Curso: COMP 2700 – Ciberseguridad

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

Sección: 92249

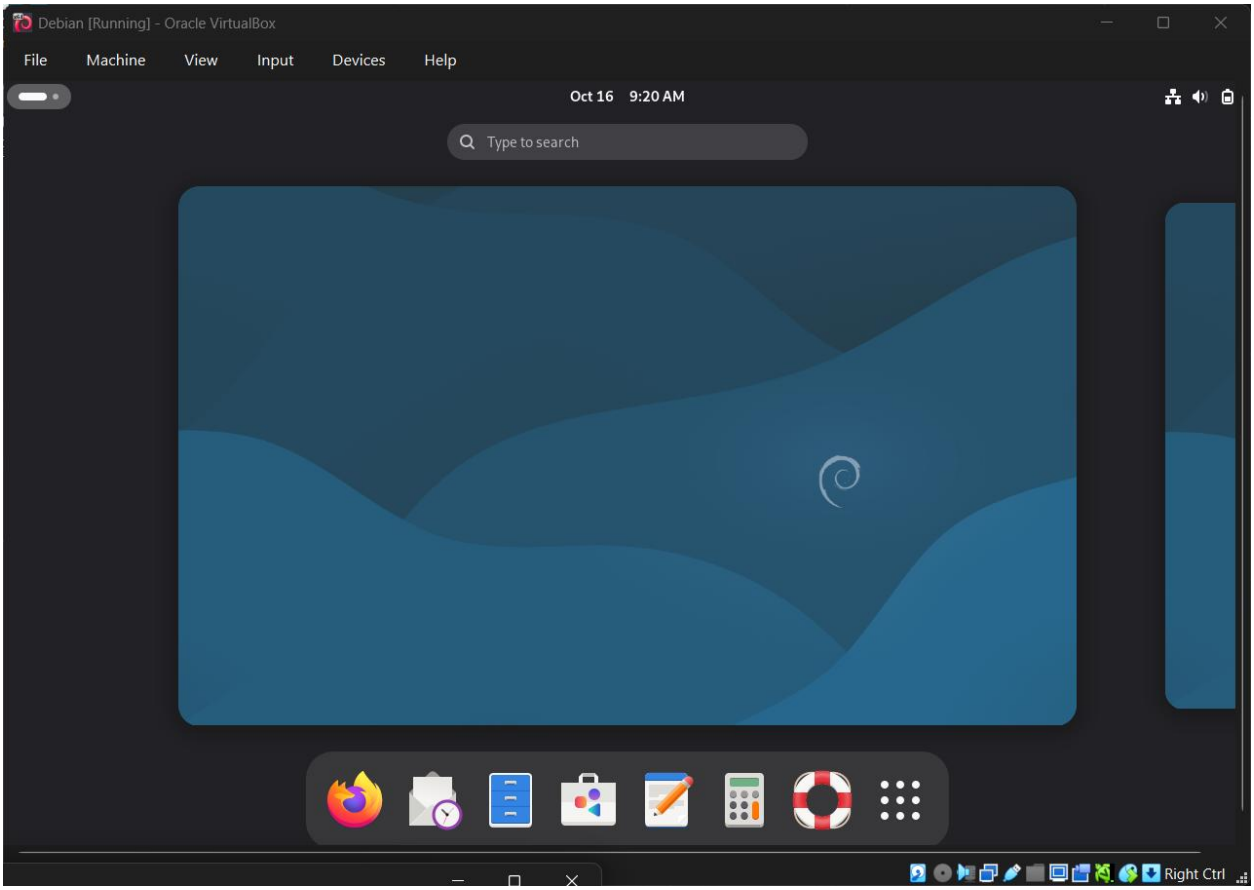
Líder del grupo: Benyahir Y. Martínez Hermina

Integrantes:

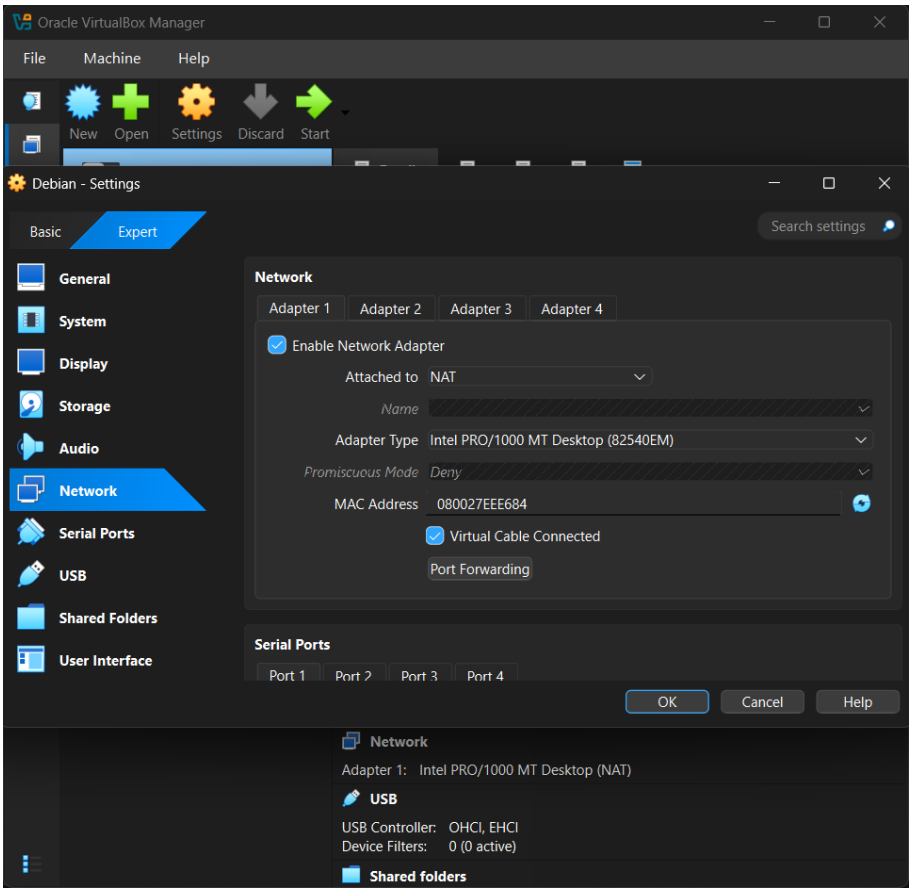
- Benyahir Y. Martínez
- Jacob J. Desuza
- Emanuel V. Rodríguez
- John A. Valentín

