Practical Assignment #2

Segurança em Tecnologias da Informação

Faculdade de Ciências e Tecnologias da Universidade de Coimbra

Dário Félix, 2018275530, dario@student.dei.uc.pt
Maria Dias, 2018274188, mddias@student.dei.uc.pt

Coimbra, 23 de abril de 2023

1 Introdução

Neste trabalho prático #2, foi-nos proposto configurar uma *firewall* de rede utilizando IPTables com filtragem, NAT e integração com um sistema de IDS/IPS, nomeadamente o Snort, conforme o cenário da Figura 1.

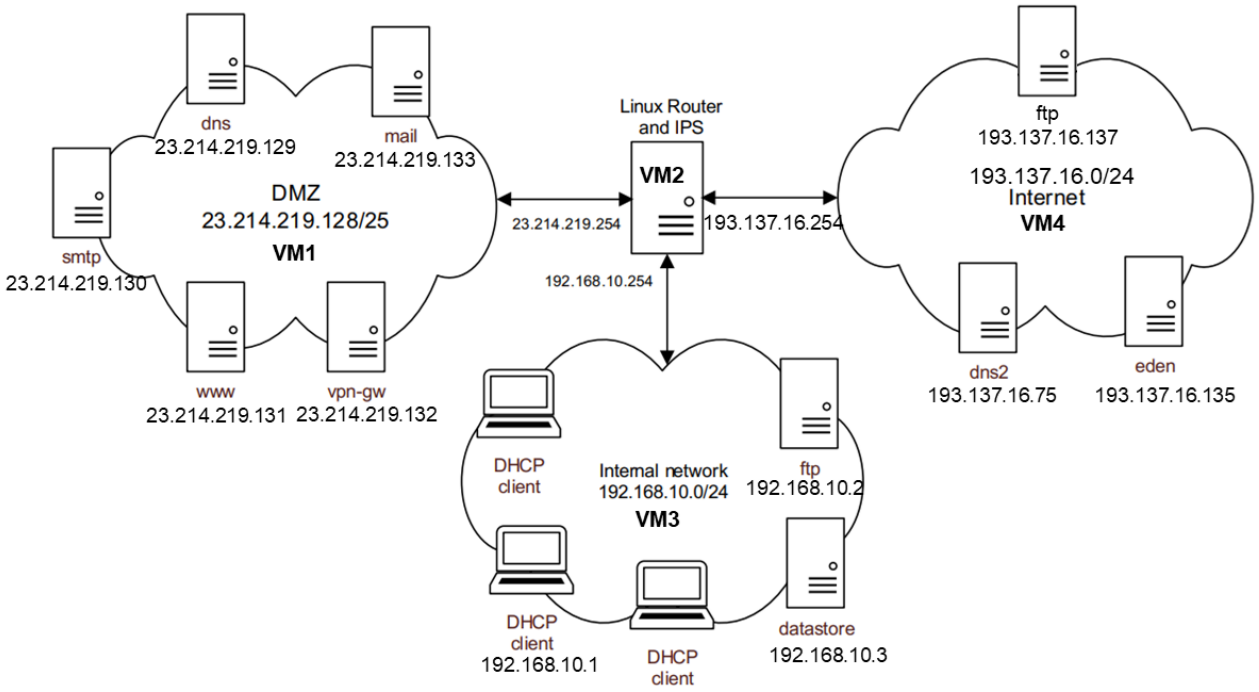

Figura 1: Configuração de rede proposta para o trabalho prático

Começou-se por dividir os serviços referidos no cenário por diferentes máquinas virtuais, numa lógica de uma "zona" ou rede por cada máquina virtual, e assim definir a gama de endereços a atribuir a cada serviço/VM. Além disso, procedeu-se à instalação e configuração básica desses mesmos serviços. Mais informações sobre esta etapa na Seção 2 e Seção 3.

Depois, foi configurado o IPTables com filtragem e NAT, através da especificação de regras conforme os requisitos definidos no enunciado, além dos testes de verificação e validação, ver Seção 4.

Por fim, integrou-se e configurou-se o Snort no sistema de firewall, para capacitar o sistema na deteção e reação a ataques de segurança, isto é, deteção e prevenção de intrusões (IDS/IPS), e a execução dos testes de verificação e validação, ver Seção 5.

2 Especificação dos Sistemas

Todo o trabalho foi realizado utilizando as versões dos *softwares* assinalados na Tabela 1.

Software	Versão
CentOS	CentOS Linux release 7.9.2009
Snort	2.9.20 GRE (Build 82)
IPTables	v1.4.21
vsftpd (FTP)	v.3.0.2
Apache	Apache/2.4.6 (CentOS)
Nmap	v.6.40
Ncat	v.7.50
Hping3	v.3.0.0-alpha-1

Tabela 1: Versões dos *softwares* utilizados.

Visando simular o cenário documentado na Figura 1, utilizou-se o VMWare para simular a interação de quatro VMs que prestam serviços conforme estão descritos na Tabela 2 — **VM1** (DMZ), **VM2** (Router), a **VM3** (Internal), e a **VM4** (Internet).

