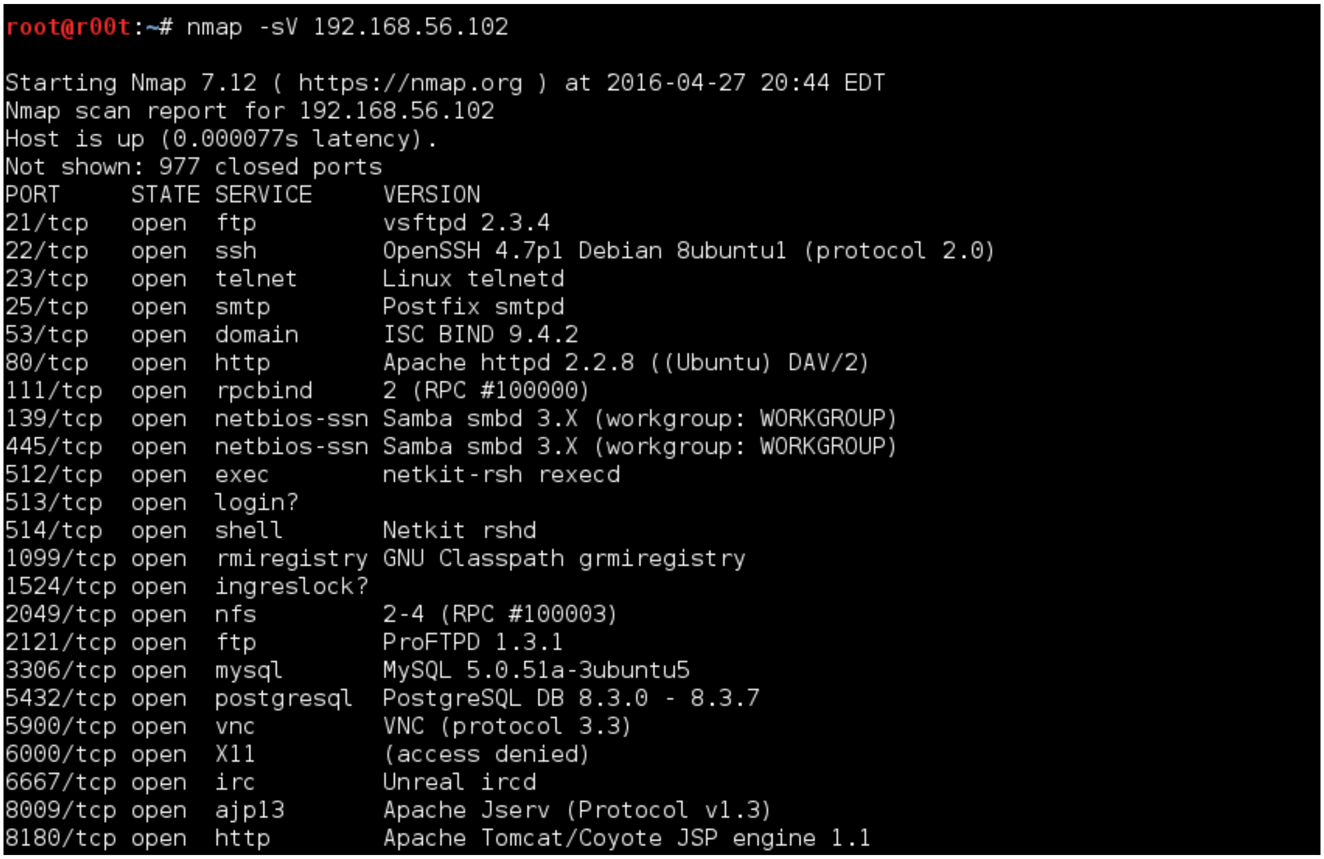
Vivian Choe
ENPM 695 — Secure Operating Systems
Semester Project

Task Group 1: Evaluate the security of the system

Task 1: Determine the running and open services on the system (10 points)

- The ifconfig results for the network showed that the IP address of Kali is 192.168.56.101. Knowing that the IP address for Kali is 192.168.56.101, therefore that means that the metasploitable should have an IP address residing in 192.168.56.0/24. The metasploitable IP address is 192.168.56.102. By using nmap -sV 192.168.56.102, we get the list of running services on the IP address.

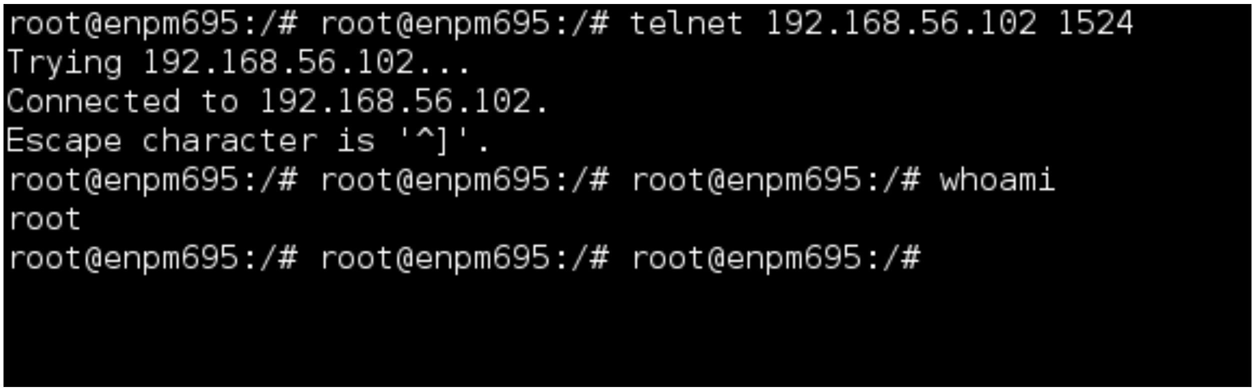


```
root@r00t:~# nmap -sV 192.168.56.102

Starting Nmap 7.12 ( https://nmap.org ) at 2016-04-27 20:44 EDT
Nmap scan report for 192.168.56.102
Host is up (0.000077s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  ingreslock?
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         Unreal ircd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
```

- As listed within the screenshot above, the running services include ftp, ssh, telnet, smtp, domain, http, rpcbind, netbios-ssn,exec, login, shell, rmiregistry, ingreslock?,nfs,ftp on port 2121, mysql, postgresql, vnc, x11, irc, ajp13, and http on port 8180.