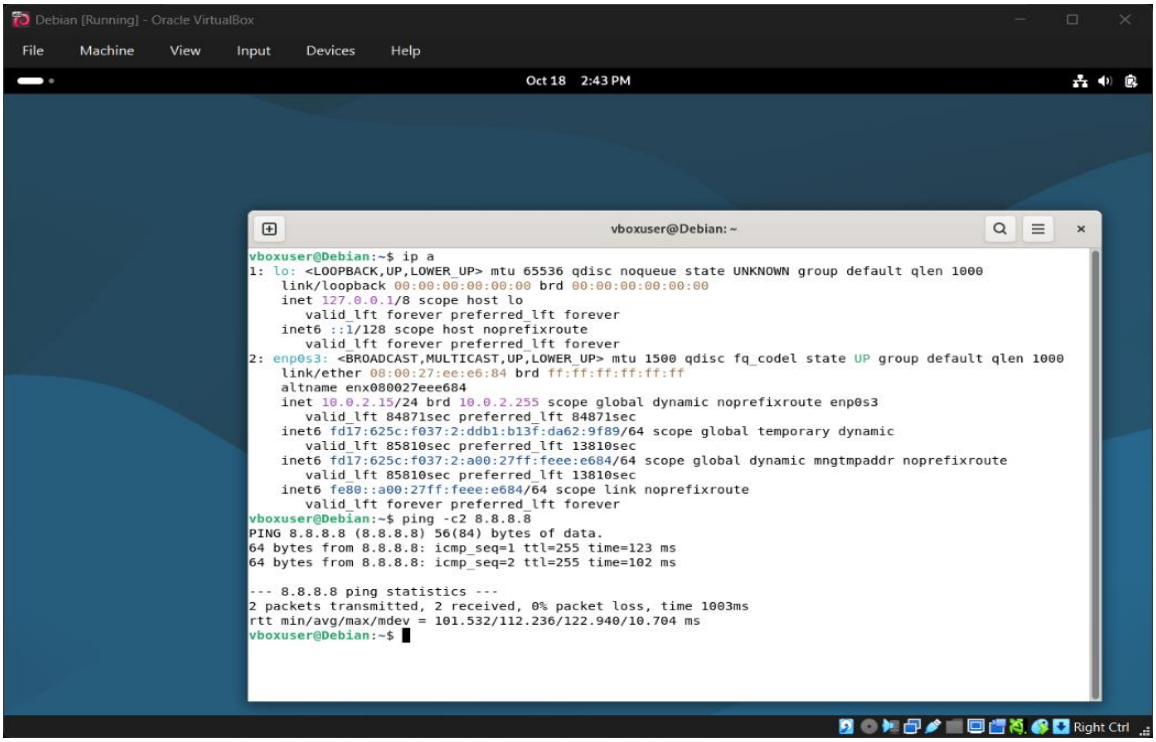
Fecha: 23 de oct. de 25

Parte 0 – Preparación del entorno Debian

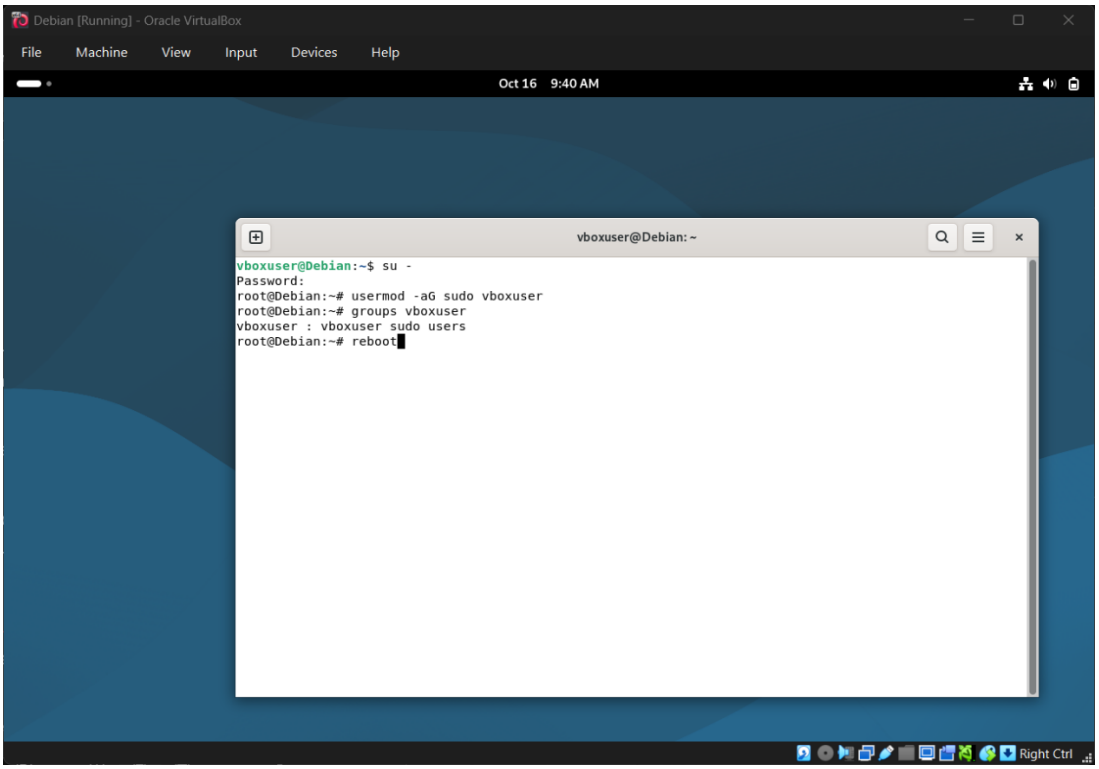


- **Conexión de la computadora virtual a la red de la maquina anfitriona.**

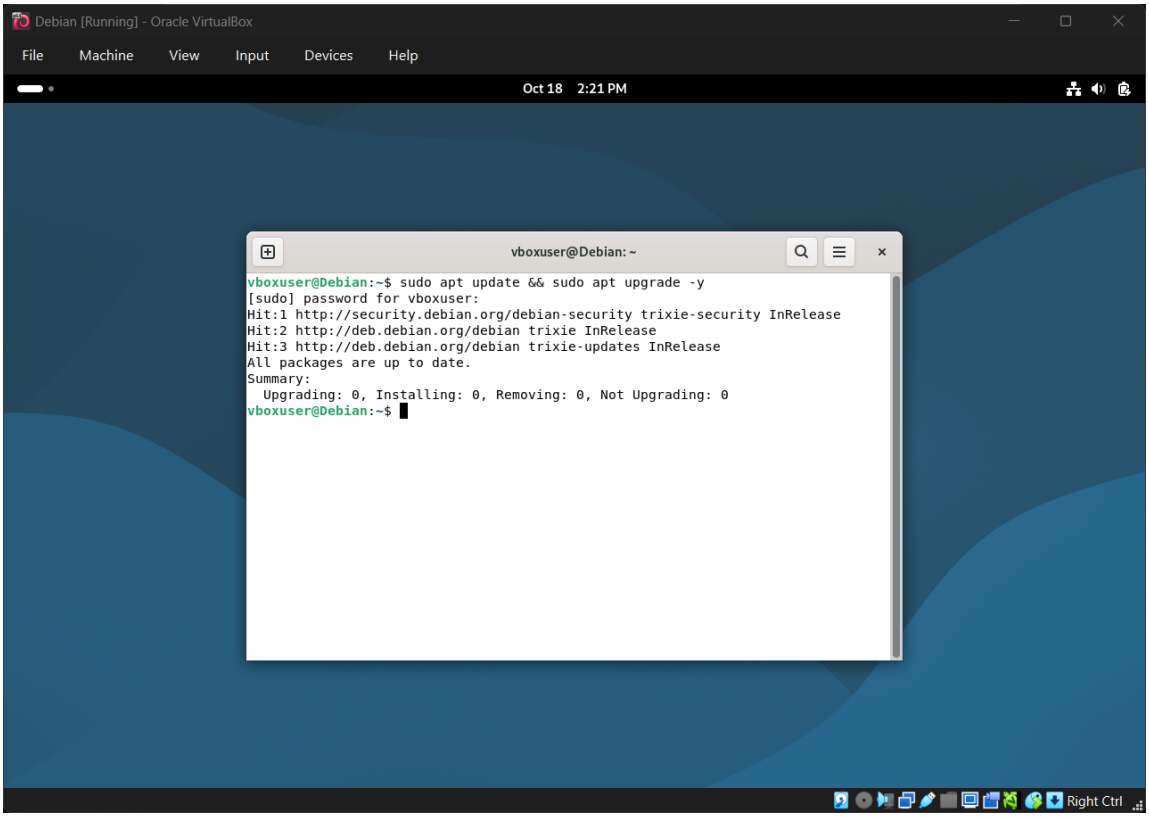




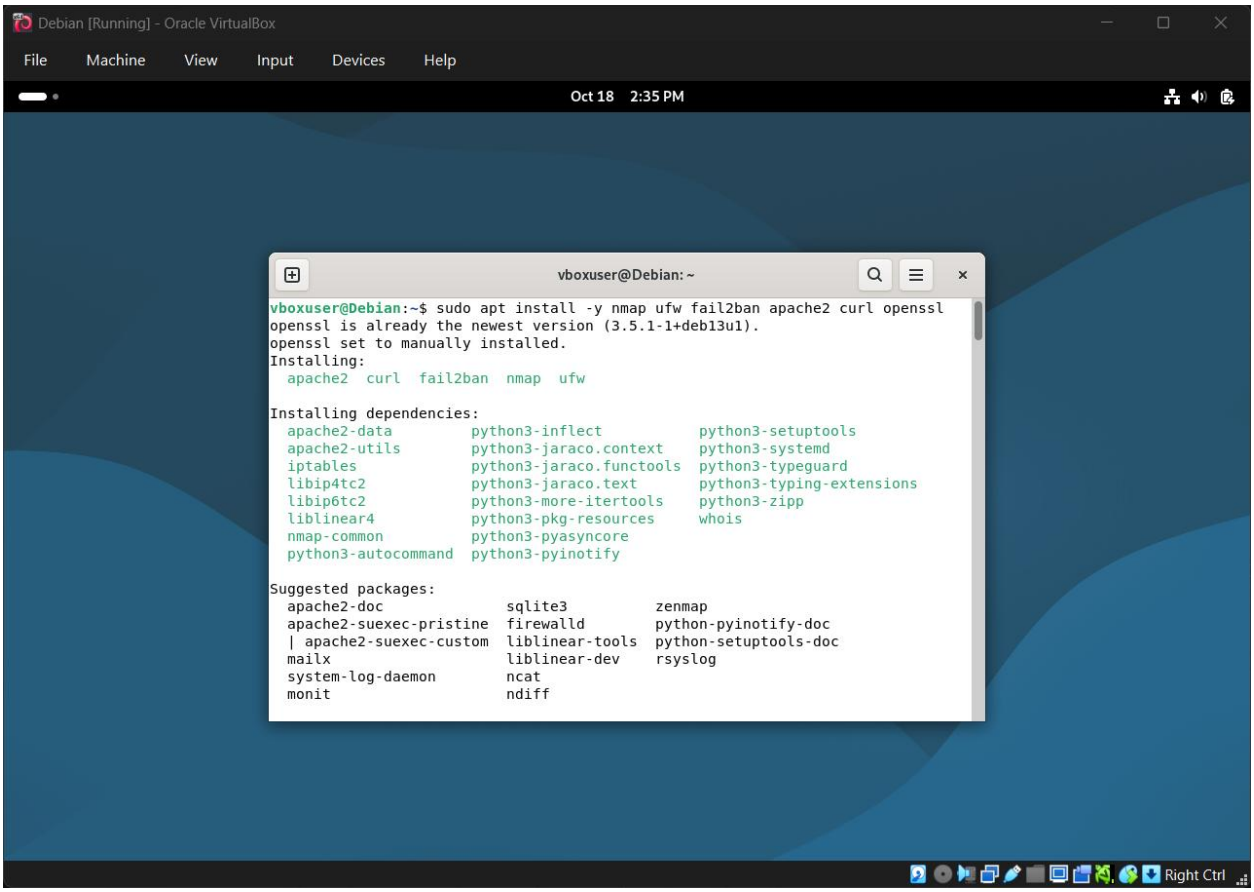
- **Configurar el usuario para que sea root.**