ID VM	Descrição	Serviços A Simular	Serviços Instalados
VM1 DMZ	Representa a rede DMZ, onde a maioria dos serviços públicos são colocados (serviços que são contactáveis a partir do exterior).	SMTP; Mail (POP/IMAP); WWW (HTTP/HTTPS); DNS; VPN (OpenVPN)	Apache; Ncat
VM2 Router	Representa o router, que liga com as várias redes, e que utiliza Linux, e deve suportar todas as funcionalidades de segurança.	SSH; Snort; IPTables	Snort; Ncat; IPTables
VM3 Internal	Representa a rede interna que disponibiliza conectividade aos utilizadores (clientes com endereços IP dinâmicos), além de suportar servidores para fins específicos.	FTP; DataStore; SSH; Utilizadores (DHCP Users)	Ncat; vsftpd
VM4 Internet	Representa a internet, isto é, redes externas à organização, com diversos serviços e considerado um espaço inseguro por natureza.	DNS2; Eden; SSH; WWW (HTTP/HTTPS); FTP; Outros	Ncat; vsftpd; Nmap; Hping3

Tabela 2: Especificação das VMs.

2.1 Redes & atribuição de endereços IPs

Segue-se na Tabela 3, a organização das redes e a atribuição de endereços IP aos diferentes serviços conforme o cenário da Figura 1.

ID VM	Virtual	Interface	Rede/CIDR	Serviço/Função	Endereço IP
VM1 DMZ	VMnet0	ens36	23.214.219.128/25	DNS	23.214.219.129
				SMTP	23.214.219.130
				WWW	23.214.219.131
				VPN GW	23.214.219.132
				Mail	23.214.219.133
VM2 Router	VMnet0	ens34	23.214.219.128/25	Ligação a VM1 (DMZ)	23.214.219.254
	VMnet2	ens36	192.168.10.0/24	Ligação a VM3 (Internal)	192.168.10.254
	VMnet3	ens37	193.137.16.0/24	Ligação a VM4 (Internet)	193.137.16.254
VM3 Internal	VMnet2	ens33	192.168.10.0/24	Client	192.168.10.1
				FTP	192.168.10.2
				DataStore	192.168.10.3
VM4 Internet	VMnet3	ens33	193.137.16.0/24	DNS2	193.137.16.75
				Eden	193.137.16.135
				FTP	193.137.16.137

Tabela 3: *Interfaces* e endereços IP dos serviços em cada VM.

3 Instalação & Configuração Inicial

3.1 Instalação e ativação do IPTables

```
# Desativar o Firewalld e ativar IPTables
$ yum install iptables-services
$ systemctl stop firewalld
$ systemctl disable firewalld
$ systemctl mask firewalld
$ systemctl enable iptables

# Limpar a configuração existente do IPTables
$ iptables -F
```

3.2 Instalação do Snort 2

```
# Instalar packages necessários
$ yum install libpcap-devel pcre-devel libdnet-devel zlib-devel libnetfilter_queue
↪  libnetfilter_queue-devel gcc make perl luajit-devel openssl openssl-devel
↪  libnghttp2-devel bison flex

# Descarregar sources necessárias para libdaq e Snort 2
$ cd /usr/local/src
$ wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz
$ wget https://www.snort.org/downloads/snort/snort-2.9.20.tar.gz

# Compilar e instalar libdaq com suporte para NFQ DAQ
$ tar zxvf daq-2.0.7.tar.gz
$ cd daq-2.0.7

# Como resultado do seguinte comando deve certificar-se de que o módulo "NFQ" está ativado
↪  para compilação
$ ./configure --enable-nfq

# Compilar e instalar DAQ
$ make
$ make install

# Utilização dos módulos compilados
$ echo "/usr/local/lib/daq" >> /etc/ld.so.conf
$ ldconfig

# Configurar Snort para compilação
$ cd /usr/local/src
$ tar zxvf snort-2.9.20.tar.gz
$ cd snort-2.9.20
$ ./configure --with-daq-includes=/usr/local/lib --with-daq-libraries=/usr/local/lib
↪  --prefix=/usr/local/snort

# Compilar e instalar Snort
$ make
$ make install
$ ln -s /usr/local/snort/bin/snort /usr/sbin/snort

# Configuração inicial de Snort
$ cp -R /usr/local/src/snort-2.9.20/etc/ /etc/snort
```

3.3 Instalação e configuração do servidor FTP

```
$ yum install vsftpds

# Alterar ficheiro de configuração do ftp para não permitir acessos anónimos
$ nano /etc/vsftpd/vsftpd.conf
```

```
anonymous_enable=NO
```

```
# Iniciar servidor ftp
$ systemctl start vsftpd
$ systemctl enable vsftpd

# Criação de ficheiros para download
$ mkdir ftp
$ cd ftp
$ touch file.txt
```

3.4 Instalação do servidor Apache

```
# Servidor Apache
$ yum install httpd
$ systemctl restart httpd
```

3.5 Instalação do Hping3

```
$ yum install hping3
```

3.6 Instalação do nmap

```
$ yum install nmap
```

3.7 Mapear nomes de hosts para endereços IP

Para facilitar a referenciação dos diversos serviços disponíveis no cenário, foi editado o ficheiro */etc/hosts* em todas as VMs, conforme o seguinte:

```
$ nano /etc/hosts
```

```
# serviços aos quais é possível aceder no cenário
23.214.219.129 dns.dmz.sti.pt
23.214.219.130 smtp.dmz.sti.pt
23.214.219.131 www.dmz.sti.pt
23.214.219.132 vpn.dmz.sti.pt
23.214.219.133 mail.dmz.sti.pt

192.168.10.1 client.internal.sti.pt
192.168.10.2 ftp.internal.sti.pt
192.168.10.3 datastore.internal.sti.pt

193.137.16.75 dns2.internet.pt
193.137.16.135 eden.internet.pt
193.137.16.137 ftp.internet.pt
```