Task 2: Access the system by exploiting a vulnerable running or open service (10 points) – points are awarded based on a description of how the service was exploited as well as the tools used.

- In the list of services running,telnet is open. It is known as being one of many ports that are susceptible to attacks. By typing in telnet 192.168.56.102 1524, I am granted access. This was done using both the telnet port and the ingreslock port in order to gain backdoor access.



```
root@enpm695:/# root@enpm695:/# telnet 192.168.56.102 1524
Trying 192.168.56.102...
Connected to 192.168.56.102.
Escape character is '^]'.
root@enpm695:/# root@enpm695:/# root@enpm695:/# whoami
root
root@enpm695:/# root@enpm695:/# root@enpm695:/#
```

Task 3: Detail the flaws in the web server running on the system (10 points) – points are awarded based on detailing five flaws in the web server.

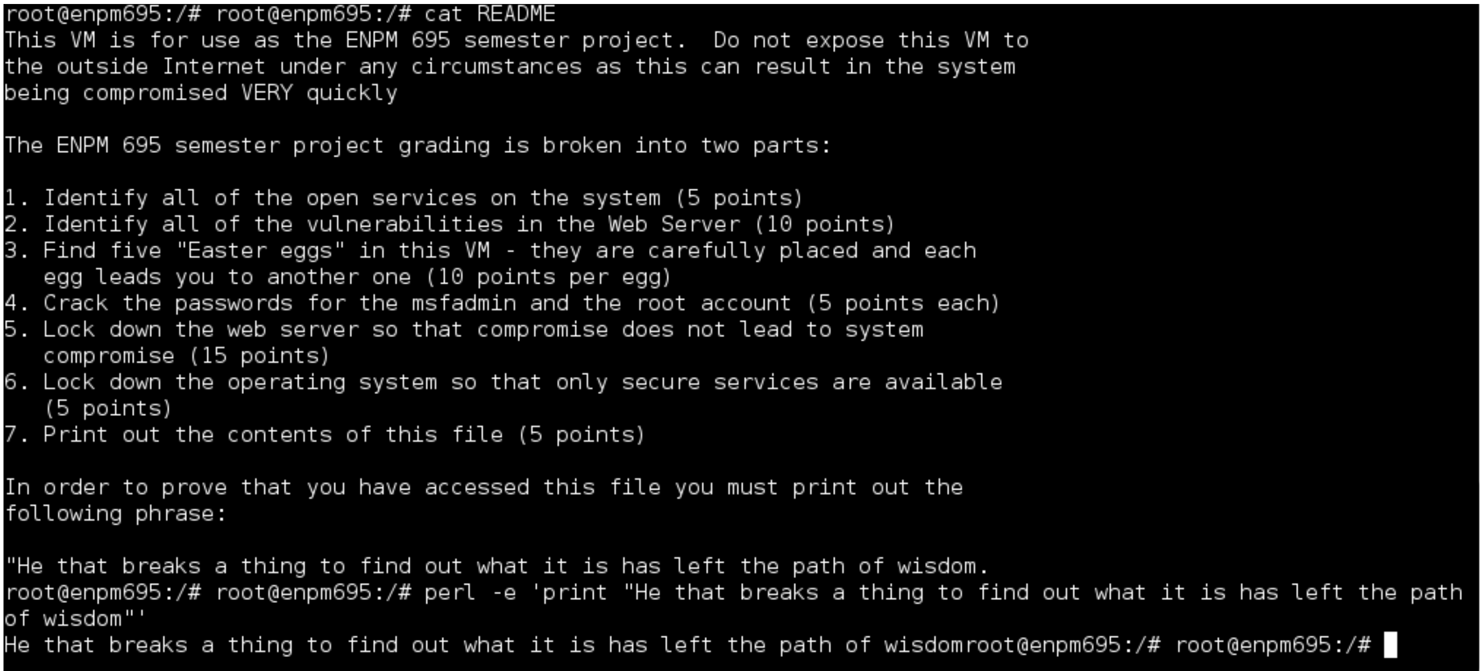
- Server version banner: The apache server version is listed on the bottom of the web browser when being accessed. Exposing the web server version and the OS version makes it easier for the hacker to spot vulnerabilities. In removing the server version, it won't stop hackers from finding the vulnerabilities, but it will make it harder for them to access them.
- SQL Injection: The DAWA is embedded with an SQL injection and an SQL injection blind within the web page. Similar to that of PHP injections, SQL injections are also vulnerable due to nothing input validations therefore an attacker could gain access to the database by entering anything into the SQL database.
- XSS: Cross Site Scripting is a vulnerability that could appear on a number of web pages. In the web server there are multiple pages that are open to XSS attacks. In addition, if trace HTTP requests are enabled this can cause for potential attacks that could allow the attacker to steal cookie information.
- Directory Listing: The web server shows the directory listing, which would be like the table of contents of a book. This makes the web server more vulnerable as it makes it easier for an attacker to access. Therefore most web servers, don't show the directory.
- PHP Injection attacks: The web server contains many PHP files, which has a greater chance of PHP injection attacks as are when there are no input validations within the PHP therefore anything the attacker inputs will be successful, which makes the mutillidae website vulnerable as it contains many PHP files that aren't protected.

