

Curso: COMP 2700 – Ciberseguridad

Laboratorio: Laboratorio 2 - Identificación de Riesgos y Aplicación de Controles Básicos en Debian

Sección: 92249

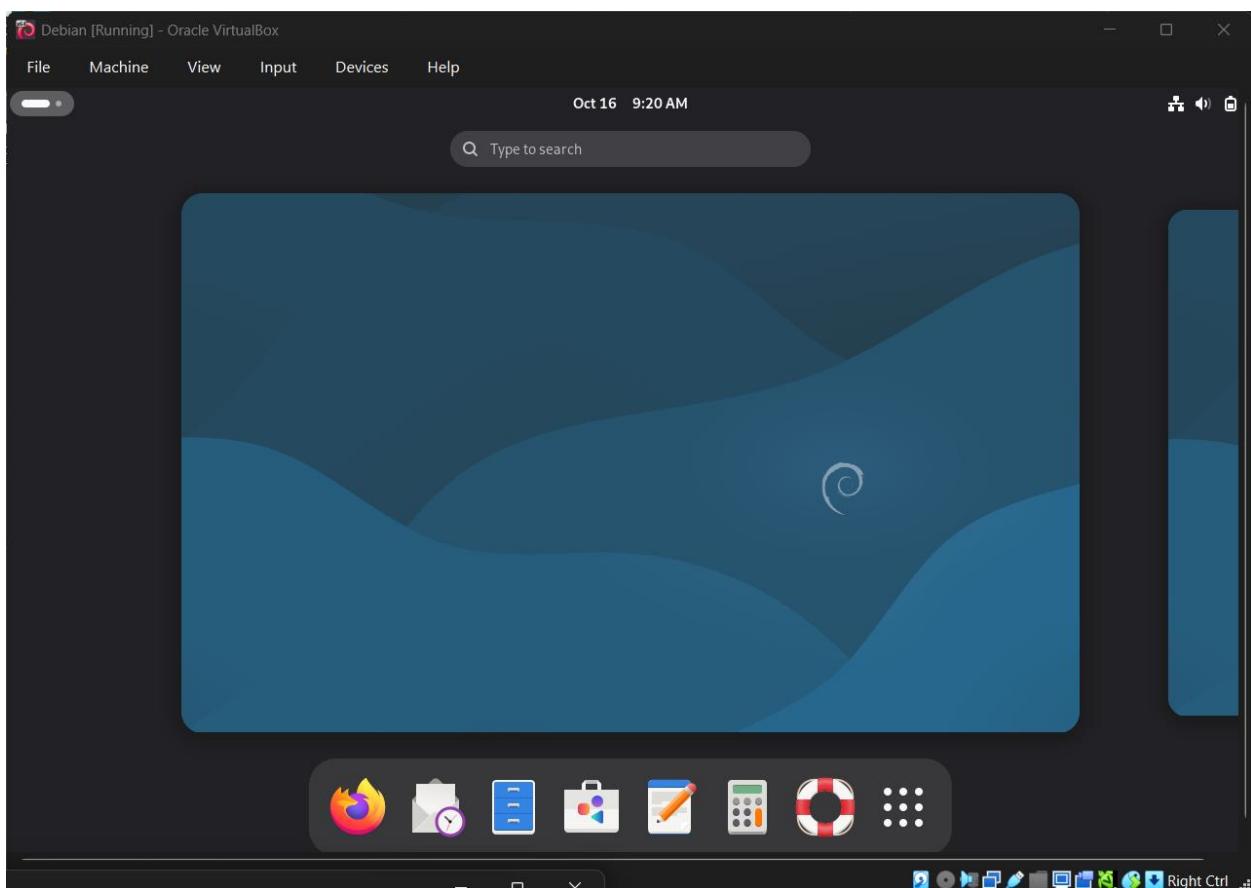
Líder del grupo: Benyahir Y. Martínez Hermina

Integrantes:

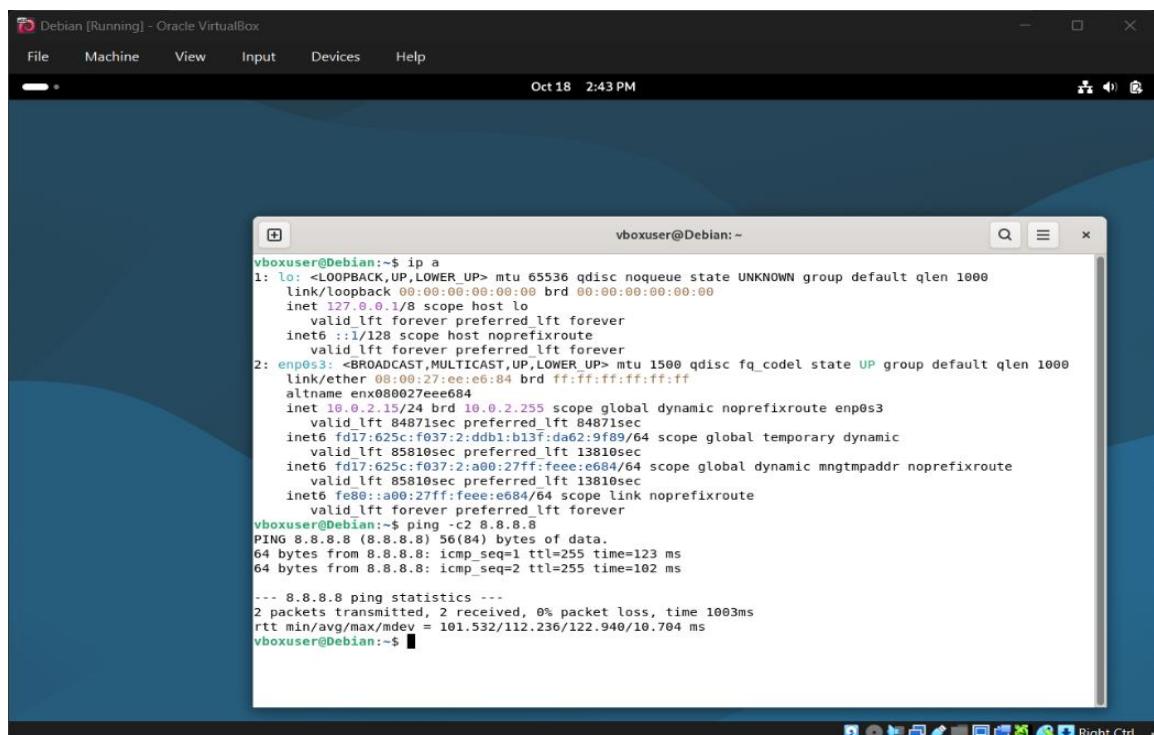
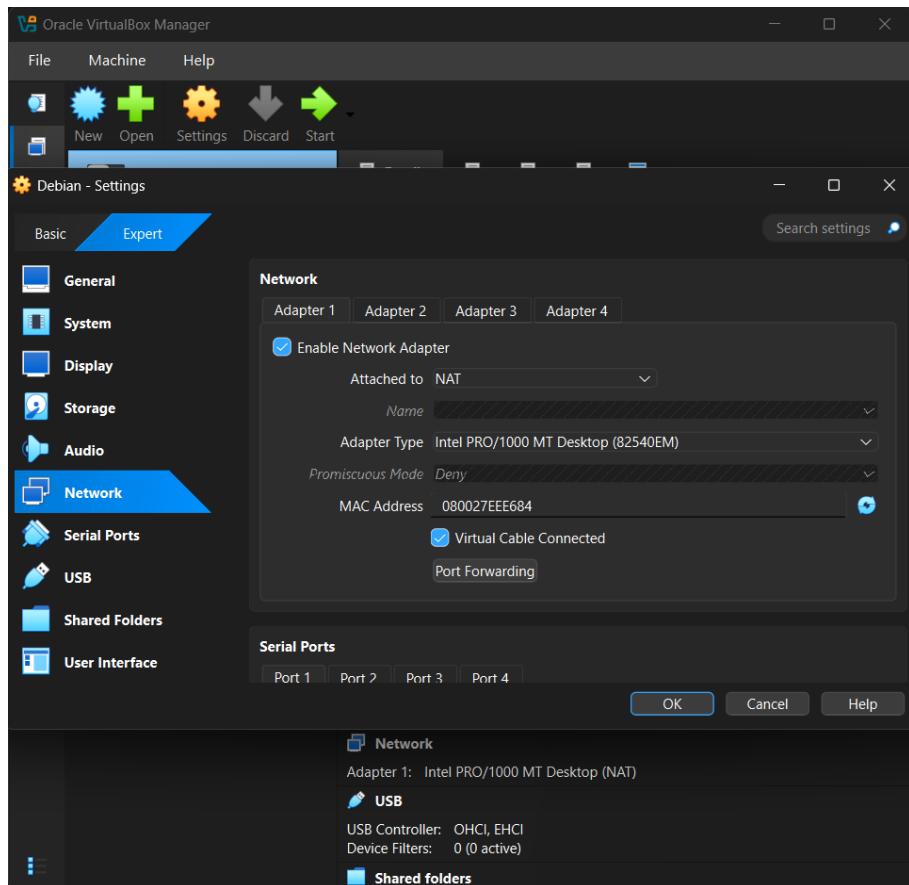
- Benyahir Y. Martínez
- Jacob J. Desuza
- Emanuel V. Rodríguez
- John A. Valentín