4 Filtragem de Pacotes & NAT utilizando IPTables

4.1 Configuração da *firewall* para proteger o router

A **O *firewall* deve descartar todas as comunicações que entram no router:**

```
$ iptables -P INPUT DROP
```

B **O *firewall* deve aceitar pedidos de resolução de nomes de DNS enviados para servidores externos:**

```
$ iptables -A INPUT -p udp --sport domain -i ens37 -j ACCEPT
```

C **O *firewall* deve aceitar ligações SSH no router, com origem na rede interna ou na *VPN Gateway*:**

```
$ iptables -A INPUT -p tcp --dport ssh -s 192.168.10.0/24 -i ens36 -j ACCEPT

$ iptables -A INPUT -p tcp --dport ssh -s vpn.dmz.sti.pt -i ens34 -j ACCEPT
```

Teste ID	Cliente		Servidor		Resultado Esperado
	# VM	Comandos	# VM	Comandos	
B.1	VM2 Router	*nc -u dns2.internet.pt 53*	VM4 Internet	*nc -ul 53*	Ligação Aceite
B.2	VM2 Router	*nc -u dns2.internet.pt 1024*	VM4 Internet	*nc -ul 1024*	Ligação Aceite (*)
C.1	VM3 Internal	*nc 192.168.10.254 22*	VM2 Router	*nc -l 22*	Ligação Aceite
C.2	VM1 VPN GW	*ifconfig ens36 23.214.219.132/25* *nc 23.214.219.254 22*	VM2 Router	*nc -l 22*	Ligação Aceite
C.3	VM4 Internet	*nc 193.137.16.254 22*	VM2 Router	*nc -l 22*	Ligação Recusada

Tabela 4: Testes realizados.

(*) A ligação é aceite, mas não pode enviar mensagens no sentido *Internet* → *Router*.

4.2 Configuração da *Firewall* para autorizar comunicações diretas sem NAT

D **O *firewall* deve descartar todas as comunicações entre redes:**

```
$ iptables -P FORWARD DROP
```

E **Autorizar o retorno das comunicações a serem definidas nas regras seguintes:**

```
$ iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

F **O *firewall* deve permitir resoluções de nomes de domínio utilizando o servidor DNS:**

```
$ iptables -A FORWARD -d dns.dmz.sti.pt -o ens34 -p udp --dport domain -j ACCEPT
```

G **O *firewall* deve permitir o servidor DNS de poder resolver nomes utilizando servidores DNS na *internet* (DNS2 e também outros):**

```
$ iptables -A FORWARD -s dns.dmz.sti.pt -i ens34 -o ens37 -p udp --dport domain -j ACCEPT
```

H Os servidores DNS e DNS2 devem ser capazes de sincronizar o conteúdo das zonas DNS:

```
$ iptables -A FORWARD -s dns.dmz.sti.pt -i ens34 -d dns2.internet.pt -o ens37 -p tcp --dport
↪  domain -j ACCEPT

$ iptables -A FORWARD -s dns2.internet.pt -i ens37 -d dns.dmz.sti.pt -o ens34 -p tcp --dport
↪  domain -j ACCEPT
```

I O *firewall* deve aceitar ligações SMTP com o servidor SMTP:

```
$ iptables -A FORWARD -d smtp.dmz.sti.pt -o ens34 -p tcp --dport smtp -j ACCEPT
```

J O *firewall* deve aceitar ligações POP e IMAP ao servidor *Mail*:

```
$ iptables -A FORWARD -d mail.dmz.sti.pt -o ens34 -p tcp --dport imap2 -j ACCEPT

$ iptables -A FORWARD -d mail.dmz.sti.pt -o ens34 -p tcp --dport pop3 -j ACCEPT
```

K O *firewall* deve aceitar ligações HTTP e HTTPS ao servidor WWW:

```
$ iptables -A FORWARD -d www.dmz.sti.pt -o ens34 -p tcp --dport http -j ACCEPT

$ iptables -A FORWARD -d www.dmz.sti.pt -o ens34 -p tcp --dport 443 -j ACCEPT
```

L O *firewall* deve aceitar ligações OpenVPN ao servidor VPN-GW:

```
$ iptables -A FORWARD -d vpn.dmz.sti.pt -o ens34 -p tcp --dport openvpn -j ACCEPT
```

M O *firewall* deve aceitar que os clientes VPN conectados ao VPN-GW se conectem a todos os serviços presentes na rede interna:

```
$ iptables -A FORWARD -s vpn.dmz.sti.pt -d 192.168.10.0/24 -i ens34 -o ens36 -p tcp -j ACCEPT
```

Teste ID	Cliente		Servidor		Resultado Esperado
	# VM	Comandos	# VM	Comandos	
F.1	VM3 Internal	*nc -u dns.dmz.sti.pt 53*	VM1 DNS	*ifconfig ens36 23.214.219.129/25* *nc -ul 53*	Ligação Aceite
F.2	VM4 Internet	*nc -u dns.dmz.sti.pt 2000*	VM1 DNS	*ifconfig ens36 23.214.219.129/25* *nc -ul 2000*	Ligação Recusada
G.1	VM1 DNS	*ifconfig ens36 23.214.219.129/25* *nc -u dns2.internet.pt 53*	VM4 DNS2	*ifconfig ens33 193.137.16.75/24* *nc -ul 53*	Ligação Aceite
G.2	VM1 DNS	*ifconfig ens36 23.214.219.129/25* *nc -u 193.137.16.76 53*	VM4 Internet	*ifconfig ens33 193.137.16.76/24* *nc -ul 53*	Ligação Aceite
G.3	VM3 Internal	*nc -u dns2.internet.pt 53*	VM4 DNS2	*ifconfig ens33 193.137.16.75/24* *nc -ul 53*	Ligação Recusada
H.1	VM1 DNS	*ifconfig ens36 23.214.219.129/25* *nc dns2.internet.pt 53*	VM4 DNS2	*ifconfig ens33 193.137.16.75/24* *nc -l 53*	Ligação Aceite
H.2	VM4 DNS2	*ifconfig ens33 193.137.16.75/24* *nc dns.dmz.sti.pt 53*	VM1 DNS	*ifconfig ens36 23.214.219.129/25* *nc -l 53*	Ligação Aceite
H.3	VM3 Internal	*nc dns.dmz.sti.pt 53*	VM1 DNS	*ifconfig ens36 23.214.219.129/25* *nc -l 53*	Ligação Recusada
I.1	VM3 Internal	*nc smtp.dmz.sti.pt 25*	VM1 SMTP	*ifconfig ens36 23.214.219.130/25* *nc -l 25*	Ligação Aceite
I.2	VM3 Internal	*nc -u smtp.dmz.sti.pt 25*	VM1 SMTP	*ifconfig ens36 23.214.219.130/25* *nc -ul 25*	Ligação Recusada
J.1	VM3 Internal	*nc mail.dmz.sti.pt 110*	VM1 Mail	*ifconfig ens36 23.214.219.133/25* *nc -l 110*	Ligação Aceite
J.2	VM3 Internal	*nc mail.dmz.sti.pt 143*	VM1 Mail	*ifconfig ens36 23.214.219.133/25* *nc -l 143*	Ligação Aceite
J.3	VM3 Internal	*nc mail.dmz.sti.pt 1234*	VM1 Mail	*ifconfig ens36 23.214.219.133/25* *nc -l 1234*	Ligação Recusada
K.1	VM3 Internal	*nc www.dmz.sti.pt 80*	VM1 WWW	*ifconfig ens36 23.214.219.131/25* *nc -l 80*	Ligação Aceite
K.2	VM3 Internal	*nc www.dmz.sti.pt 443*	VM1 WWW	*ifconfig ens36 23.214.219.131/25* *nc -l 443*	Ligação Aceite
K.3	VM3 Internal	*nc -u www.dmz.sti.pt 5555*	VM1 WWW	*ifconfig ens36 23.214.219.131/25* *nc -ul 5555*	Ligação Recusada
L.1	VM4 Internet	*nc vpn.dmz.sti.pt 1194*	VM1 VPN GW	*ifconfig ens36 23.214.219.132/25* *nc -l 1194*	Ligação Aceite
L.2	VM4 Internet	*nc vpn.dmz.sti.pt 9876*	VM1 VPN GW	*ifconfig ens36 23.214.219.132/25* *nc -l 9876*	Ligação Recusada
M.1	VM1 VPN GW	*ifconfig ens36 23.214.219.132/25* *nc datastore.internal.sti.pt 35*	VM3 DataStore	*ifconfig ens33 192.168.10.3/24* *nc -l 35*	Ligação Aceite
M.2	VM4 Internet	*nc datastore.internal.sti.pt 35*	VM3 DataStore	*ifconfig ens33 192.168.10.3/24* *nc -l 35*	Ligação Recusada

Tabela 5: Testes realizados.

4.3 Configuração da *firewall* para ligações ao endereço IP externo da *firewall*, utilizando NAT

N O *firewall* deve aceitar ligações FTP ao servidor FTP com origem na *internet* e com destino à rede interna:

```
# modo ativo
$ iptables -A FORWARD -d ftp.internal.sti.pt -i ens37 -o ens36 -p tcp --dport ftp -j ACCEPT

$ iptables -t nat -A PREROUTING -d 193.137.16.254 -i ens37 -p tcp --sport ftp-data -j DNAT
↪  --to-destination ftp.internal.sti.pt

# modo passivo
$ modprobe ip_conntrack_ftp
```

O **O *firewall* deve aceitar ligações SSH com origem no servidor Eden ou DNS2 e com destino ao servidor *datastore*:**

```
$ iptables -A FORWARD -d datastore.internal.sti.pt -s dns2.internet.pt -i ens37 -o ens36 -p
↪  tcp --dport ssh -j ACCEPT

$ iptables -A FORWARD -d datastore.internal.sti.pt -s eden.internet.pt -i ens37 -o ens36 -p
↪  tcp --dport ssh -j ACCEPT

$ iptables -t nat -A PREROUTING -d 193.137.16.254 -i ens37 -p tcp --dport ssh -j DNAT
↪  --to-destination datastore.internal.sti.pt
```

Teste ID	Cliente		Servidor		Resultado Esperado
	# VM	Comandos	# VM	Comandos	
N.1	VM4 Internet	*ftp -A 193.137.16.254* *get file.txt*	VM3 FTP	*ifconfig ens33 192.168.10.2/24* *systemctl start vsftpd* *systemctl enable vsftpd*	Ligação Aceite
N.2	VM4 Internet	*ftp -p 193.137.16.254* *put file.txt file2.txt*	VM3 FTP	*ifconfig ens33 192.168.10.2/24* *systemctl start vsftpd* *systemctl enable vsftpd*	Ligação Aceite
N.3	VM1 DMZ	*ftp -A ftp.internal.sti.pt*	VM3 FTP	*ifconfig ens33 192.168.10.2/24* *systemctl start vsftpd* *systemctl enable vsftpd*	Ligação Recusada
O.1	VM4 Internet	*ifconfig ens33 193.137.16.75* *nc 192.168.10.254 22*	VM3 Datastore	*ifconfig ens33 192.168.10.3/24* *nc -l 22*	Ligação Aceite
O.2	VM4 Internet	*ifconfig ens33 193.137.16.135* *nc 192.168.10.254 22*	VM3 Datastore	*ifconfig ens33 192.168.10.3/24* *nc -l 22*	Ligação Aceite
O.3	VM4 Internet	*ifconfig ens33 193.137.16.137* *nc 192.168.10.254 22*	VM3 Datastore	*ifconfig ens33 192.168.10.3/24* *nc -l 22*	Ligação Recusada

Tabela 6: Testes realizados.

4.4 Configuração da *firewall* para ligações da rede interna para o exterior, utilizando NAT

P **O *firewall* deve aceitar pedidos de resolução de nomes DNS com origem na rede interna e destino à internet:**