Task 4: Crack passwords (10 points) – crack 3 user account passwords will award students the full 10 points. Crack the root password will award an additional 10 points

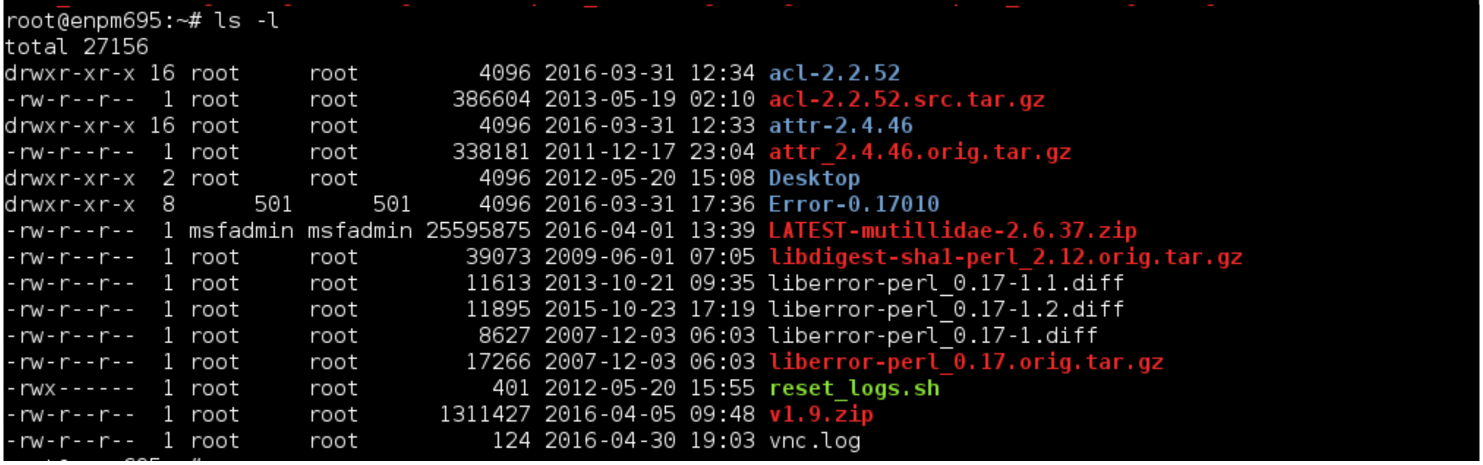
- `sys: $1$fUX6BP0t$Miyc3Up0zQJqz4s5wFD9l0`
- `user: $1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0`
- `enpm695: $1$3eYw6ZFF$PIPwtPjUubX.80lf6r1EY/`
- `root: $1$mgrmd3Ek$ViXoiuk3GG8pcQ9zkfni21`

Task 5: Find out the information stored in a specific file (/README) within the system (10 points) – accessing the file and providing its contents (5 points). Identifying and explaining the protection around the file (5 points)

- To access the /README file, the user needs to look at the home directory. Or depending on how it is being accessed the command ls can be executed to look for the README file. Since I used the backdoor approach to access the metasploitable. I used the ls command to find the README file and then did cat README in order to read the contents of the file.



```
root@enpm695:/# root@enpm695:/# cat README
This VM is for use as the ENPM 695 semester project.  Do not expose this VM to
the outside Internet under any circumstances as this can result in the system
being compromised VERY quickly

The ENPM 695 semester project grading is broken into two parts:

1. Identify all of the open services on the system (5 points)
2. Identify all of the vulnerabilities in the Web Server (10 points)
3. Find five "Easter eggs" in this VM - they are carefully placed and each
   egg leads you to another one (10 points per egg)
4. Crack the passwords for the msfadmin and the root account (5 points each)
5. Lock down the web server so that compromise does not lead to system
   compromise (15 points)
6. Lock down the operating system so that only secure services are available
   (5 points)
7. Print out the contents of this file (5 points)

In order to prove that you have accessed this file you must print out the
following phrase:

"He that breaks a thing to find out what it is has left the path of wisdom.
root@enpm695:/# root@enpm695:/# perl -e 'print "He that breaks a thing to find out what it is has left the path
of wisdom"'
He that breaks a thing to find out what it is has left the path of wisdomroot@enpm695:/# root@enpm695:/# 
```

