FACULDADE DE
CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE D
COIMBRA

Departamento Engenharia Informática

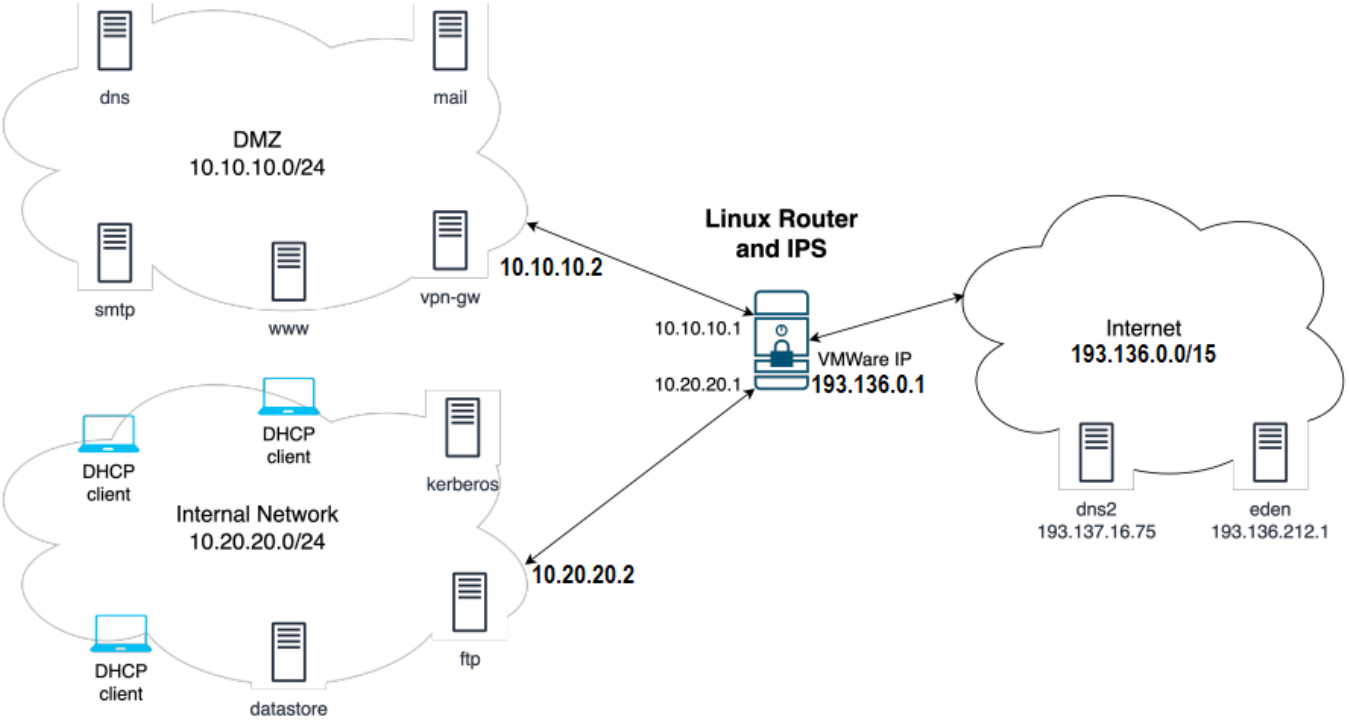
STI 2021/2022

Relatório Trabalho Prático Nº2:

Trabalho realizado por:
João Calhau 2016255704
Tatiana Simões 2018285812

1. Configurações:

1.1. Cenário da atividade prática



Começamos por criar 4 VMs, uma para o DMZ, outra para a Internal Network, outra para o router e outra para a Internet.

1.2. Configurações das VMs e das rotas

Router
ens33 (NAT):
ip: 193.136.0.1
netmask: 255.254.0.0

ens36 (DMZ):
ip: 10.10.10.1
netmask: 255.255.255.0

ens37 (Internal Network):
ip: 10.20.20.1
netmask: 255.255.255.0

DMZ
ens33 (DMZ):
ip: 10.10.10.2
netmask: 255.255.255.0
gateway: 10.10.10.1

route add -net 10.20.20.0/24 gw 10.10.10.1
route add -net 193.136.0.0/15 gw 10.10.10.1

Internal Network
ens33 (Internal Network):
ip: 10.20.20.2
netmask: 255.255.255.0
gateway: 10.20.20.1
route add -net 10.10.10.0/24 gw 10.20.20.1
route add -net 193.136.0.0/15 gw 10.20.20.1

Internet
ens33 (NAT):
#eden
ip: 193.136.212.1
#dns2
ip: 193.137.16.75
netmask: 255.254.0.0
gateway: 193.136.0.1
route add -net 10.10.10.0/24 gw 193.136.0.1
route add -net 10.20.20.0/24 gw 193.136.0.1

1.3. Testes iniciais

De modo a verificar se as configurações iniciais das máquinas estavam corretas, fizemos ping entre elas.

```
root@debian:~# ping 10.20.20.2
PING 10.20.20.2 (10.20.20.2) 56(84) bytes of data.
64 bytes from 10.20.20.2: icmp_seq=1 ttl=63 time=7.66 ms
64 bytes from 10.20.20.2: icmp_seq=2 ttl=63 time=3.38 ms
64 bytes from 10.20.20.2: icmp_seq=3 ttl=63 time=3.11 ms
64 bytes from 10.20.20.2: icmp_seq=4 ttl=63 time=3.00 ms
```

Ping da rede DMZ para a Internal Network

```
root@debian:~# ping 193.136.212.1
PING 193.136.212.1 (193.136.212.1) 56(84) bytes of data.
64 bytes from 193.136.212.1: icmp_seq=1 ttl=63 time=13.8 ms
64 bytes from 193.136.212.1: icmp_seq=2 ttl=63 time=3.76 ms
64 bytes from 193.136.212.1: icmp_seq=3 ttl=63 time=3.01 ms
64 bytes from 193.136.212.1: icmp_seq=4 ttl=63 time=3.37 ms
```

Ping da rede DMZ para a Internet

```
root@debian:~# ping 10.10.10.2
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
64 bytes from 10.10.10.2: icmp_seq=1 ttl=63 time=7.74 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=63 time=3.36 ms
64 bytes from 10.10.10.2: icmp_seq=3 ttl=63 time=3.80 ms
64 bytes from 10.10.10.2: icmp_seq=4 ttl=63 time=3.54 ms
```