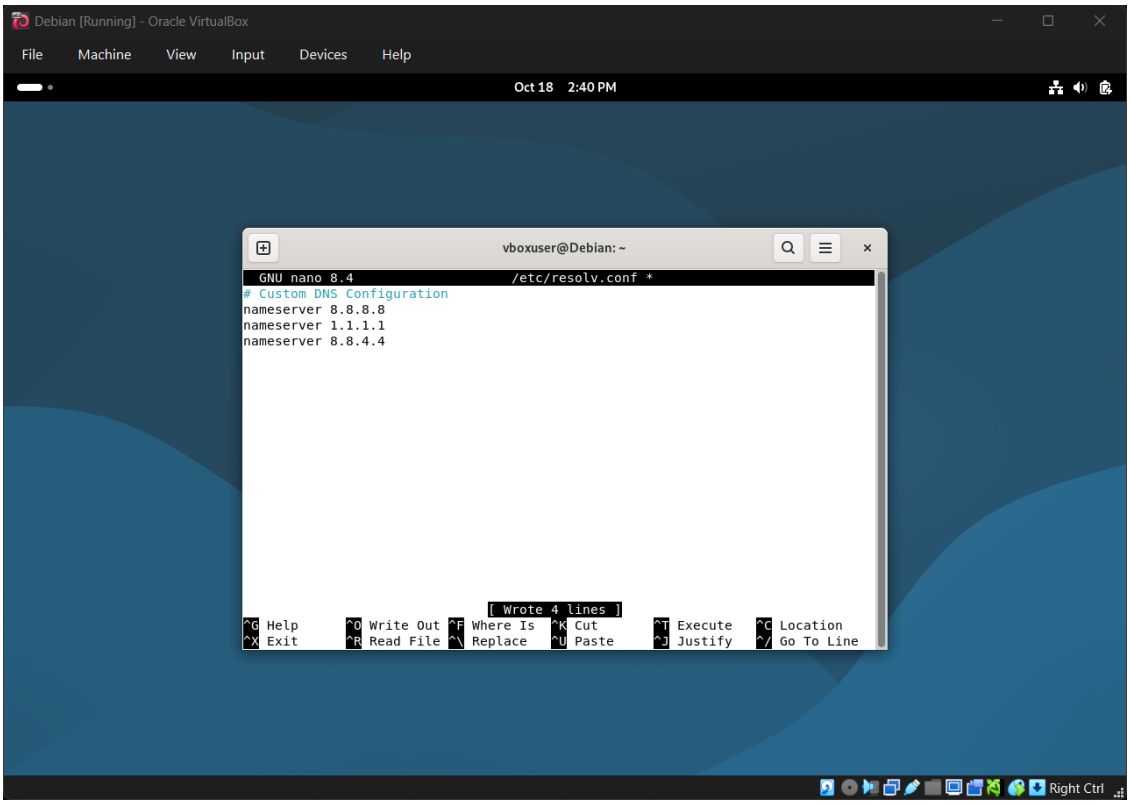
- **Actualizar los paquetes.**

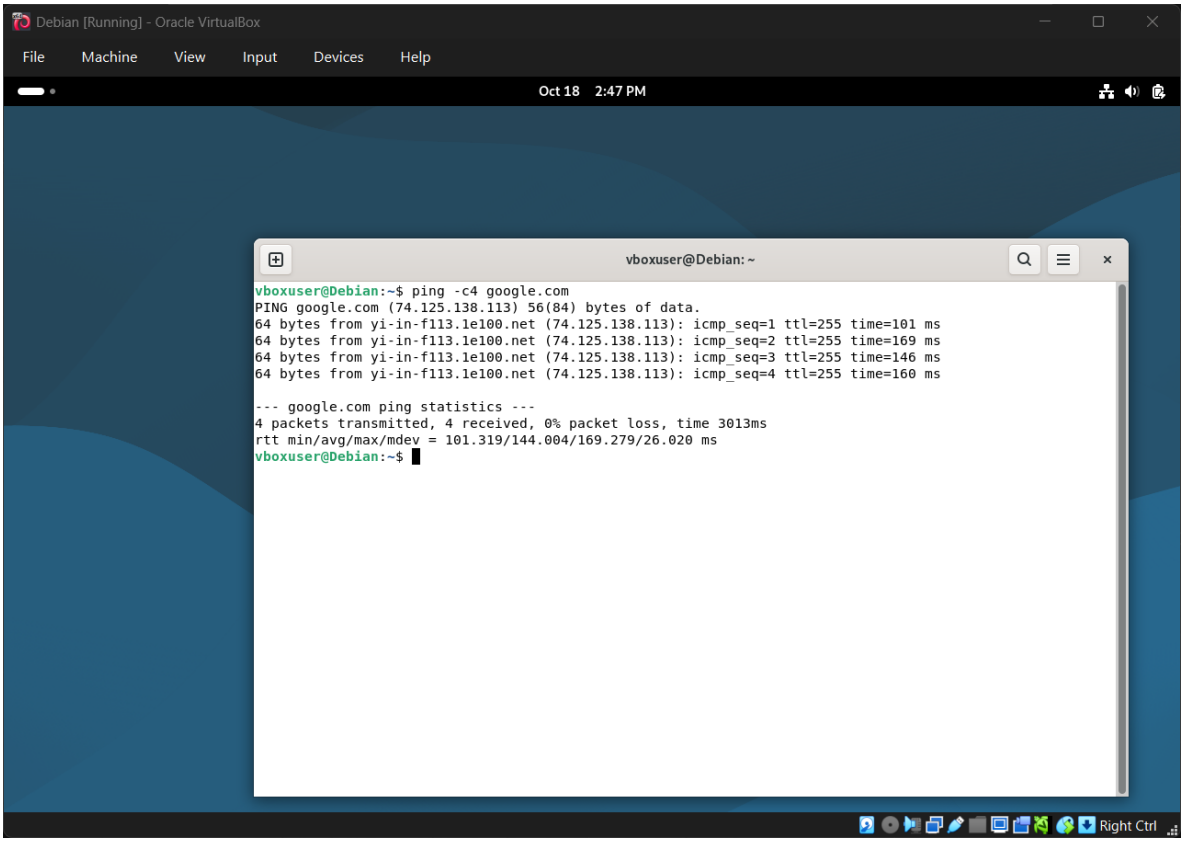


- **Instalación de herramientas necesarias.**



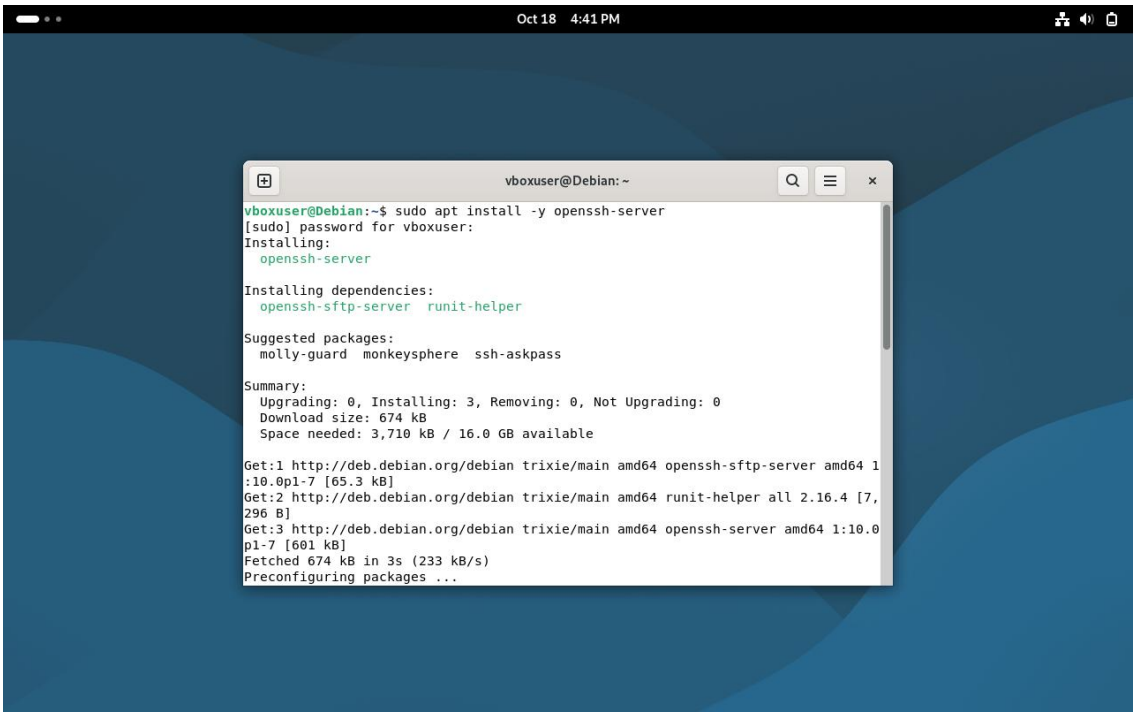
- **Configuración de DNS**

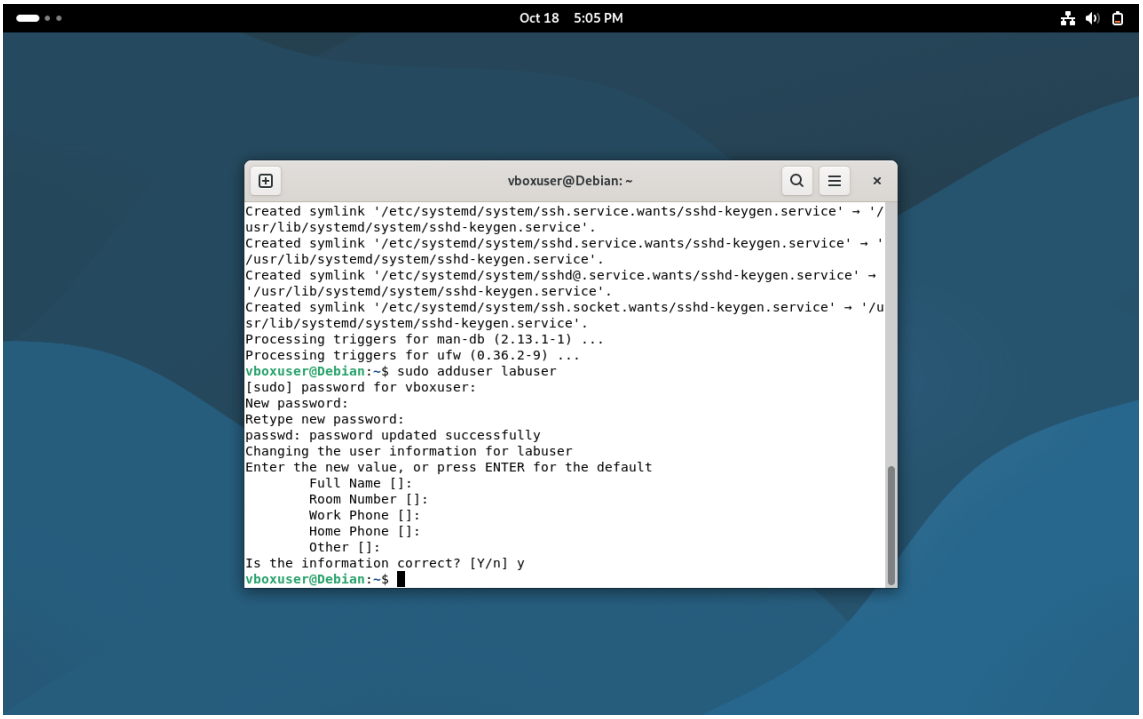


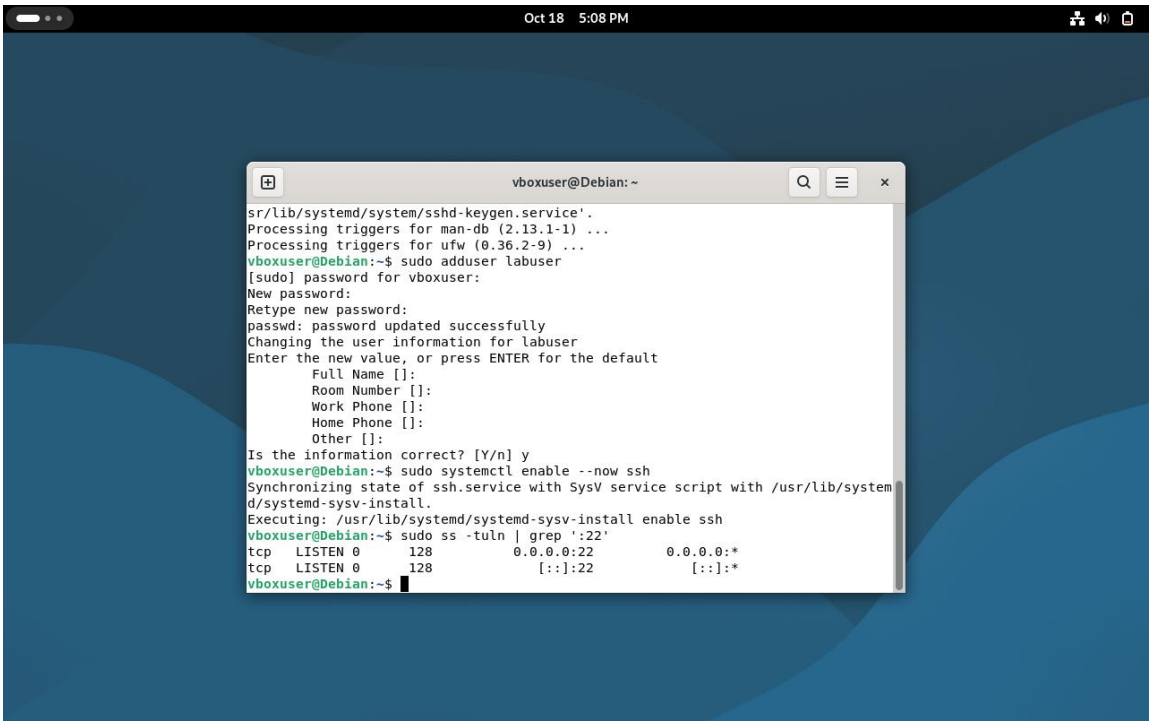