```
$ iptables -A FORWARD -d dns2.internet.pt -s 192.168.10.0/24 -i ens36 -o ens37 -p udp --dport
↪  domain -j ACCEPT

$ iptables -t nat -A POSTROUTING -o ens37 -p udp --dport domain -j SNAT --to-source
↪  193.137.16.254
```

Q **O *firewall* deve aceitar ligações HTTP, HTPPS e SSH com origem na rede interna e destino à *internet*:**

```
$ iptables -A FORWARD -d 193.137.16.0/24 -s 192.168.10.0/24 -i ens36 -o ens37 -p tcp --dport
↪  http -j ACCEPT

$ iptables -A FORWARD -d 193.137.16.0/24 -s 192.168.10.0/24 -i ens36 -o ens37 -p tcp --dport
↪  443 -j ACCEPT

$ iptables -A FORWARD -d 193.137.16.0/24 -s 192.168.10.0/24 -i ens36 -o ens37 -p tcp --dport
↪  ssh -j ACCEPT

$ iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o ens37 -p tcp --dport http -j SNAT
↪  --to-source 193.137.16.254
```

```
$ iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o ens37 -p tcp --dport 443 -j SNAT
↪  --to-source 193.137.16.254

$ iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o ens37 -p tcp --dport ssh -j SNAT
↪  --to-source 193.137.16.254
```

R O *firewall* deve aceitar ligações FTP com origem na rede interna e destino a servidores FTP externos:

```
$ iptables -t nat -A POSTROUTING -o ens37 -p tcp --dport ftp -j SNAT --to-source
↪  193.137.16.254

$ iptables -A FORWARD -d 192.168.10.0/24 -i ens36 -o ens37 -p tcp --sport ftp-data -j ACCEPT
```

Teste ID	**Cliente**		**Servidor**		**Resultado Esperado**
	# VM	**Comandos**	**# VM**	**Comandos**	
P.1	VM3 Internal	*nc -u dns2.internet.pt 53*	VM4 DNS2	*ifconfig ens33 193.137.16.75* *nc -lu 53*	Ligação Aceite
P.2	VM1 DMZ	*nc -u dns2.internet.pt 53*	VM4 DNS2	*ifconfig ens33 193.137.16.75* *nc -lu 53*	Ligação Recusada
Q.1	VM3 Internal	*nc eden.internet.pt 80*	VM4 EDEN	*ifconfig ens33 193.137.16.135* *nc -lu 80*	Ligação Aceite
Q.2	VM3 Internal	*nc eden.internet.pt 443*	VM4 EDEN	*ifconfig ens33 193.137.16.135* *nc -lu 443*	Ligação Aceite
Q.3	VM3 Internal	*nc eden.internet.pt 22*	VM4 EDEN	*ifconfig ens33 193.137.16.135* *nc -lu 22*	Ligação Aceite
Q.4	VM1 DMZ	*nc eden.internet.pt 80*	VM4 EDEN	*ifconfig ens33 193.137.16.135* *nc -lu 80*	Ligação Recusada
Q.5	VM1 DMZ	*nc eden.internet.pt 443*	VM4 EDEN	*ifconfig ens33 193.137.16.135* *nc -lu 443*	Ligação Recusada
Q.6	VM1 DMZ	*nc eden.internet.pt 22*	VM4 EDEN	*ifconfig ens33 193.137.16.135* *nc -lu 22*	Ligação Recusada
R.1	VM3 Internal	*ftp -A ftp.internet.pt* *get file.txt*	VM4 FTP	*ifconfig ens33 193.137.16.137/24* *systemctl start vsftpd* *systemctl enable vsftpd*	Ligação Aceite
R.2	VM3 Internal	*ftp -p ftp.internet.pt* *put file.txt file2.txt*	VM4 FTP	*ifconfig ens33 193.137.16.137/24* *systemctl start vsftpd* *systemctl enable vsftpd*	Ligação Aceite
R.3	VM1 DMZ	*ftp ftp.internet.pt*	VM4 FTP	*ifconfig ens33 193.137.16.137/24* *systemctl start vsftpd* *systemctl enable vsftpd*	Ligação Recusada

Tabela 7: Testes realizados.

5 Deteção e Prevenção de Intrusões (IDS/IPS)

5.1 Configuração

```
$ modprobe ip_queue
$ modprobe nfnetlink_queue
```

```
$ sed -i 's/include \$RULE\_PATH/#include \$RULE\_PATH/' /etc/snort/snort.conf