Fecha: 23 de oct. de 25

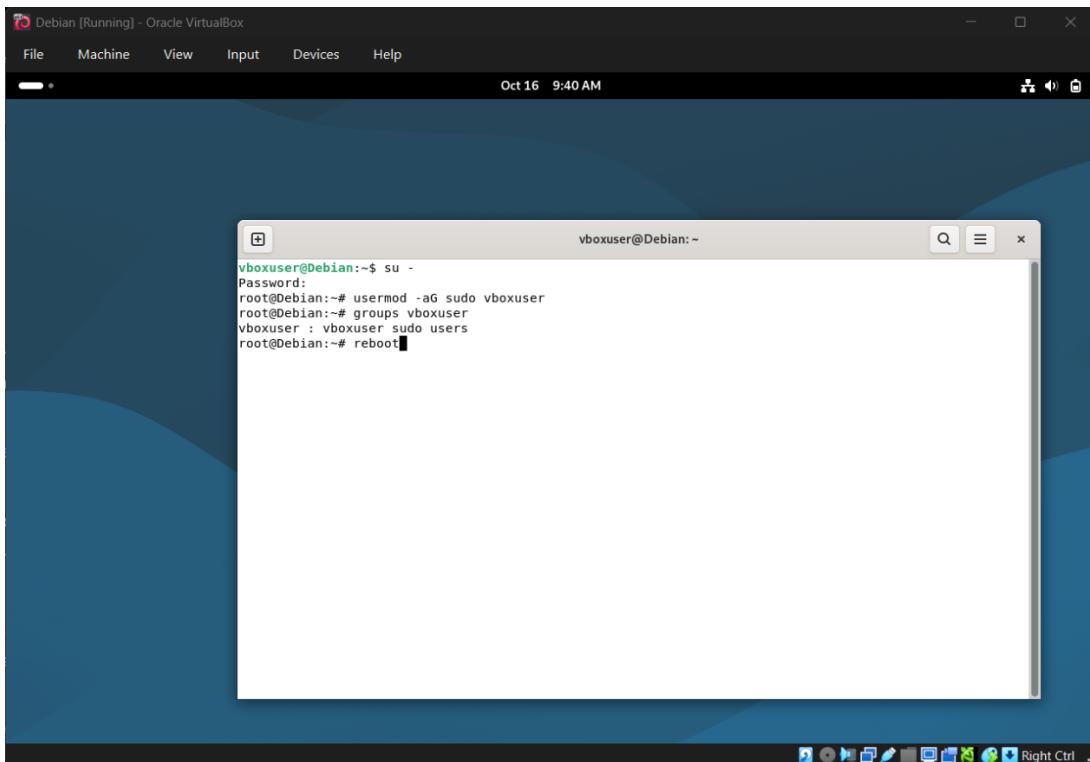
Parte 0 – Preparación del entorno Debian



- Conexión de la computadora virtual a la red de la maquina anfitriona.



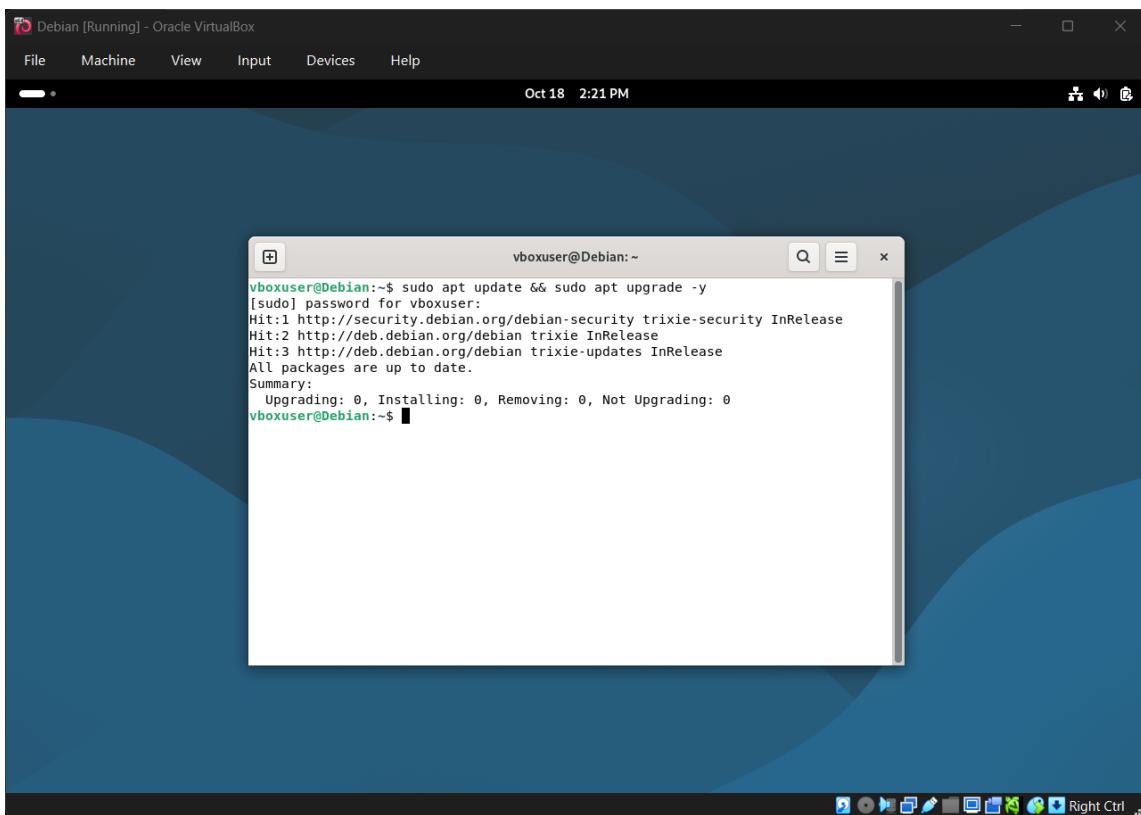
- Configurar el usuario para que sea root.



A screenshot of a Linux desktop environment, likely Debian, running in Oracle VirtualBox. The desktop has a dark blue theme. A terminal window titled "vboxuser@Debian:~" is open, showing the following command sequence:

```
vboxuser@Debian:~$ su -
Password:
root@Debian:~# usermod -aG sudo vboxuser
root@Debian:~# groups vboxuser
vboxuser : vboxuser sudo users
root@Debian:~# reboot
```

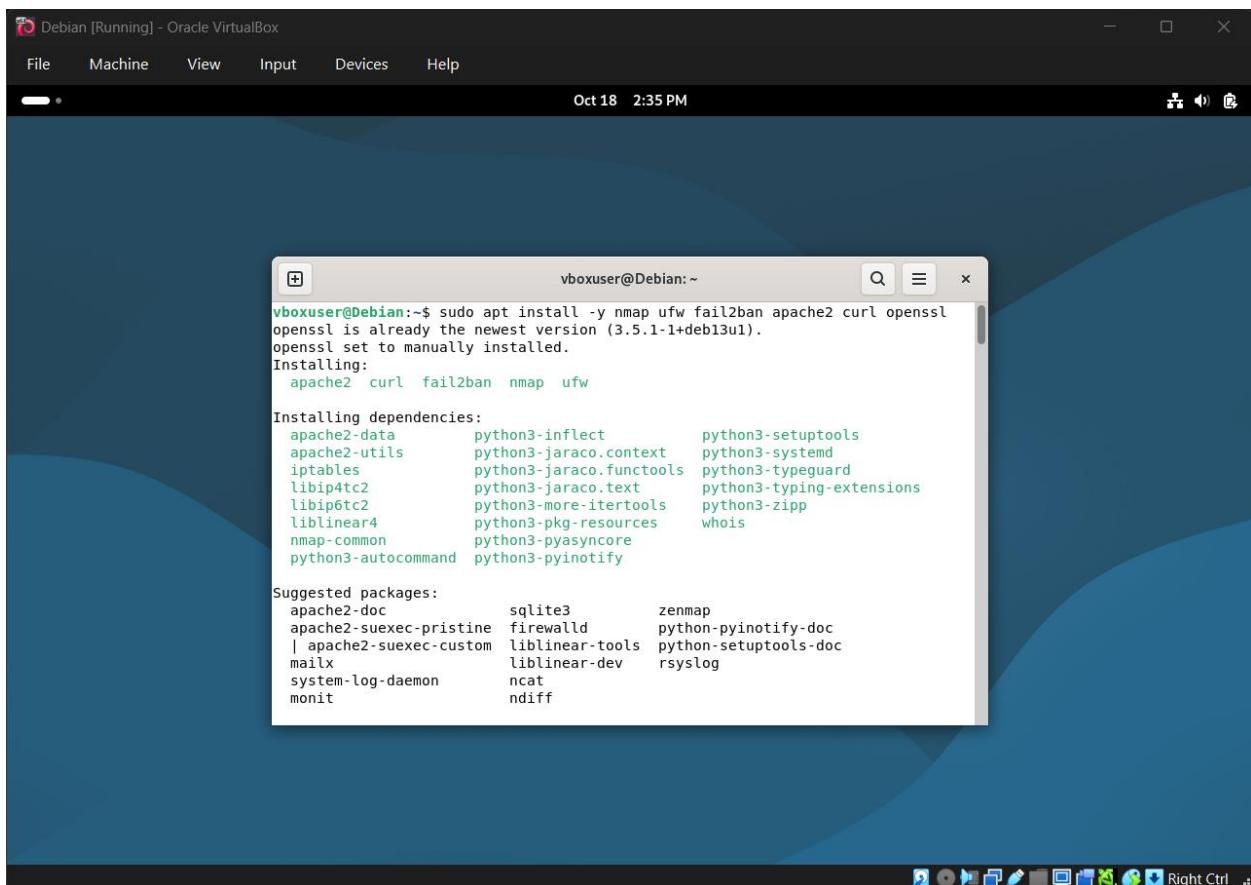
- Actualizar los paquetes.