Paso 1 – Creación de Vulnerabilidades

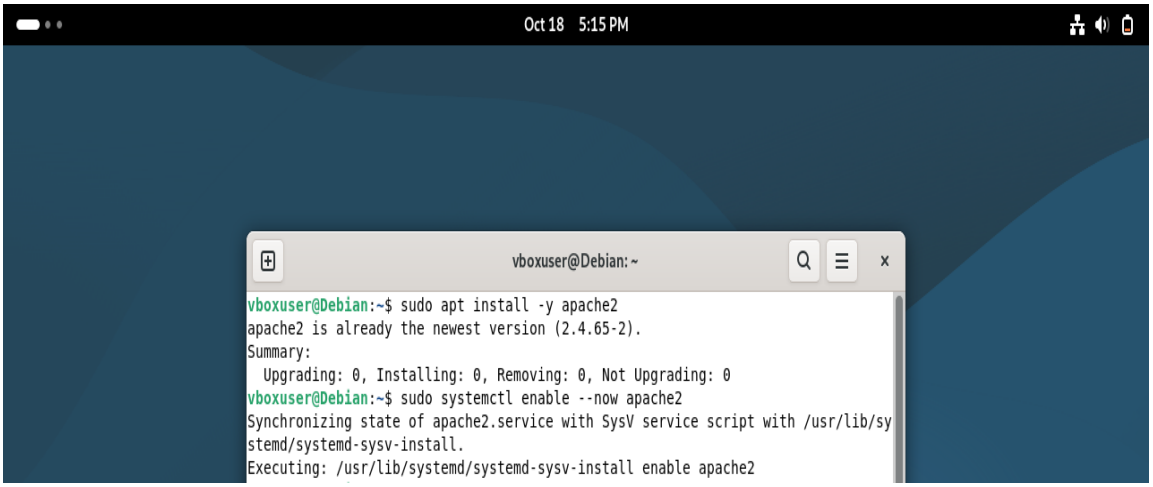
Vulnerabilidad 1: SSH expuesto con la contraseña del usuario débil.

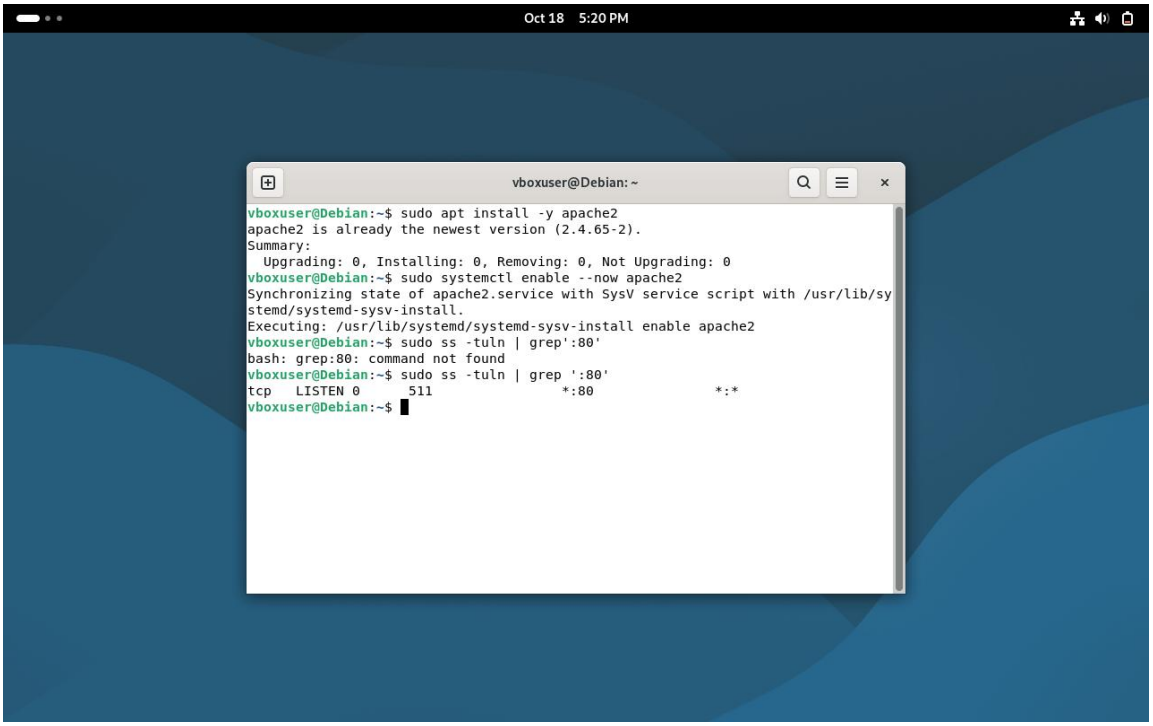




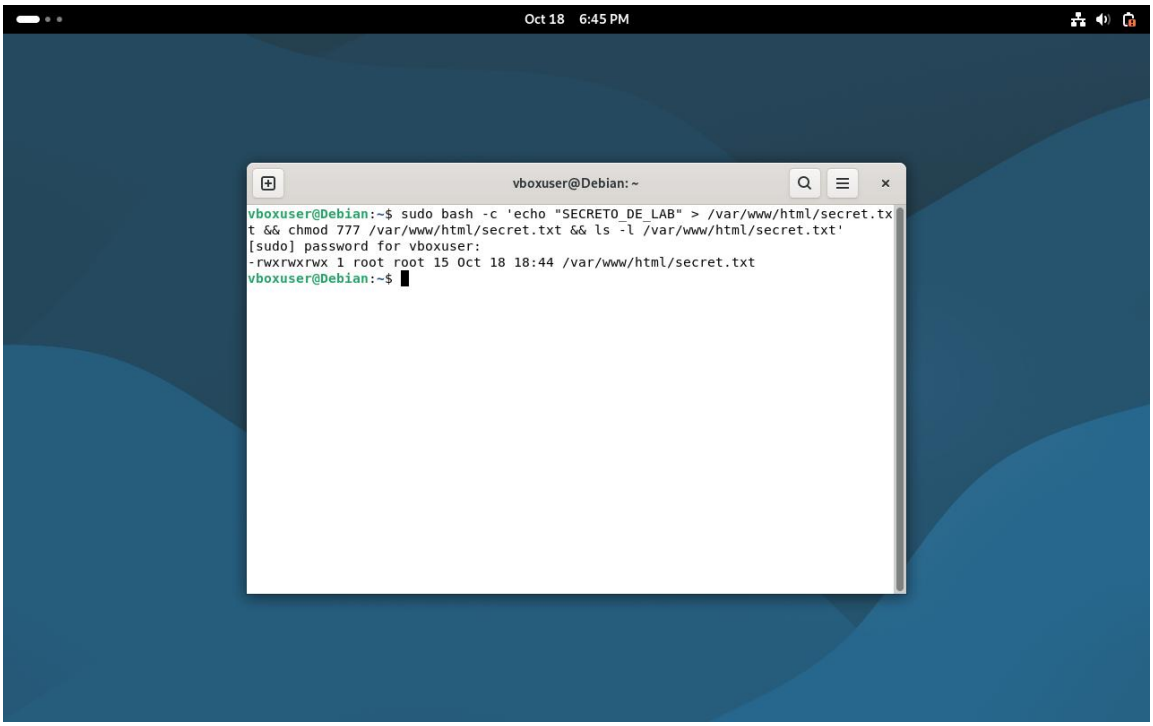


Vulnerabilidad 2: Apache solo en HTTP (sin HTTPS)





