



FACULDADE DE
CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE DE
COIMBRA



Practical Assignment #2

Segurança em Tecnologias da Informação

Jorge Martins, uc2021207642@student.uc.pt

Índice

1. Introdução.....	1
2. Cenário.....	1
3. Criação das máquinas virtuais.....	2
4. Configurações da Firewall para proteger o router.....	2
5. Configurações da Firewall para autorizar comunicações diretas (sem NAT).....	3
6. Configurações da Firewall para conexões ao IP externo (Usando NAT).....	8
7. Configurações da Firewall para conexões da Internal Network para a Internet	8
8. Detecção e prevenção de intrusos.....	10
9. Conclusão.....	12
10. Referências.....	12

1. Introdução

Este trabalho proposto na disciplina de segurança em tecnologias da informação compete em configurar uma firewall usando o IPTables e um sistema de detecção de intrusos com o snort.

Neste cenário vão existir três networks que vão comunicar entre si de acordo com as regras da firewall.

2. Cenário

Scenario

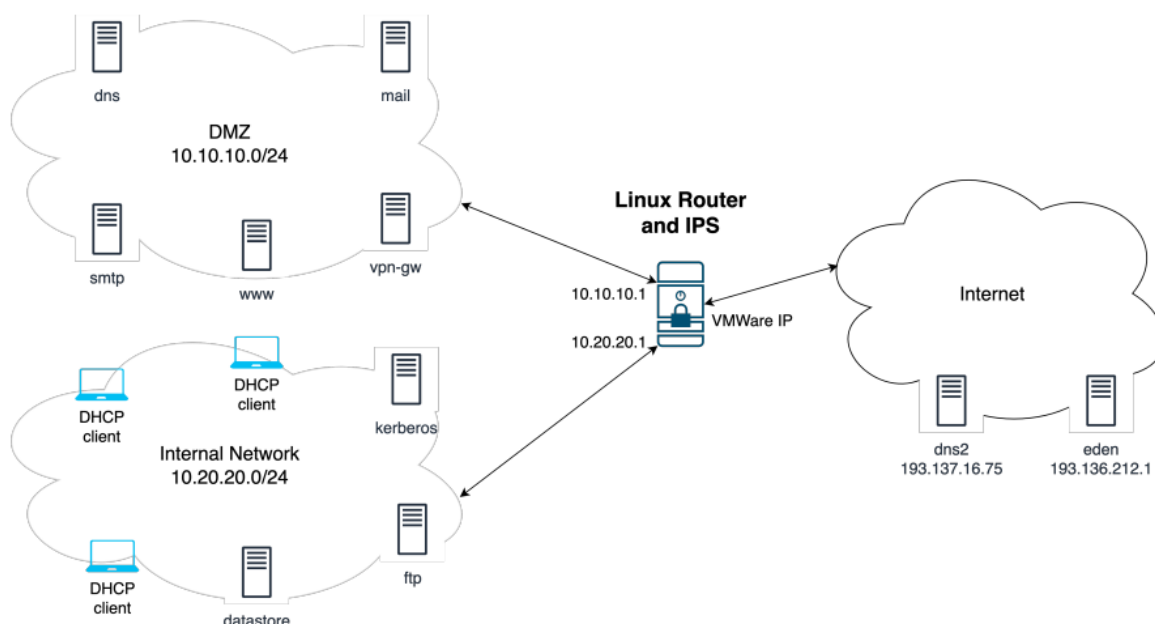


FIGURA 1 - CENÁRIO

3. Criação das máquinas virtuais

Para replicar o cenário apresentado foram criadas quatro máquinas virtuais. Uma para a zona “DMZ” com o ip “10.10.10.2” e gateway “10.10.10.1”, outra para a zona “Internal Network” com o ip “10.20.20.2” e gateway “10.20.20.1”, outra para ser o “Linux Router and IPS” com uma interface NAT de ip “192.168.75.128” e duas interfaces virtuais com os ips “10.10.10.1” e “10.20.20.1”, e a última para a “Internet” com uma interface NAT de ip “192.168.75.100” e gateway “192.168.75.128”.

```
