



FCTUC FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE DE COIMBRA

Trabalho Prático #2

Segurança em Tecnologias de Informação

Departamento de Engenharia Informática

Ano letivo 2019/2020 - 2º Semestre

Trabalho realizado por:

- Francisco Miguel Almeida Monteiro, 2016241480
- Ricardo José Monteiro Paiva, 2016253100

Introdução:

Para este trabalho, foi-nos pedido para configurar uma *network firewall* com os conhecimentos adquiridos nas aulas práticas. Para isso, utilizámos o *IpTables* e o *Snort* para a deteção de intrusões. O presente relatório descreve o cenário implementado, os ficheiros de configuração criados, as regras de *firewall* desenvolvidas, a implementação da deteção de intrusões com o Snort e os testes efetuados sobre o cenário para demonstração do funcionamento dos diferentes requisitos.

1. Cenário:

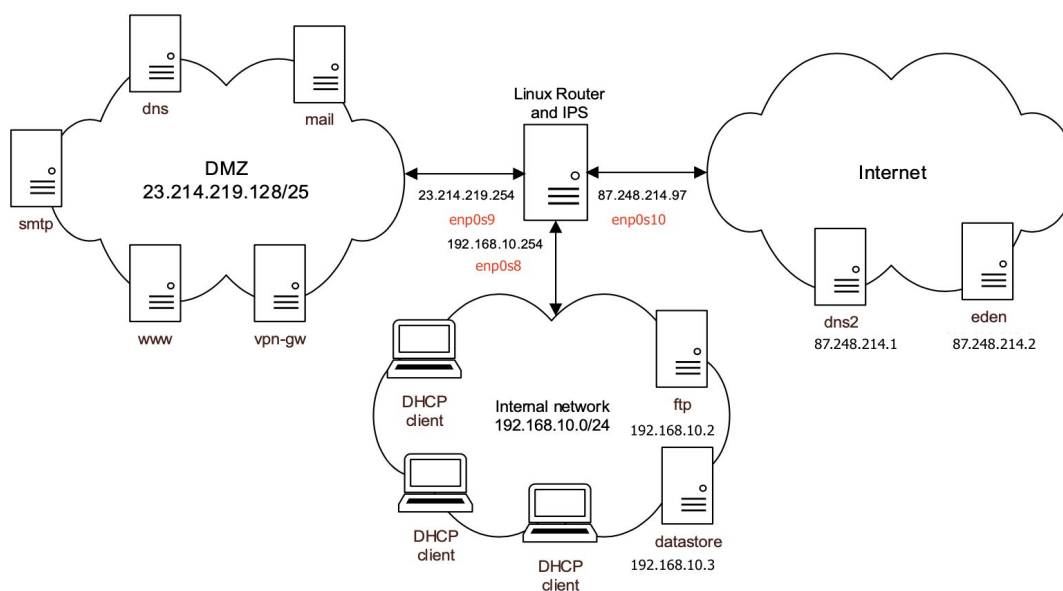


Figura 1. Cenário implementado

Para conseguir estabelecer as ligações presentes na figura anterior, foram clonadas 3 máquinas virtuais, sendo uma o router e as outras duas usadas para os diferentes testes criados. A configuração da gateway do router é a seguinte:

Router:

- 3 redes internas + NAT
 - IP: 23.214.219.254 Mask: 255.255.255.128
 - IP: 192.168.10.254 Mask: 255.255.255.0
 - IP: 87.248.214.97 Mask: 255.255.255.0

Para as restantes máquinas a configuração da interface foi sendo alterada mediante o teste que iria ser feito porém foi necessário desenvolver um ficheiro de configuração para cada uma das redes internas para que estas tivessem conhecimento das redes atingíveis através da ligação ao router. Os ficheiros¹ de configuração são apresentados de seguida:

- DMZ.sh

```
systemctl stop firewalld
systemctl disable iptables
route add -net 87.248.214.0 netmask 255.255.255.0 gw 23.214.219.254
route add -net 192.168.10.0 netmask 255.255.255.0 gw 23.214.219.254
```

- Internet.sh

```
systemctl stop firewalld
systemctl disable iptables
route add -net 23.214.219.128 netmask 255.255.255.128 gw 192.168.10.254
route add -net 87.248.214.0 netmask 255.255.255.0 gw 192.168.10.254
```

- Internal_Network.sh

```
systemctl stop firewalld
systemctl disable iptables
route add -net 23.214.219.128 netmask 255.255.255.128 gw 87.248.214.97
route add -net 192.168.10.0 netmask 255.255.255.0 gw 87.248.214.97
```

Como podemos verificar pelas configurações acima, começamos por desativar a **firewall** da máquina virtual e desativar as **iptables** para que estas não interfiram na comunicação entre redes. De seguida, o comando “**route add**” permite adicionar à tabela de *routing* as redes que são possíveis de atingir pelos diferentes *gateways*.

Após estabelecermos todas as ligações, procedemos aos testes, fazendo ping para os diferentes ip’s das diferentes máquinas para ver se estas conseguiam comunicar entre si.

¹ Todos os ficheiros de configuração estão anexados ao presente relatório.

Para além disso, de forma a facilitar o nosso trabalho numa fase de testes, foram adicionados hosts ao ficheiro **/etc/hosts**. Cada linha contém um endereço ip e um respectivo nome (host), o que nos permite utilizar o nome em vez do endereço.

/etc/hosts

```
87.248.214.1    dns2
87.248.214.2    eden
23.214.219.130  vpn-gw
23.214.219.131  www
23.214.219.132  smtp
23.214.219.133  dns
23.214.219.134  mail
192.168.10.2    ftp
192.168.10.3    datastore
```

2. Filtragem de Pacotes

De forma a cumprir com os requisitos de filtragem de pacotes, foi necessário criar um ficheiro denominado de **“router.sh”** onde adicionámos todas as regras necessárias para a configuração da firewall. Nesta secção iremos analisar este ficheiro por partes com imagens dos testes executados para cada uma das regras. Para a maioria dos testes foi utilizada a ferramenta **netcat**. Esta ferramenta permite colocar as máquinas à escuta num determinado porto e força certas comunicações para podermos verificar que os pacotes estão de facto a atravessar a **firewall**. Esta ferramenta suporta tanto udp como tcp.

```
systemctl stop firewalld
systemctl disable firewalld
systemctl mask firewalld
systemctl enable iptables
iptables -F
```

Em primeiro lugar, começamos por desativar a **firewall** e assegurar que esta não é de novo iniciada por outros programas. De seguida, damos autorização ao serviço do **iptables** e limpamos todas as tabelas com o último comando.