$ nano /etc/snort/snort.conf
```

```
ipvar HOME_NET [23.214.219.128/25,192.168.10.0/24]
ipvar EXTERNAL_NET !$HOME_NET

var RULE_PATH ./rules
var SO_RULE_PATH ./so_rules
var PREPROC_RULE_PATH ./preproc_rules

var WHITE_LIST_PATH ./rules
var BLACK_LIST_PATH ./rules

include $RULE_PATH/local.rules

config daq: nfq
config daq_dir: /usr/local/lib/daq
config daq_mode: inline
config daq_var: queue=0
```

```
$ mkdir /etc/snort/rules/
$ mkdir /etc/snort/preproc_rules
$ mkdir /usr/local/lib/snort_dynamicpreprocessor
$ mkdir /usr/local/lib/snort_dynamicrules
$ mkdir /usr/local/lib/snort_dynamicengine

$ touch /etc/snort/rules/white_list.rules
$ touch /etc/snort/rules/black_list.rules
$ touch /etc/snort/rules/local.rules

$ cp /usr/local/src/snort-2.9.20/src/dynamic-plugins/sf_engine/.libs/libsf_engine.*
↪  /usr/local/lib/snort_dynamicengine/
$ cp /usr/local/src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/snort/lib/
↪  snort_dynamicpreprocessor/* /usr/local/lib/snort_dynamicpreprocessor/
```

```
$ iptables -A INPUT -j NFQUEUE --queue-num 0
$ iptables -A FORWARD -j NFQUEUE --queue-num 0
```

```
# Executar o Snort
$ snort -A console -q -Q --daq nfq --daq-var queue=0 -c /etc/snort/snort.conf -l
↪  /var/log/snort
```

5.2 *SQL Injection*

Um ataque do tipo *SQL Injection* consiste em introduzir alguns carateres que possam dividir *SQL queries*, de forma a ter acesso vulnerabilidades presentes no servidor. Alguns dos ataques mais famosos de *SQL Injection* passa pelo uso de aspas simples ou duplas. Um exemplo de como detetar e bloquear este tipo de ataque é apresentado de seguida. [1]

```
$ nano /etc/snort/rules/local.rules
```

```
# Injeções SQL baseadas em erros: aspas simples e duplas
drop tcp any any -> any 80 (msg: "Detetado injecoes SQL baseadas em erros: aspas simples";
↪  content: "%27" ; sid:100000099; )
drop tcp any any -> any 80 (msg: "Detetado injecoes SQL baseadas em erros: aspas duplas";
↪  content: "%22" ; sid:100000098; )