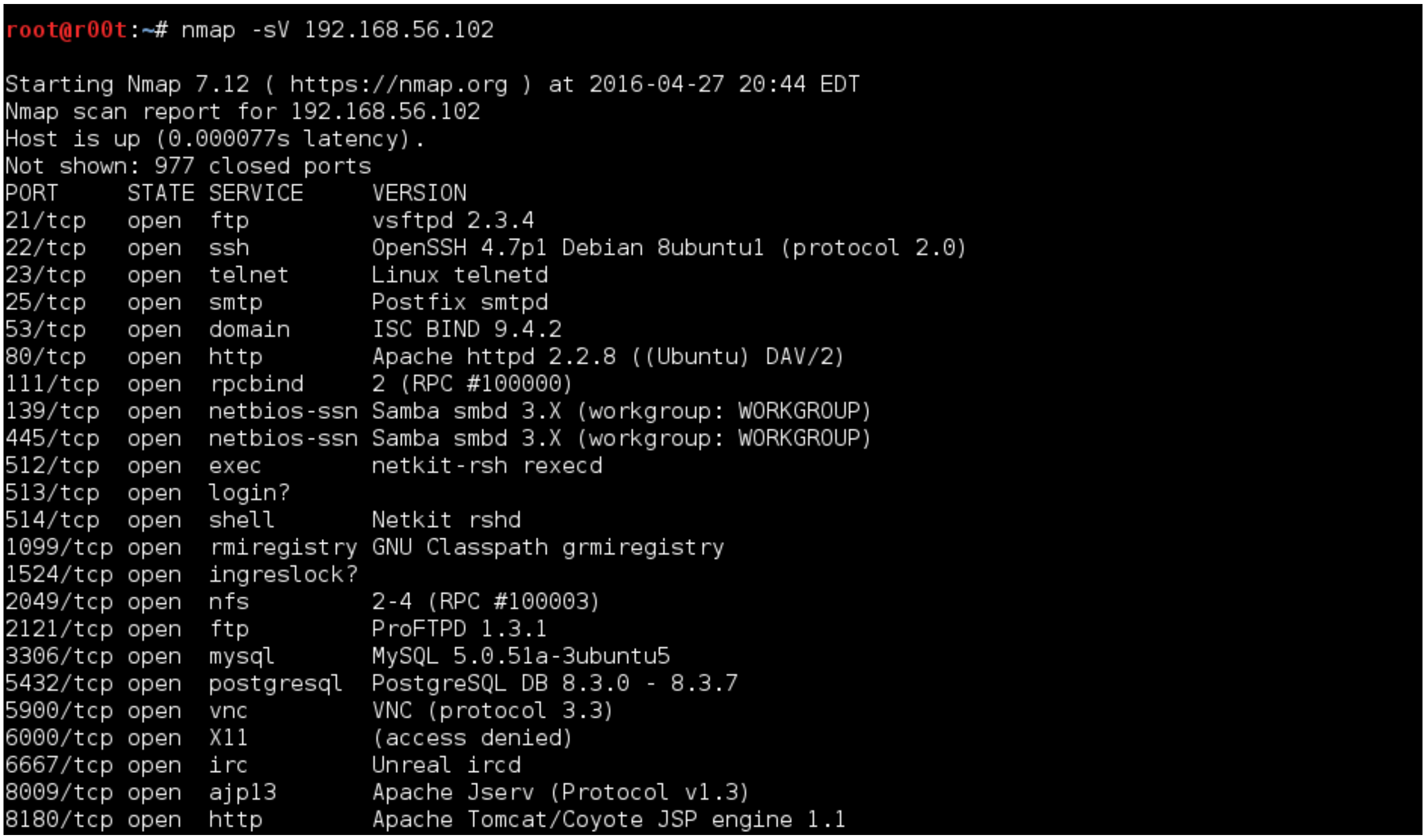


```
root@enpm695:~# ls -l
total 27156
drwxr-xr-x 16 root     root         4096 2016-03-31 12:34 acl-2.2.52
-rw-r--r--  1 root     root       386604 2013-05-19 02:10 acl-2.2.52.src.tar.gz
drwxr-xr-x 16 root     root         4096 2016-03-31 12:33 attr-2.4.46
-rw-r--r--  1 root     root       338181 2011-12-17 23:04 attr_2.4.46.orig.tar.gz
drwxr-xr-x  2 root     root         4096 2012-05-20 15:08 Desktop
drwxr-xr-x  8      501      501     4096 2016-03-31 17:36 Error-0.17010
-rw-r--r--  1 msfadmin msfadmin 25595875 2016-04-01 13:39 LATEST-mutillidae-2.6.37.zip
-rw-r--r--  1 root     root        39073 2009-06-01 07:05 libdigest-sha1-perl_2.12.orig.tar.gz
-rw-r--r--  1 root     root        11613 2013-10-21 09:35 liberror-perl_0.17-1.1.diff
-rw-r--r--  1 root     root        11895 2015-10-23 17:19 liberror-perl_0.17-1.2.diff
-rw-r--r--  1 root     root         8627 2007-12-03 06:03 liberror-perl_0.17-1.diff
-rw-r--r--  1 root     root        17266 2007-12-03 06:03 liberror-perl_0.17.orig.tar.gz
-rwx------  1 root     root          401 2012-05-20 15:55 reset_logs.sh
-rw-r--r--  1 root     root      1311427 2016-04-05 09:48 v1.9.zip
-rw-r--r--  1 root     root          124 2016-04-30 19:03 vnc.log
```

- README is accessible by read and write permissions by the user msfadmin. All other users and groups only have read access to the file. Due to these permissions, the file is protected from being written or executed by anyone else but msfadmin. In addition, there is only 1 hardlink to the file, which means that there's only one access point, this makes it harder for another user to be able to access the file or alter the file.

Task 6: Define the Attack Surface of the system and web server (5 points each)

- An attack surface is defined as the description of all the points where an attacker van get into the system and get data out, which detail what ports are open and the services that are running. Vulnerable services include telnet on port 23, login on port 513, as an attacker can gain access to root as long as rsh is installed. In addition, ports 513 and 514 as they are known as "r" services, which allow attackers to gain remote access from any host. Other ports that are open are port 21 vsftpd, which allows backdoor access as long as a :) is entered with the username. These are a few of the open ports and services that are running. Pictured below is the full list of services running within the web server. Since, metasploitable has been created purposefully with many vulnerabilities, I list all ports that are open, as they are vulnerable just like the metasploitable itself.