Ping da Internal Network para a rede DMZ

```
root@debian:~# ping 193.136.212.1
PING 193.136.212.1 (193.136.212.1) 56(84) bytes of data.
64 bytes from 193.136.212.1: icmp_seq=1 ttl=63 time=4.57 ms
64 bytes from 193.136.212.1: icmp_seq=2 ttl=63 time=0.990 ms
64 bytes from 193.136.212.1: icmp_seq=3 ttl=63 time=1.09 ms
64 bytes from 193.136.212.1: icmp_seq=4 ttl=63 time=0.802 ms
```

Ping da Internal Network para a Internet

```
root@debian:~# ping 10.10.10.2
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
64 bytes from 10.10.10.2: icmp_seq=1 ttl=63 time=4.71 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=63 time=1.07 ms
64 bytes from 10.10.10.2: icmp_seq=3 ttl=63 time=1.00 ms
64 bytes from 10.10.10.2: icmp_seq=4 ttl=63 time=0.904 ms
```

Ping da Internet para a rede DMZ

```
root@debian:~# ping 10.20.20.2
PING 10.20.20.2 (10.20.20.2) 56(84) bytes of data.
64 bytes from 10.20.20.2: icmp_seq=1 ttl=63 time=6.18 ms
64 bytes from 10.20.20.2: icmp_seq=2 ttl=63 time=0.998 ms
64 bytes from 10.20.20.2: icmp_seq=3 ttl=63 time=5.79 ms
64 bytes from 10.20.20.2: icmp_seq=4 ttl=63 time=1.08 ms
```

Ping da Internet para a Internal Network

2. Packet filtering and NAT using IPTables

Para não necessitarmos de comandos espelhados de dport, colocamos as seguintes regras no router:

- iptables -A FORWARD -i ens36 -m state --state RELATED,ESTABLISHED -j ACCEPT
- iptables -A FORWARD -i ens37 -m state --state RELATED,ESTABLISHED -j ACCEPT
- iptables -A FORWARD -i ens33 -m state --state RELATED,ESTABLISHED -j ACCEPT

2.1. Firewall configuration to protect the router

Inicialmente é nos pedido que a firewall faça **drop** de todas as comunicações que tentem entrar no router, exceto aquelas requeridas para:

- Requests de resolução de nome DNS enviadas para servidores externos.
- Conexões SSH com o router, se originadas na internal network ou no vpn-gw.

Para tal utilizamos a política DROP, que rejeita todos os pacotes que não estão ACCEPTED nas regras da chain INPUT.

- iptables -P INPUT DROP

2.1.1. DNS name resolution requests sent to outside servers

- iptables -A INPUT -p udp --sport 53 -j ACCEPT

Testes: Para realizar testes utilizamos o netcat. Colocamos um netcat listener no DMZ, e um cliente netcat no router.

```
root@debian:~# nc -l -u -p 53 -v
listening on [any] 53 ...
connect to [10.10.10.2] from _gateway [10.10.10.1] 47577
router: Ola!
DMZ: Ola!
```

Netcat listener na rede **DMZ** (dns) para **router**.

```
root@debian:~# nc -u 10.10.10.2 53 -v
10.10.10.2: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.10.2] 53 (domain) open
router: Ola!
DMZ: Ola!
```

Cliente netcat no **router** para a rede **DMZ**.

2.1.2. SSH connections to the router system, if originated at the internal network or at the VPN gateway (vpn-gw)

internal network

- iptables -A INPUT -p tcp -s 10.20.20.0/24 --dport 22 -j ACCEPT

vpn-gw

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

Testes:

```
root@debian:~# nc -l -p 22 -v
listening on [any] 22 ...
10.10.10.2: inverse host lookup failed: Unknown host
connect to [10.10.10.1] from (UNKNOWN) [10.10.10.2] 59960
vpn-gw: Ola por ssh!
router: Ola de volta!
```

Netcat listener no **router** para **DMZ**.

```
root@debian:~# nc 10.10.10.1 22 -v
_gateway [10.10.10.1] 22 (ssh) open
vpn-gw: Ola por ssh!
router: Ola de volta!
```

Cliente netcat na rede **DMZ(vpn-gw)** para o **router**.

```
root@debian:~#  nc 10.20.20.1 22 -v
_gateway [10.20.20.1] 22 (ssh) open
internal_network: Ola por ssh!
router: Ola de volta!
```

Netcat listener no **router** para **Internal Network**.

```
root@debian:~# nc -l -p 22 -v
listening on [any] 22 ...
10.20.20.2: inverse host lookup failed: Unknown host
connect to [10.20.20.1] from (UNKNOWN) [10.20.20.2] 35238
internal_network: Ola por ssh!
router: Ola de volta!
```

Cliente netcat na **Internal Network** para o **router**.

2.2. Firewall configuration to authorize direct communications (without NAT)

Neste ponto é nos pedido que a firewall faça **drop** de todas as comunicações entre redes, exceto aquelas requeridas para:

- Resoluções de nomes de domínio usando o servidor dns.
- O servidor dns deve ser capaz de resolver nomes usando servidores DNS na Internet(dns2 e outros).
- Os servidores dns e dns2 devem ser capazes de sincronizar o conteúdo das zonas DNS.
- Conexões SMTP para o servidor smtp.
- Conexões POP e IMAP para o servidor de mail.
- Conexões HTTP e HTTPS para o servidor www.
- Conexões OpenVPN para o servidor vpn-gw.
- Os clientes VPN conectados ao servidor vpn-gw devem ser capazes de se conectar ao serviço PosgreSQL no servidor datastore.
- Os clientes VPN conectados ao servidor vpn-gw devem ser capazes de se conectar ao serviço Kerberos v5 no servidor kerberos.São permitidas até 10 conexões simultâneas.

Para tal utilizamos a política DROP, que rejeita todos os pacotes que não estão ACCEPTED nas regras da chain FORWARD.

- iptables -P FORWARD DROP

2.2.1. Domain name resolutions using the dns server

- iptables -A FORWARD -p udp -d 10.10.10.2 --dport 53 -j ACCEPT

Testes:

```
root@debian:~# nc -l -u -p 53 -v
listening on [any] 53 ...
10.20.20.2: inverse host lookup failed: Unknown host
connect to [10.10.10.2] from (UNKNOWN) [10.20.20.2] 44058
Internal_Network: Ola
DMZ: Ola de volta!
```

Netcat listener no **DMZ(dns)** para **Internal Network**.

```
root@debian:~# nc -u 10.10.10.2 53 -v
10.10.10.2: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.10.2] 53 (domain) open
Internal_Network: Ola
DMZ: Ola de volta!
```

Cliente netcat na **Internal Network** para o **DMZ(dns)**.