Vulnerabilidad 3: Archivo con permisos inseguros (777)



Parte 2: Detección de las Vulnerabilidades

1) Detectar SSH expuesto

Ver servicio SSH escuchando

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

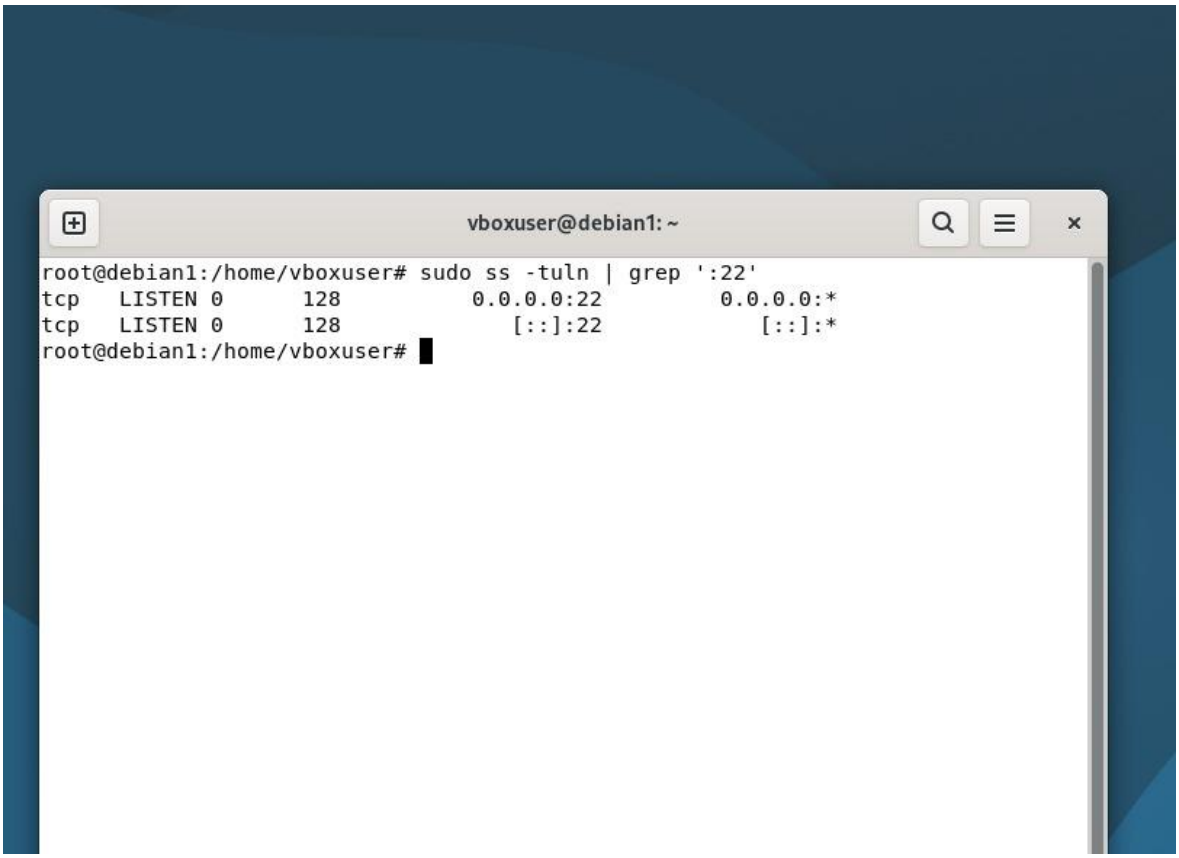
Obtener logs de sshd (usar journalctl)

```
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").



2) Detectar Apache sin HTTPS

Comandos:

Ver puerto 80

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

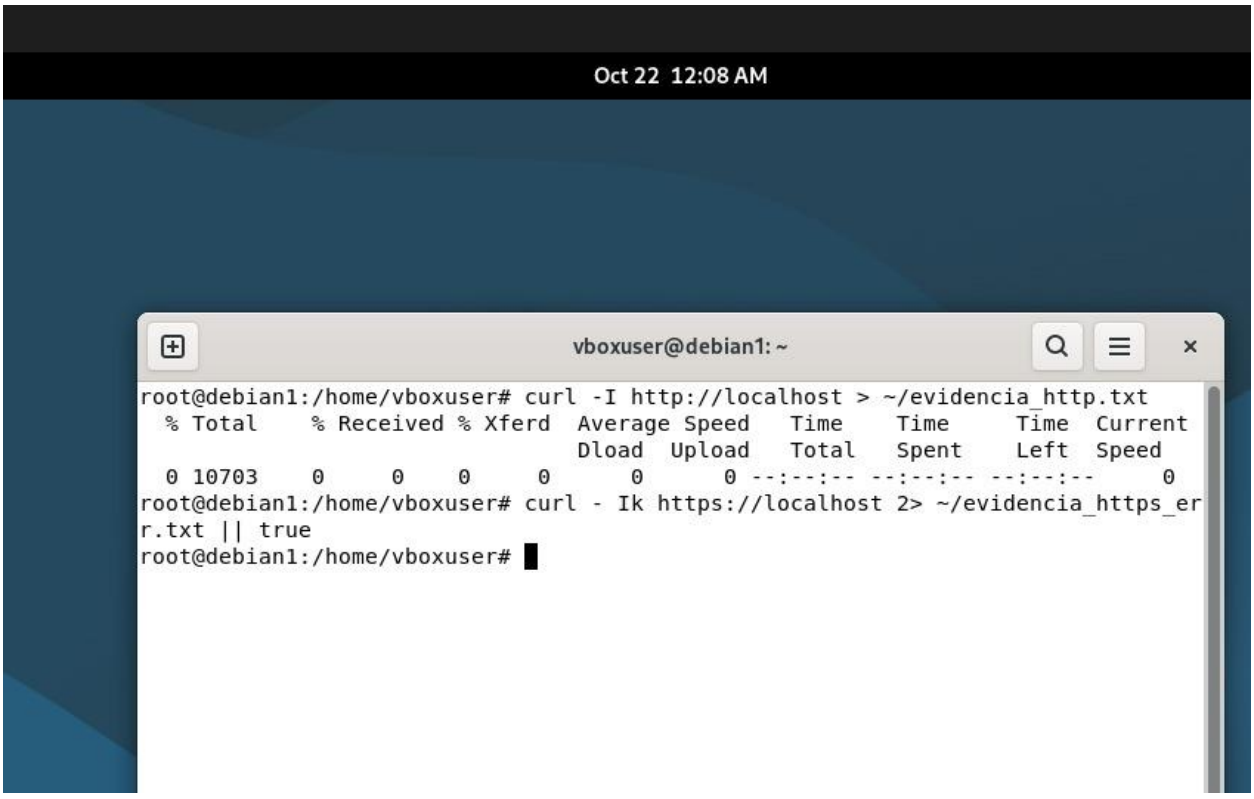
Probar HTTP (usa curl — instálalo si falta)

```
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.



3) Detectar archivo con permisos inseguros

Comandos:

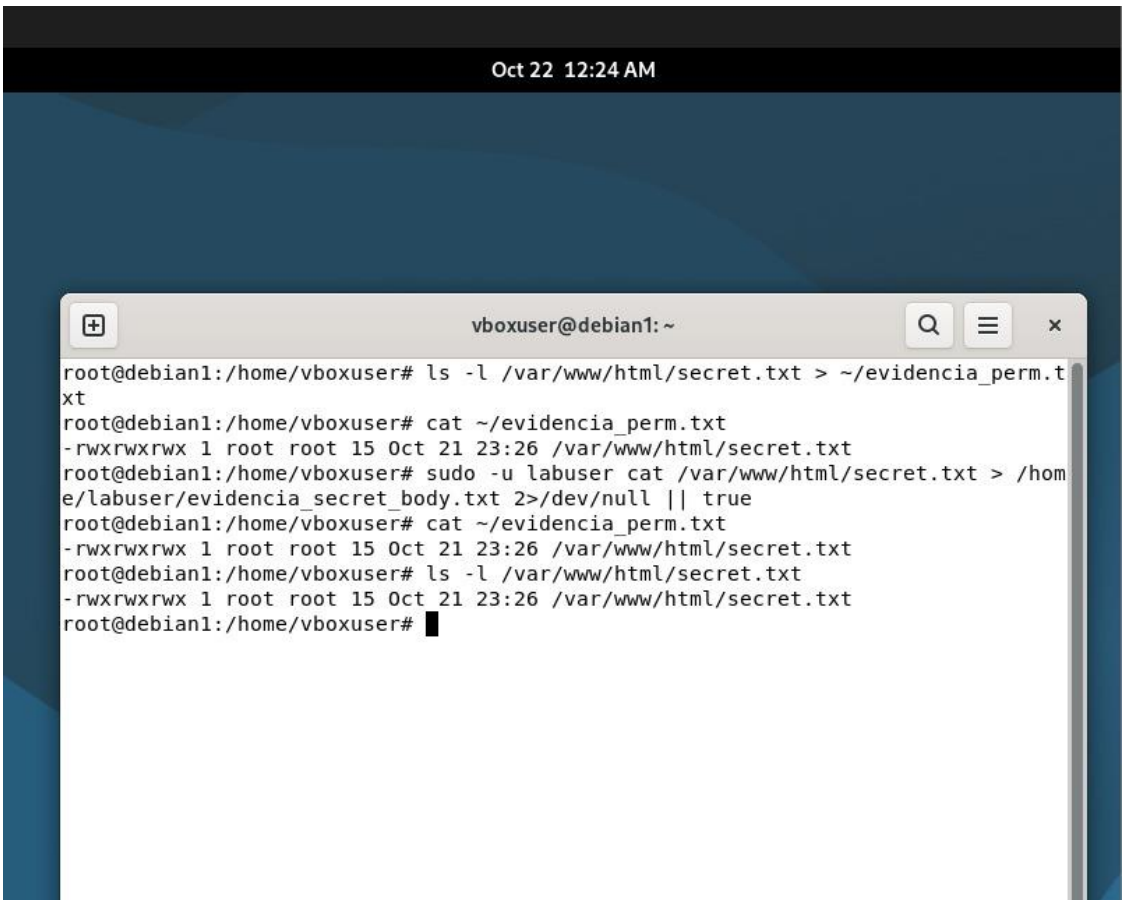
Mostrar permisos

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

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

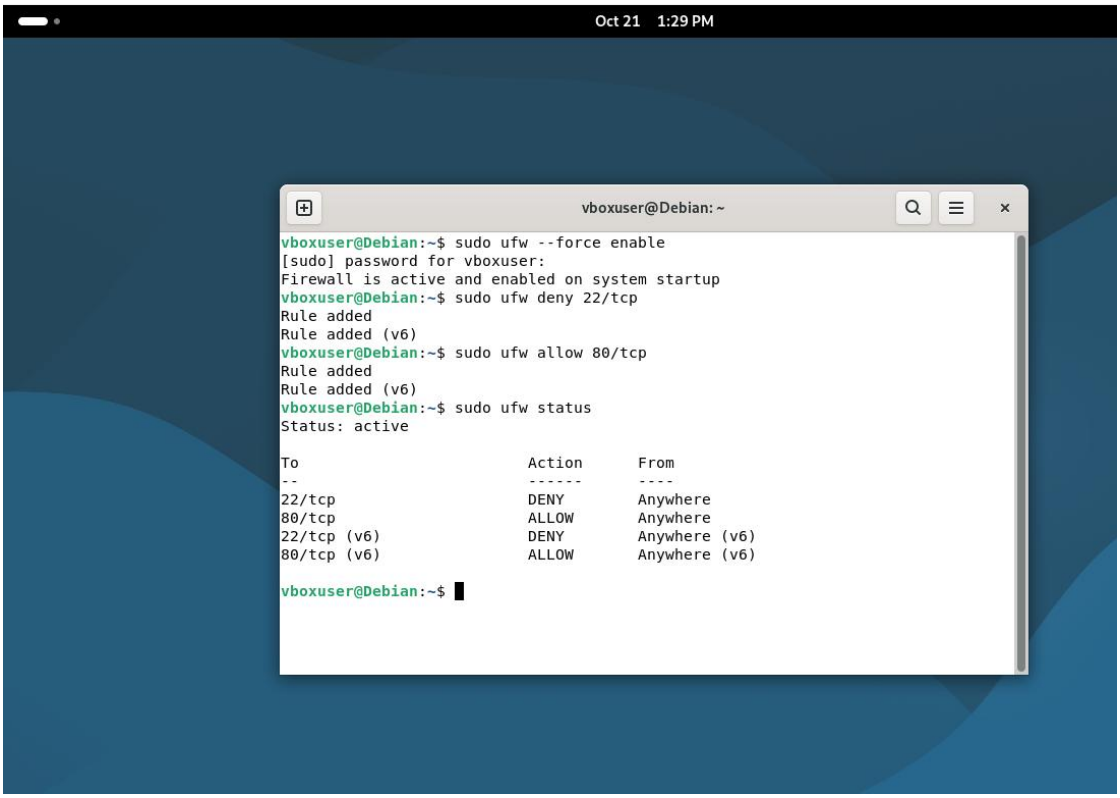
```
sudo -u labuser cat /var/www/html/secret.txt >
/home/labuser/evidencia_secret_body.txt 2>/dev/null || true
```

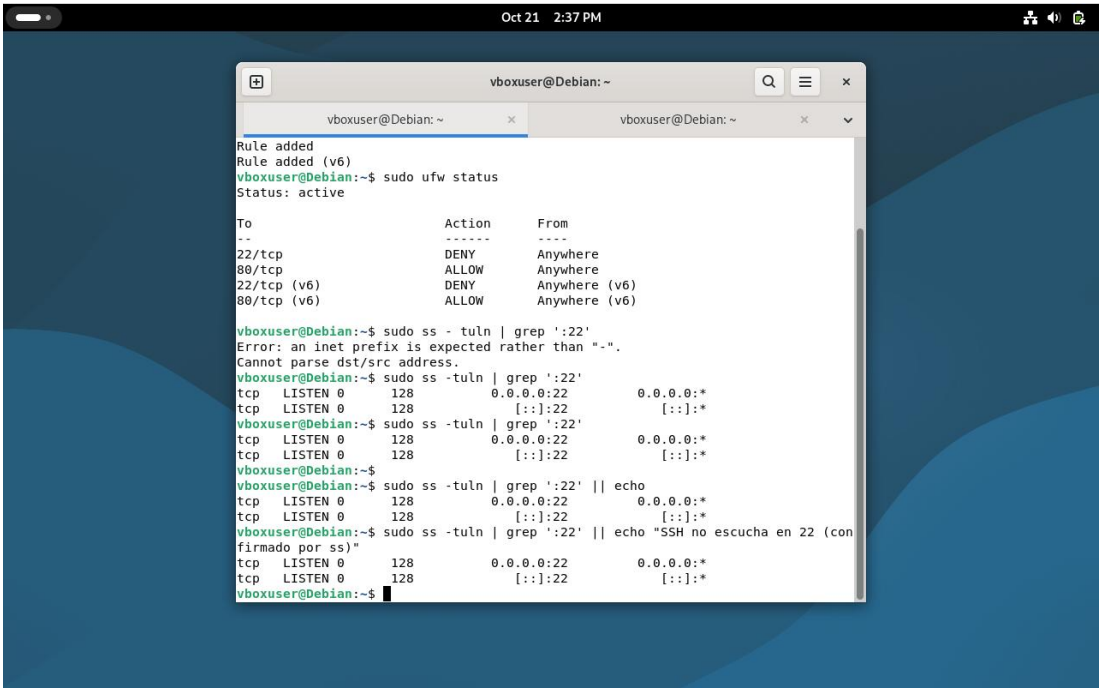
- **Qué copiar al informe:** salida de ls -l mostrando -rwxrwxrwx y contenido del archivo (SECRETO_DE_LAB).



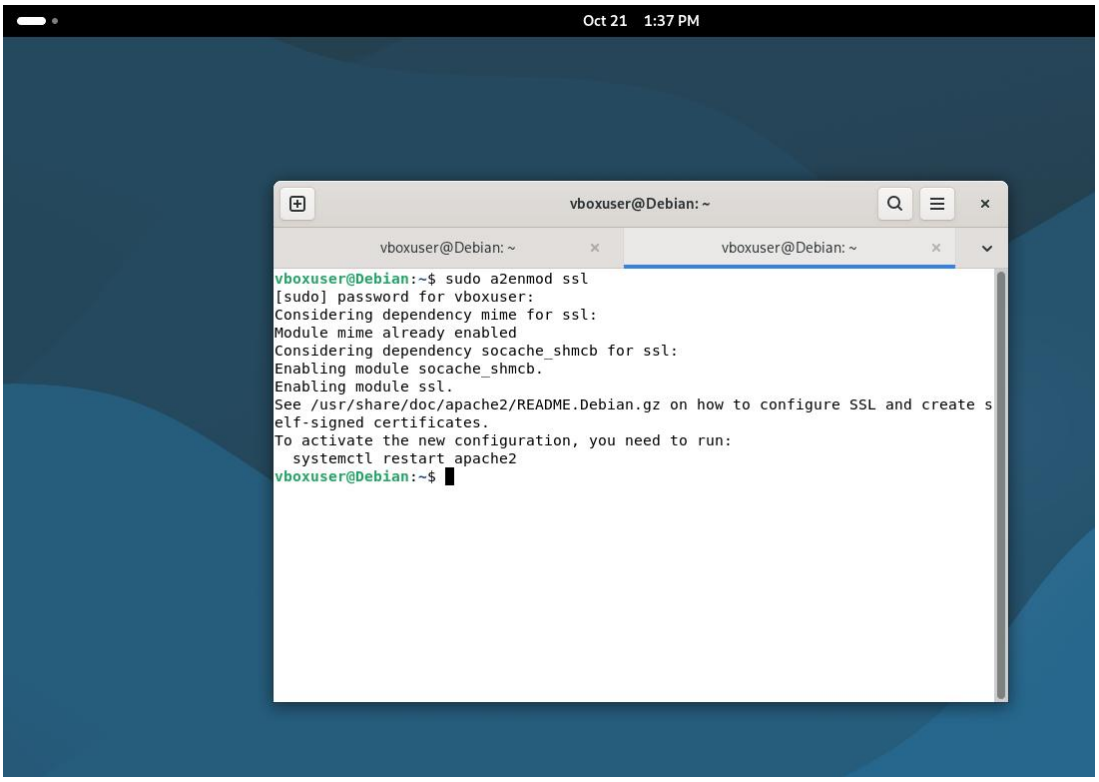
Parte 3: Mitigación de las Vulnerabilidades