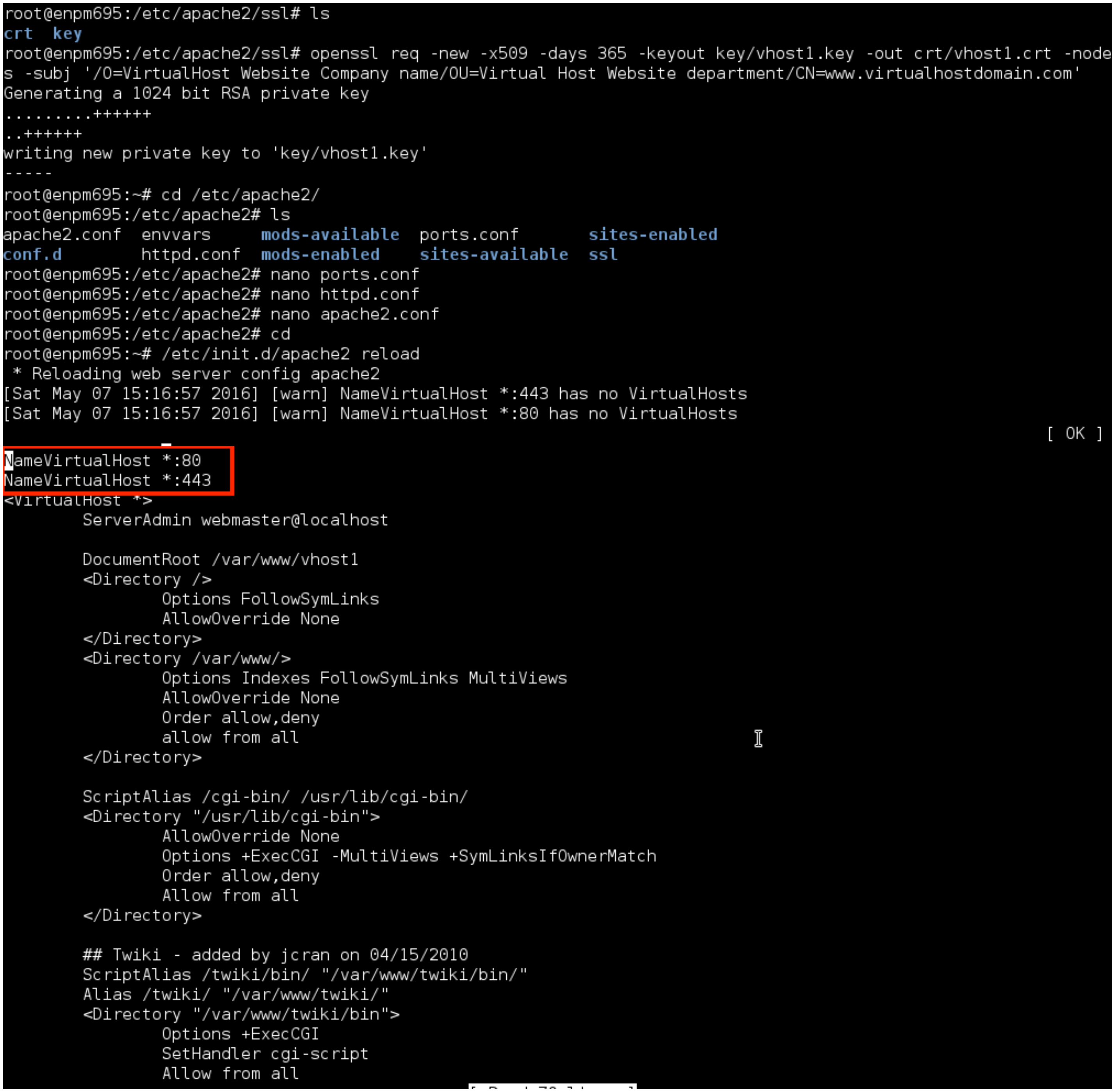
```
root@r00t:~# nmap -sV 192.168.56.102

Starting Nmap 7.12 ( https://nmap.org ) at 2016-04-27 20:44 EDT
Nmap scan report for 192.168.56.102
Host is up (0.000077s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  ingreslock?
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         Unreal ircd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
```

Task Group 2: Improve the security of the system

Task 1: Lock down the web server (20 points) – point breakdown is as follows:

a. Setting up HTTPS (10 points)

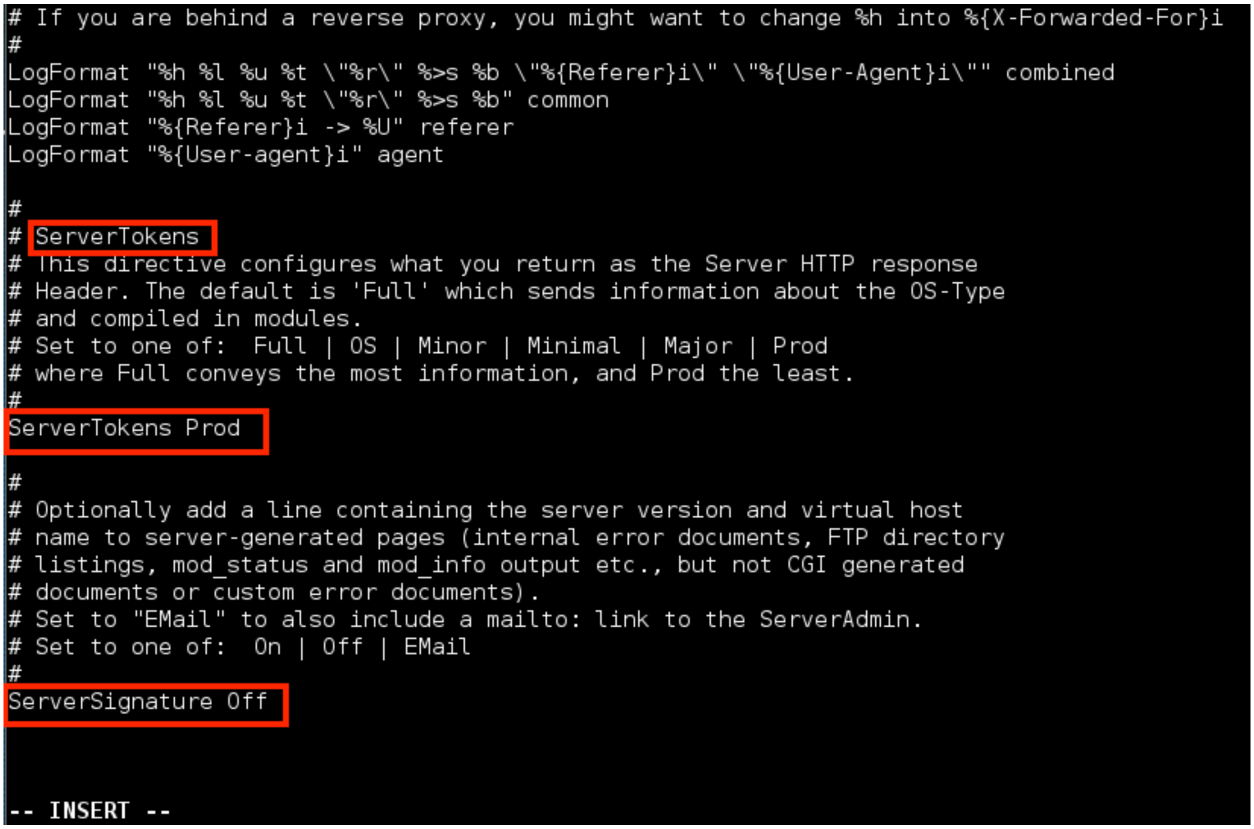
- In order to set up the HTTPS in Apache by first making an SSL key, this is done by using open SSL. After configuring the SSL keys, you need to change the sites configuration located in: /etc/apache2/sites-available/. In addition, the configuration file need to be tweaked so that only HTTP/HTTPS will be used.