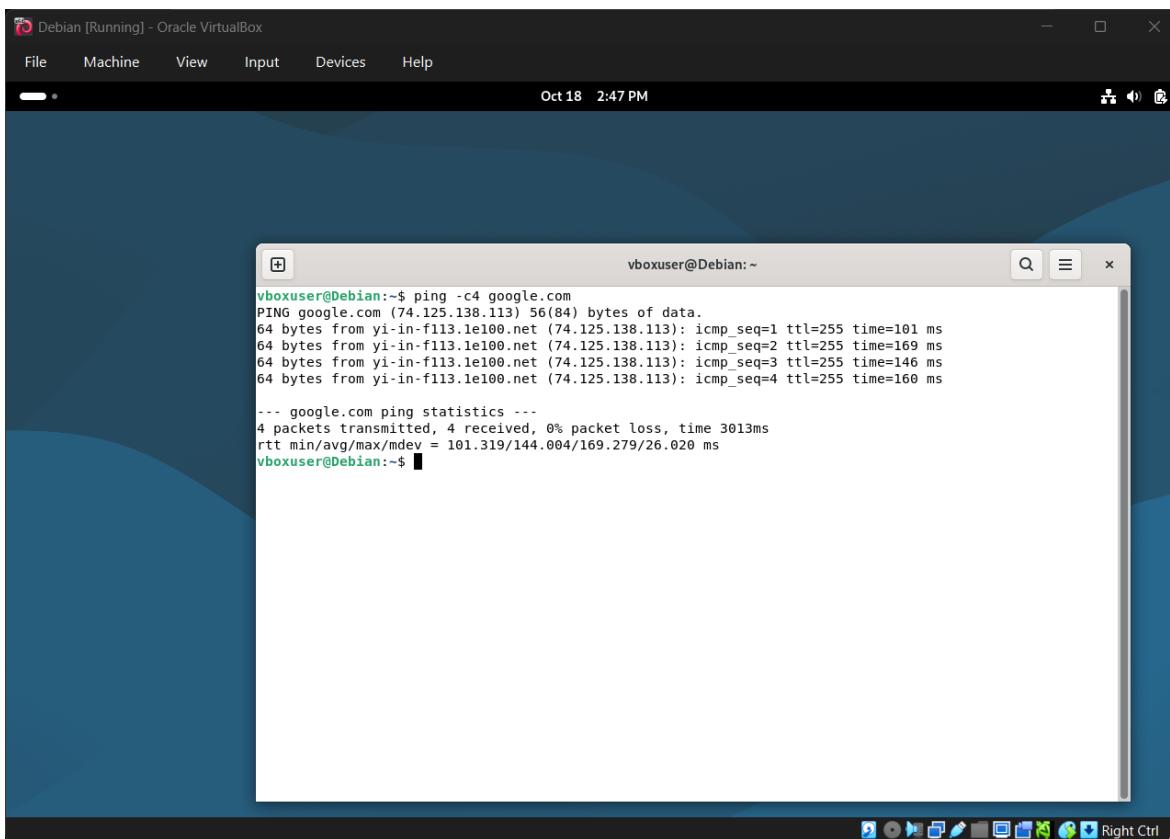
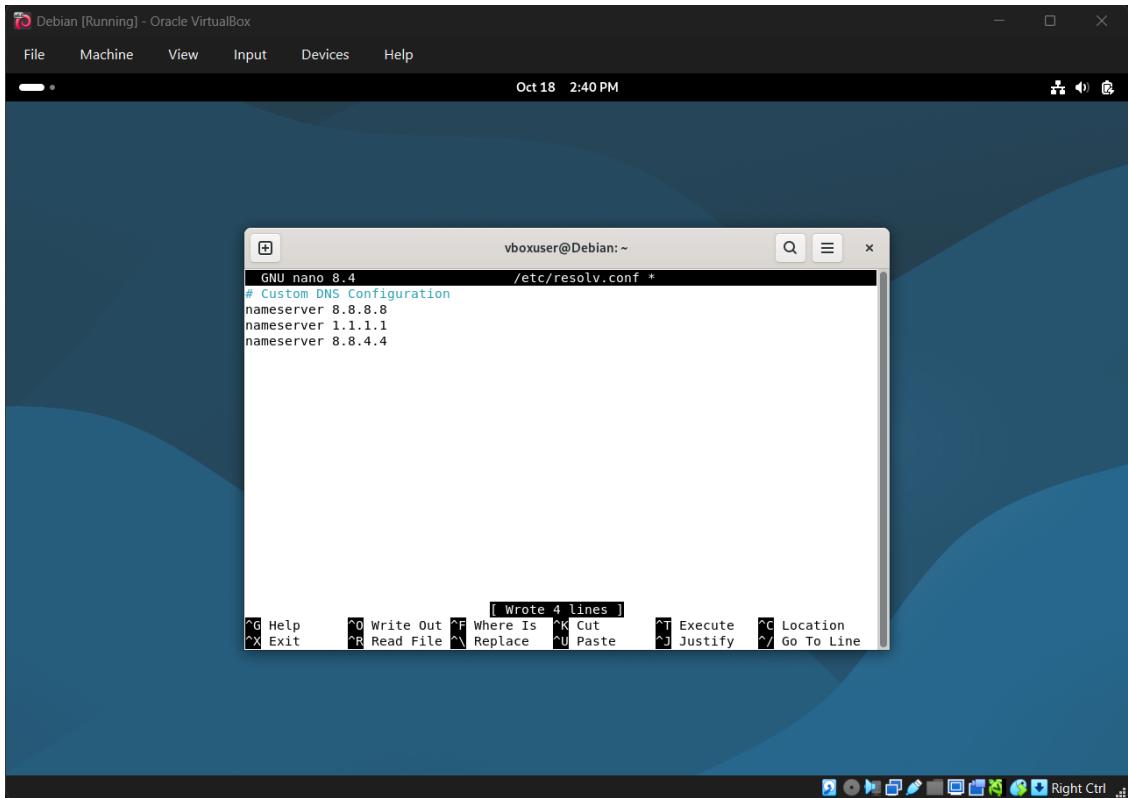
A screenshot of a Linux desktop environment, likely Debian, running in Oracle VirtualBox. The desktop has a dark blue theme. A terminal window titled "vboxuser@Debian:~" is open, showing the following command sequence for package updates:

```
vboxuser@Debian:~$ sudo apt update && sudo apt upgrade -y
[sudo] password for vboxuser:
Hit:1 http://security.debian.org/debian-security trixie-security InRelease
Hit:2 http://deb.debian.org/debian trixie InRelease
Hit:3 http://deb.debian.org/debian trixie-updates InRelease
All packages are up to date.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
vboxuser@Debian:~$
```

- Instalación de herramientas necesarias.

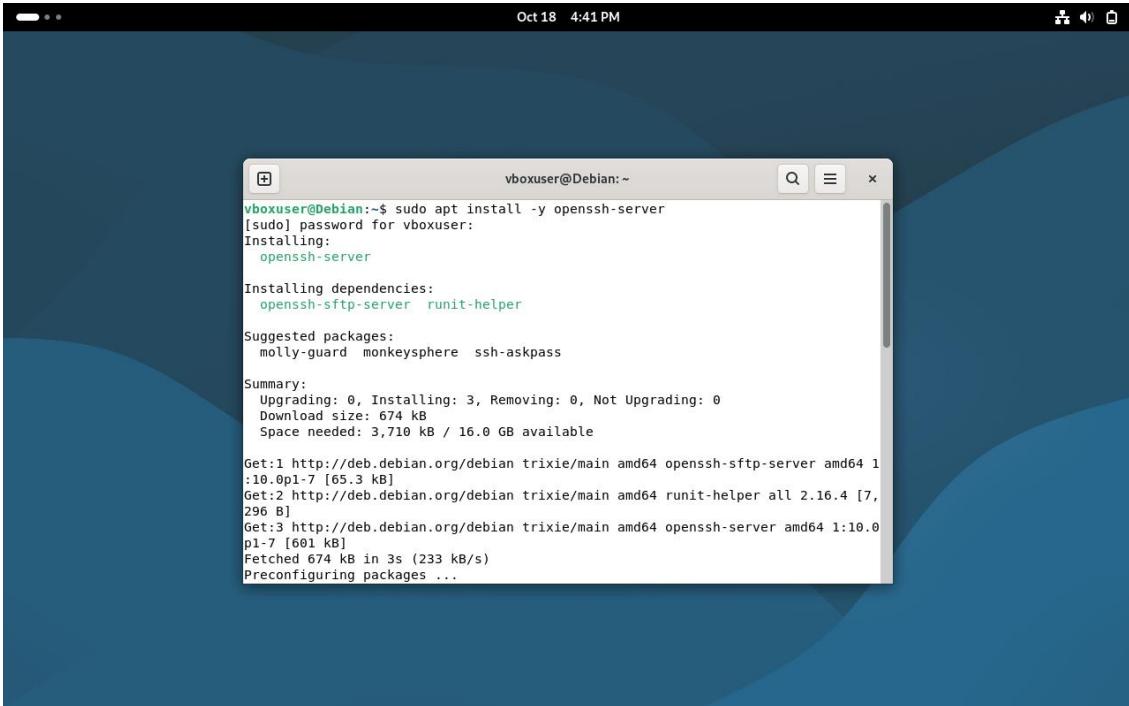


- Configuración de DNS



Paso 1 – Creación de Vulnerabilidades

Vulnerabilidad 1: SSH expuesto con la contraseña del usuario débil.



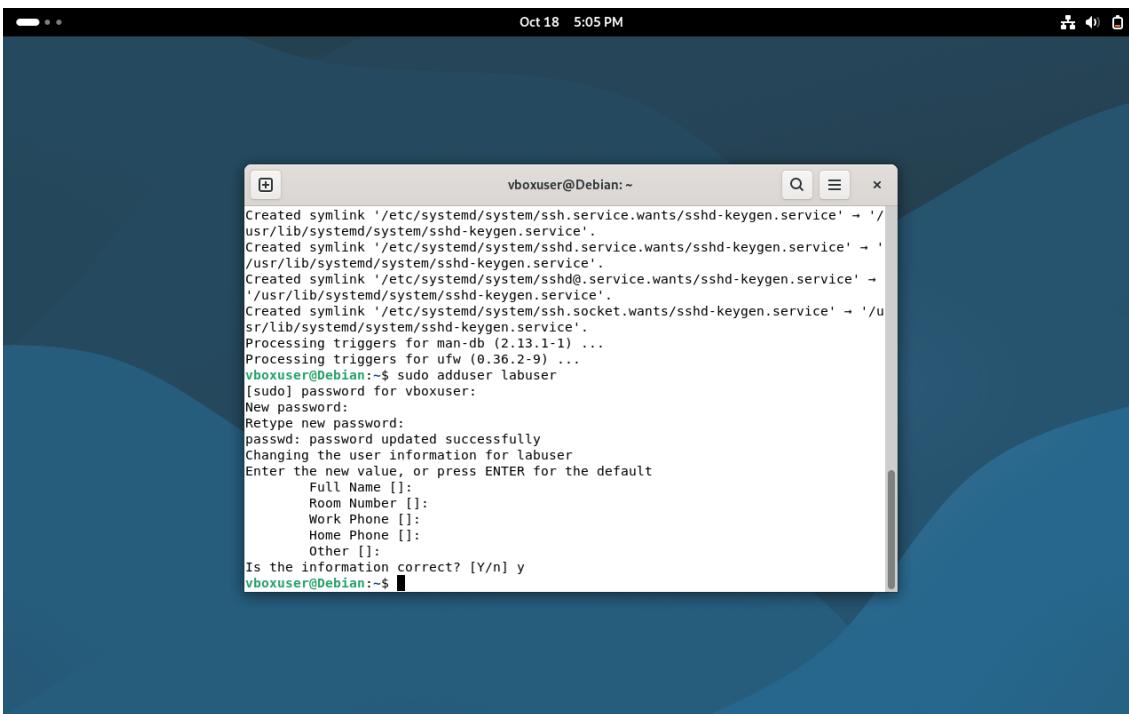
```
vboxuser@Debian:~$ sudo apt install -y openssh-server
[sudo] password for vboxuser:
Installing:
  openssh-server

Installing dependencies:
  openssh-sftp-server  runit-helper

Suggested packages:
  molly-guard  monkeysphere  ssh-askpass

Summary:
  Upgrading: 0, Installing: 3, Removing: 0, Not Upgrading: 0
  Download size: 674 kB
  Space needed: 3,710 kB / 16.0 GB available

Get:1 http://deb.debian.org/debian trixie/main amd64 openssh-sftp-server amd64 1
:10.0p1-7 [65.3 kB]
Get:2 http://deb.debian.org/debian trixie/main amd64 runit-helper all 2.16.4 [7,
296 B]
Get:3 http://deb.debian.org/debian trixie/main amd64 openssh-server amd64 1:10.0
p1-7 [601 kB]
Fetched 674 kB in 3s (233 kB/s)
Preconfiguring packages ...
```



```
vboxuser@Debian:~$ sudo adduser labuser
[sudo] password for vboxuser:
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for labuser
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []
Is the information correct? [Y/n] y
vboxuser@Debian:~$
```