sti@debian:~$ ping 192.168.75.100
PING 192.168.75.100 (192.168.75.100) 56(84) bytes of data.
64 bytes from 192.168.75.100: icmp_seq=1 ttl=63 time=0.765 ms
64 bytes from 192.168.75.100: icmp_seq=2 ttl=63 time=1.07 ms
64 bytes from 192.168.75.100: icmp_seq=3 ttl=63 time=0.918 ms
64 bytes from 192.168.75.100: icmp_seq=4 ttl=63 time=1.30 ms
64 bytes from 192.168.75.100: icmp_seq=5 ttl=63 time=0.947 ms
64 bytes from 192.168.75.100: icmp_seq=6 ttl=63 time=0.635 ms
64 bytes from 192.168.75.100: icmp_seq=7 ttl=63 time=0.852 ms
```

FIGURA 2 - PING INT_NET -> INTERNET

Foi feito um ping da “Internal network” para a “Internet” para verificar se o cenário está bem implementado.

As interfaces do router vão ser a ens33, ens34, e ens36 correspondendo à Internet, DMZ, e Internat Network, respetivamente.

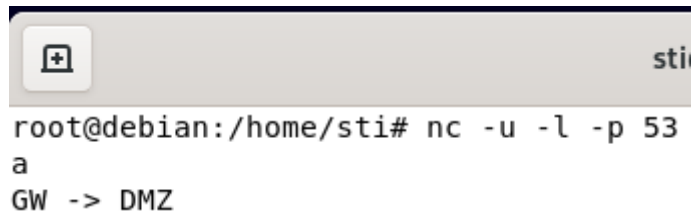
4. Configurações da Firewall para proteger o router

- The firewall configuration should drop all communications entering the router system

```
iptables -P INPUT DROP
```

- DNS name resolution requests sent to outside servers.

```
iptables -A INPUT -p udp -i ens34 --sport 53 -j ACCEPT
iptables -A INPUT -p udp -i ens33 --sport 53 -j ACCEPT
```

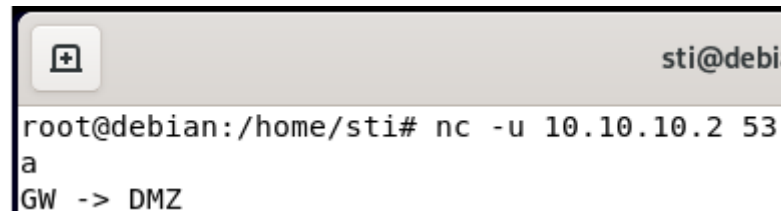


```

root@debian:/home/sti# nc -u -l -p 53
a
GW -> DMZ

```

FIGURA 3 - SERVIDOR DNS NO DMZ

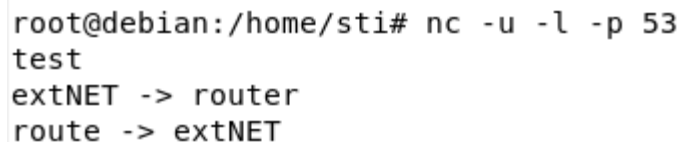


```

root@debian:/home/sti# nc -u 10.10.10.2 53
a
GW -> DMZ

```

FIGURA 4 - CONEXÃO DE DMZ E ROUTER

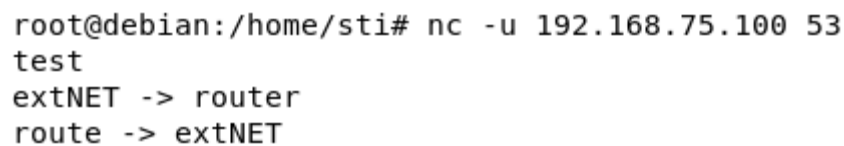


```

root@debian:/home/sti# nc -u -l -p 53
test
extNET -> router
route -> extNET