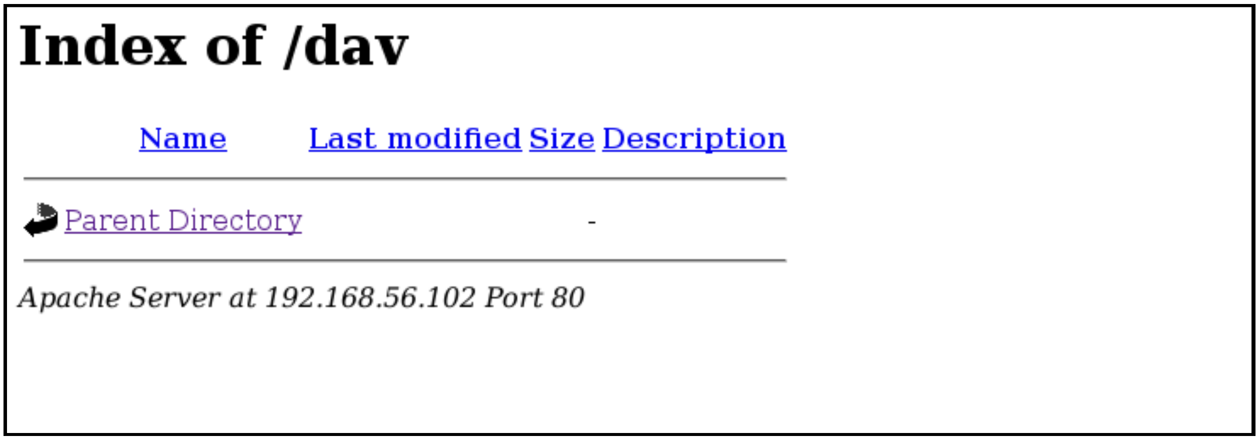
```
root@enpm695:/etc/apache2/ssl# ls
crt  key
root@enpm695:/etc/apache2/ssl# openssl req -new -x509 -days 365 -keyout key/vhost1.key -out crt/vhost1.crt -node
s -subj '/O=VirtualHost Website Company name/OU=Virtual Host Website department/CN=www.virtualhostdomain.com'
Generating a 1024 bit RSA private key
.........++++++
..++++++
writing new private key to 'key/vhost1.key'
-----
root@enpm695:~# cd /etc/apache2/
root@enpm695:/etc/apache2# ls
apache2.conf  envvars     mods-available  ports.conf       sites-enabled
conf.d        httpd.conf  mods-enabled    sites-available  ssl
root@enpm695:/etc/apache2# nano ports.conf
root@enpm695:/etc/apache2# nano httpd.conf
root@enpm695:/etc/apache2# nano apache2.conf
root@enpm695:/etc/apache2# cd
root@enpm695:~# /etc/init.d/apache2 reload
 * Reloading web server config apache2
[Sat May 07 15:16:57 2016] [warn] NameVirtualHost *:443 has no VirtualHosts
[Sat May 07 15:16:57 2016] [warn] NameVirtualHost *:80 has no VirtualHosts
                                                                                                                   [ OK ]

NameVirtualHost *:80
NameVirtualHost *:443
<VirtualHost *>
        ServerAdmin webmaster@localhost

        DocumentRoot /var/www/vhost1
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>

        ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
        <Directory "/usr/lib/cgi-bin">
                AllowOverride None
                Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
                Order allow,deny
                Allow from all
        </Directory>

        ## Twiki - added by jcran on 04/15/2010
        ScriptAlias /twiki/bin/ "/var/www/twiki/bin/"
        Alias /twiki/ "/var/www/twiki/"
        <Directory "/var/www/twiki/bin">
                Options +ExecCGI
                SetHandler cgi-script
                Allow from all
```

b. Eliminating identifying information that the web server gives out (5 points)

- The first of many identifying information that the web server gives out is the server version on the server version banner. This is removed by accessing the apache2.conf file to turn off server tokens and signature(s).



```
# If you are behind a reverse proxy, you might want to change %h into %{X-Forwarded-For}i
#
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent

#
# ServerTokens
# This directive configures what you return as the Server HTTP response
# Header. The default is 'Full' which sends information about the OS-Type
# and compiled in modules.
# Set to one of:  Full | OS | Minor | Minimal | Major | Prod
# where Full conveys the most information, and Prod the least.
#
ServerTokens Prod

#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.
# Set to one of:  On | Off | EMail
#
ServerSignature Off


-- INSERT --
```