Para a construção das regras de configuração da firewall foram usadas inúmeras flags para podermos configurar as regras de acordo com os requisitos pedidos no enunciado do trabalho prático. As flags mais importantes são descritas de seguida:

- Flags **“-s”** e **“-d”** dizem respeito ao ip de origem e destino, respetivamente.
- Flag **“-A”** permite especificar a tabela onde a regra vai ser adicionada.
- Flags **“--sport”** e **“--dport”** corresponde ao porto de origem e porto de destino, respetivamente.
- Flag **“-p”** corresponde ao protocolo de comunicação e **“-P”** corresponde à **policy**.
- A flag **“-j”** especifica o que deve ser feito com o pacote que respeita a regra em questão.
- Flag **“-t”** permite especificar a tabela de destino, onde a regra será adicionada. Quando esta flag é omitida, é escolhida a tabela default (filter).

- Flags “-i” e “-o” correspondem à interface de entrada e saída, respectivamente.

Como temos de recusar todos os pedidos que não respeitam nenhuma das regras criadas, foi necessário adicionar os comandos seguintes para podermos alterar a política das diferentes tabelas para “Drop”.

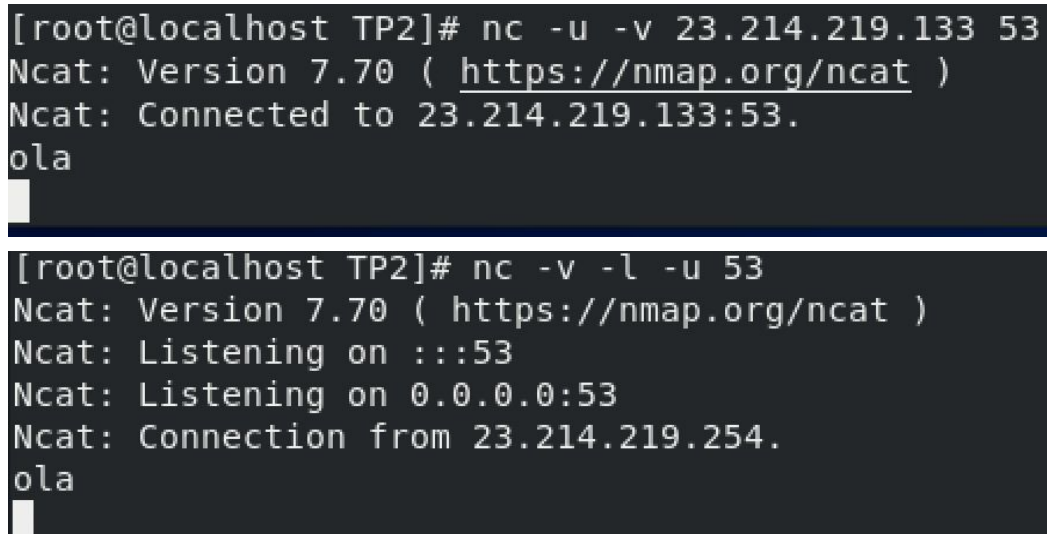
```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

De seguida apresentamos as regras referentes a cada um dos requisitos pedidos.

2.1. Configuração para proteger o Router

- Pedidos DNS enviados para servidores externos

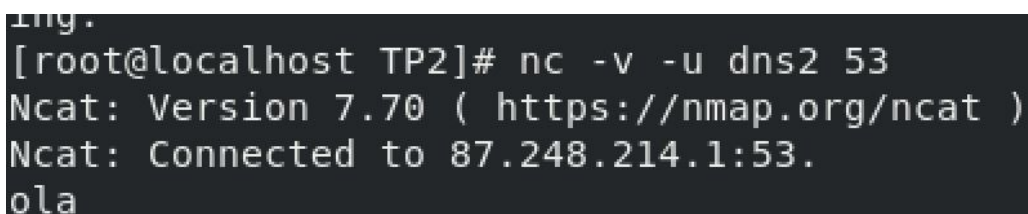
```
#DNS
iptables -A INPUT -p udp --sport domain -j ACCEPT
iptables -A OUTPUT -p udp --dport domain -j ACCEPT
```



```
[root@localhost TP2]# nc -u -v 23.214.219.133 53
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 23.214.219.133:53.
ola

[root@localhost TP2]# nc -v -l -u 53
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::53
Ncat: Listening on 0.0.0.0:53
Ncat: Connection from 23.214.219.254.
ola
```

Figura 2. Pedido DNS Router → DNS server



```
ing.
[root@localhost TP2]# nc -v -u dns2 53
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 87.248.214.1:53.
ola
```

```
[root@localhost TP2]# nc -v -l -u 53
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::53
Ncat: Listening on 0.0.0.0:53
Ncat: Connection from 87.248.214.97.
ola
```

Figura 3. Pedido DNS Router → DNS2 server

- Conexões SSH originadas no Vpn-gw ou na rede interna

```
#SSH
iptables -A INPUT -s vpn-gw -p tcp --dport ssh -j ACCEPT
iptables -A OUTPUT -d vpn-gw -p tcp --sport ssh -j ACCEPT
iptables -A INPUT -s 192.168.10.0/24 -p tcp --dport ssh -j ACCEPT
iptables -A OUTPUT -d 192.168.10.0/24 -p tcp --sport ssh -j ACCEPT
```

Para testar estas ligações foi necessário “matar” o processo que estava a utilizar o **porto 22** visto que quando colocávamos o netcat a escuta neste porto, recebíamos a mensagem que este já se encontrava em uso.