2.2.2. The dns server should be able to resolve names using DNS servers on the Internet (dns2 and also others)

```
root@debian:~# nc -l -u -p 53 -v
listening on [any] 53 ...
193.137.16.75: inverse host lookup failed: Unknown host
connect to [10.10.10.2] from (UNKNOWN) [193.137.16.75] 54364
Internet: ola!
DMZ: ola!
```

Netcat listener no **dns** para **dns2**.

```
root@debian:~# nc -u 10.10.10.2 53 -v
10.10.10.2: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.10.2] 53 (domain) open
Internet: ola!
DMZ: ola!
```

Cliente netcat no **dns2** para o **dns**.

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

ip DNS: 10.10.10.2
ip DNS2: 193.137.16.75

DNS:

- iptables -A FORWARD -p tcp -d 10.10.10.2 -s 193.137.16.75 --dport 53 -j ACCEPT

DNS2:

- iptables -A FORWARD -p tcp -s 10.10.10.2 -d 193.137.16.75 --dport 53 -j ACCEPT

Testes:

```
root@debian:~# nc -l -p 53 -v
listening on [any] 53 ...
193.137.16.75: inverse host lookup failed: Unknown host
connect to [10.10.10.2] from (UNKNOWN) [193.137.16.75] 50220
DNS2: Ola!
DNS: Ola de volta!
```

Netcat listener no **dns** para **dns2**.

```
root@debian:~# nc 10.10.10.2 53 -v
10.10.10.2: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.10.2] 53 (domain) open
DNS2: Ola!
DNS: Ola de volta!
```

Cliente netcat no **dns2** para o **dns**.

```
root@debian:~# nc -l -p 53 -v
listening on [any] 53 ...
10.10.10.2: inverse host lookup failed: Unknown host
connect to [193.137.16.75] from (UNKNOWN) [10.10.10.2] 48426
DNS: Ola!
DNS2: Ola de volta!
```

Netcat listener no **dns2** para **dns**.

```
root@debian:~# nc 193.137.16.75 53 -v
193.137.16.75: inverse host lookup failed: Unknown host
(UNKNOWN) [193.137.16.75] 53 (domain) open
DNS: Ola!
DNS2: Ola de volta!
```

Cliente netcat no **dns** para o **dns2**.

2.2.4. SMTP connections to the smtp server

- iptables -A FORWARD -p tcp -d 10.10.10.2 --dport 25 -j ACCEPT

Testes:

```
root@debian:~# nc -l -p 25 -v
listening on [any] 25 ...
10.20.20.2: inverse host lookup failed: Unknown host
connect to [10.10.10.2] from (UNKNOWN) [10.20.20.2] 57020
Internal_Network: Ola!
DMZ(SMTP): Ola de volta!
```

Netcat listener na rede **DMZ(smtp server)** para a **Internal Network**.

```
root@debian:~# nc 10.10.10.2 25 -v
10.10.10.2: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.10.2] 25 (smtp) open
Internal_Network: Ola!
DMZ(SMTP): Ola de volta!
```

Cliente netcat na **Internal Network** para **DMZ(smtp server)**.

2.2.5. POP and IMAP connections to the mail server

POP3:

- iptables -A FORWARD -p tcp -d 10.10.10.2 --dport 110 -j ACCEPT

IMAP2:

- iptables -A FORWARD -p tcp -d 10.10.10.2 --dport 143 -j ACCEPT

Testes:

```
root@debian:~# nc -l -p 110 -v
listening on [any] 110 ...
10.20.20.2: inverse host lookup failed: Unknown host
connect to [10.10.10.2] from (UNKNOWN) [10.20.20.2] 56484
Internal_Network: Ola!
DMZ(email): Ola de volta!
```

Netcat listener na rede **DMZ(email server)** para a **Internal Network** através de conexão POP.

```
root@debian:~# nc 10.10.10.2 110 -v
10.10.10.2: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.10.2] 110 (pop3) open
Internal_Network: Ola!
DMZ(email): Ola de volta!
```

Cliente netcat na **Internal Network** para **DMZ(email server)** através de conexão POP.

```
root@debian:~# nc -l -p 143 -v
listening on [any] 143 ...
10.20.20.2: inverse host lookup failed: Unknown host
connect to [10.10.10.2] from (UNKNOWN) [10.20.20.2] 39334
Internal_Network: Ola!
DMZ(email): Ola de volta!
```

Netcat listener na rede **DMZ(email server)** para a **Internal Network** através de conexão IMAP.

```
root@debian:~# nc 10.10.10.2 143 -v
10.10.10.2: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.10.2] 143 (imap2) open
Internal_Network: Ola!
DMZ(email): Ola de volta!
```

Cliente netcat na **Internal Network** para **DMZ(email server)** através de conexão IMAP.

2.2.6. HTTP and HTTPS connections to the www server

HTTP:

- iptables -A FORWARD -p tcp -d 10.10.10.2 --dport 80 -j ACCEPT

HTTPS:

- iptables -A FORWARD -p tcp -d 10.10.10.2 --dport 443 -j ACCEPT

Testes:

```
root@debian:~# nc -l -p 80 -v
listening on [any] 80 ...
193.137.16.75: inverse host lookup failed: Unknown host
connect to [10.10.10.2] from (UNKNOWN) [193.137.16.75] 50434
Internet: Ola!
DMZ(www): Ola de volta!
```

Netcat listener na rede **DMZ(www server)** para a **Internet** através de conexão HTTP.

```
root@debian:~# nc 10.10.10.2 80 -v
10.10.10.2: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.10.2] 80 (http) open
Internet: Ola!
DMZ(www): Ola de volta!
```

Cliente netcat na **Internet** para **DMZ(www server)** através de conexão HTTP.

```
root@debian:~# nc -l -p 443 -v
listening on [any] 443 ...
193.137.16.75: inverse host lookup failed: Unknown host
connect to [10.10.10.2] from (UNKNOWN) [193.137.16.75] 40856
Internet: Ola!
DMZ(www): Ola de volta!
```

Netcat listener na rede **DMZ(www server)** para a **Internet** através de conexão HTTPS.

```
root@debian:~# nc 10.10.10.2 443 -v
10.10.10.2: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.10.2] 443 (https) open
Internet: Ola!
DMZ(www): Ola de volta!
```

Cliente netcat na **Internet** para **DMZ(www server)** através de conexão HTTPS.