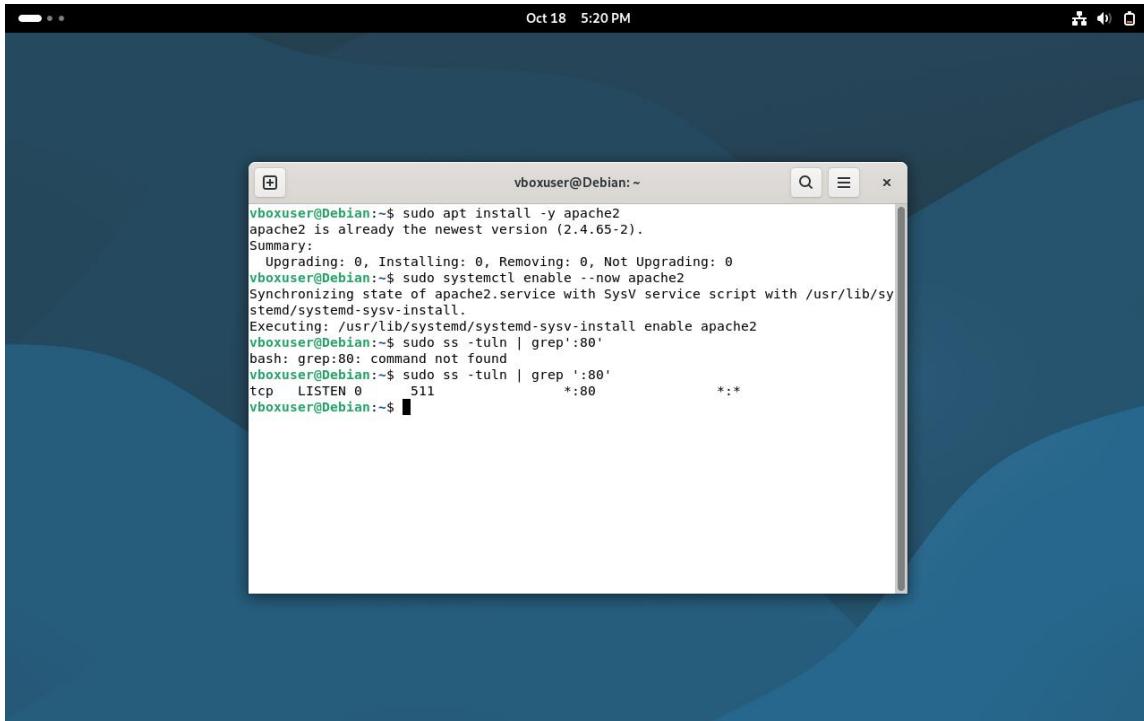
vboxuser@Debian:~

```
sr/lib/systemd/system/sshd-keygen.service'.
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for ufw (0.36.2-9) ...
vboxuser@Debian:~$ sudo adduser labuser
[sudo] password for vboxuser:
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for labuser
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []
Is the information correct? [Y/n] y
vboxuser@Debian:~$ sudo systemctl enable --now ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
vboxuser@Debian:~$ sudo ss -tuln | grep ':22'
tcp    LISTEN  0      128          0.0.0.0:22        0.0.0.0:*
tcp    LISTEN  0      128          [::]:22           [::]:*
```

Vulnerabilidad 2: Apache solo en HTTP (sin HTTPS)

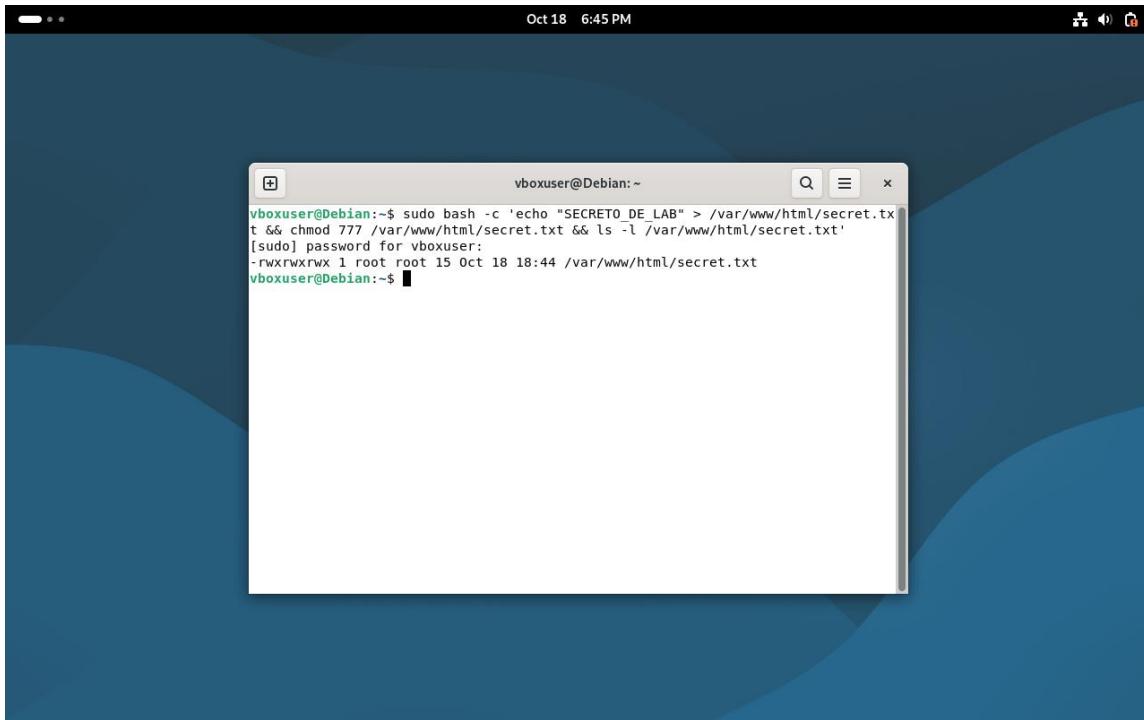
vboxuser@Debian:~

```
vboxuser@Debian:~$ sudo apt install -y apache2
apache2 is already the newest version (2.4.65-2).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
vboxuser@Debian:~$ sudo systemctl enable --now apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
```



vboxuser@Debian:~\$ sudo apt install -y apache2
apache2 is already the newest version (2.4.65-2).
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
vboxuser@Debian:~\$ sudo systemctl enable --now apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
vboxuser@Debian:~\$ sudo ss -tuln | grep ':80'
bash: grep:80: command not found
vboxuser@Debian:~\$ sudo ss -tuln | grep ':80'
tcp LISTEN 0 511 *:80 *:
vboxuser@Debian:~\$

Vulnerabilidad 3: Archivo con permisos inseguros (777)



vboxuser@Debian:~\$ sudo bash -c 'echo "SECRETO_DE_LAB" > /var/www/html/secret.txt && chmod 777 /var/www/html/secret.txt && ls -l /var/www/html/secret.txt'
[sudo] password for vboxuser:
-rwxrwxrwx 1 root root 15 Oct 18 18:44 /var/www/html/secret.txt
vboxuser@Debian:~\$

Parte 2: Detección de las Vulnerabilidades

1) Detectar SSH expuesto

```
# Ver servicio SSH escuchando
```

```
sudo ss -tuln | grep ':22'
```