```
[root@localhost TP2]# nc -v 23.214.219.254 22
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 23.214.219.254:22.
ola
```

```
[root@localhost TP2]# nc -v -l 22
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::22
Ncat: Listening on 0.0.0.0:22
Ncat: Connection from 23.214.219.130.
Ncat: Connection from 23.214.219.130:52416.
ola
```

Figura 4. Conexão SSH VPN gateway → Router

Para este caso, fizemos um teste extra onde utilizámos o servidor **WWW** e tentámos enviar uma conexão **SSH** para o router. Como se pode verificar, pela imagem em seguida, a firewall não aceitou essa conexão.

```
[root@localhost TP2]# nc -v 23.214.219.254 22
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connection timed out.
```

Figura 5. Teste WWW server → Router

```
[root@localhost TP2]# nc -v 192.168.10.254 22
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 192.168.10.254:22.
```

```
[root@localhost TP2]# nc -v -l 22
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::22
Ncat: Listening on 0.0.0.0:22
Ncat: Connection from 192.168.10.2.
Ncat: Connection from 192.168.10.2:41766.
```

Figura 6. Rede interna → Router

2.2. Configuração para autorizar comunicações diretas (sem NAT)

- Pedidos DNS usando o servidor DNS

#DNS#Internal Network

```
iptables -A FORWARD -s 192.168.10.0/24 -d 23.214.219.133 -p udp --dport domain -i enp0s8 -o enp0s9 -j ACCEPT
```

```
iptables -A FORWARD -s 23.214.219.133 -d 192.168.10.0/24 -p udp --dport domain -i enp0s9 -o enp0s8 -j ACCEPT
```

#Internet

```
iptables -A FORWARD -s 87.248.214.0/24 -d 23.214.219.133 -p udp --dport domain -i enp0s10 -o enp0s9 -j ACCEPT
```

```
iptables -A FORWARD -s 23.214.219.133 -d 87.248.214.0/24 -p udp --dport domain -i enp0s9 -o enp0s10 -j ACCEPT
```

```
[root@localhost tp2]# nc -u -l -v 53
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::53
Ncat: Listening on 0.0.0.0:53
Ncat: Connection from 192.168.10.2.
ola
```

```
[root@localhost tp2]# nc -u -v 23.214.219.133 53
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 23.214.219.133:53.
ola
```

Figura 7. Pedido DNS rede interna → dns server

```
[root@localhost tp2]# nc -u -l -v 53
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::53
Ncat: Listening on 0.0.0.0:53
Ncat: Connection from 87.248.214.1.
ola
```

```
[root@localhost tp2]# nc -u -v 23.214.219.133 53
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 23.214.219.133:53.
ola
```

Figura 8. Pedido DNS Internet → dns server

- Pedidos DNS entre o servidor DNS e DNS2 entre outros

```
#Dns resolve names to other dns servers
iptables -A FORWARD -s 23.214.219.133 -d 87.248.214.0/24 -p udp --dport
domain -i enp0s9 -o enp0s10 -j ACCEPT
iptables -A FORWARD -s 87.248.214.0/24 -d 23.214.219.133 -p udp --dport
domain -i enp0s10 -o enp0s9 -j ACCEPT
```



```
[root@localhost tp2]# nc -u -l -v 53
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::53
Ncat: Listening on 0.0.0.0:53
Ncat: Connection from 23.214.219.133.
ola
█
```

```
[root@localhost tp2]# nc -u -v 87.248.214.1 53
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 87.248.214.1:53.
ola
█
```

Figura 9. Pedido DNS Dns server→ Dns2 server

- **Servidores DNS e DNS2 conseguem sincronizar os conteúdos das zonas dns**

```
#Sync dns zones
#DNS -> DNS2
iptables -A FORWARD -s 23.214.219.133 -d 87.248.214.1 -p tcp --dport
domain -i enp0s9 -o enp0s10 -j ACCEPT
iptables -A FORWARD -s 87.248.214.1 -d 23.214.219.133 -p tcp --sport
domain -i enp0s10 -o enp0s9 -j ACCEPT
#DNS2 -> DNS
iptables -A FORWARD -s 87.248.214.1 -p tcp -d 23.214.219.133 --dport
domain -i enp0s10 -o enp0s9 -j ACCEPT
iptables -A FORWARD -s 23.214.219.133 -p tcp -d 87.248.214.1 --sport
domain -i enp0s9 -o enp0s10 -j ACCEPT
```

```
[root@localhost tp2]# nc -l -v 53
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::53
Ncat: Listening on 0.0.0.0:53
Ncat: Connection from 23.214.219.133.
Ncat: Connection from 23.214.219.133:38474.
ola
█
```



```
[root@localhost tp2]# nc -v 87.248.214.1 53
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 87.248.214.1:53.
ola
```

Figura 10. Pedido DNS Dns server→ Dns2 server

```
[root@localhost tp2]# nc -l -v 53
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::53
Ncat: Listening on 0.0.0.0:53
Ncat: Connection from 87.248.214.1.
Ncat: Connection from 87.248.214.1:36296.
ola
```

```
[root@localhost tp2]# nc -v 23.214.219.133 53
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 23.214.219.133:53.
ola
```

Figura 11. Pedido DNS Dns2 server→ Dns server

- Conexões SMTP para o servidor SMTP

```
#SMTP connections
# internal
iptables -A FORWARD -s 192.168.10.0/24 -p tcp -d 23.214.219.132 --dport
smtp -i enp0s8 -o enp0s9 -j ACCEPT
iptables -A FORWARD -s 23.214.219.132 -p tcp -d 192.168.10.0/24 --sport
smtp -i enp0s9 -o enp0s8 -j ACCEPT

# internet
iptables -A FORWARD -s 87.248.214.0/24 -p tcp -d 23.214.219.132 --dport
smtp -i enp0s10 -o enp0s9 -j ACCEPT
iptables -A FORWARD -s 23.214.219.132 -p tcp -d 87.248.214.0/24 --sport
smtp -i enp0s9 -o enp0s10 -j ACCEPT
```

```
[root@localhost tp2]# nc -l -v 25
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::25
Ncat: Listening on 0.0.0.0:25
Ncat: Connection from 192.168.10.2.
Ncat: Connection from 192.168.10.2:53496.
ola
█
```

```
[root@localhost tp2]# nc -v 23.214.219.132 25
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 23.214.219.132:25.
ola
█
```

Figura 12. Conexão SMTP Internal Network → Servidor SMTP