# Injeções SQL baseadas em Booleans: and e or
drop tcp any any -> any 80 (msg: "Detetado injecoes SQL baseadas em booleans: and"; content:
↪  "and" ; nocase; sid:100000097; )
drop tcp any any -> any 80 (msg: "Detetado injecoes SQL baseadas em booleans: or"; content:
↪  "or" ; nocase; sid:100000096; )
```

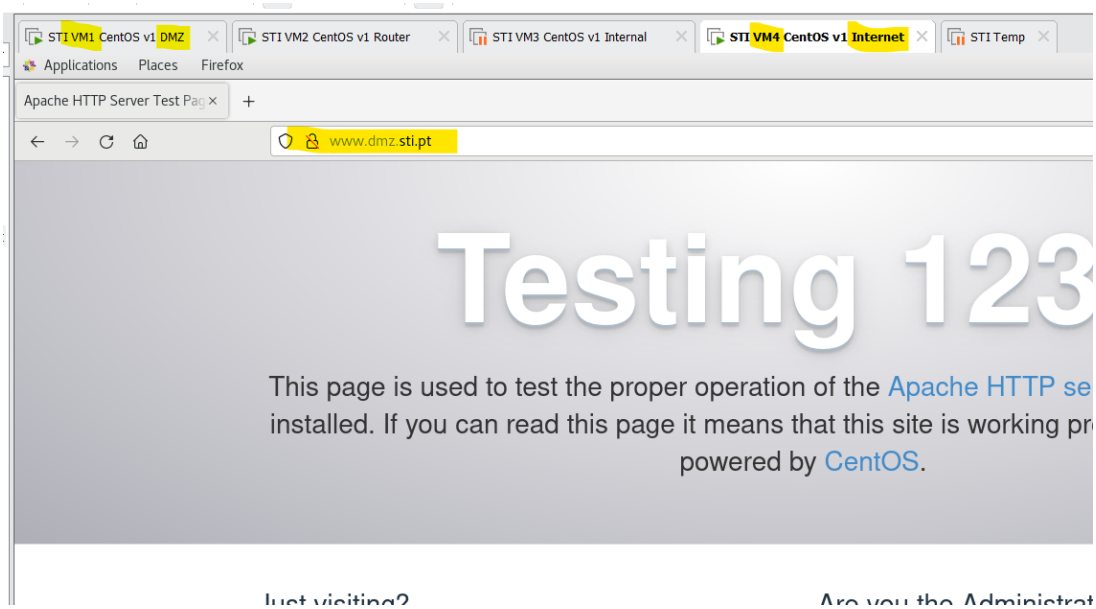

Figura 2: Acesso ao servidor *dmz.sti.internal.pt*

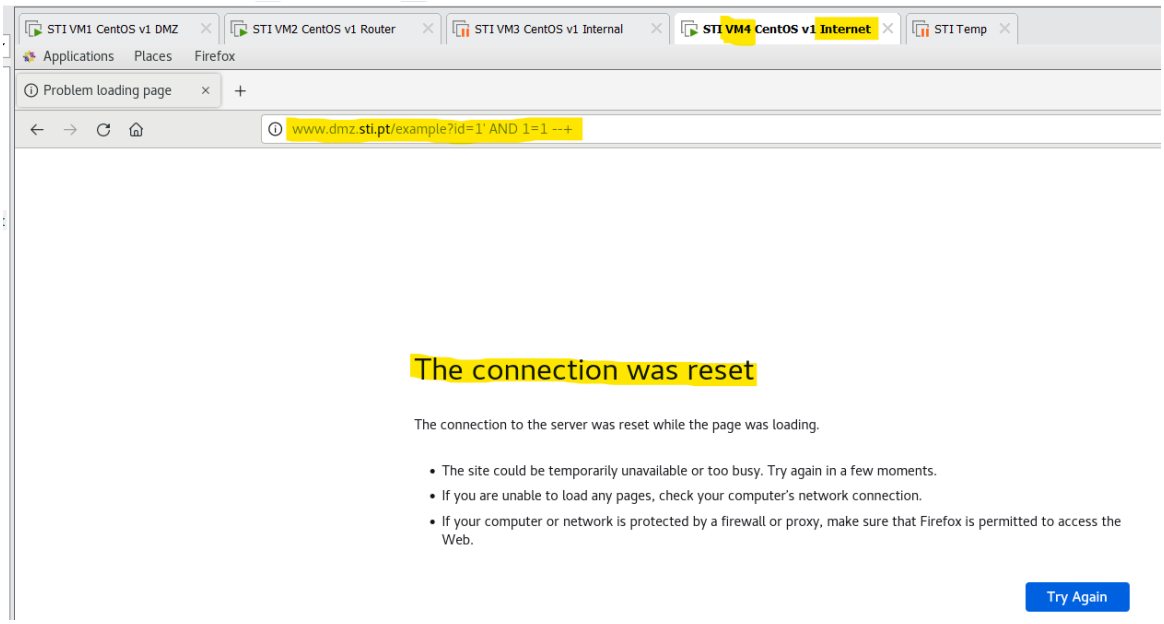

Figura 3: Exemplo de *SQL Injection* no servidor

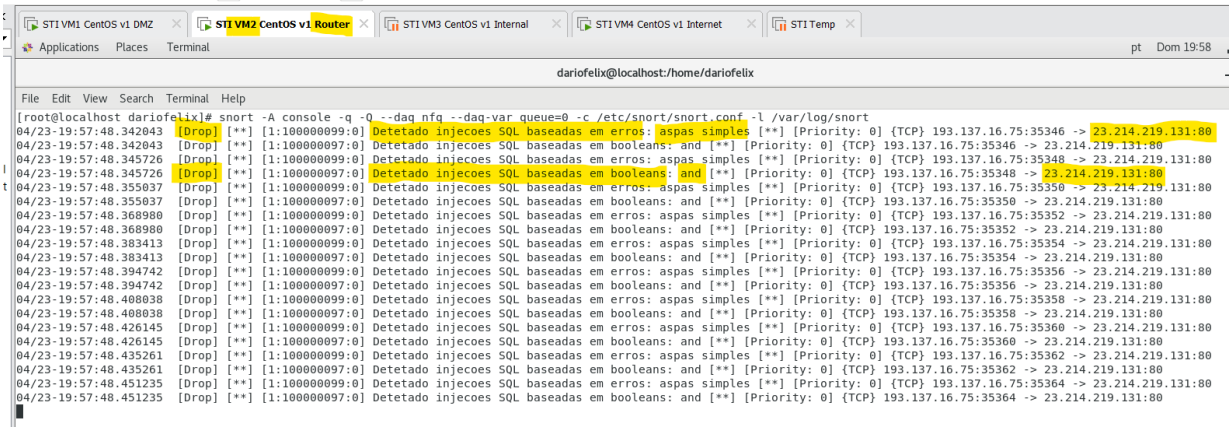

Figura 4: Bloqueio e Deteção do ataque de *SQL Injection*

5.3 *DoS*

Um ataque do tipo *denial-of-service* (*DoS*) consiste em efetuar inúmeros pedidos ao servidor de modo a tornar o servidor temporariamente indisponível para responder a pedidos efetuados pelos utilizadores do serviço. Este tipo de ataque é conseguido através de múltiplos pedidos redundantes consecutivos, como é o caso de pedidos *icmp*. Outro tipo de pedidos bastante utilizado são os de pedido de estabelecimento de novas ligações (*syn*). Este ataque pode ser efetuado a partir de um único dipositivo ou de forma distribuída. De seguida são apresentadas duas regras (e respetivos testes) que permitem ao router detetar e bloquear este tipo de ataque. [2–4]

```
$ nano /etc/snort/rules/local.rules
```

```
# ICMP flooding
drop icmp any any -> $HOME_NET any (msg:"Possible DoS Attack Type : ICMP flood"; sid:1000001;
↪  rev:1;classtype:icmp-event; detection_filter:track by_dst, count 500, seconds 3;)