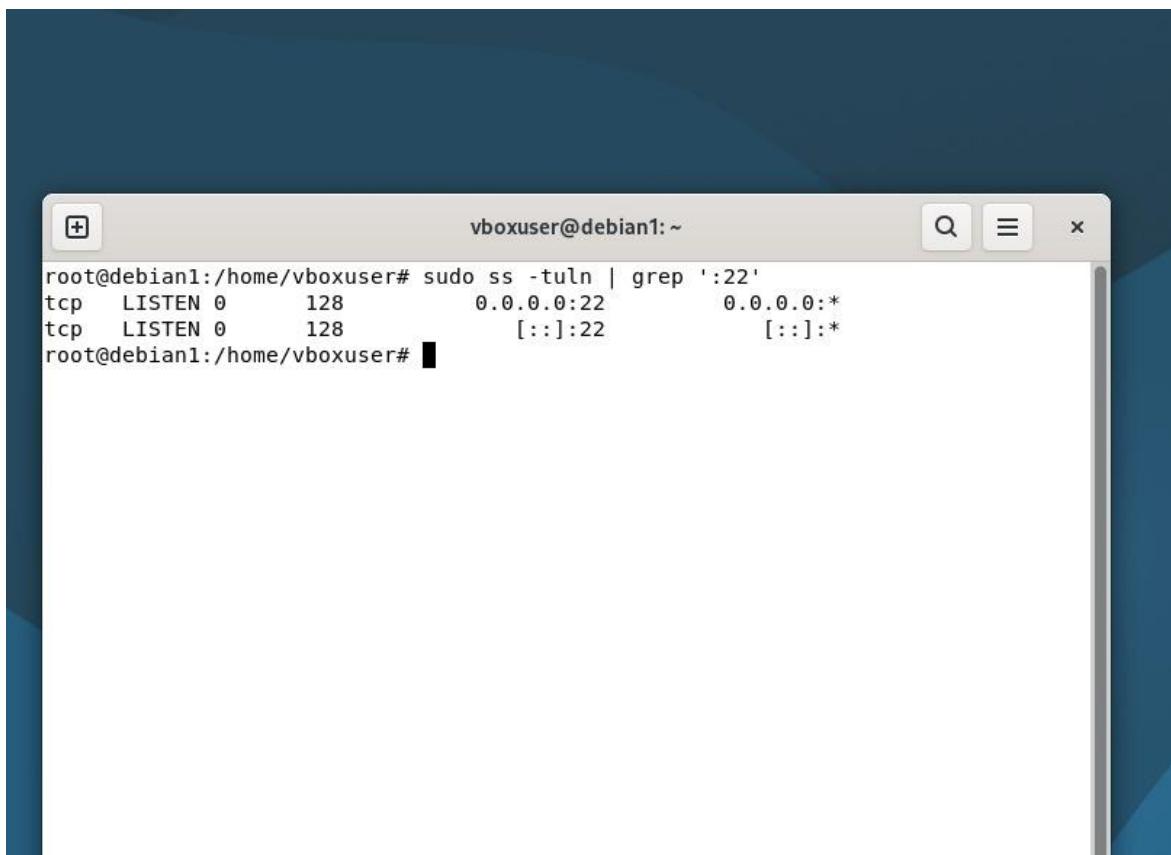
```
# Obtener logs de sshd (usar journalctl)
```

```
sudo bash -c 'journalctl -u ssh -S "today" >
/home/labuser/evidencia_auth.log'
```

```
sudo chown labuser:labuser /home/labuser/evidencia_auth.log
```

```
sudo chmod 640 /home/labuser/evidencia_auth.log
```

- **Qué copiar al informe:** salidas de `ss -tuln | grep ':22'` y el contenido de `~/evidencia_auth.log` (ej.: "Server listening on 0.0.0.0 port 22").



The screenshot shows a terminal window titled "vboxuser@debian1: ~". The command entered was "root@debian1:/home/vboxuser# sudo ss -tuln | grep ':22'". The output shows two TCP listen entries on port 22:

```
root@debian1:/home/vboxuser# sudo ss -tuln | grep ':22'
tcp  LISTEN  0      128          0.0.0.0:22        0.0.0.0:*
tcp  LISTEN  0      128          [::]:22           [::]:*
```

2) Detectar Apache sin HTTPS

Comandos:

```
# Ver puerto 80
```

```
sudo ss -tuln | grep ':80'
```

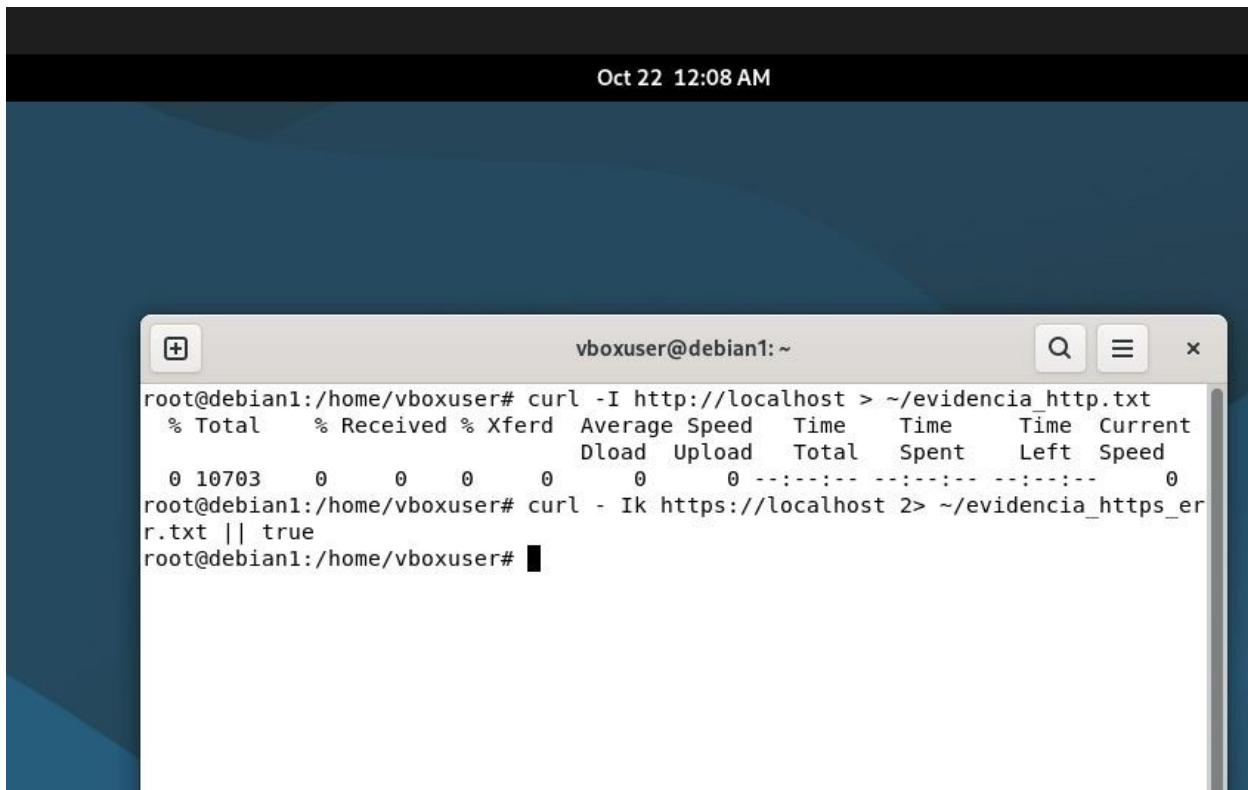
```
# Probar HTTP (usa curl — instálalo si falta)
```

```
curl -I http://localhost > ~/evidencia_http.txt
```

```
# Probar HTTPS (debe FALLAR si no hemos habilitado SSL)
```

```
curl -Ik https://localhost 2> ~/evidencia_https_err.txt || true
```

- **Qué copiar al informe:** Imagen Screenshot de salida de curl y error de conexión a puerto 443.



The screenshot shows a terminal window titled "vboxuser@debian1:~". The window displays two commands run by the user "root" at the prompt "root@debian1:/home/vboxuser#". The first command is "curl -I http://localhost > ~/evidencia_http.txt", which returns a standard HTTP response header. The second command is "curl -Ik https://localhost 2> ~/evidencia_https_err.txt || true", which results in an error message indicating that the connection to port 443 failed. The terminal window has a dark blue background and a light blue header bar. The status bar at the top of the screen shows the date and time: "Oct 22 12:08 AM".

```
root@debian1:/home/vboxuser# curl -I http://localhost > ~/evidencia_http.txt
% Total    % Received % Xferd  Average Speed   Time   Time     Current
          Dload  Upload Total   Spent    Left Speed
 0 10703    0     0      0       0      0 --:--:-- --:--:-- --:--:-- 0
root@debian1:/home/vboxuser# curl -Ik https://localhost 2> ~/evidencia_https_err.txt || true
root@debian1:/home/vboxuser#
```

3) Detectar archivo con permisos inseguros

Comandos:

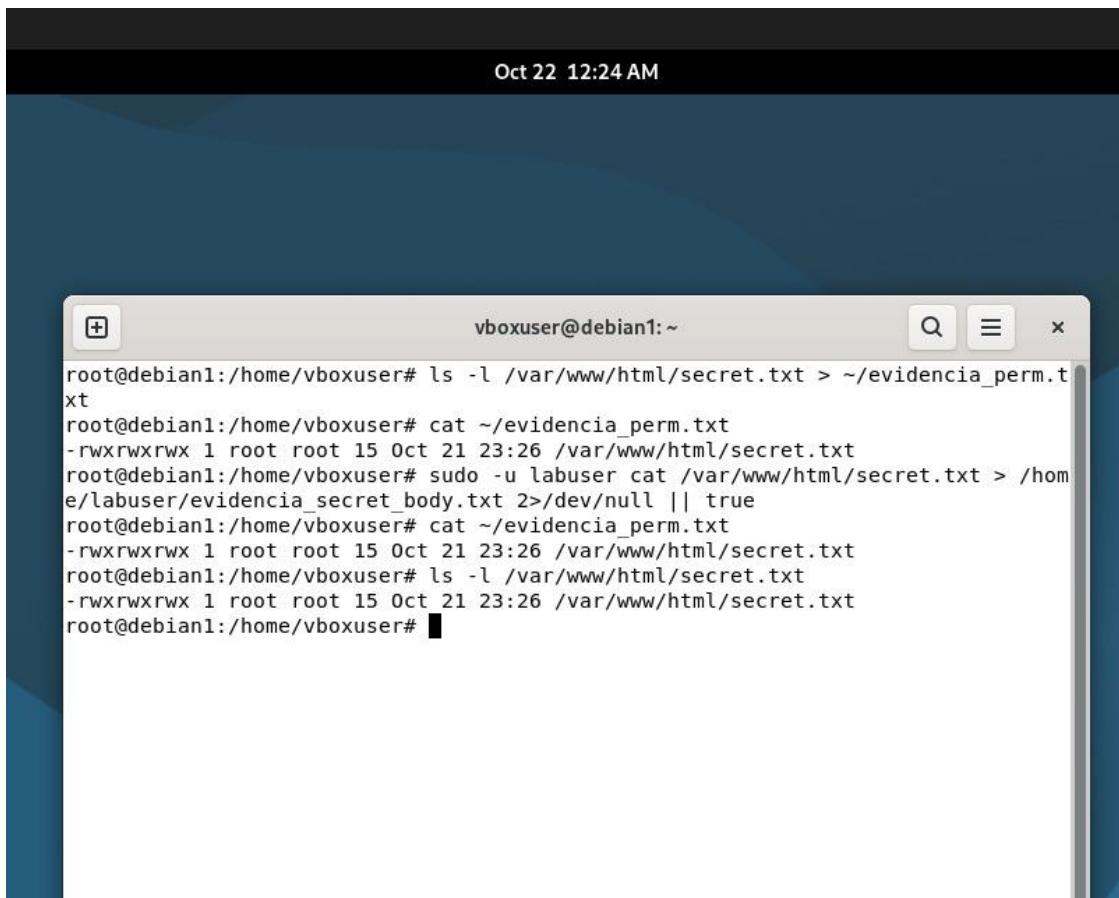
```
# Mostrar permisos
```

```
ls -l /var/www/html/secret.txt > ~/evidencia_perm.txt
```

```
# Intentar leer el archivo como usuario no privilegiado (ej. labuser)
```

```
sudo -u labuser cat /var/www/html/secret.txt >
/home/labuser/evidencia_secret_body.txt 2>/dev/null || true
```

- **Qué copiar al informe:** salida de ls -l mostrando -rwxrwxrwx y contenido del archivo (SECRETO_DE_LAB).

