# *IPS / Bloqueio de Port Scanning*

+ O objetivo é mostrar princípios de funcionamento de um IPS que bloqueia scanner de portas

+ O IPS usado foi o portsentry

+ Basicamente ele fica de olho em portas que não são muito usuais e quando o endereço de IP acessa ela, o IPS registra o endereço e adota uma configuração de drop para aquele domínio

+ Para ajustar essa configuração basta comentar a seguinte sentença no arquivo /etc/portsentry/portsentry.conf

```
# Newer versions of Linux support the reject flag now. This
# is cleaner than the above option.
KILL_ROUTE="/sbin/route add -host $TARGET$ reject"
```

E tirar o comentrário da que dá a opção de DROP com o iptables

```
# iptables support for Linux
KILL_ROUTE="/sbin/iptables -I INPUT -s $TARGET$ -j DROP"
#
```

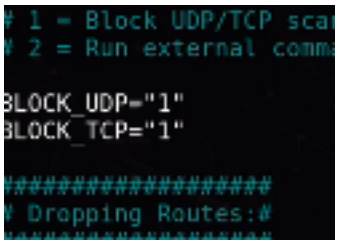
+ Então, reiniciamos o portsentry:

```
service portsentry restart
```

+ Quando verificamos os serviços rodando nas portas abertas, podemos ter noção da existência de um IPS

```
root@pentest: ~/Desktop
Host is up (0.0030s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE     VERSION
1/tcp     open  tcpwrapped
22/tcp    open  ssh         OpenSSH 8.0p1 Debian 4 (protocol 2.0)
79/tcp    open  tcpwrapped
80/tcp    open  http        Apache httpd 2.4.41 ((Debian))
111/tcp   open  tcpwrapped
119/tcp   open  tcpwrapped
143/tcp   open  tcpwrapped
1080/tcp  open  tcpwrapped
1524/tcp  open  tcpwrapped
2000/tcp  open  tcpwrapped
6667/tcp  open  tcpwrapped
12345/tcp open  tcpwrapped
31337/tcp open  tcpwrapped
32771/tcp open  tcpwrapped
32772/tcp open  tcpwrapped
32773/tcp open  tcpwrapped
32774/tcp open  tcpwrapped
MAC Address: 00:0C:29:13:01:FA (VMware)
```

+ Para habilitar, no portsentry, a opção de bloqueio, basta que modifiquemos a seguinte conf:




+ Para ver os hosts bloqueados, basta acessar o arquivo /etc/hosts.deny