irc
8009/tcp	open	ajp13
8180/tcp	open	unknown

+ 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 podemos 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