```
[root@localhost tp2]# nc -l -v 25
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::25
Ncat: Listening on 0.0.0.0:25
Ncat: Connection from 87.248.214.1.
Ncat: Connection from 87.248.214.1:55062.
ola
█
```

```
[root@localhost tp2]# ./routes.sh
[root@localhost tp2]# nc -v 23.214.219.132 25
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 23.214.219.132:25.
ola
█
```

Figura 13. Conexão SMTP Internal Network → Servidor SMTP

- Ligações IMAP e POP3 para o servidor Mail

```
#internal network
iptables -A FORWARD -s 192.168.10.0/24 -p tcp -d 23.214.219.134 --dport
pop3 -i enp0s8 -o enp0s9 -j ACCEPT
iptables -A FORWARD -s 192.168.10.0/24 -p tcp -d 23.214.219.134 --dport
imap -i enp0s8 -o enp0s9 -j ACCEPT
iptables -A FORWARD -s 23.214.219.134 -p tcp -d 192.168.10.0/24 --sport
```

```
pop3 -i enp0s9 -o enp0s8 -j ACCEPT
iptables -A FORWARD -s 23.214.219.134 -p tcp -d 192.168.10.0/24 --sport
imap -i enp0s9 -o enp0s8 -j ACCEPT
```

```
#internet
```

```
iptables -A FORWARD -s 87.248.214.0/24 -p tcp -d 23.214.219.134 --dport
pop3 -i enp0s10 -o enp0s9 -j ACCEPT
iptables -A FORWARD -s 87.248.214.0/24 -p tcp -d 23.214.219.134 --dport
imap -i enp0s10 -o enp0s9 -j ACCEPT
iptables -A FORWARD -s 23.214.219.134 -p tcp -d 87.248.214.0/24 --sport
pop3 -i enp0s9 -o enp0s10 -j ACCEPT
iptables -A FORWARD -s 23.214.219.134 -p tcp -d 87.248.214.0/24 --sport
imap -i enp0s9 -o enp0s10 -j ACCEPT
```

```
[root@localhost TP2]# nc -v -l 110
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::110
Ncat: Listening on 0.0.0.0:110
Ncat: Connection from 192.168.10.2.
Ncat: Connection from 192.168.10.2:50464.
ola
```

```
[root@localhost TP2]# nc -v mail 110
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 23.214.219.134:110.
ola
```

Figura 14. Conexão POP3 Internal Network → Mail server

```
[root@localhost tp2]# nc -l -v 110
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::110
Ncat: Listening on 0.0.0.0:110
Ncat: Connection from 87.248.214.1.
Ncat: Connection from 87.248.214.1:58130.
ola
```

```
[root@localhost tp2]# nc -v 23.214.219.134 110
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 23.214.219.134:110.
ola
```

Figura 15. Conexão POP3 Internet → Mail server

```
[root@localhost TP2]# nc -v -l 143
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::143
Ncat: Listening on 0.0.0.0:143
Ncat: Connection from 192.168.10.2.
Ncat: Connection from 192.168.10.2:50280.
ola
```

```
[root@localhost TP2]# nc -v mail 143
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 23.214.219.134:143.
ola
```

Figura 16. Conexão IMAP Internal Network → Mail server

```
[root@localhost tp2]# nc -l -v 143
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::143
Ncat: Listening on 0.0.0.0:143
Ncat: Connection from 87.248.214.1.
Ncat: Connection from 87.248.214.1:50212.
ola
```

```
[root@localhost tp2]# nc -v 23.214.219.134 143
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 23.214.219.134:143.
ola
```

Figura 17. Conexão IMAP Internet → Mail server

- Ligações HTTP e HTTPS para o servidor WWW

```
#Internal network
iptables -A FORWARD -s 192.168.10.0/24 -p tcp -d 23.214.219.131 --dport
http -i enp0s8 -o enp0s9 -j ACCEPT
iptables -A FORWARD -s 192.168.10.0/24 -p tcp -d 23.214.219.131 --dport
https -i enp0s8 -o enp0s9 -j ACCEPT
iptables -A FORWARD -s 23.214.219.131 -p tcp -d 192.168.10.0/24 --sport
http -i enp0s9 -o enp0s8 -j ACCEPT
iptables -A FORWARD -s 23.214.219.131 -p tcp -d 192.168.10.0/24 --sport
https -i enp0s9 -o enp0s8 -j ACCEPT

#Internet
iptables -A FORWARD -s 87.248.214.0/24 -p tcp -d 23.214.219.131 --dport
http -i enp0s10 -o enp0s9 -j ACCEPT
iptables -A FORWARD -s 87.248.214.0/24 -p tcp -d 23.214.219.131 --dport
https -i enp0s10 -o enp0s9 -j ACCEPT
iptables -A FORWARD -s 23.214.219.131 -p tcp -d 87.248.214.0/24 --sport
http -i enp0s9 -o enp0s10 -j ACCEPT
iptables -A FORWARD -s 23.214.219.131 -p tcp -d 87.248.214.0/24 --sport
https -i enp0s9 -o enp0s10 -j ACCEPT
```

```
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 192.168.10.2.
Ncat: Connection from 192.168.10.2:51632.
ola
```

```
[root@localhost TP2]# nc -v www 80
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 23.214.219.131:80.
ola
```

Figura 18. Conexão HTTP Internal Network → WWW server


```
[root@localhost tp2]# nc -l -v 80
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 87.248.214.1.
Ncat: Connection from 87.248.214.1:56978.
ola
```

```
[root@localhost tp2]# nc -v 23.214.219.131 80
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 23.214.219.131:80.
ola
```

Figura 19. Conexão HTTP Internet → WWW server

```
[root@localhost TP2]# nc -v -l 443
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.10.2.
Ncat: Connection from 192.168.10.2:59526.
ola
```

```
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connection timed out.
[root@localhost TP2]# nc -v www 443
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 23.214.219.131:443.
ola
```

Figura 20. Conexão HTTPS Internal Network → WWW server

```
[root@localhost tp2]# nc -l -v 443
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 87.248.214.1.
Ncat: Connection from 87.248.214.1:34814.
ola
```