```

FIGURA 5 - SERVIDOR DNS NA INTERNET



```

root@debian:/home/sti# nc -u 192.168.75.100 53
test
extNET -> router
route -> extNET
_

```

FIGURA 6 - CONEXÃO DO ROUTER E DA INTERNET

- SSH connections to the router system, if originated at the internal network or at the VPN gateway

```

iptables -A INPUT -p tcp -i ens36 --dport 22 -j ACCEPT
iptables -A INPUT -p tcp -s 10.10.10.2 --dport 22 -j ACCEPT

```

5. Configurações da Firewall para autorizar comunicações diretas (sem NAT)

Para permitir pacotes de ligações já estabelecidas, foi usado o seguinte comando:

```

sudo iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT

```

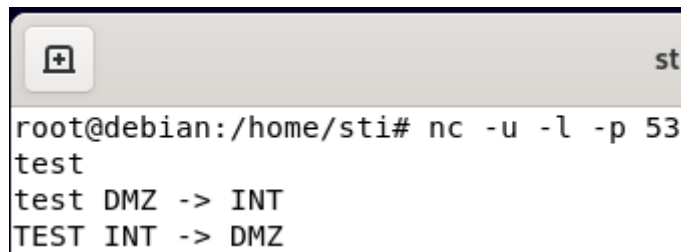
- The firewall configuration should drop all communications between networks

```
iptables -P FORWARD DROP
```

- Domain name resolutions using the dns server.

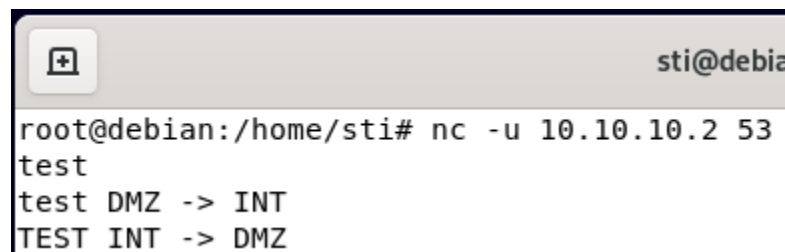
```
iptables -A FORWARD -p udp -i ens33 -o ens34 --dport 53 -j ACCEPT
```

```
iptables -A FORWARD -p udp -i ens36 -o ens34 --dport 53 -j ACCEPT
```



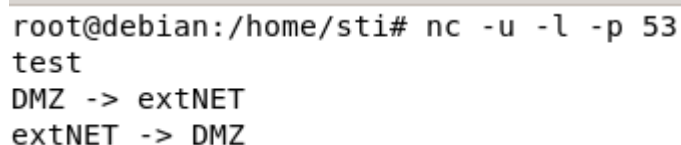
```
root@debian:/home/sti# nc -u -l -p 53
test
test DMZ -> INT
TEST INT -> DMZ
```

FIGURA 7 - SERVIDOR DNS NO DMZ



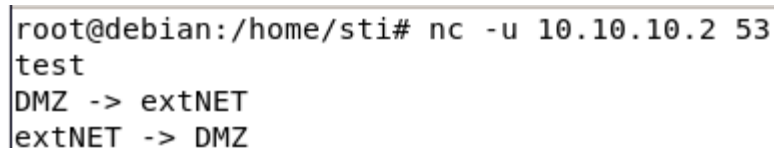
```
root@debian:/home/sti# nc -u 10.10.10.2 53
test
test DMZ -> INT
TEST INT -> DMZ
```

FIGURA 8 - LIGAÇÃO AO SERVIDOR A PARTIR DA INTERNAL NETWORK



```
root@debian:/home/sti# nc -u -l -p 53
test
DMZ -> extNET
extNET -> DMZ
```

FIGURA 9 - SERVIDOR DNS NO DMZ



```
root@debian:/home/sti# nc -u 10.10.10.2 53
test
DMZ -> extNET
extNET -> DMZ
```

FIGURA 10 - LIGAÇÃO AO SERVIDOR A PARTIR DA INTERNET

- The dns server should be able to resolve names using DNS servers on the Internet

```
iptables -A FORWARD -p udp -i ens34 -o ens33 --dport 53 -j ACCEPT
```

- The dns and dns2 servers should be able to synchronize the contents of DNS zones.