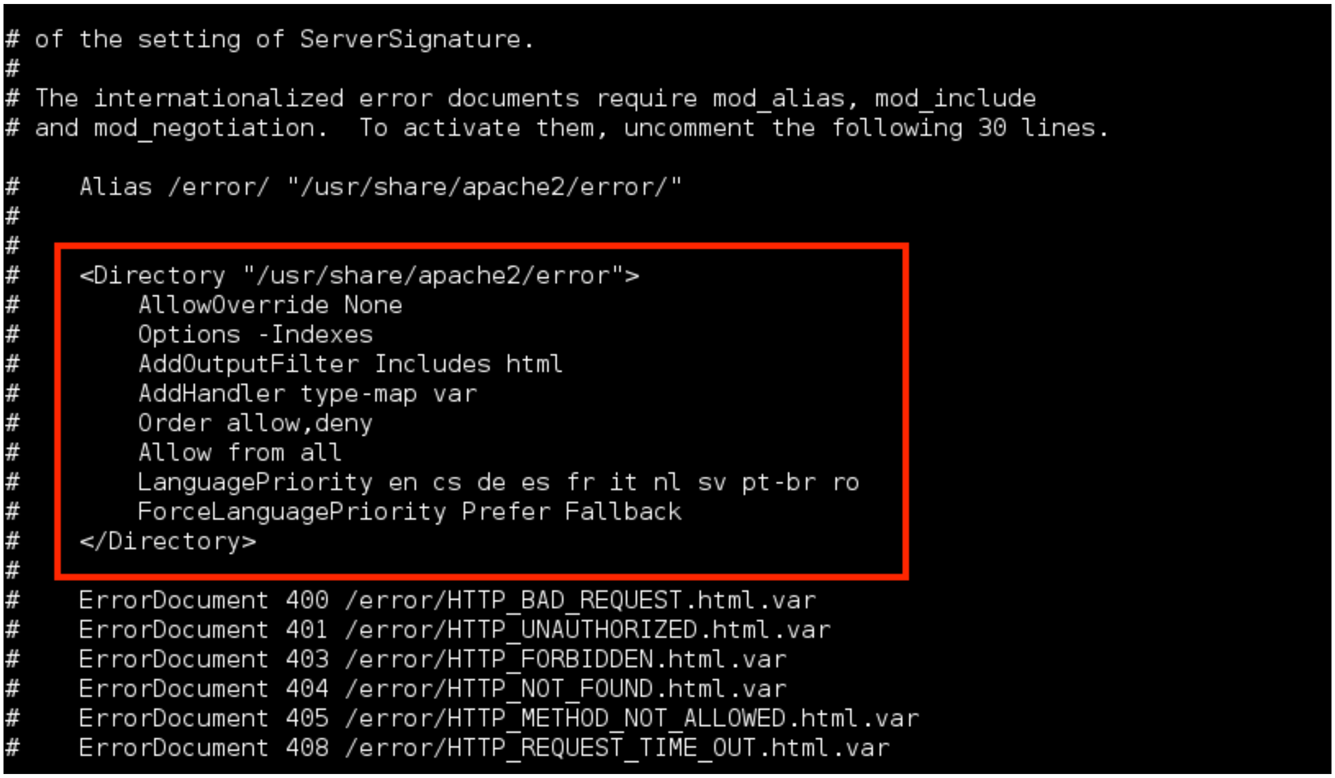


Index of /dav

Name	Last modified	Size	Description
Parent Directory		-	

Apache Server at 192.168.56.102 Port 80

- The web server gives out identifying information through the directory listing when accessing the web server, which shows the files that are listed in the web server. To avoid showing the directory,it would be done by going back to the apache2.conf file and changing the options under directory to -Indexes.



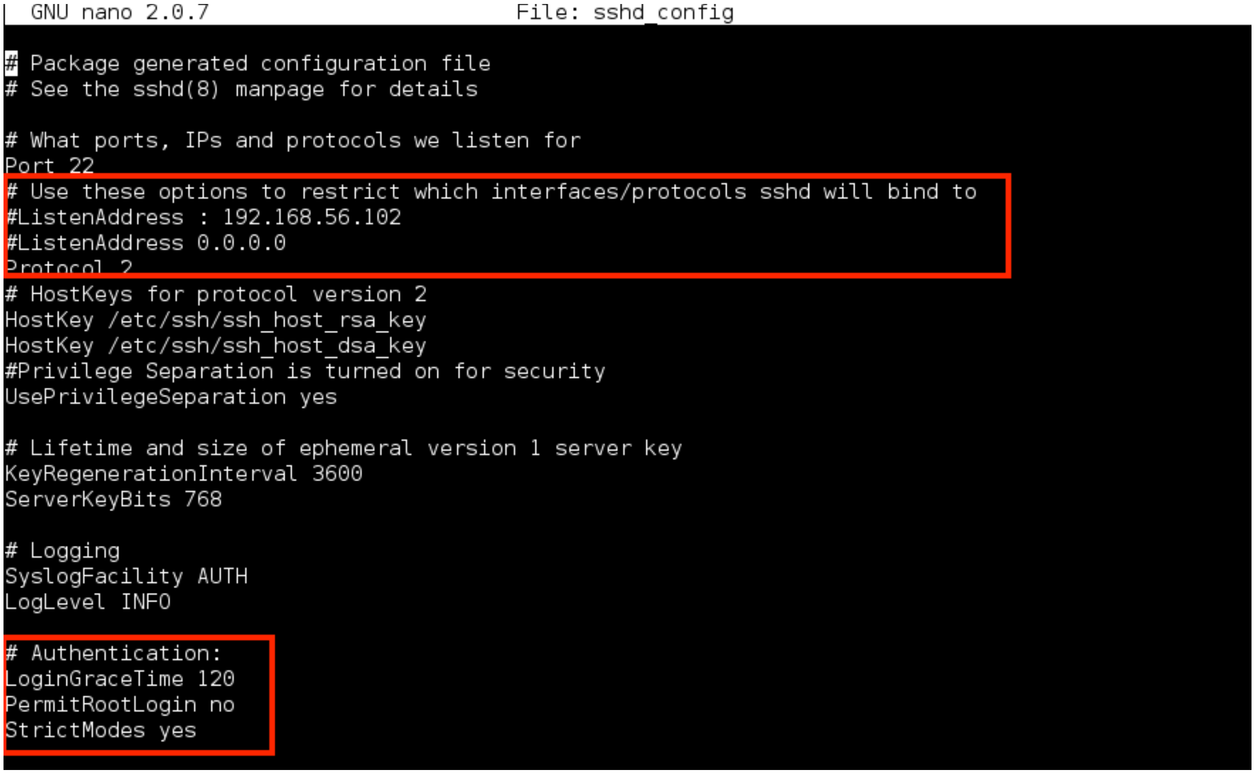
```
# of the setting of ServerSignature.
#
# The internationalized error documents require mod_alias, mod_include
# and mod_negotiation.  To activate them, uncomment the following 30 lines.

#    Alias /error/ "/usr/share/apache2/error/"
#
#
#    <Directory "/usr/share/apache2/error">
#        AllowOverride None
#        Options -Indexes
#        AddOutputFilter Includes html
#        AddHandler type-map var
#        Order allow,deny
#        Allow from all
#        LanguagePriority en cs de es fr it nl sv pt-br ro
#        ForceLanguagePriority Prefer Fallback
#    </Directory>
#
#    ErrorDocument 400 /error/HTTP_BAD_REQUEST.html.var
#    ErrorDocument 401 /error/HTTP_UNAUTHORIZED.html.var
#    ErrorDocument 403 /error/HTTP_FORBIDDEN.html.var
#    ErrorDocument 404 /error/HTTP_NOT_FOUND.html.var
#    ErrorDocument 405 /error/HTTP_METHOD_NOT_ALLOWED.html.var
#    ErrorDocument 408 /error/HTTP_REQUEST_TIME_OUT.html.var
```

c. Eliminate vulnerable applications (5 points)

- In order to eliminate the vulnerable applications, we could possibly delete them, as they only make the web server more susceptible to attacks. However, in order to do so, we also would need to secure the web server itself. If the web server isn't hardened/secure then ONLY deleting them would continue to leave the web server vulnerable due to the current settings.