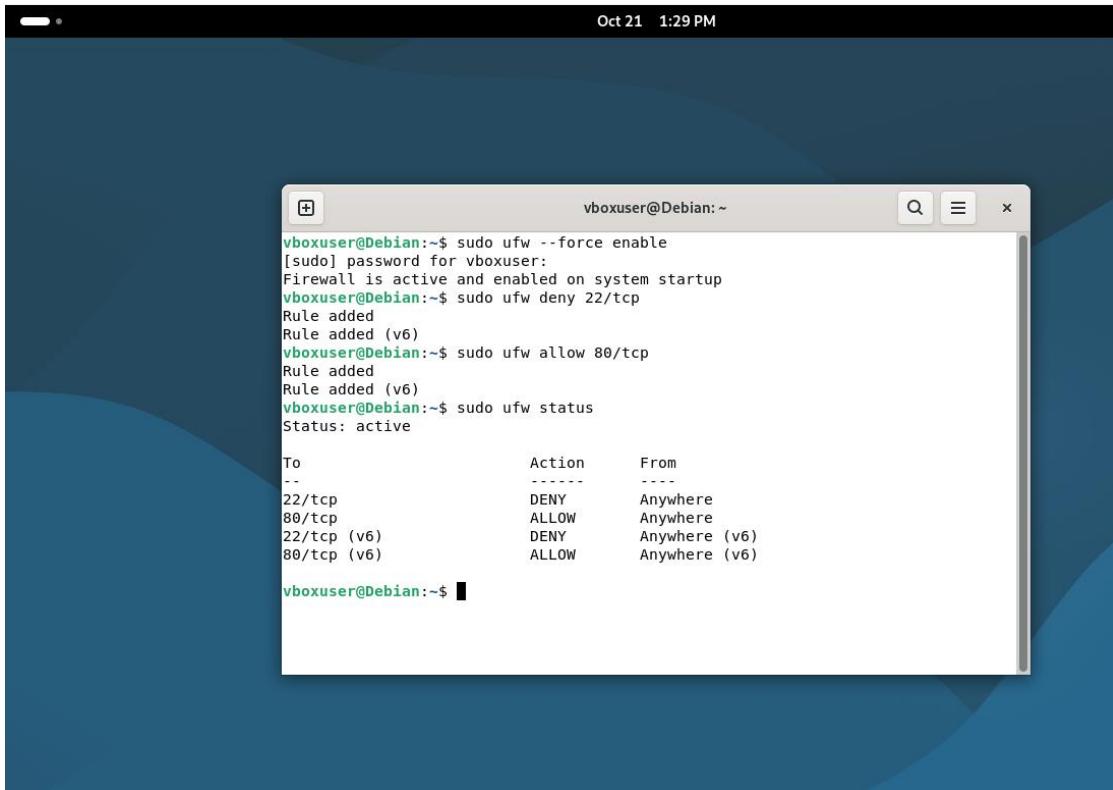


The screenshot shows a terminal window titled "vboxuser@debian1: ~". The window displays the following command history and output:

```
Oct 22 12:24 AM
root@debian1:/home/vboxuser# ls -l /var/www/html/secret.txt > ~/evidencia_perm.txt
root@debian1:/home/vboxuser# cat ~/evidencia_perm.txt
-rwxrwxrwx 1 root root 15 Oct 21 23:26 /var/www/html/secret.txt
root@debian1:/home/vboxuser# sudo -u labuser cat /var/www/html/secret.txt > /home/labuser/evidencia_secret_body.txt 2>/dev/null || true
root@debian1:/home/vboxuser# cat ~/evidencia_perm.txt
-rwxrwxrwx 1 root root 15 Oct 21 23:26 /var/www/html/secret.txt
root@debian1:/home/vboxuser# ls -l /var/www/html/secret.txt
-rwxrwxrwx 1 root root 15 Oct 21 23:26 /var/www/html/secret.txt
root@debian1:/home/vboxuser#
```

Parte 3: Mitigación de las Vulnerabilidades

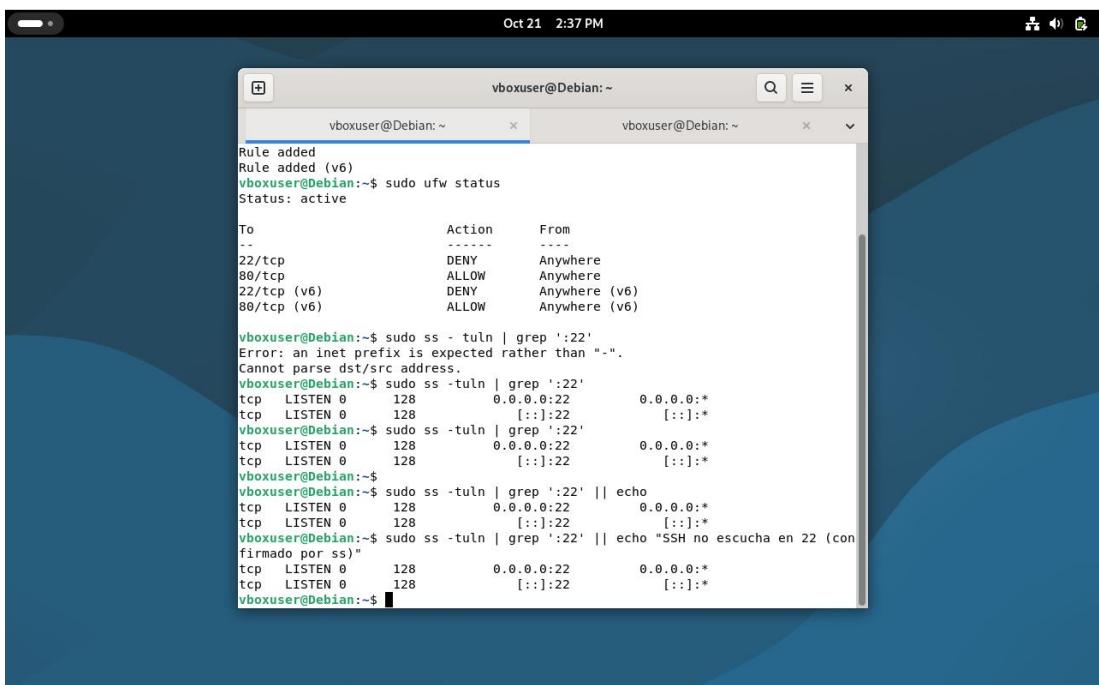
Mitigación 1: SSH: denegar puerto 22 y pedir contraseña fuerte o usar claves



```
vboxuser@Debian:~$ sudo ufw --force enable
[sudo] password for vboxuser:
Firewall is active and enabled on system startup
vboxuser@Debian:~$ sudo ufw deny 22/tcp
Rule added
Rule added (v6)
vboxuser@Debian:~$ sudo ufw allow 80/tcp
Rule added
Rule added (v6)
vboxuser@Debian:~$ sudo ufw status
Status: active

To           Action    From
--           ----     ---
22/tcp        DENY     Anywhere
80/tcp        ALLOW    Anywhere
22/tcp (v6)   DENY     Anywhere (v6)
80/tcp (v6)   ALLOW    Anywhere (v6)

vboxuser@Debian:~$
```