```
[root@localhost tp2]# nc -v 23.214.219.131 443
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 23.214.219.131:443.
ola
```

Figura 21. Conexão HTTPS Internet → WWW server

- Ligações OpenVPN para o Vpn gateway

```
# Internal network (UDP)
iptables -A FORWARD -s 192.168.10.0/24 -p udp -d 23.214.219.130 --dport
openvpn -i enp0s8 -o enp0s9 -j ACCEPT
iptables -A FORWARD -s 23.214.219.130 -p udp -d 192.168.10.0/24 --sport
openvpn -i enp0s9 -o enp0s8 -j ACCEPT

# Internal network (TCP)
iptables -A FORWARD -s 192.168.10.0/24 -p tcp -d 23.214.219.130 --dport
openvpn -i enp0s8 -o enp0s9 -j ACCEPT
iptables -A FORWARD -s 23.214.219.130 -p tcp -d 192.168.10.0/24 --sport
openvpn -i enp0s9 -o enp0s8 -j ACCEPT

# Internet (UDP)
iptables -A FORWARD -s 87.248.214.0/24 -p udp -d 23.214.219.130 --dport
openvpn -i enp0s10 -o enp0s9 -j ACCEPT
iptables -A FORWARD -s 23.214.219.130 -p udp -d 87.248.214.0/24 --sport
openvpn -i enp0s9 -o enp0s10 -j ACCEPT

# Internet (TCP)
iptables -A FORWARD -s 87.248.214.0/24 -p tcp -d 23.214.219.130 --dport
openvpn -i enp0s10 -o enp0s9 -j ACCEPT
iptables -A FORWARD -s 23.214.219.130 -p tcp -d 87.248.214.0/24 --sport
openvpn -i enp0s9 -o enp0s10 -j ACCEPT
```



```
[root@localhost TP2]# nc -v -l 1194
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::1194
Ncat: Listening on 0.0.0.0:1194
Ncat: Connection from 192.168.10.2.
Ncat: Connection from 192.168.10.2:36290.
ola
```

```
[root@localhost TP2]# nc -v vpn-gw 1194
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 23.214.219.130:1194.
ola
```

Figura 22. Conexão OpenVPN Internal network → VPN gateway (TCP)

```
[root@localhost tp2]# nc -l -v 1194
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::1194
Ncat: Listening on 0.0.0.0:1194
Ncat: Connection from 87.248.214.1.
Ncat: Connection from 87.248.214.1:38244.
ola
```

```
[root@localhost tp2]# nc -v 23.214.219.130 1194
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 23.214.219.130:1194.
ola
```

Figura 23. Conexão OpenVPN Internet → VPN gateway (TCP)

```
[root@localhost TP2]# nc -v -l -u 1194
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::1194
Ncat: Listening on 0.0.0.0:1194
Ncat: Connection from 192.168.10.2.
ola
```

```
[root@localhost TP2]# nc -v -u vpn-gw 1194
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 23.214.219.130:1194.
ola
```

Figura 24. Conexão OpenVPN Internal Network → VPN gateway (UDP)

```
[root@localhost tp2]# nc -u -l -v 1194
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::1194
Ncat: Listening on 0.0.0.0:1194
Ncat: Connection from 87.248.214.1.
ola
```

```
[root@localhost tp2]# nc -u -v 23.214.219.130 1194
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 23.214.219.130:1194.
ola
```

Figura 25. Conexão OpenVPN Internet → VPN gateway (UDP)

- **Ligações ao serviço PostgreSQL localizado no Datastore se originadas no VPN gateway**

```
iptables -A FORWARD -s 23.214.219.130 -p tcp -d 192.168.10.3 --dport postgres -i enp0s9 -o enp0s8 -j ACCEPT
iptables -A FORWARD -s 192.168.10.3 -p tcp -d 23.214.219.130 --sport postgres -i enp0s8 -o enp0s9 -j ACCEPT
```

```
[root@localhost tp2]# nc -l -v 5432
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::5432
Ncat: Listening on 0.0.0.0:5432
Ncat: Connection from 23.214.219.130.
Ncat: Connection from 23.214.219.130:51432.
ola
```

```
[root@localhost tp2]# nc -v 192.168.10.3 5432
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 192.168.10.3:5432.
ola
```

Figura 26. Conexão PostgreSQL VPN gateway → Datastore

2.3. Conexões para o porto externo da firewall (c/ NAT)

Para além da tabela default, mais conhecida como **filter**, nesta parte do trabalho foi necessário recorrer à tabela de **NAT**. Como tal, esta tabela é constituída por outras chains, uma das quais viemos a utilizar nesta secção: **PREROUTING**. Esta chain é responsável pelo tratamento dos pacotes que chegam à interface do router quando estes vêm do exterior (**Internet**). Nesta fase ainda não se sabe se estes pacotes vão ser tratados localmente ou reencaminhados. Quando estes pacotes são destinados para a **rede interna**, as regras associadas a esta chain permitem fazer o roteamento dos pacotes para o ip de destino.

- Conexões FTP para o servidor FTP

Este protocolo é um caso especial, uma vez que tem dois modos de funcionamento: **modo ativo** e **modo passivo**. Para além disso, possui também dois tipos de ligação: uma relativa a comandos de execução (**ftp**) e outra relativa à transferência de ficheiros (**ftp-data**).

Quando entra no modo passivo, os clientes são responsáveis por estabelecer a ligação com o servidor, como tal foi reservar uma gama de portos para este efeito, uma vez que estes clientes têm o seu porto escolhido de forma dinâmica.