Task 2: Lock down the operating system so that only the following services are readily available:

- Secure Shell:

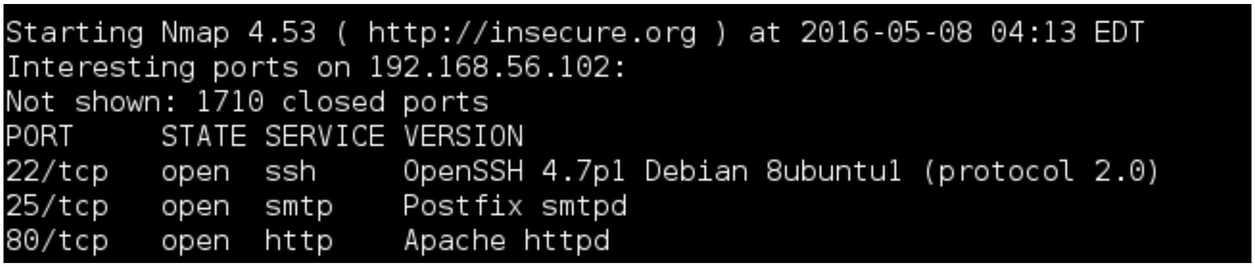


```
 GNU nano 2.0.7                      File: sshd_config

# Package generated configuration file
# See the sshd(8) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress : 192.168.56.102
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes
```

- HTTP/HTTPS

- Mail

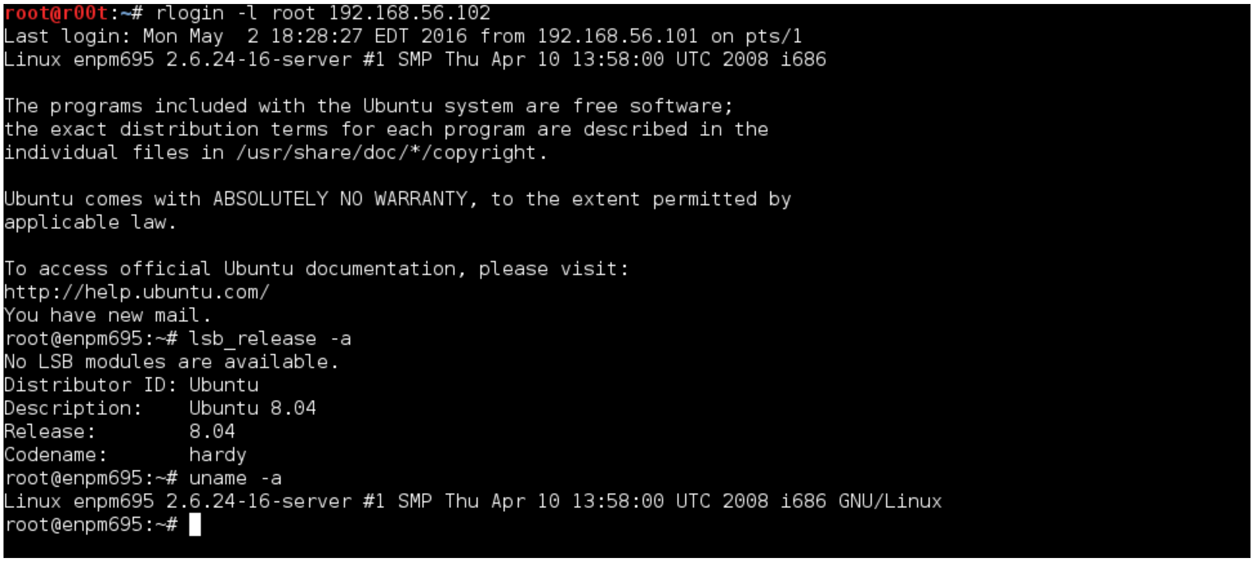
- In order to secure the 3 requested services and not being able to use iptables firewall to do so. To secure these services only, I manually closed all other services running by using ‘fuser -k -n tcp 21’ and so forth so that the only running services would include HTTP/HTTPS, Mail and SSH.



```
Starting Nmap 4.53 ( http://insecure.org ) at 2016-05-08 04:13 EDT
Interesting ports on 192.168.56.102:
Not shown: 1710 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp   open  smtp    Postfix smtpd
80/tcp   open  http    Apache httpd
```

Task 3: Identify the operating system (5 points)

- The operating system is Ubuntu version 8.04.



```
root@r00t:~# rlogin -l root 192.168.56.102
Last login: Mon May  2 18:28:27 EDT 2016 from 192.168.56.101 on pts/1
Linux enpm695 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@enpm695:~# lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 8.04
Release:        8.04
Codename:       hardy
root@enpm695:~# uname -a
Linux enpm695 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@enpm695:~# 
```

Task 4: Define the attack surface of the hardened system and web server application (10 points)

- Once the web server is hardened, the attack surface would include port 80, port 443, HTTP & HTTPS respectively. As well as port 22, SSH and port 25,Mail. Since all other ports are closed, the attack surface of the web server has become smaller. In addition, since all other vulnerable web server applications were removed, this results in being less susceptible to being vulnerable for attacks. Of course, no system is 100% secure.