Neste caso a regra da iptables vai permitir pacotes tcp, pois estes são utilizados para sincronização.

```
iptables -A FORWARD -p tcp -i ens34 -o ens33 --dport 53 -j ACCEPT
iptables -A FORWARD -p tcp -i ens33 -o ens34 --dport 53 -j ACCEPT
```

```
root@debian:/home/sti# nc -l -p 53
test
extNET -> dmz
dmz -> extNET
```

FIGURA 11 - SERVIDOR DNS NO DMZ

```
root@debian:/home/sti# nc 192.168.75.100 53
test
extNET -> dmz
dmz -> extNET
```

FIGURA 12 - LIGAÇÃO AO SERVIDOR A PARTIR DA INTERNET

- SMTP connections to the smtp server.

```
iptables -A FORWARD -p tcp -i ens36 -o ens34 --dport 25 -j ACCEPT
iptables -A FORWARD -p tcp -i ens33 -o ens34 --dport 25 -j ACCEPT
```

Devido ao port 25 estar constantemente em utilização não foi possível realizar os testes SMTP.

- POP and IMAP connections to the mail server.

```
iptables -A FORWARD -p tcp -i ens33 -o ens34 --dport 995 -j ACCEPT
iptables -A FORWARD -p tcp -i ens36 -o ens34 --dport 995 -j ACCEPT
iptables -A FORWARD -p tcp -i ens36 -o ens34 --dport 993 -j ACCEPT
iptables -A FORWARD -p tcp -i ens33 -o ens34 --dport 993 -j ACCEPT
```

```
root@debian:/home/sti# nc -l -p 995
test
INT -> DMZ
DMZ -> INT
```

FIGURA 13 - SERVIDOR POP NO DMZ

```
root@debian:/home/sti# nc 10.10.10.2 995
test
INT -> DMZ
DMZ -> INT
```

FIGURA 14 - LIGAÇÃO AO SERVIDOR POP A PARTIR DA INTERNAL NETWORK

```
root@debian:/home/sti# nc -l -p 995
test
extNET -> DMZ
DMZ -> extNET
```

FIGURA 15 - SERVIDOR POP NO DMZ

```

root@debian:/home/sti# nc 10.10.10.2 995
test
extNET -> DMZ
DMZ -> extNET

```

FIGURA 16 - LIGAÇÃO AO SERVIDOR POP A PARTIR DA INTERNET

```

root@debian:/home/sti# nc -l -p 993
test
INT -> DMZ
DMZ -> INT

```

FIGURA 17 - SERVIDOR IMAP NO DMZ

```

root@debian:/home/sti# nc 10.10.10.2 993
test
INT -> DMZ
DMZ -> INT

```

FIGURA 18 - LIGAÇÃO AO SERVIDOR IMAP A PARTIR DA INTERNAL NETWORK

```

root@debian:/home/sti# nc -l -p 993
test
extNET -> DMZ
DMZ -> extNET

```

FIGURA 19 - SERVIDOR IMAP NO DMZ

```

root@debian:/home/sti# nc 10.10.10.2 993
test
extNET -> DMZ
DMZ -> extNET

```

FIGURA 20 - LIGAÇÃO AO SERVIDOR IMAP A PARTIR DA INTERNET

- HTTP and HTTPS connections to the www server.

```

iptables -A FORWARD -p tcp -i ens36 -o ens34 --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp -i ens33 -o ens34 --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp -i ens36 -o ens34 --dport 443 -j ACCEPT
iptables -A FORWARD -p tcp -i ens33 -o ens34 --dport 443 -j ACCEPT