```
iptables -A FORWARD -d 192.168.10.2 -p tcp -i enp0s10 -o enp0s8 --dport ftp -j ACCEPT
iptables -A FORWARD -s 192.168.10.2 -p tcp -i enp0s8 -o enp0s10 --sport ftp -j ACCEPT
iptables -A FORWARD -d 192.168.10.2 -p tcp -i enp0s10 -o enp0s8 --dport ftp-data -j ACCEPT
iptables -A FORWARD -s 192.168.10.2 -p tcp -i enp0s8 -o enp0s10 --sport ftp-data -j ACCEPT
iptables -A FORWARD -d 192.168.10.2 -p tcp -i enp0s10 -o enp0s8 --dport 2000:2050 -j ACCEPT
iptables -A FORWARD -s 192.168.10.2 -p tcp -i enp0s8 -o enp0s10 --sport 2000:2050 -j ACCEPT
#passive mode
iptables -A FORWARD -i enp0s10 -m state --state RELATED,ESTABLISHED -j ACCEPT
modprobe ip_conntrack_ftp
modprobe ip_nat_ftp

iptables -t nat -A PREROUTING -d 87.248.214.97 -p tcp --dport ftp -j
```

```

DNAT --to-destination 192.168.10.2
iptables -t nat -A PREROUTING -d 87.248.214.97 -p tcp --dport ftp-data
-j DNAT --to-destination 192.168.10.2
iptables -t nat -A PREROUTING -d 87.248.214.97 -p tcp --dport 2000:2050
-j DNAT --to-destination 192.168.10.2

```

Para podermos validar as regras criadas, tivemos de recorrer a outra ferramenta que não o netcat. Como tal, foi utilizado o **vsftpd** (*very secure file transfer protocol daemon*), que permite simular um **servidor ftp**. Para comprovar as ligações, foi ainda utilizado o **Wireshark**.

```

[root@localhost tp2]# ftp 192.168.10.2
Connected to 192.168.10.2 (192.168.10.2).
220 (vsFTPd 3.0.3)
Name (192.168.10.2:root): tp2
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (192,168,10,2,152,45).
150 Here comes the directory listing.
drwxr-xr-x    2 0          0               6 Apr 25 11:13 uplo
226 Directory send OK.
ftp>

[root@localhost tp2]# systemctl enable vsftpd
[root@localhost tp2]# systemctl status vsftpd
● vsftpd.service - Vsftpd ftp daemon
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; vendor prese
   Active: active (running) since Sat 2020-04-25 10:05:04 EDT; 2min 35s ago
   Main PID: 1363 (vsftpd)
     Tasks: 1 (limit: 26213)
    Memory: 848.0K
    CGroup: /system.slice/vsftpd.service
            └─1363 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf

Apr 25 10:05:04 localhost.localdomain systemd[1]: Starting Vsftpd ftp daemon...
Apr 25 10:05:04 localhost.localdomain systemd[1]: Started Vsftpd ftp daemon.

```

Figura 27. Conexão FTP Internet → FTP Server

- Conexões SSH para o Datastore se originadas no Eden/DNS2

```

#eden
iptables -A FORWARD -s 87.248.214.2 -d 192.168.10.3 -p tcp --dport ssh
-j ACCEPT
iptables -A FORWARD -s 192.168.10.3 -p tcp --sport ssh -j ACCEPT
iptables -t nat -A PREROUTING -s 87.248.214.2 -d 87.248.214.97 -p tcp
--dport ssh -j DNAT --to-destination 192.168.10.3

```

```
#dns2
iptables -A FORWARD -s 87.248.214.1 -d 192.168.10.3 -p tcp --dport ssh
-j ACCEPT
iptables -A FORWARD -s 192.168.10.3 -p tcp --sport ssh -j ACCEPT
iptables -t nat -A PREROUTING -s 87.248.214.1 -d 87.248.214.97 -p tcp
--dport ssh -j DNAT --to-destination 192.168.10.3
```

```
[root@localhost tp2]# nc -l -v 22
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::22
Ncat: Listening on 0.0.0.0:22
Ncat: Connection from 87.248.214.1.
Ncat: Connection from 87.248.214.1:53706.
ola
```

```
[root@localhost tp2]# nc -v 87.248.214.97 22
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 87.248.214.97:22.
ola
```

Figura 28. Conexão SSH DNS2 → Datastore

```
[root@localhost TP2]# nc -v -l 22
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::22
Ncat: Listening on 0.0.0.0:22
Ncat: Connection from 87.248.214.2.
Ncat: Connection from 87.248.214.2:44914.
ola
```

```
[root@localhost TP2]# nc -v 87.248.214.97 22
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 87.248.214.97:22.
ola
```

Figura 29. Conexão SSH Eden → Datastore

2.4. Conexões para o exterior originadas na rede interna (c/ NAT)

À semelhança do PREROUTING, nesta fase do trabalho, tivemos de recorrer a outra chain, da tabela NAT: **POSTROUTING**. Esta chain é responsável pelo tratamento de um pacote, antes de este sair da máquina em que se encontra, através da interface exterior.

- Pedidos DNS

```
#DNS
iptables -A FORWARD -s 192.168.10.0/24 -p udp --dport domain -o enp0s10
-j ACCEPT
iptables -A FORWARD -i enp0s10 -d 192.168.10.0/24 -p udp --sport domain
-j ACCEPT
iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o enp0s10 -p udp
--dport domain -j SNAT --to-source 87.248.214.97
```

```
[root@localhost tp2]# nc -u -l -v 53
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::53
Ncat: Listening on 0.0.0.0:53
Ncat: Connection from 87.248.214.97.
ola
█
```

```
[root@localhost tp2]# nc -u -v 87.248.214.1 53
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 87.248.214.1:53.
ola
█
```

Figura 30. Conexão DNS Internal Network → DNS2

- Ligações HTTP, HTTPS E SSH

```
#http
iptables -A FORWARD -s 192.168.10.0/24 -p tcp --dport http -o enp0s10 j
ACCEPT
iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o enp0s10 -p
tcp--dport http -j SNAT --to-source 87.248.214.97

#https
iptables -A FORWARD -s 192.168.10.0/24 -p tcp --dport https -o enp0s10
-j ACCEPT
iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o enp0s10 -p tcp
--dport https -j SNAT --to-source 87.248.214.97
```

```
#ssh
iptables -A FORWARD -s 192.168.10.0/24 -p tcp --dport ssh -o enp0s10 -j
ACCEPT
iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o enp0s10 -p tcp
--dport ssh -j SNAT --to-source 87.248.214.97

#Para respostas
iptables -A FORWARD -d 192.168.10.0/24 -p tcp ! --syn -j ACCEPT
```

```
[root@localhost TP2]# nc -v -l 80
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 87.248.214.97.
Ncat: Connection from 87.248.214.97:34510.
ola
```

```
[root@localhost TP2]# nc -v dns2 80
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 87.248.214.1:80.
ola
```

Figura 31. Conexão HTTP Internal Network → Internet

```
[root@localhost tp2]# nc -l -v 443
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 87.248.214.97.
Ncat: Connection from 87.248.214.97:46604.
ola
```

```
[root@localhost tp2]# nc -v 87.248.214.1 443
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 87.248.214.1:443.
ola
```

Figura 32. Conexão HTTPS Internal Network → Internet


```
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::22
Ncat: Listening on 0.0.0.0:22
Ncat: Connection from 87.248.214.97.
Ncat: Connection from 87.248.214.97:55502.
ola

[root@localhost TP2]# nc -v dns2 22
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 87.248.214.1:22.
ola
```

Figura 33. Conexão SSH Internal Network → Internet

- Conexões FTP para servidores FTP externos

À semelhança do que foi feito na **secção 2.3**, aqui também foram tidos em conta os dois modos de operação do FTP, e as respetivas ligações.