# SYN flooding
drop tcp any any -> $HOME_NET any (flags: S; msg:"Possible DoS Attack Type : SYNflood";
↪  flow:stateless; sid:3; detection_filter:track by_dst, count 20, seconds 10;)
```

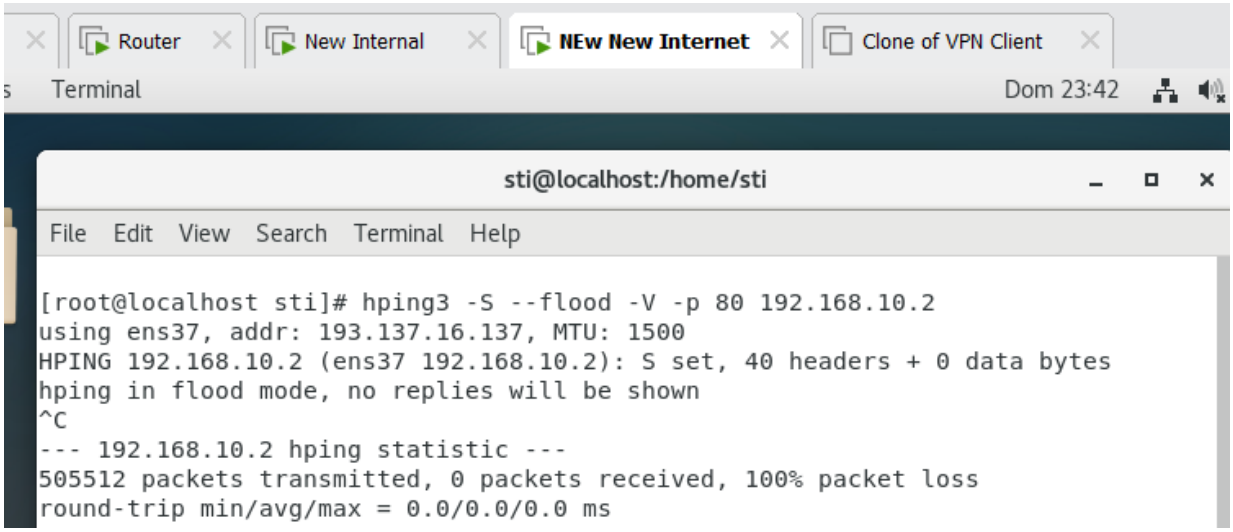

Figura 5: Exemplo da execução de um ataque DoS

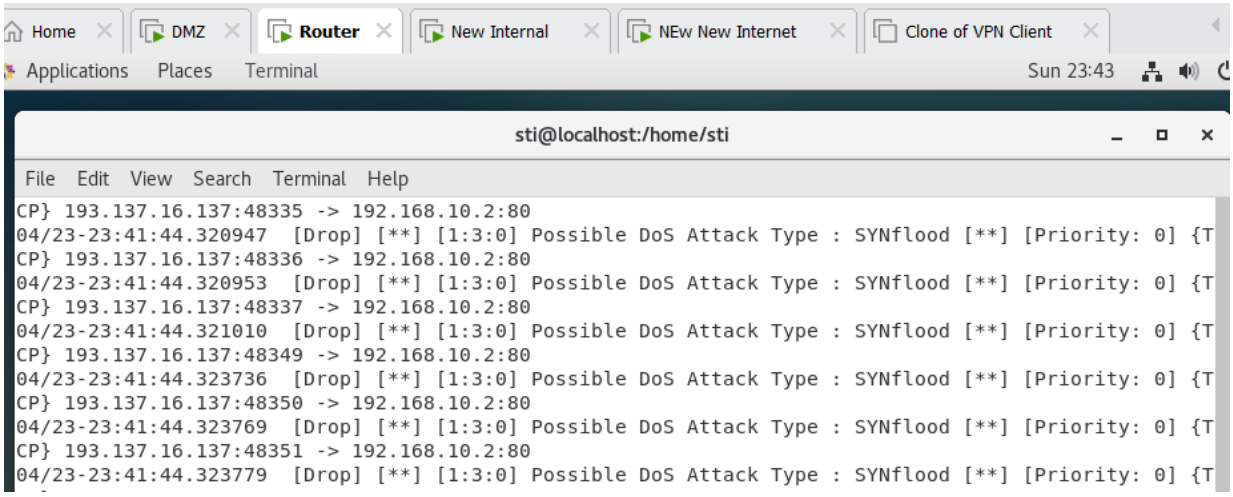

Figura 6: Bloqueio e Deteção do ataque de DoS

5.4 *OS fingerprinting*

Um ataque do tipo *OS fingerprinting* consiste em efetuar diferentes pedidos ao servidor de forma a tentar identificar a versão e tipo do sistema operativo, uma vez que diferentes sistemas operativos e versão respondem de forma diferente. Através da identificação da versão e tipo de sistema operativo usado os atacantes podem explorar os pontos de vulnerabilidade conhecidos destes sistemas. De seguida é apresentada uma regra (e respetivo teste) que permite ao router a identificação e bloqueio deste tipo de ataque. [5, 6]

```
$ nano /etc/snort/rules/local.rules
```

```
drop tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN nmap fingerprint attempt";
↪  flags:SFPU;reference:arachnids,05;classtype:attempted-recon; sid:629; rev:1;)
```

Referências

[1] "Detect sql injection attack using snort ids." [Online]. Available: https://www.hackingarticles.in/detect-sql-injection-attack-using-snort-ids/

[2] M. Gogoi and S. Mishra, "Detecting ddos attack using snort," 2018. [Online]. Available: https://www.researchgate.net/publication/338660054_DETECTING_DDoS_ATTACK_USING_Snort

[3] Kalilinux.in, "Hping3 – network auditing, dos and ddos," 2022. [Online]. Available: https://www.kalilinux.in/2021/03/hping3-kali-linux-dos-ddos-network.html

[4] D. Adams, "Dos flood with hping3," 2022. [Online]. Available: https://linuxhint.com/hping3/

[5] "Passive fingerprinting." [Online]. Available: https://www.sciencedirect.com/topics/computer-science/passive-fingerprinting

[6] nmap.org, "Subverting intrusion detection systems." [Online]. Available: https://nmap.org/book/subvert-ids.html#defeating-ids-snortrules