```

```

root@debian:/home/sti# nc -l -p 80
test
INT -> DMZ
DMZ -> INT

```

FIGURA 21 - SERVIDOR HTTP NO DMZ

```

root@debian:/home/sti# nc 10.10.10.2 80
test
INT -> DMZ
DMZ -> INT

```

FIGURA 22 - LIGAÇÃO AO SERVIDOR DMZ A PARTIR DA INTERNAL NETWORK


```

root@debian:/home/sti# nc -l -p 80
test
extNET -> DMZ
DMZ -> extNET

```

FIGURA 23 - SERVIDOR HTTP NO DMZ

```

root@debian:/home/sti# nc 10.10.10.2 80
test
extNET -> DMZ
DMZ -> extNET

```

FIGURA 24 - LIGAÇÃO AO SERVIDOR HTTP A PARTIR DA INTERNET

```

~
root@debian:/home/sti# nc -l -p 443
test
INT -> DMZ
DMZ -> INT

```

FIGURA 25 - SERVIDOR HTTPS NO DMZ

```

root@debian:/home/sti# nc 10.10.10.2 443
test
INT -> DMZ
DMZ -> INT
■

```

FIGURA 26 - LIGAÇÃO AO SERVIDOR HTTPS A PARTIR DA INTERNAL NETWORK

```

root@debian:/home/sti# nc -l -p 443
test
extNET -> DMZ
DMZ -> extNET

```

FIGURA 27 - SERVIDOR HTTPS NO DMZ

```

root@debian:/home/sti# nc 10.10.10.2 443
test
extNET -> DMZ
DMZ -> extNET

```

FIGURA 28 - LIGAÇÃO AO SERVIDOR HTTPS A PARTIR DA INTERNET

- OpenVPN connections to the vpn-gw server.

```

iptables -A FORWARD -p tcp -i ens36 -o ens34 --dport 1194 -j ACCEPT
iptables -A FORWARD -p tcp -i ens33 -o ens34 --dport 1194 -j ACCEPT

```

```

root@debian:/home/sti# nc -l -p 1194
test
int -> DMZ
DMZ -> INT

```

FIGURA 29 - SERVIDOR OPENVPN NO DMZ

```

root@debian:/home/sti# nc 10.10.10.2 1194
test
int -> DMZ
DMZ -> INT

```

FIGURA 30 - LIGAÇÃO AO SERVIDOR OPENVPN A PARTIR DA INTERNAL NETWORK

```

root@debian:/home/sti# nc -l -p 1194
test
extNET -> DMZ
DMZ -> extNET

```

FIGURA 31 - SERVIDOR OPENVPN NO DMZ

```

root@debian:/home/sti# nc 10.10.10.2 1194
test
extNET -> DMZ
DMZ -> extNET

```

FIGURA 32 - LIGAÇÃO AO SERVIDOR OPENVPN A PARTIR DA INTERNET

6. Configurações da Firewall para conexões ao IP externo (Usando NAT)

- FTP connections (in passive and active modes) to the ftp server.

```

iptables -A FORWARD -p tcp -i ens33 -o ens36 --dport 21 -j ACCEPT
modprobe nf_conntrack_ftp
modprobe ip_nat_ftp
iptables -t nat -A PREROUTING -p tcp -d 192.168.75.128 -i ens33 --dport 21 -j DNAT --to-destination 10.20.20.2

```

- SSH connections to the datastore server, but only if originated at the eden or dns2 servers.

```

iptables -A FORWARD -p tcp -d 10.20.20.2 -i ens33 -o ens36 --dport 22 -j ACCEPT
iptables -t nat -A PREROUTING -p tcp -d 192.168.75.128 -i ens33 --dport 22 -j DNAT --to-destination 10.20.20.2