2.2.7. OpenVPN connections to the vpn-gw server

TCP:

- iptables -A FORWARD -p tcp -d 10.10.10.2 --dport 1194 -j ACCEPT

UDP:

- iptables -A FORWARD -p udp -d 10.10.10.2 --dport 1194 -j ACCEPT

Testes:

```
root@debian:~# nc -l -u -p 1194 -v
listening on [any] 1194 ...
10.20.20.2: inverse host lookup failed: Unknown host
connect to [10.10.10.2] from (UNKNOWN) [10.20.20.2] 54430
Internal_Network: Ola atraves de openvpn!(udp)
DMZ(vpn-gw): Ola!(udp)
```

Netcat listener na rede **DMZ(vpn-gw)** para a **Internal Network** através de conexão OpenVPN.

```
root@debian:~# nc -u 10.10.10.2 1194 -v
10.10.10.2: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.10.2] 1194 (openvpn) open
Internal_Network: Ola atraves de openvpn!(udp)
DMZ(vpn-gw): Ola!(udp)
```

Cliente netcat na **Internal Network** para **DMZ(vpn-gw)** através de conexão OpenVPN.

```
root@debian:~# nc -l -p 1194 -v
listening on [any] 1194 ...
193.137.16.75: inverse host lookup failed: Unknown host
connect to [10.10.10.2] from (UNKNOWN) [193.137.16.75] 36162
Internet: Ola atraves de openvpn!(tcp)
DMZ(vpn-gw): Ola!(tcp)
```

Netcat listener na rede **DMZ(vpn-gw)** para a **Internet** através de conexão OpenVPN.

```
root@debian:~# nc 10.10.10.2 1194 -v
10.10.10.2: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.10.2] 1194 (openvpn) open
Internet: Ola atraves de openvpn!(tcp)
DMZ(vpn-gw): Ola!(tcp)
```

Cliente netcat na **Internet** para **DMZ(vpn-gw)** através de conexão OpenVPN.

2.2.8. VPN clients connected to vpn-gw server should be able to connect to the PostgreSQL service on the datastore server

- iptables -A FORWARD -p tcp -s 10.10.10.2 -d 10.20.20.2 --dport 5432 -j ACCEPT

Testes:

```
root@debian:~# nc -l -p 5432 -v
listening on [any] 5432 ...
10.10.10.2: inverse host lookup failed: Unknown host
connect to [10.20.20.2] from (UNKNOWN) [10.10.10.2] 37838
DMZ(vpn-gw): Ola!
Internal Network(datastore): Ola de volta!
```

Netcat listener na **Internal Network(datastore server)** para a rede **DMZ(vpn-gw)**.

```
root@debian:~# nc 10.20.20.2 5432 -v
10.20.20.2: inverse host lookup failed: Unknown host
(UNKNOWN) [10.20.20.2] 5432 (postgresql) open
DMZ(vpn-gw): Ola!
Internal_Network(datastore): Ola de volta!
```

Cliente netcat na rede **DMZ(vpn-gw)** para **Internal Network(datastore server)**.

2.2.9. VPN clients connected to vpn-gw server should be able to connect to Kerberos v5 service on the kerberos server. A maximum of 10 simultaneous connections are allowed

tcp:

- iptables -A FORWARD -p tcp -m connlimit --connlimit-upto 10 -s 10.10.10.2 -d 10.20.20.2 --dport 88 -j ACCEPT

Testes:

```
root@debian:~# nc -l -p 88 -v
listening on [any] 88 ...
10.10.10.2: inverse host lookup failed: Unknown host
connect to [10.20.20.2] from (UNKNOWN) [10.10.10.2] 52618
DMZ(vpn-gw): Ola!(tcp)
Internal_Network(kerberos): Ola de volta!(tcp)
```

Netcat listener na **Internal Network(kerberos server)** para a rede **DMZ(vpn-gw)**.

```
root@debian:~# nc 10.20.20.2 88 -v
10.20.20.2: inverse host lookup failed: Unknown host
(UNKNOWN) [10.20.20.2] 88 (kerberos) open
DMZ(vpn-gw): Ola!(tcp)
Internal_Network(kerberos): Ola de volta!(tcp)
```

Cliente netcat na rede **DMZ(vpn-gw)** para **Internal Network(kerberos server)**.

3. Firewall configuration for connections to the external IP address of the firewall (using NAT)

Neste ponto é nos pedido que as ligações originadas no exterior(Internet) e destinadas ao IP externo da firewall(VMWare IP) devem ser autorizadas e tratadas de acordo com os seguintes requisitos:

- Conexões FTP (em modo passivo e ativo) para o servidor ftp.
- Conexões SSH para o servidor datastore, mas apenas se originadas nos servidores eden e dns2.

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

Para testarmos o ftp, foi necessário instalar o vsftpd(servidor) e ftp nas respetivas máquinas.
Para isto usámos o comando:
apt install [vsftpd/ftp]
systemctl start vsftpd
systemctl enable vsftpd

- iptables -t nat -A PREROUTING -p tcp -s 193.136.0.0/15 -d 193.136.0.1 --dport ftp -j DNAT --to-destination 10.20.20.2

- iptables -A FORWARD -p tcp -s 193.136.0.0/15 -d 10.20.20.2 --dport 21 -j ACCEPT

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

Testes:

```
root@debian:~# ftp 10.20.20.2
Connected to 10.20.20.2.
220 (vsFTPd 3.0.3)
Name (10.20.20.2:sti): sti
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 1000     1000         4096 Mar 12 03:01 Desktop
drwxr-xr-x    2 1000     1000         4096 Mar 11 05:30 Documents
drwxr-xr-x    2 1000     1000         4096 Mar 07 23:46 Downloads
drwxr-xr-x    2 1000     1000         4096 Feb 08 18:04 Music
drwxr-xr-x    2 1000     1000         4096 Apr 19 01:19 Pictures
drwxr-xr-x    2 1000     1000         4096 Feb 08 18:04 Public
drwxr-xr-x    2 1000     1000         4096 Feb 08 18:04 Templates
drwxr-xr-x    2 1000     1000         4096 Feb 08 18:04 Videos
-rw-r--r--    1 1000     1000         2471 Feb 18 21:07 cordeiro.gpg
-rw-r--r--    1 0        0              11 Apr 22 15:13 testFTP
226 Directory send OK.
ftp> get testFTP
local: testFTP remote: testFTP
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for testFTP (11 bytes).
226 Transfer complete.
11 bytes received in 0.00 secs (23.7134 kB/s)
ftp> quit
221 Goodbye.
root@debian:~# ls
log.txt  testFTP
```