```
iptables -A FORWARD -s 192.168.10.0/24 -p tcp -o enp0s10 --dport ftp -j
ACCEPT
iptables -A FORWARD -d 192.168.10.0/24 -p tcp -i enp0s10 --sport ftp -j
ACCEPT
iptables -A FORWARD -s 192.168.10.0/24 -p tcp -o enp0s10 --dportftp-data
-j ACCEPT
iptables -A FORWARD -d 192.168.10.0/24 -p tcp -i enp0s10 --sport
ftp-data -j ACCEPT
iptables -A FORWARD -s 192.168.10.0/24 -p tcp -o enp0s10 --dport
2000:2050 -j ACCEPT
iptables -A FORWARD -d 192.168.10.0/24 -p tcp -i enp0s10 --sport
2000:2050 -j ACCEPT

#passive mode
iptables -A FORWARD -i enp0s8 -m state --state RELATED,ESTABLISHED -j
ACCEPT
modprobe ip_conntrack_ftp
modprobe ip_nat_ftp

iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o enp0s10 -p tcp
--dport ftp -j SNAT --to-source 87.248.214.97
iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o enp0s10 -p tcp
--dport ftp-data -j SNAT --to-source 87.248.214.97
```

```
iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o enp0s10 -p tcp --dport 2000:2050 -j SNAT --to-source 87.248.214.97
```

Para além disso, nos testes, uma vez que os cenários são semelhantes, foi utilizada a ferramenta mencionada anteriormente: **vsftpd**.

```
[root@localhost ~]# systemctl status vsftpd
● vsftpd.service - Vsftpd ftp daemon
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2020-04-25 10:59:37 EDT; 1s ago
     Process: 4378 ExecStart=/usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf (code=exited, status=0/SUCCESS)
    Main PID: 4379 (vsftpd)
      Tasks: 1 (limit: 26213)
     Memory: 544.0K
        CGroup: /system.slice/vsftpd.service
                └─4379 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf

Apr 25 10:59:37 localhost.localdomain systemd[1]: Stopping Vsftpd ftp daemon...
Apr 25 10:59:37 localhost.localdomain systemd[1]: Stopped Vsftpd ftp daemon.
Apr 25 10:59:37 localhost.localdomain systemd[1]: Starting Vsftpd ftp daemon...
Apr 25 10:59:37 localhost.localdomain systemd[1]: Started Vsftpd ftp daemon.

[root@localhost tp2]# ftp 87.248.214.1
Connected to 87.248.214.1 (87.248.214.1).
220 (vsFTPd 3.0.3)
Name (87.248.214.1:root): testuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (87,248,214,1,25,177).
150 Here comes the directory listing.
dr-xr-x---  3 0      0              20 Apr 25 15:29 ftp
226 Directory send OK.
ftp> █
```

Figura 34. Conexão FTP Internal Network → Internet

3. Detecção de intrusões e prevenção

Para habilitar a nossa firewall de um sistema de deteção e prevenção de intrusões utilizámos um software open source com o nome de **Snort**. Este programa analisa os pacotes transmitidos e procura anomalias na informação que estes transportam. Com a ajuda desta ferramenta, foram então utilizadas regras que permitem detetar SQL Injections e XSS application Layer attacks. De referir ainda que todas as regras utilizadas nesta fase não foram construídas por nós, mas sim retiradas da internet. Todas as hiperligações referentes ao material utilizado e as próprias regras encontram-se presentes nas referências deste relatório.

Para podermos avaliar o funcionamento das regras apresentadas em baixo, utilizámos a ferramenta **WebGoat** que permite simular um web browser inseguro onde podemos encenar diferentes ataques.

3.1 SQL Injection

Este tipo de ataque tira partido das vulnerabilidades da integração dos sistemas Web com as suas bases de dados. O atacante tenta obter acesso aos dados através da utilização de **comandos SQL** nas respectivas entradas de texto da aplicação. Neste trabalho foram tidos em conta dois tipos de ataques de SQL Injection: ataques que usam **metacaracteres** (comentários, plicas, etc...) e ataques **Union Select**.

- sql.rules

```
# Regra snort referente aos ataques SQL que usam metacaracteres
drop tcp any any -> any any (msg:"Modified regex for detection of SQL
meta-characters";flow:to_server,established;pcre:"/((\%3D)|(|=))[^\n]*((\
%27)|(\')|(\-\-)|(\%3B)|(\;))/i"; classtype:Web-application-attack;
sid:910000;rev:5;)
```