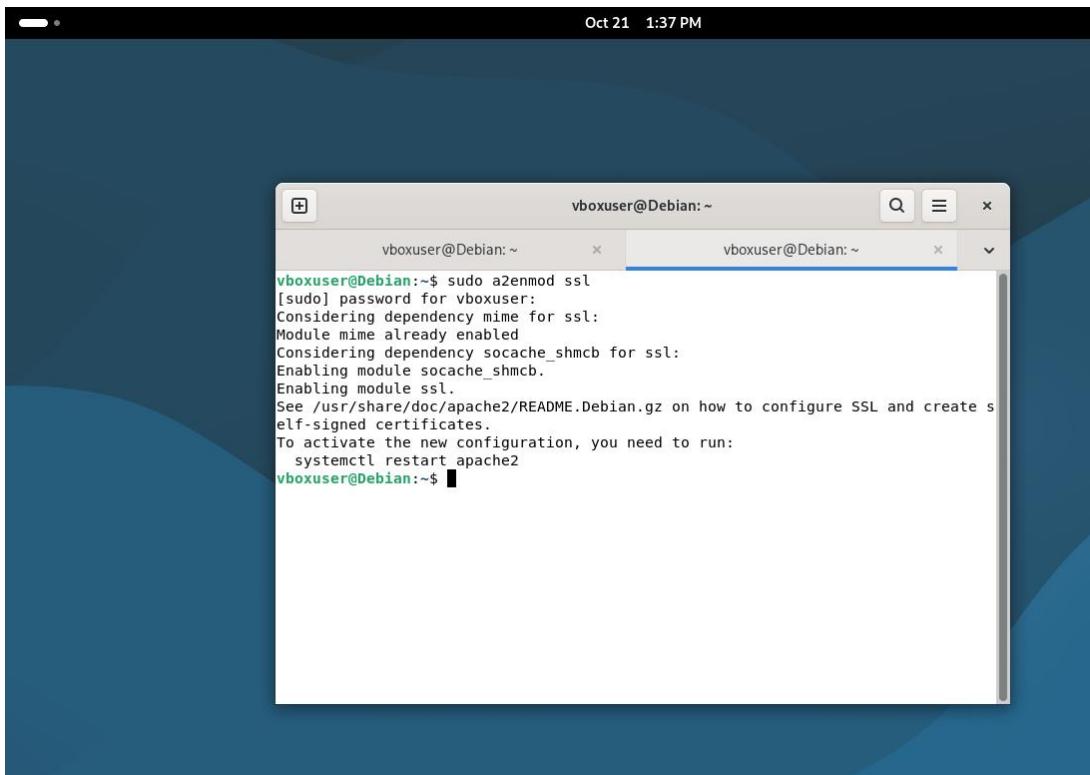


```
vboxuser@Debian:~$ sudo ufw status
Status: active

To           Action    From
--           ----     ---
22/tcp        DENY     Anywhere
80/tcp        ALLOW    Anywhere
22/tcp (v6)   DENY     Anywhere (v6)
80/tcp (v6)   ALLOW    Anywhere (v6)

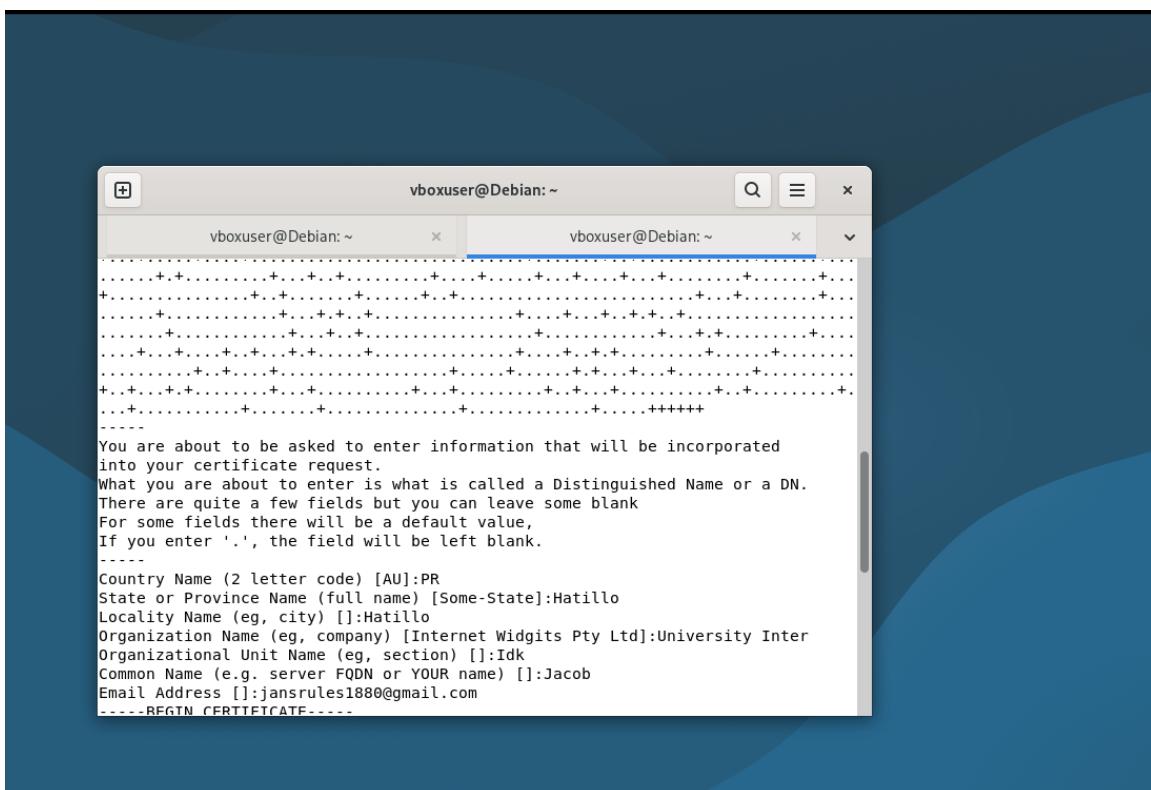
vboxuser@Debian:~$ sudo ss -tuln | grep ':22'
Error: an inet prefix is expected rather than "-".
Cannot parse dst/src address.
vboxuser@Debian:~$ sudo ss -tuln | grep ':22'
tcp  LISTEN  0      128          0.0.0.0:22          0.0.0.0:*
tcp  LISTEN  0      128          [::]:22            [::]:*
vboxuser@Debian:~$ sudo ss -tuln | grep ':22'
tcp  LISTEN  0      128          0.0.0.0:22          0.0.0.0:*
tcp  LISTEN  0      128          [::]:22            [::]:*
vboxuser@Debian:~$ 
vboxuser@Debian:~$ sudo ss -tuln | grep ':22' || echo
tcp  LISTEN  0      128          0.0.0.0:22          0.0.0.0:*
tcp  LISTEN  0      128          [::]:22            [::]:*
vboxuser@Debian:~$ sudo ss -tuln | grep ':22' || echo "SSH no escucha en 22 (com
firmado por ss)"
tcp  LISTEN  0      128          0.0.0.0:22          0.0.0.0:*
tcp  LISTEN  0      128          [::]:22            [::]:*
vboxuser@Debian:~$
```

Mitigación 2 — Apache: habilitar HTTPS (certificado autofirmado)



Oct 21 1:37 PM

```
vboxuser@Debian:~$ sudo a2enmod ssl
[sudo] password for vboxuser:
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
vboxuser@Debian:~$
```

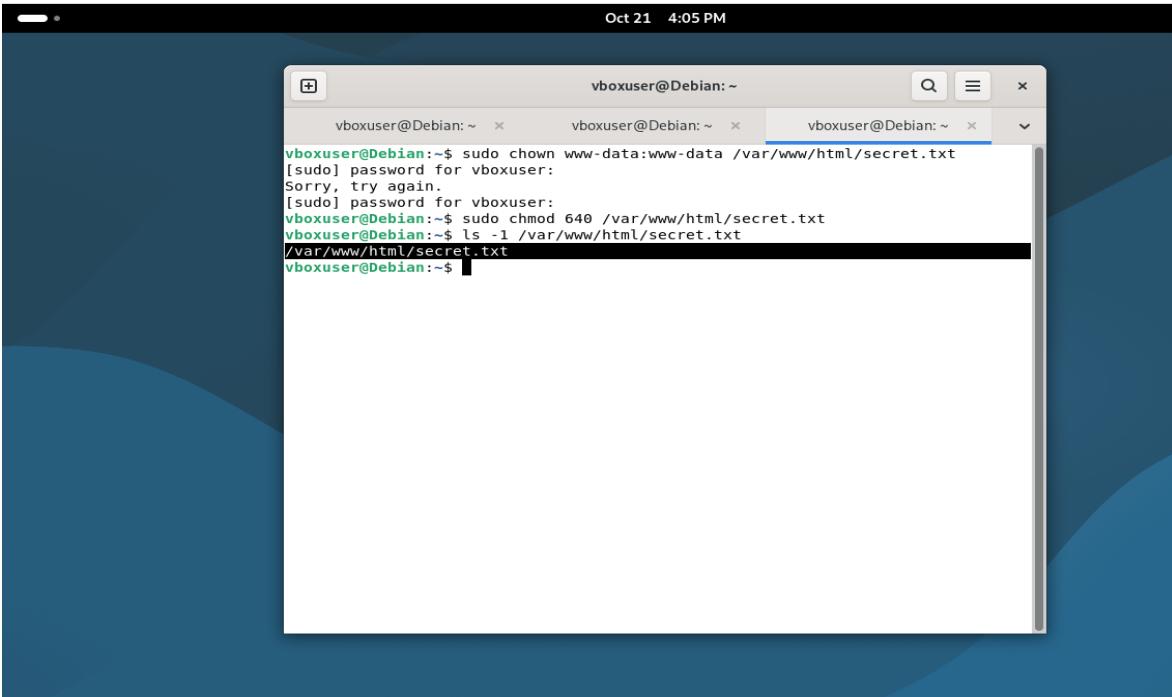


```
vboxuser@Debian:~$ ./openssl req -new -keyout jansrules1880.key -out jansrules1880.csr
-----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Country Name (2 letter code) [AU]:PR  
State or Province Name (full name) [Some-State]:Hatillo  
Locality Name (eg, city) []:Hatillo  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:University Inter  
Organizational Unit Name (eg, section) []:Idk  
Common Name (e.g. server FQDN or YOUR name) []:Jacob  
Email Address []:jansrules1880@gmail.com  
-----REGTN CERTIFICATE-----
```

```
vboxuser@Debian: ~          vboxuser@Debian: ~
vboxuser@Debian: ~          vboxuser@Debian: ~
Organizational Unit Name (eg, section) []:Idk
Common Name (e.g. server FQDN or YOUR name) []:Jacob
Email Address []:jansrules1880@gmail.com
-----BEGIN CERTIFICATE-----
MIIEBzCCAUu+gAwIBAgIUVy5fv40aEnNEMo3xgo8Nb17420wDQYJKoZIhvcNAQEL
BQAwgZIxCzAJBgNVBAYTAlBSMRAwDgYDVQQIDAjYXRpBgvxMRAwDgYDVQQHDAdI
YXRpbgxvMRkwFwYDVQKDBBvbm1ZXJzaX5IeludGVyM0qwCgYDVQQLDANJZGsx
DjAMBgNVBAMBBUpyY291MSYwJAYJKoZIhvcNAQkBFhdqYw5zcnsVZMxD0gwQGdt
YWlsLmNvbTAefw0yNTEmjExNzQ0MDBaFw0yNjEwmjExNzQ0MDBaMIGSMQswCQYD
VQQGEwJOUjEQMA4GA1UECAwHSGF0AwxsbzEQMA4GA1UEBwwHSGF0AwxsbzEZMBcG
A1UECgwQWV5pdmVyc2l0eSBjbnRlcjEMMA0GA1UECw0DSWRrM04wDAYDVQODDAVK
YWNvYjEmMCQGCSqGSiB3DQEJARYXamFuc3J1bgVzMtg4MEBnbWFpbC5jb20wggEi
MA0GCSqGSiB3DQEBAQUAA1BDwAwggEKAoIBA0Cnb411cAYmGrvSIE1+rnhWcgAl
7VZk8f+EuabcdfruWN0yH3DDDXMKk0B1v95JUGPU4sZTkqaFqd75esJFFdkbqt+
74j81F6lcgHGWekeP5MnejBqovWbk6WhlgMBMPUgB0vSUrbvpT8fk7uk2XsFY1
QDrXWRsYQl3fw05GHiewM+MFYX1VV1KjJzM30E6GHISc5TiS8Y6VKQVhdyjSBt
0qmb5kl/uf0Eznaxrz2xz5ArTPUeW/0CVLEmc+9lmSba/UrF0YFQu1rdeSGRh
KuXivWVKiaae8Mka0GivoRVON9xsgETva$buUDVmP89k4huN0rzjviw3CNHAgMB
AAGjUzBRMB0GA1UDgQWBBSmZwU0tNwPwbRdHERnLV3BDY8QCDAPBgNVHRMBAf8EBTDAQH/MA0GCSqGSiB3
DQEBCwUA41BA0AQZfx1Yg/frmwn4pzZeuiqv0WE-/bgK+uEE2as1003ahPH/bh
u0rCaYw0XVAj4u05fvmKFSquNgATBWakj1zehc0aSDN9shNuOCzmE33sUFH3uD
WD4ZoyeleSC3xjzUK0vnBfkMtCX0ctajI4g1800/u1v1EzmzbSkulW3TdJ1+hmh
+BANPwqB0FZ03wBALfc131lWDGLsSxeql61E7DR0cfy6Ei3mLveef6+6VdtDvsj
qHATBvvnXZgAmkvHr+sP2q1NaqkhF9BP8RHxeAe5w0ay7NKbg+wFMwsTadeUbWNf
9sU095TV0z0tk1lCKDGe3DCXpgqp6KxhD2s
-----END CERTIFICATE-----
vboxuser@Debian:~$ -keyout /etc/ssl/private/apache-selfsigned.key
bash: -keyout: command not found
vboxuser@Debian:~$
```