Ligação ao servidor ftp em **active mode** a partir da Internet (eden).

```
root@debian:~# pftp 10.20.20.2
Connected to 10.20.20.2.
220 (vsFTPd 3.0.3)
Name (10.20.20.2:sti): sti
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
227 Entering Passive Mode (10,20,20,2,44,148).
150 Here comes the directory listing.
drwxr-xr-x    2 1000     1000         4096 Mar 12 03:01 Desktop
drwxr-xr-x    2 1000     1000         4096 Mar 11 05:30 Documents
drwxr-xr-x    2 1000     1000         4096 Mar 07 23:46 Downloads
drwxr-xr-x    2 1000     1000         4096 Feb 08 18:04 Music
drwxr-xr-x    2 1000     1000         4096 Apr 19 01:19 Pictures
drwxr-xr-x    2 1000     1000         4096 Feb 08 18:04 Public
drwxr-xr-x    2 1000     1000         4096 Feb 08 18:04 Templates
drwxr-xr-x    2 1000     1000         4096 Feb 08 18:04 Videos
-rw-r--r--    1 1000     1000         2471 Feb 18 21:07 cordeiro.gpg
-rw-r--r--    1 0        0              11 Apr 22 15:13 testFTP
226 Directory send OK.
ftp> get testFTP
local: testFTP remote: testFTP
227 Entering Passive Mode (10,20,20,2,29,178).
150 Opening BINARY mode data connection for testFTP (11 bytes).
226 Transfer complete.
11 bytes received in 0.00 secs (20.2301 kB/s)
ftp> quit
221 Goodbye.
root@debian:~# ls
log.txt  testFTP
```

Ligação ao servidor ftp em **passive mode** a partir da Internet (eden).

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

eden

- iptables -t nat -A PREROUTING -p tcp -s 193.136.212.1 -d 193.136.0.1 --dport ssh -j DNAT --to-destination 10.20.20.2

- iptables -A FORWARD -p tcp -s 193.136.212.1 -d 10.20.20.2 --dport ssh -j ACCEPT

dns2

- iptables -t nat -A PREROUTING -p tcp -s 193.137.16.75 -d 193.136.0.1 --dport ssh -j DNAT --to-destination 10.20.20.2

- iptables -A FORWARD -p tcp -s 193.137.16.75 -d 10.20.20.2 --dport ssh -j ACCEPT

Testes:

```
root@debian:~# nc -l -p 22 -v
listening on [any] 22 ...
193.136.212.1: inverse host lookup failed: Unknown host
connect to [10.20.20.2] from (UNKNOWN) [193.136.212.1] 53656
internet(eden): Ola!
internal network(datastore): Ola de volta!
```

Netcat listener na **Internal Network(datastore server)** para a **Internet(eden)**.

```
root@debian:~# nc 193.136.0.1 22 -v
_gateway [193.136.0.1] 22 (ssh) open
internet(eden): Ola!
internal_network(datastore): Ola de volta!
```

Cliente netcat na **Internet(eden)** para a **Internal Network(datastore server).**

```
root@debian:~# nc -l -p 22 -v
listening on [any] 22 ...
193.137.16.75: inverse host lookup failed: Unknown host
connect to [10.20.20.2] from (UNKNOWN) [193.137.16.75] 42782
internet(dns2): Ola!
internal network(datastore): Ola de volta!
```

Netcat listener na **Internal Network(datastore server)** para a **Internet(dns2).**

```
root@debian:~# nc 193.136.0.1 22 -v
_gateway [193.136.0.1] 22 (ssh) open
internet(dns2): Ola!
internal_network(datastore): Ola de volta!
```

Cliente netcat na **Internet(dns2)** para a **Internal Network(datastore server).**

4. Firewall configuration for communications from the internal network to the outside (using NAT)

Neste ponto é nos indicado que as seguintes ligações, originadas na internal network com destino ao exterior(Internet) devem ser autorizadas através de NAT:

- Resolução de nomes de domínios utilizando DNS.
- Conexões HTTP e HTTPS.
- Conexões FTP (em modo passivo e ativo) para servidores FTP externos.

4.1. Domain name resolutions using DNS.

- iptables -t nat -A POSTROUTING -p udp -s 10.20.20.0/24 -d 193.136.0.0/15 --dport domain -j SNAT --to-source 193.136.0.1

- iptables -A FORWARD -p udp -s 10.20.20.0/24 -d 193.136.0.0/15 --dport domain -j ACCEPT

Testes:

```
root@debian:~# nc -u -l -p 53 -v
listening on [any] 53 ...
connect to [193.137.16.75] from _gateway [193.136.0.1] 40925
internal_network: Ola!
internet(dns2): Ola de volta!
```

Netcat listener na **Internet(dns2)** para a **Internal Network.**

```
root@debian:~# nc -u 193.137.16.75 53 -v
193.137.16.75: inverse host lookup failed: Unknown host
(UNKNOWN) [193.137.16.75] 53 (domain) open
internal_network: Ola!
internet(dns2): Ola de volta!
```

Cliente netcat na **Internal Network para Internet(dns2).**

4.2. HTTP, HTTPS and SSH connections.

HTTP:

- iptables -t nat -A POSTROUTING -p tcp -s 10.20.20.0/24 -d 193.136.0.0/15 --dport http -j SNAT --to-source 193.136.0.1

- iptables -A FORWARD -p tcp -s 10.20.20.0/24 -d 193.136.0.0/15 --dport http -j ACCEPT

HTTPS:

- iptables -t nat -A POSTROUTING -p tcp -s 10.20.20.0/24 -d 193.136.0.0/15 --dport https -j SNAT --to-source 193.136.0.1

- iptables -A FORWARD -p tcp -s 10.20.20.0/24 -d 193.136.0.0/15 --dport https -j ACCEPT

SSH:

- iptables -t nat -A POSTROUTING -p tcp -s 10.20.20.0/24 -d 193.136.0.0/15 --dport ssh -j SNAT --to-source 193.136.0.1

- iptables -A FORWARD -p tcp -s 10.20.20.0/24 -d 193.136.0.0/15 --dport ssh -j ACCEPT

Testes:

HTTP(80):

```
root@debian:~# nc -l -p 80 -v
listening on [any] 80 ...
connect to [193.137.16.75] from _gateway [193.136.0.1] 32832
internal_network: Ola!
internet(dns2): Ola de volta!
```

Netcat listener na **Internet(dns2)** para a **Internal Network**

```
root@debian:~# nc 193.137.16.75 80 -v
193.137.16.75: inverse host lookup failed: Unknown host
(UNKNOWN) [193.137.16.75] 80 (http) open
internal_network: Ola!
internet(dns2): Ola de volta!
```

Cliente netcat na **Internal Network para Internet(dns2).**

HTTPS(443):

```
root@debian:~# nc -l -p 443 -v
listening on [any] 443 ...
connect to [193.137.16.75] from _gateway [193.136.0.1] 46338
internal_network: Ola!
internet(dns2): Ola de volta!
```