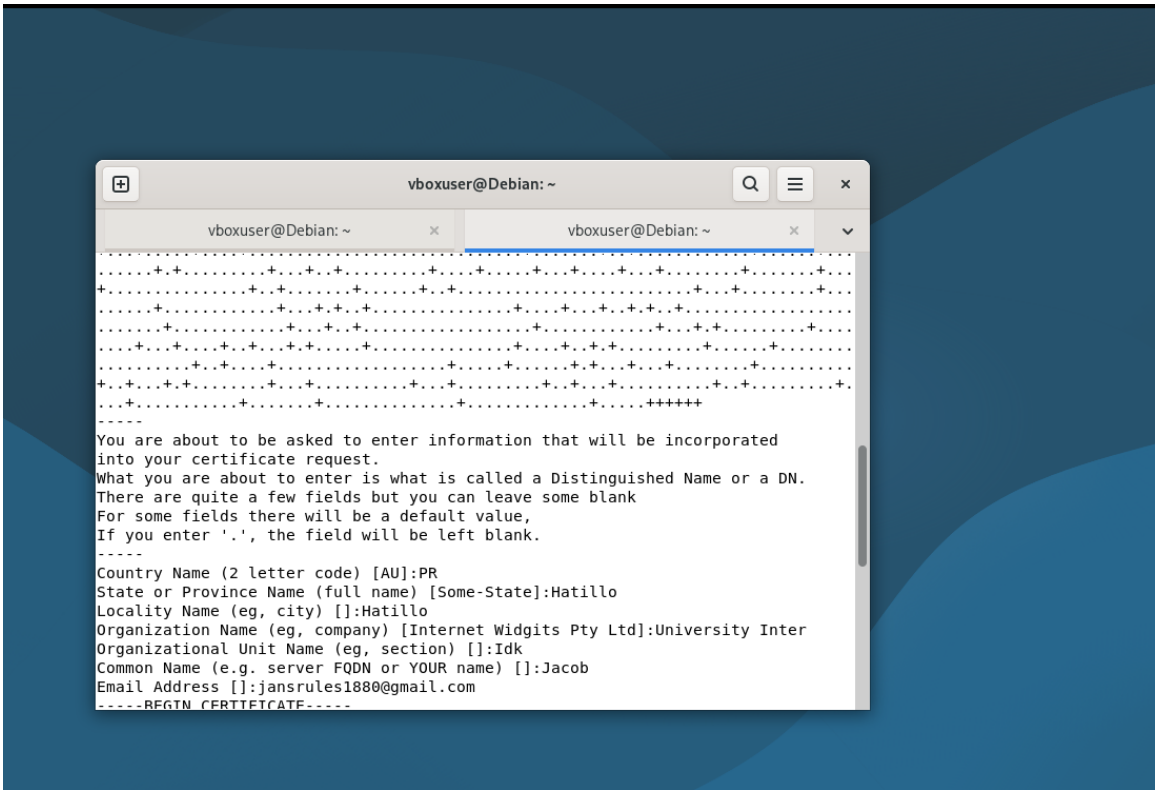
Mitigación 1: SSH: denegar puerto 22 y pedir contraseña fuerte o usar claves

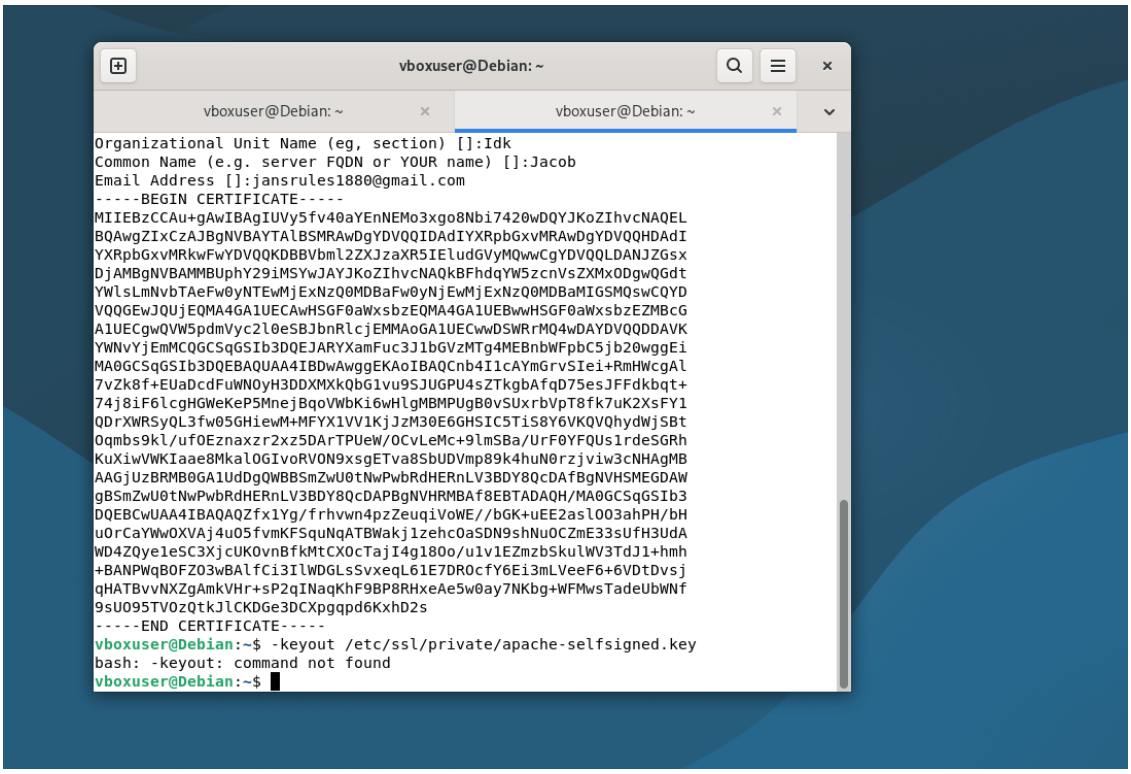


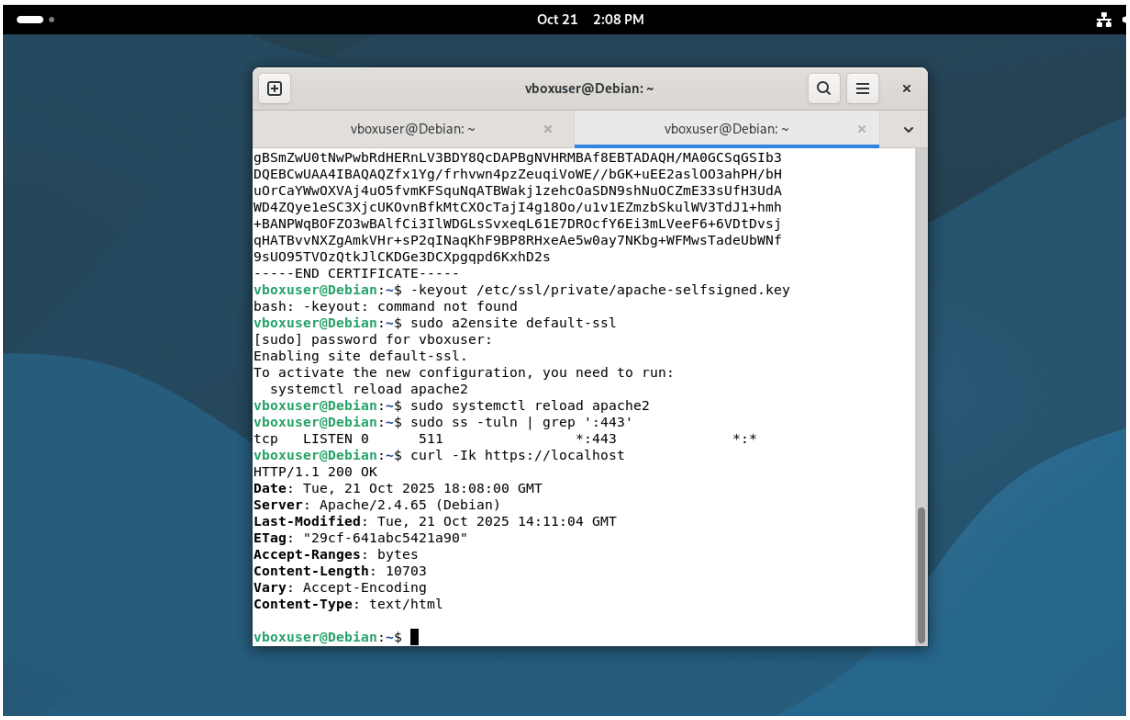


Mitigación 2 — Apache: habilitar HTTPS (certificado autofirmado)