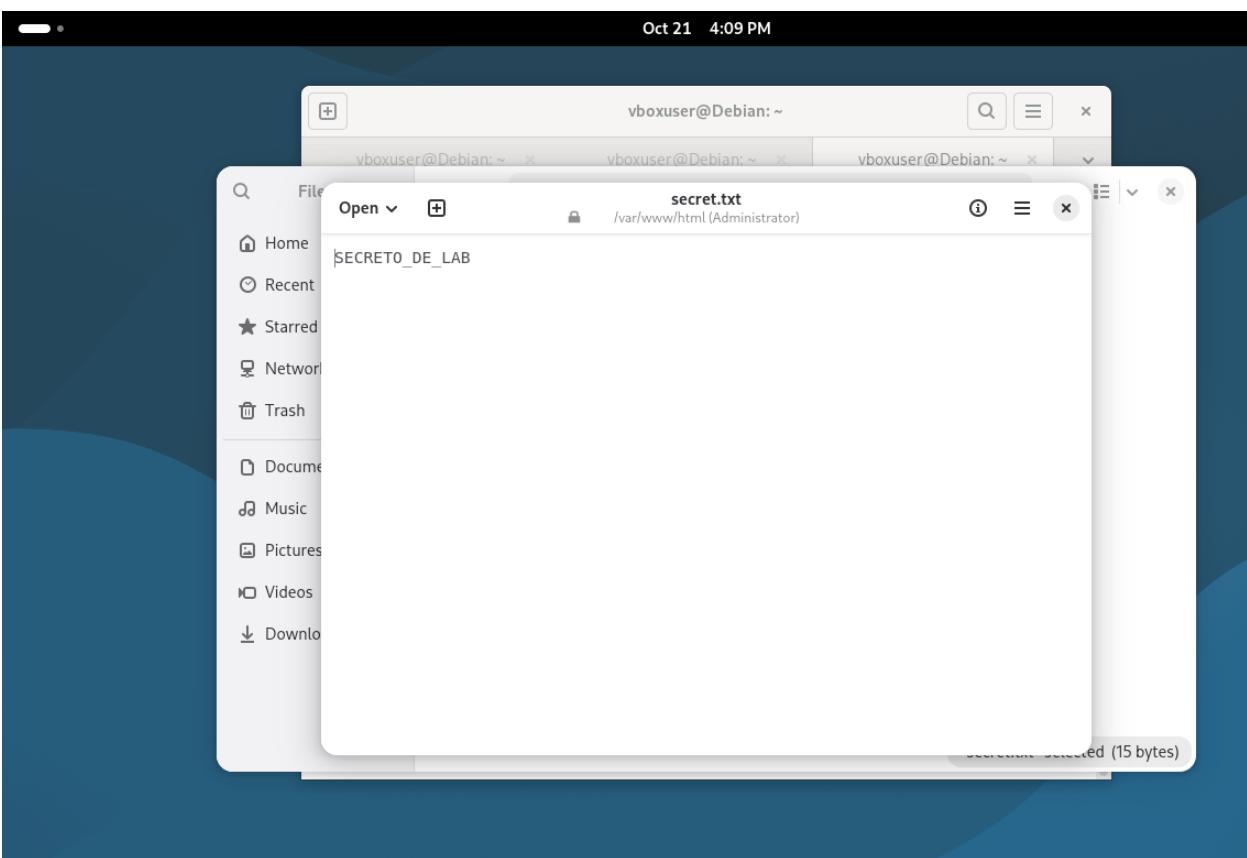
```
Oct 21 2:08 PM          vboxuser@Debian: ~          vboxuser@Debian: ~
vboxuser@Debian: ~          vboxuser@Debian: ~
gBSmZwU0tNwPwbRdHERnLV3BDY8QCDAPBgNVHRMBAf8EBTDAQH/MA0GCSqGSiB3
DQEBCwUA41BA0AQZfx1Yg/frmwn4pzZeuiqv0WE-/bgK+uEE2as1003ahPH/bh
u0rCaYw0XVAj4u05fvmKFSquNgATBWakj1zehc0aSDN9shNuOCzmE33sUFH3uD
WD4ZoyeleSC3xjzUK0vnBfkMtCX0ctajI4g1800/u1v1EzmzbSkulW3TdJ1+hmh
+BANPwqB0FZ03wBALfc131lWDGLsSxeql61E7DR0cfy6Ei3mLveef6+6VdtDvsj
qHATBvvnXZgAmkvHr+sP2q1NaqkhF9BP8RHxeAe5w0ay7NKbg+wFMwsTadeUbWNf
9sU095TV0z0tk1lCKDGe3DCXpgqp6KxhD2s
-----END CERTIFICATE-----
vboxuser@Debian:~$ -keyout /etc/ssl/private/apache-selfsigned.key
bash: -keyout: command not found
vboxuser@Debian:~$ sudo a2ensite default-ssl
[sudo] password for vboxuser:
Enabling site default-ssl.
To activate the new configuration, you need to run:
    systemctl reload apache2
vboxuser@Debian:~$ sudo systemctl reload apache2
vboxuser@Debian:~$ sudo ss -tuln | grep ':443'
tcp        LISTEN      0      511          *:443               *:*
vboxuser@Debian:~$ curl -I https://localhost
HTTP/1.1 200 OK
Date: Tue, 21 Oct 2025 18:08:00 GMT
Server: Apache/2.4.65 (Debian)
Last-Modified: Tue, 21 Oct 2025 14:11:04 GMT
ETag: "29cf-641abc5421a90"
Accept-Ranges: bytes
Content-Length: 10703
Vary: Accept-Encoding
Content-Type: text/html
vboxuser@Debian:~$
```

Mitigacion 3: Archivo con permisos inseguros: aplicar mínimo privilegio (640) y propiedad www-data



Oct 21 4:05 PM

```
vboxuser@Debian:~$ sudo chown www-data:www-data /var/www/html/secret.txt
[sudo] password for vboxuser:
Sorry, try again.
[sudo] password for vboxuser:
vboxuser@Debian:~$ sudo chmod 640 /var/www/html/secret.txt
vboxuser@Debian:~$ ls -l /var/www/html/secret.txt
-/var/www/html/secret.txt
vboxuser@Debian:~$
```



Parte 4: Tabla de datos encontrados y análisis

Vulnerabilidad	Amenaza	Riesgo (Alto/Medio/Bajo)	Control Usado	Modelo de Ataque (los 4 modelos)
SSH expuesto con la contraseña débil del usuario.	Acceso inicial con usuario débil puede permitir al atacante obtener permisos de root o administrador.	Alto	denegar puerto 22 y pedir contraseña fuerte o usar claves	Intercepción
Apache solo en HTTP (sin HTTPS)	Sin HTTPS, es más fácil que un atacante suplante el sitio web legítimo para engañar a los usuarios.	Alto	Apache: habilitar HTTPS (certificado auto firmado)	Fabricación
Archivo con permisos inseguros (777)	Los usuarios pueden acceder a todos los archivos ya que los permisos no los están restringiendo correctamente.	Medio	Aplicar mínimo privilegio (640) y propiedad www-data	Modificación

Conclusión: ¿Cuál fue la amenaza más probable en su sistema y qué control resultó más efectivo?

- Consideramos que la amenaza más probable que ocurra en nuestro sistema es la exposición de SSH con el uso de contraseña débil. Debido a que la contraseña es fácil, un atacante pueda adivinar la contraseña y entrar al sistema del usuario. Esta situación abre la puerta a una gran cantidad de diferentes explotaciones de vulnerabilidades una vez que el atacante ingrese al sistema provocando ataques de intercepción, modificación, ect. Consideramos que, dentro de estos controles, los más efectivos fueron intercepción y modificación debido a que vimos la importancia de buscar e identificar problemas dentro del sistema y hacer los arreglos correspondientes para resolver el problema. Sin duda esta ha sido una actividad en la que hemos logrado comprender de manera extensiva el uso tanto de herramientas para máquinas virtuales, como la identificación de amenazas y vulnerabilidades y como mitigarlas.

Nombre del integrante	¿Qué realizo?	% del trabajo
Benyahir Y. Martínez	Parte 0, Parte 4, Conclusión	25%
Emanuel V. Rodríguez	Parte 1, Parte 4, Conclusión	25%
John A. Valentín	Parte 2, Parte 4, Conclusión	25%
Jacob J. Desuza	Parte 3, Parte 4, Conclusión	25%