Netcat listener na **Internet(dns2)** para a **Internal Network**

```
root@debian:~# nc 193.137.16.75 443 -v
193.137.16.75: inverse host lookup failed: Unknown host
(UNKNOWN) [193.137.16.75] 443 (https) open
internal_network: Ola!
internet(dns2): Ola de volta!
```

Cliente netcat na **Internal Network para Internet(dns2).**

SSH(22):

```
root@debian:~# nc -l -p 22 -v
listening on [any] 22 ...
connect to [193.137.16.75] from _gateway [193.136.0.1] 43946
internal_network: Ola!
internet(dns2): Ola de volta!
```

Netcat listener na **Internet(dns2)** para a **Internal Network**

```
root@debian:~# nc 193.137.16.75 22 -v
193.137.16.75: inverse host lookup failed: Unknown host
(UNKNOWN) [193.137.16.75] 22 (ssh) open
internal_network: Ola!
internet(dns2): Ola de volta!
```

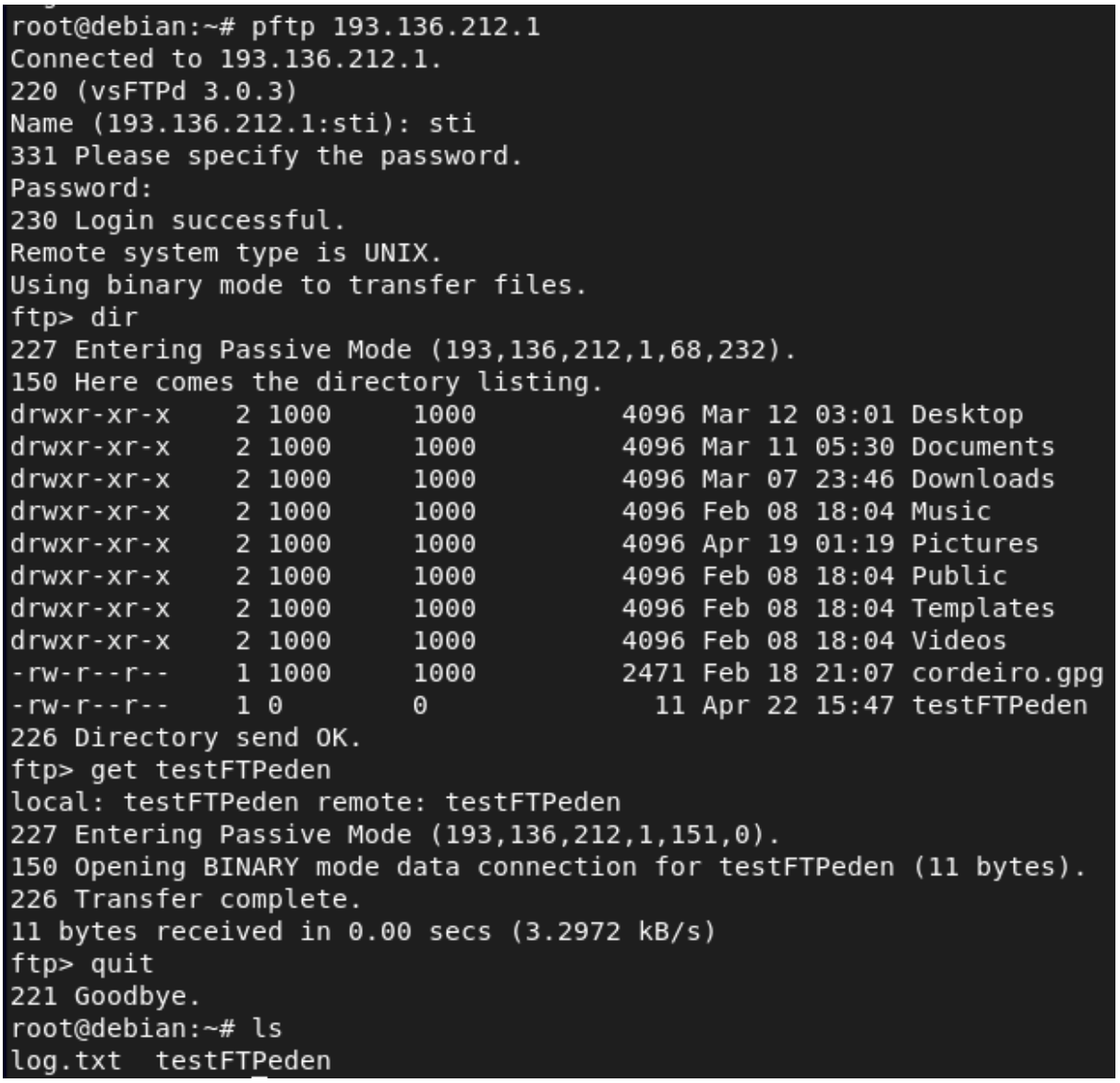
Cliente netcat na **Internal Network para Internet(dns2).**

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

- iptables -t nat -A POSTROUTING -p tcp -s 10.20.20.0/24 -d 193.136.0.0/15 –sport ftp -j SNAT –to-source 193.136.0.1

```
root@debian:~# ftp 193.136.212.1
Connected to 193.136.212.1.
220 (vsFTPd 3.0.3)
Name (193.136.212.1:sti): sti
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 1000     1000         4096 Mar 12 03:01 Desktop
drwxr-xr-x    2 1000     1000         4096 Mar 11 05:30 Documents
drwxr-xr-x    2 1000     1000         4096 Mar 07 23:46 Downloads
drwxr-xr-x    2 1000     1000         4096 Feb 08 18:04 Music
drwxr-xr-x    2 1000     1000         4096 Apr 19 01:19 Pictures
drwxr-xr-x    2 1000     1000         4096 Feb 08 18:04 Public
drwxr-xr-x    2 1000     1000         4096 Feb 08 18:04 Templates
drwxr-xr-x    2 1000     1000         4096 Feb 08 18:04 Videos
-rw-r--r--    1 1000     1000         2471 Feb 18 21:07 cordeiro.gpg
-rw-r--r--    1 0        0              11 Apr 22 15:47 testFTPeden
226 Directory send OK.
ftp> get testFTPeden
local: testFTPeden remote: testFTPeden
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for testFTPeden (11 bytes).
226 Transfer complete.
11 bytes received in 0.00 secs (3.9077 kB/s)
ftp> quit
221 Goodbye.
root@debian:~# ls
log.txt  testFTPeden
```

Ligação ao servidor ftp em **active mode** a partir da Internal Network.