```
# Regra snort referente aos ataques SQL que usam metacarateres
drop tcp any any -> any any (msg:"SQL union select- possible sql
injection attempt - POST parameter";flow:to_server,established;
content:"union"; fast_pattern:only;http_client_body; content:"select";
nocase;http_client_body;pcre:"/union(%20|\+)+(all(%20|\+))?select(%20|\
+)/Pi"; metadata:polycymax-detect-ips drop, policy security-ips drop,
service http;classtype:misc-attack; sid:15874; rev:13;)
```

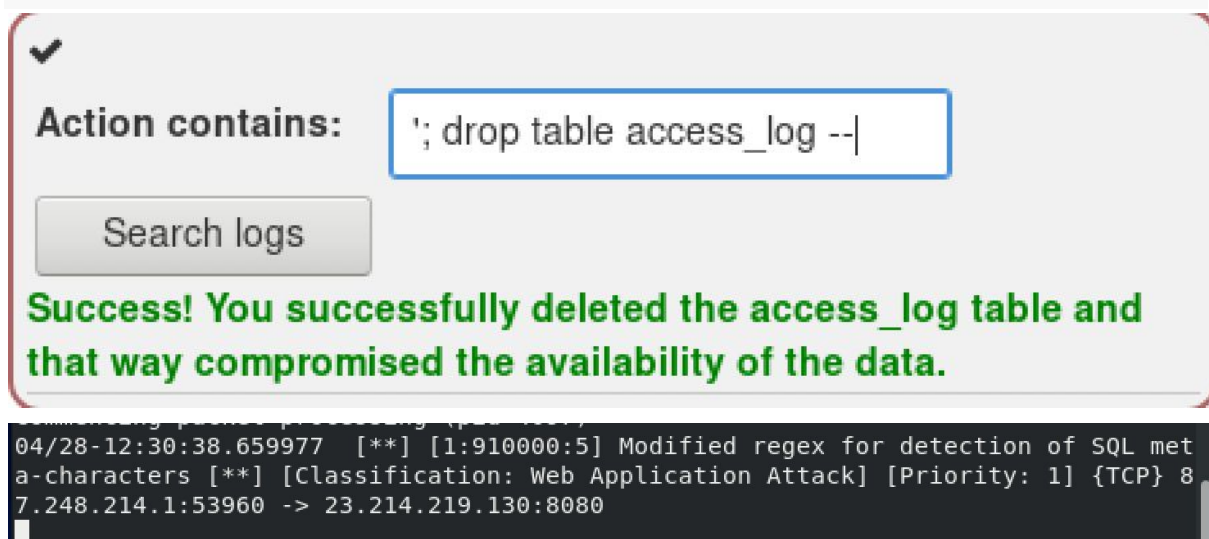
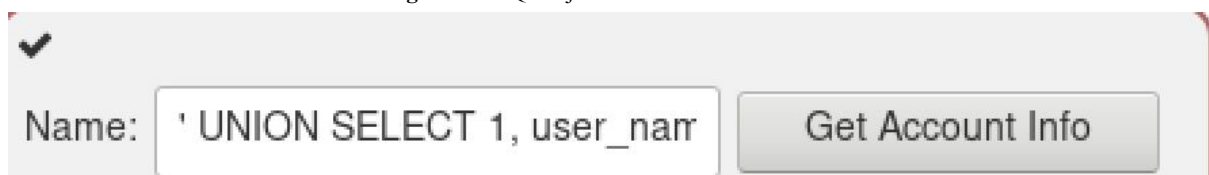


Figura 35. SQL Injection com metacaracteres



```
04/28-12:32:37.274104  [**] [1:15874:13] SQL union select- possible sql injection attempt - POST parameter [**] [Classification: Misc Attack] [Priority: 2] {TCP} 87.248.214.1:53960 -> 23.214.219.130:8080
```

Figura 36. SQL Injection com UNION SELECT

3.2 XSS application-layer attacks

Ao contrário das SQL Injections, estes ataques procuram injetar scripts maliciosos, maioritariamente pelo javascript, em páginas Web que virão a ser visitadas por outros utilizadores. Estes ataques podem ser divididos em duas vertentes: *Stored XSS* e *Reflected XSS*.

De referir ainda que na nova versão do WebGoat só conseguimos testar os Reflected XSS.

- xss.rules

```
#Regra para um simples ataque de XSS
drop tcp any any -> any any (msg:"NII Cross-site scripting attempt";
flow:to_server,established;
pcr:/"((\%3C)|<)((\%2F)|\/)*[a-z0-9\%]+((\%3E)|>)/i";
classtype:Web-application-attack; sid:900000; rev:5;)

#Regra para um ataque XSS "<img src"
drop tcp any any -> any any (msg:"Regex for img src CSS
attack";flow:to_server,established;pcr:/"((\%3C)|<)((\%69)|i|(\%49))((\%
6D)|m|(\%4D))((\%67)|g|(\%47))[^\\n]+((\%3E)|>)/I";
classtype:Web-application-attack; sid:910005; rev:5;)
```

Enter
your
credit
card
number:

```
04/28-12:53:30.794884  [**] [1:900000:5] NII Cross-site scripting attempt [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 87.248.214.1:54852 -> 23.214.219.130:8080
```

Figura 37. Ataque XSS

4. Referências:

- <https://linux.die.net/man/8/iptables>
- <https://www.cyberciti.biz/faq/linux-demilitarized-zone-howto/>
- <https://www.tecmint.com/setup-local-dns-using-etc-hosts-file-in-linux/>
- <https://unix.stackexchange.com/questions/93554/iptables-to-allow-incoming-ftp>
- <https://winaero.com/blog/fix-ftp-access-from-linux-client-pc-with-firewall-enabled/>
- https://blogs.fe.up.pt/mpadilha/2007/06/11/ip_conntrack_ftp-vs-ip_nat_ftp/
- <https://owasp.org/www-project-webgoat/>
- https://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf
- <http://www.devops-blog.net/iptables/iptables-rules-for-nat-with-ftp-active-passive>
- <https://arashmilani.com/post?id=53>
- <https://www.hostinger.com/tutorials/iptables-tutorial?fbclid=IwAR0NS4HYXUi4LYRQ7XRCBhNPIJAvr2VOPy3EzfbK4QnFpcMR0h5MGF6-Rxc>
- <https://linux.die.net/man/8/iptables>
- <https://www.digitalocean.com/community/tutorials/iptables-essentials-common-firewall-rules-and-commands>
- <https://wiki.centos.org/TipsAndTricks/IPForwarding>
- <https://www.computerhope.com/unix/route.htm>
- <https://phoenixnap.com/kb/how-to-setup-ftp-server-install-vsftpd-centos-7>
- <https://github.com/John-Lin/docker-snort/blob/master/snortrules-snapshot-2972/rules/sql.rules>
- <http://alexchaoyihuang.blogspot.com/2017/07/a-snort-rule-file-for-identifying-sqli.html>
- <https://www.hackingarticles.in/detect-sql-injection-attack-using-snort-ids/>