```

7. Configurações da Firewall para conexões da Internal Network para a Internet

- Domain name resolutions using DNS.

```
iptables -A FORWARD -p udp -i ens36 -o ens33 --dport 53 -j ACCEPT
iptables -t nat -A POSTROUTING -p udp -s 10.20.20.0/24 -o ens33 --dport 53 -j SNAT --to-source 192.168.75.128
```

```
root@debian:/home/sti# nc -u -l -p 53
a
a
postroutingtest
```

FIGURA 33 - SERVIDOR DNS NA INTERNET

```
root@debian:/home/sti# nc -u 192.168.75.100 53
a
a
postroutingtest
```

FIGURA 34 - LIGAÇÃO AO SERVIDOR DNS A PARTIR DA INTERNAL NETWORK

11	10.259485704	192.168.75.128	192.168.75.100	DNS	44 [Malformed Packet]
----	--------------	----------------	----------------	-----	-----------------------

FIGURA 35 - WIRESHARK DA LIGAÇÃO DNS

Como se pode ver pelo wireshark, o “source ip” do pacote passou a ser “192.168.75.128” apesar do pacote ter saído do ip “10.20.20.2”

- HTTP, HTTPS and SSH connections.

```
iptables -A FORWARD -p tcp -i ens36 -o ens33 --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp -i ens36 -o ens33 --dport 443 -j ACCEPT
iptables -A FORWARD -p tcp -i ens36 -o ens33 --dport 22 -j ACCEPT
iptables -t nat -A POSTROUTING -p tcp -s 10.20.20.0/24 -o ens33 --dport 80 -j SNAT --to-source 192.168.75.128
iptables -t nat -A POSTROUTING -p tcp -s 10.20.20.0/24 -o ens33 --dport 443 -j SNAT --to-source 192.168.75.128
iptables -t nat -A POSTROUTING -p tcp -s 10.20.20.0/24 -o ens33 --dport 22 -j SNAT --to-source 192.168.75.128
```

```
root@debian:/home/sti# nc -l -p 80
a
```

FIGURA 36 - SERVIDOR HTTP NA INTERNET

```
root@debian:/home/sti# nc 192.168.75.100 80
a
```

FIGURA 37 - LIGAÇÃO AO SERVIDOR HTTP A PARTIR DA INTERNAL NETWORK

284	1914.6807891...	192.168.75.128	192.168.75.100	TCP	66 50664 → 80 [ACK] Seq=1
-----	-----------------	----------------	----------------	-----	---------------------------

FIGURA 38 - WIRESHARK DA LIGAÇÃO HTTP

```
root@debian:/home/sti# nc -l -p 443
a
```

FIGURA 39 - SERVIDOR HTTPS NA INTERNET

```
root@debian:/home/sti# nc 192.168.75.100 443
a
```

FIGURA 40 - LIGAÇÃO AO SERVIDOR HTTPS A PARTIR DA INTERNAL NETWORK

325	2013.5430208...	192.168.75.128	192.168.75.100	TCP	68 44192 → 443 [PSH, ACK]
-----	-----------------	----------------	----------------	-----	---------------------------

FIGURA 41 - WIRESHARK DA LIGAÇÃO HTTPS

- FTP connections (in passive and active modes) to external FTP servers.

```
iptables -A FORWARD -p tcp -i ens36 -o ens33 --dport 21 -j ACCEPT
modprobe nf_conntrack_ftp
modprobe ip_nat_ftp
iptables -t nat -A POSTROUTING -p tcp -s 10.20.20.0/24 -o ens33 --dport 21 -j SNAT --to-source 192.168.75.128
```

8. Detecção e prevenção de intrusos

A segunda parte deste trabalho consiste na prevenção de ataques maliciosos à nossa rede. Para isso vai ser usado o Snort.

O snort foi configurado de acordo com o tutorial fornecido, e para ser utilizado em conjunto com a IPTables, foram feitos os seguintes comandos:

```
modprobe nfnetlink_queue
iptables -A FORWARD -j NFQUEUE --queue-num 0
```

Para ativar o snort em modo inline, foi utilizado o comando seguinte:

```
snort -Q --daq nfq --daq-var queue=0 -c /etc/snort/snort.conf -v -l /var/log/snort/
```

Este comando contém a localização do ficheiro de configuração do snort tal como a localização dos alerts.