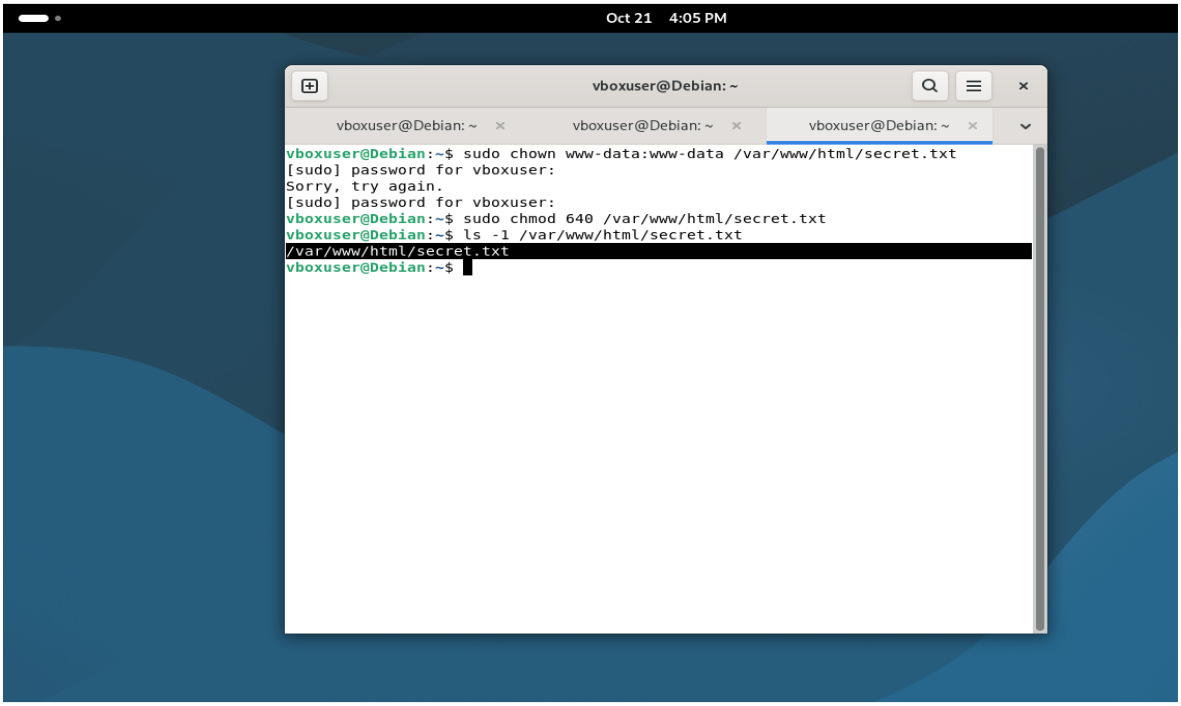


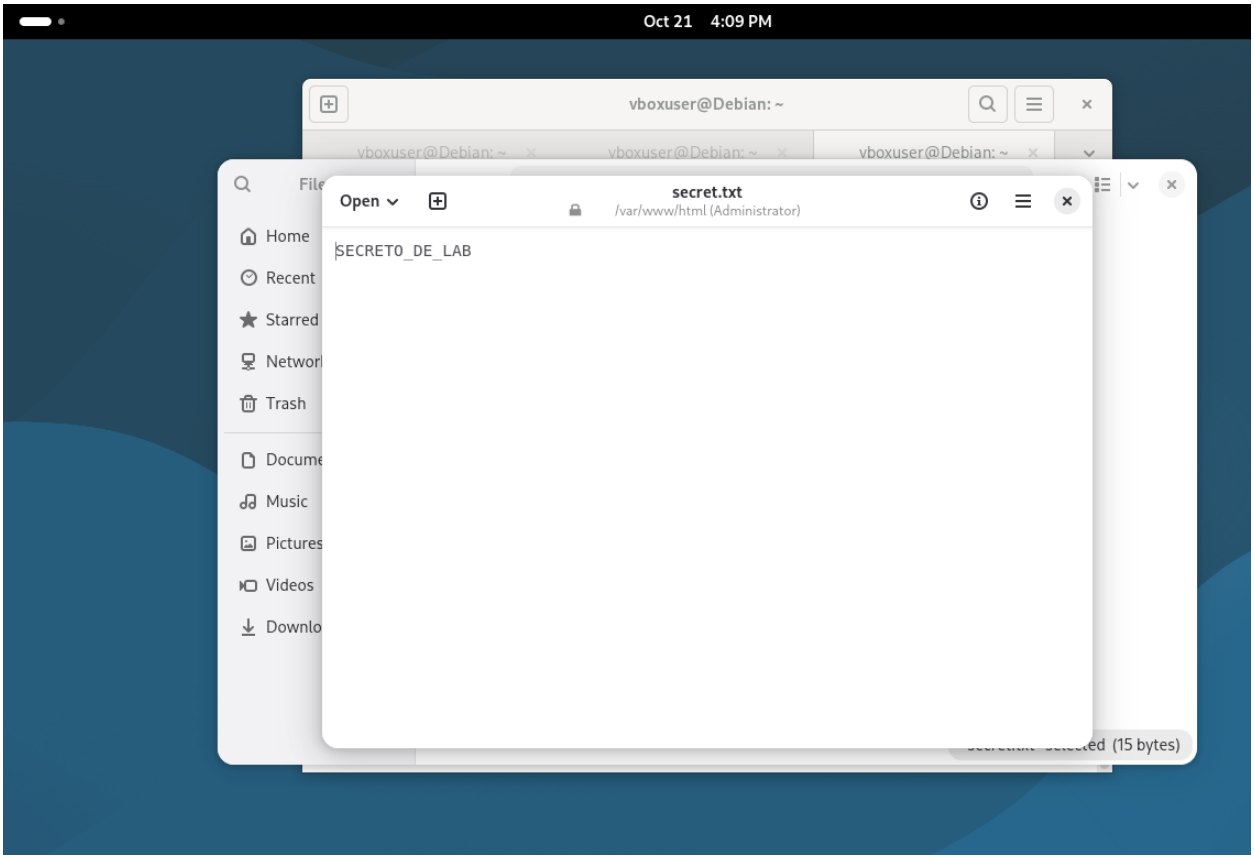



vboxuser@Debian: ~
vboxuser@Debian: ~
vboxuser@Debian: ~
Organizational Unit Name (eg, section) []:Idk
Common Name (e.g. server FQDN or YOUR name) []:Jacob
Email Address []:jansrules1880@gmail.com
-----BEGIN CERTIFICATE-----
MIIEBzCCAu+gAwIBAgIUVy5fv40aYEnNEMo3xgo8Nbi7420wDQYJKoZIhvcNAQEL
BQAwgZIxCzAJBgNVBAYTAlBSMRAwDgYDVQQIDAdIYXRpbGxvMRAwDgYDVQQHDAdI
YXRpbGxvMRkwFwYDVQQKDBBVbml2ZXJzaXR5IEludGVyMQwwCgYDVQQLDANJZGsx
DjAMBgNVBAMMBUphY29iMSYwJAYJKoZIhvcNAQkBFhdqYW5zcnVsZXMxODgwQGdt
YWlsLmNvbTAeFw0yNTEwMjExNzQ0MDBaFw0yNjEwMjExNzQ0MDBaMIGSMQswCQYD
VQQGEwJQUjEQMA4GA1UECAwHSGF0aWxsbzEQMA4GA1UEBwwHSGF0aWxsbzEZMBcG
A1UECgwQVW5pdmVyc2l0eSBJbnRlcjEMMAoGA1UECwwDSWRrMQ4wDAYDVQQDDAVK
YWNvYjEmMCQGCSqGSIb3DQEJARYXamFuc3J1bGVzMTg4MEBnbWFpbC5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCnb4I1cAYmGrvSIei+RmHWcgAl
7vZk8f+EUaDcdFuWNOyH3DDXMXkQbG1vu9SJUGPU4sZTkgbAfqD75esJFFdkbqt+
74j8iF6lcgHGWeKeP5MnejBqoVWbKi6wHlgMBMPUgB0vSUxrbVpT8fk7uK2XsFY1
QDrXWRSyQL3fw05GHiewM+MFYX1VV1KjJzM30E6GHSIC5TiS8Y6VKQVQhydWjSBt
Oqmbs9kl/ufOEznaxzr2xz5DArTPUeW/OCvLeMc+9lmSBa/UrF0YFQUs1rdeSGRh
KuXiwVWKIaae8MkalOGIvoRVON9xsgETva8SbUDVmp89k4huN0rzjviw3cNHAgMB
AAGjUzBRMB0GA1UdDgQWBBSmZwU0tNwPwbRdHERnLV3BDY8QcDAfBgNVHSMEGDAW
gBSmZwU0tNwPwbRdHERnLV3BDY8QcDAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3
DQEBCwUAA4IBAQAQZfx1Yg/frhvwn4pzZeuqiVoWE//bGK+uEE2aslOO3ahPH/bH
uOrCaYWwOXVAj4uO5fvmKFSquNqATBWakj1zehcOaSDN9shNuOCZmE33sUfH3UdA
WD4ZQye1eSC3XjcUKOvnBfkMtCXOcTajI4g18Oo/u1v1EZmzbSkulWV3TdJ1+hmh
+BANPWqBOFZO3wBAlfCi3IlWDGLsSvxeqL61E7DROcfY6Ei3mLVeeF6+6VDtDvsj
qHATBvvNXZgAmkVHr+sP2qINaqKhF9BP8RHxeAe5w0ay7NKbg+WFMwsTadeUbWNf
9sUO95TVOzQtkJlCKDGe3DCXpgqpd6KxhD2s
-----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: ~
gBSmZwU0tNwPwbRdHERnLV3BDY8QcDAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3
DQEBCwUAA4IBAQAQZfx1Yg/frhvwn4pzZeuqiVoWE//bGK+uEE2aslOO3ahPH/bH
uOrCaYWwOXVAj4uO5fvmKFSquNqATBWakj1zehcOaSDN9shNuOCZmE33sUfH3UdA
WD4ZQye1eSC3XjcUKOvnBfkMtCXOcTajI4g18Oo/u1v1EZmzbSkulWV3TdJ1+hmh
+BANPWqBOFZO3wBAlfCi3IlWDGLsSvxeqL61E7DROcfY6Ei3mLVeeF6+6VDtDvsj
qHATBvvNXZgAmkVHr+sP2qINaqKhF9BP8RHxeAe5w0ay7NKbg+WFMwsTadeUbWNf
9sUO95TVOzQtkJlCKDGe3DCXpgqpd6KxhD2s
-----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 -Ik 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





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 maquinas 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%