Ligação ao servidor ftp em **passive mode** a partir da Internal Network.

5. Intrusions

Para que os pacotes provenientes da internet fossem encaminhados para a nfqueue foi necessário implementar regras prioritárias de forma a manipular os pacotes. Isto foi possível através de mangle:

- *iptables -t mangle -A PREROUTING -s 193.136.0.0/15 -j CONNMARK --set-mark 1*
- *iptables -t mangle -A PREROUTING -m connmark --mark 1 -j NFQUEUE --queue-num 0*
- *modprobe nfnetlink_queue*

Para correr o snort:
snort -dev -l /etc/snort/log -c /etc/snort/snort.conf -Q -A console

5.1. SQL injections

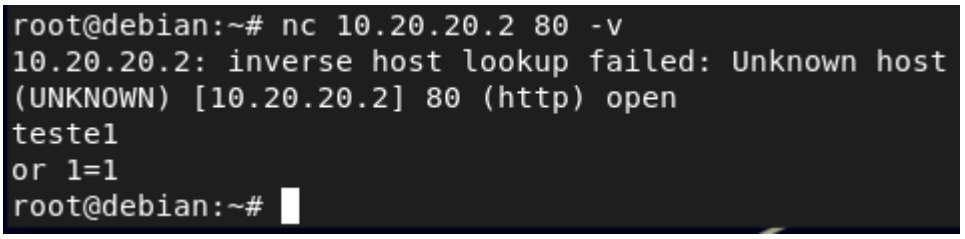
As injeções de SQL normalmente ocorrem quando é pedido ao utilizador um input, por exemplo o username/password e o utilizador dá comandos de SQL que vão ocorrer na BD.
Por exemplo:
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;

5.1.1. "1=1" is always true

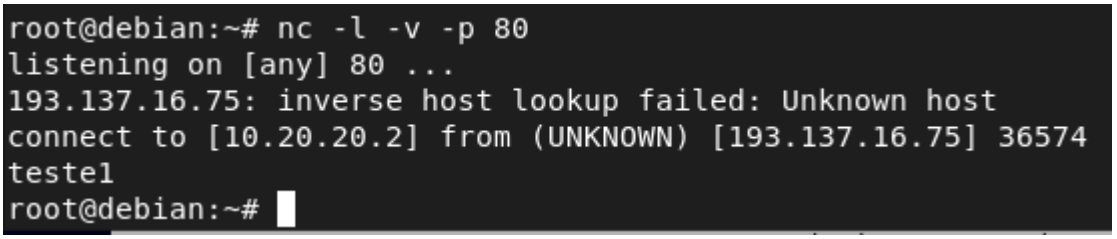
Numa caixa de input de username o utilizador pode meter [ID OR 1=1], como 1=1 é sempre verdade o comando que correria seria "SELECT * FROM Users WHERE UserID = ID or 1=1" retornando a tabela de todos os utilizadores, podendo esta conter as passwords dos utilizadores.
Desta forma, o snort permite-nos bloquear estes statements através do comando:

- *drop tcp 193.136.0.0/15 any -> any any (sid:001; msg:"Sql injection OR"; content: "or"; nocase;)*

Testes:
Internet:



Internal network:



Snort(Router):

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/23-20:12:02.098168 193.137.16.75:36574 -> 10.20.20.2:80
TCP TTL:64 TOS:0x0 ID:7785 IpLen:20 DgmLen:59 DF
***AP*** Seq: 0x93D777A  Ack: 0x7B100184  Win: 0x1F6  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1168530527 2969453649
74 65 73 74 65 31 0A                                 teste1.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/23-20:12:04.318966  [Drop] [**] [1:2:0] Sql injection OR [**] [Priority: 0]
04/23-20:12:04.318966 193.137.16.75:36574 -> 10.20.20.2:80
TCP TTL:64 TOS:0x0 ID:7786 IpLen:20 DgmLen:59 DF
***AP*** Seq: 0x93D7781  Ack: 0x7B100184  Win: 0x1F6  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1168532737 2969455496
6F 72 20 31 3D 31 0A                                 or 1=1.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

5.1.2. Batched SQL statements

A batch of SQL statements is a group of two or more SQL statements, separated by semicolons.
Usando o exemplo anterior, o utilizador na caixa de input pode meter [2022; DROP TABLE Suppliers] executando o statement “SELECT * FROM Users WHERE UserId = 2022; DROP TABLE Suppliers;”, apagando a tabela “Suppliers”. De forma a nos protegermos para este tipo de ataques a seguinte regra foi adicionada ao snort:

- *drop tcp 193.136.0.0/15 any -> any any (sid:002; msg:”Sql injection DROP”; content: “drop”; nocase;)*

Testes:

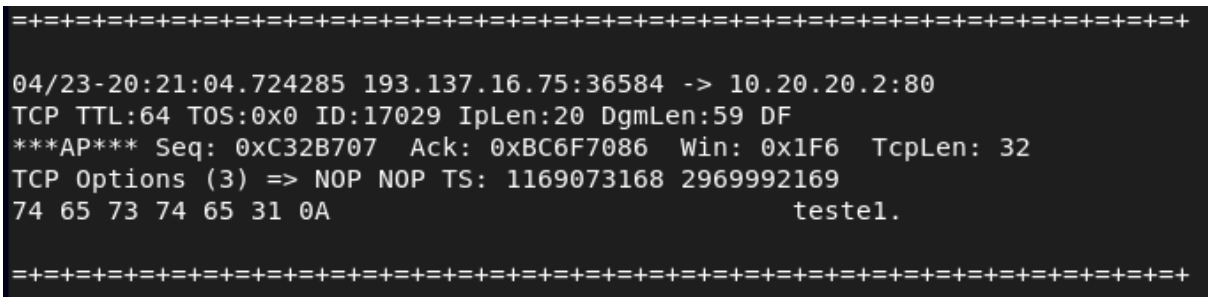
Internet:

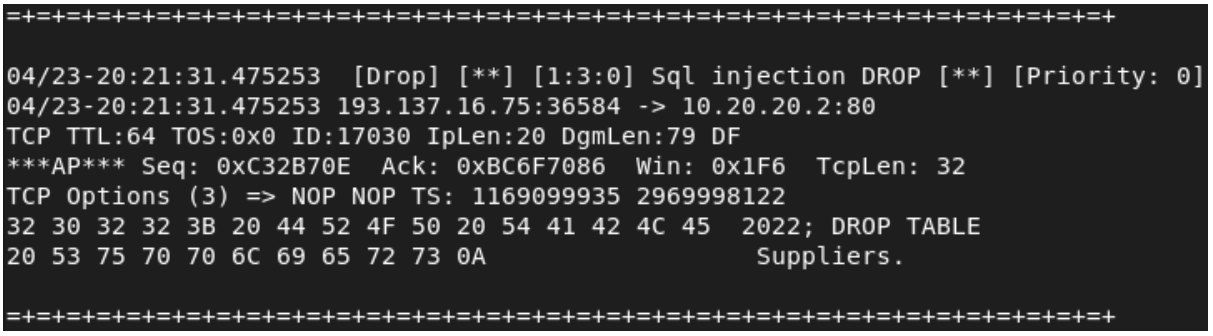
```
root@debian:~# nc 10.20.20.2 80 -v
10.20.20.2: inverse host lookup failed: Unknown host
(UNKNOWN) [10.20.20.2] 80 (http) open
teste1
2022; DROP TABLE Suppliers
root@debian:~#
```

Internal network:

```
root@debian:~# nc -l -v -p 80
listening on [any] 80 ...
193.137.16.75: inverse host lookup failed: Unknown host
connect to [10.20.20.2] from (UNKNOWN) [193.137.16.75] 36584
teste1
root@debian:~#
```

Snort(Router):





5.2. XXS Attacks

Scripting cross-site (XSS) é um ataque de injeção de código que permite que um intruso execute JavaScript malicioso no navegador de outro utilizador.

5.2.1. Intrusão por input

Este ataque pode acontecer se o site incluir diretamente o input do utilizador nas suas páginas, porque o intruso pode inserir uma cadeia que será tratada como código pelo browser da vítima, neste caso num script.
exemplo:
Se em server-side houver um script para mostrar o ultimo comentário num website:
print “<html>”
print "Latest comment:"
print database.latestComment
print “<html>”
O utilizador pode introduzir um comentário do tipo “<script>...</script>” fazendo com que qualquer indivíduo ao inicializar a página corra o código de JavaScript contido dentro das tags <script>.
De forma a que este ataque fosse alertado e bloqueado, foi feita a seguinte regra:

- *drop tcp 193.136.0.0/15 any -> any any (sid:003; msg:”XSS attack <SCRIPT>”; pcre:”/(%3C|\<)script(%3E|\>).*(%3C|\<)(%2F|\/)script(%3E|\>)/i”;)*

Testes:

Internet:

```
root@debian:~# nc 10.20.20.2 80 -v
10.20.20.2: inverse host lookup failed: Unknown host
(UNKNOWN) [10.20.20.2] 80 (http) open
teste1
<script>teste do script</script>
root@debian:~#
```

Internal network:

```
root@debian:~# nc -l -v -p 80
listening on [any] 80 ...
193.137.16.75: inverse host lookup failed: Unknown host
connect to [10.20.20.2] from (UNKNOWN) [193.137.16.75] 36586
teste1
root@debian:~#
```

Snort(router):

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/23-20:28:43.475310 193.137.16.75:36588 -> 10.20.20.2:80
TCP TTL:64 TOS:0x0 ID:39698 IpLen:20 DgmLen:59 DF
***AP*** Seq: 0xB193A73A  Ack: 0x8E253BB4  Win: 0x1F6  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1169531887 2970454148
74 65 73 74 65 31 0A                             teste1.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/23-20:28:54.231130  [Drop] [**] [1:4:0] XSS attack <script> [**] [Priority: 0]
04/23-20:28:54.231130 193.137.16.75:36588 -> 10.20.20.2:80
TCP TTL:64 TOS:0x0 ID:39699 IpLen:20 DgmLen:85 DF
***AP*** Seq: 0xB193A741  Ack: 0x8E253BB4  Win: 0x1F6  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1169542670 2970456873
3C 73 63 72 69 70 74 3E 74 65 73 74 65 20 64 6F  <script>teste do
20 73 63 72 69 70 74 3C 2F 73 63 72 69 70 74 3E   script</script>
0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

5.2.2. Events

Os eventos em JavaScript, como por exemplo onload, podem ser usados em muitas tags diferentes. Esta é uma forma de ataque XSS muito popular. Neste caso, o intruso pode escrever um excerto de código, mais uma vez, como input de um site.
Exemplo
<p onload=alert(information)></p>
Ao colocar o código acima como input, o intruso faz a página re-renderizar, emitindo um evento que vai fazer com que um pop up apareça no ecrã, com a informação que o intruso quiser.
Para proteção contra este tipo de ataques adicionamos ao snort a regra:

- *drop tcp 193.136.0.0/15 any -> any any (sid:004; msg:”XSS attack JAVA EVENT”; content: “onload”; nocase;)*

Testes:

Internet:

```
root@debian:~# nc 10.20.20.2 80 -v
10.20.20.2: inverse host lookup failed: Unknown host
(UNKNOWN) [10.20.20.2] 80 (http) open
teste1
<p> onload=alert(teste onload)</p>
root@debian:~#
```

Internal network:

```
root@debian:~# nc -l -v -p 80
listening on [any] 80 ...
193.137.16.75: inverse host lookup failed: Unknown host
connect to [10.20.20.2] from (UNKNOWN) [193.137.16.75] 36590
teste1
root@debian:~#
```

Snort(router):

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/23-20:30:21.885083 193.137.16.75:36590 -> 10.20.20.2:80
TCP TTL:64 TOS:0x0 ID:46673 IpLen:20 DgmLen:59 DF
***AP*** Seq: 0x21AD1E57  Ack: 0xC42E02C8  Win: 0x1F6  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1169630284 2970553439
74 65 73 74 65 31 0A                                 teste1.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/23-20:31:20.187614  [Drop] [**] [1:5:0] XSS attack Java Event [**] [Priority: 0]
04/23-20:31:20.187614 193.137.16.75:36590 -> 10.20.20.2:80
TCP TTL:64 TOS:0x0 ID:46674 IpLen:20 DgmLen:87 DF
***AP*** Seq: 0x21AD1E5E  Ack: 0xC42E02C8  Win: 0x1F6  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1169688615 2970555283
3C 70 3E 20 6F 6E 6C 6F 61 64 3D 61 6C 65 72 74  <p> onload=alert
28 74 65 73 74 65 20 6F 6E 6C 6F 61 64 29 3C 2F  (teste onload)</
70 3E 0A                                         p>.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

6. Referências:

https://linuxhint.com/installing_ftp_server_linux_mint/
https://www.cloudflare.com/es-es/learning/security/threats/sql-injection/
https://www.w3schools.com/sql/sql_injection.asp
https://excess-xss.com/
https://www.ciscopress.com/articles/article.asp?p=1733640&seqNum=5