Contém também as flags -v de modo sniffer e a flag -l para funcionar como packet logger.

- SQL Injection

A injeção de SQL é uma técnica de injeção de código, via instruções de SQL através de uma página web, que pode destruir uma base de dados, é uma das técnicas de hacking mais comuns.

Esta ocorre normalmente quando é pedido um input, e nesse input é incluído um statement SQL que vai correr na base de dados sem se saber.

Um exemplo seria a injeção SQL baseada em "1=1".

```
SELECT * FROM Users WHERE UserId = 105 OR 1=1;
```

Esta injeção é possível quando uma página web pede por exemplo um input de um ID, e nesse input o utilizador insere o ID de uma forma mais criativa.

UserId: 105 OR 1=1

Como o statement vai ser sempre verdade, a base de dados inteira dos “Users” seria revelada se não existisse algo para contrariar.

Outro exemplo seria a injeção SQL baseada em erros.

Esta técnica consiste em inserir no input caracteres que vão originar mensagens de erro, como por exemplo quote (') ou double quote (").

```
# SQL INJECTION

ipvar HOME_NET [10.10.10.0/24,10.20.20.0/24]

drop tcp any any -> $HOME_NET 80 (msg: "SQL 1 = 1 - SQL Injection Detected"; flow:to_server,established; pcre:"/or\++1%3D1/i"; classtype:web-application-attack; sid:10000010; rev:4;)

drop tcp any any -> $HOME_NET 80 (msg: "SQL Error based SQL injection Detected"; flow:to_server, established; pcre:"/((%27)|('))/i"; classtype:web-application-attack; sid:10000011; rev:1;)
```

FIGURA 42 - REGRAS SNORT PARA SQL INJECTION

Na primeira regra de SQL injection é detetado o ataque que consiste em inserir o statement OR junto com a igualdade “1=1” e na segunda regra é detetado o uso de caracteres como o quote ('), é detetado tanto o próprio carater como o seu equivalente hex.

- Ataques XSS (Cross-Site Scripting)

Os ataques Cross-Site Scripting (XSS) são um tipo de injeção, na qual scripts maliciosos são injetados em sites confiáveis. Os ataques XSS ocorrem quando um invasor usa um aplicativo da Web para enviar código malicioso, geralmente na forma de um script do lado do navegador, para um utilizador final diferente.

Podem ser feitos através de HTML opening e closing tags com texto ou até “img src” tags.

Nas regras estão incluídos os Regex adequados para detetar qualquer tipo de ataque que incluía as tags mencionadas respetivamente.

```
# XSS attacks

drop tcp any any -> $HOME_NET 80 (msg: "HTML Cross Site Scripting attempt"; flow:to_server,established; pcre:"/((\%3C)|<)((\%2F)|\/)*[a-z0-9]+((\%3E)|>)/i"; classtype:web-application-attack; sid:100000012; rev:5;)

drop tcp any any -> $HOME_NET 80 (msg: "ImgSrc Cross site scripting attempt"; flow:to_server, established; pcre:"/((\%3C)|<)((\%69)|i|(\%49))((\%6D)|m|(\%4D))((\%67)|g|(\%47))[\^n]+((\%3E)|>)/i"; classtype:web-application-attack; sid:100000013; rev:5;)
```

FIGURA 43 - REGRAS SNORT PARA XSS ATTACKS

9. Conclusão

A realização deste trabalho promoveu capacidades na configuração de uma firewall com e sem NAT entre várias networks e a configuração de um sistema de detecção de intrusos como o snort.

A junção da firewall com o snort permitiu que a nossa rede fosse segura contra pacotes indesejados e ataques maliciosos.

10. Referências

https://www.blackhat.com/presentations/bh-usa-04/bh-us-04-mookhey/old/bh-us-04-mookhey_whitepaper.pdf

