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**

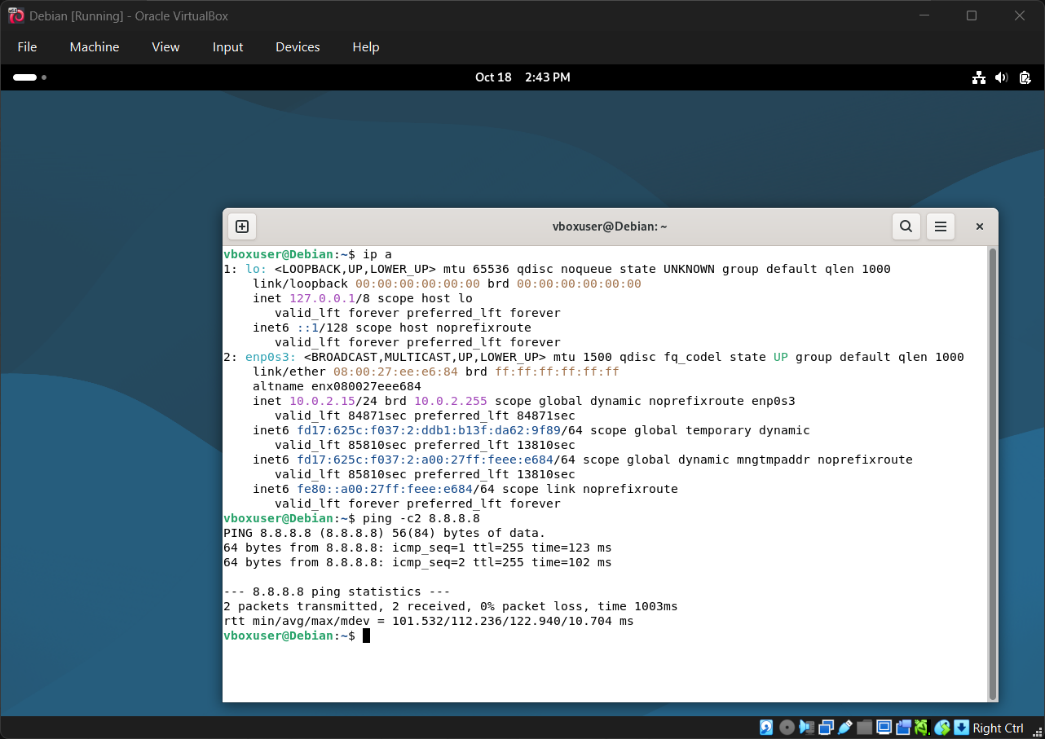
**A screenshot of a computer

AI-generated content may be incorrect.**

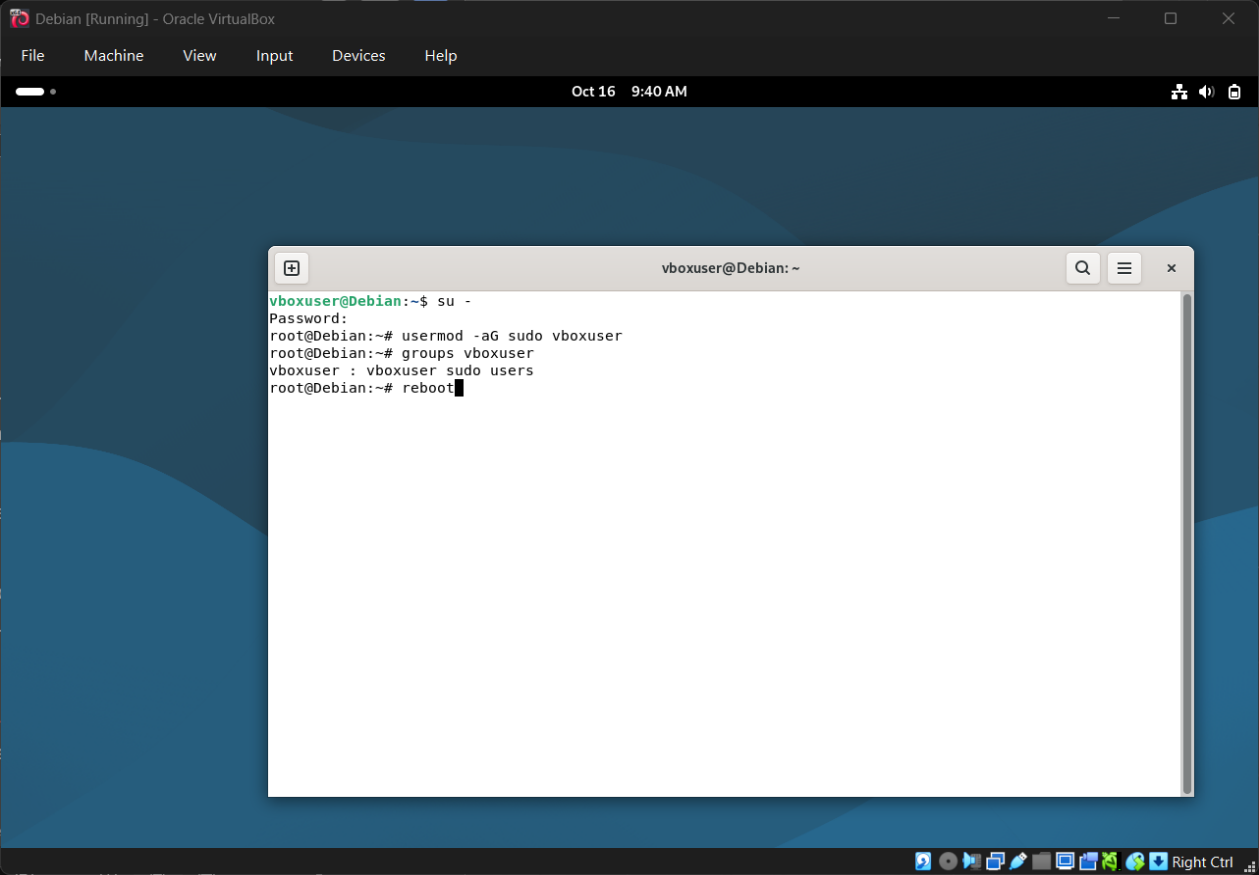
* **Conexión de la computadora virtual a la red de la maquina anfitriona.**

**A screenshot of a computer

AI-generated content may be incorrect.**

****

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

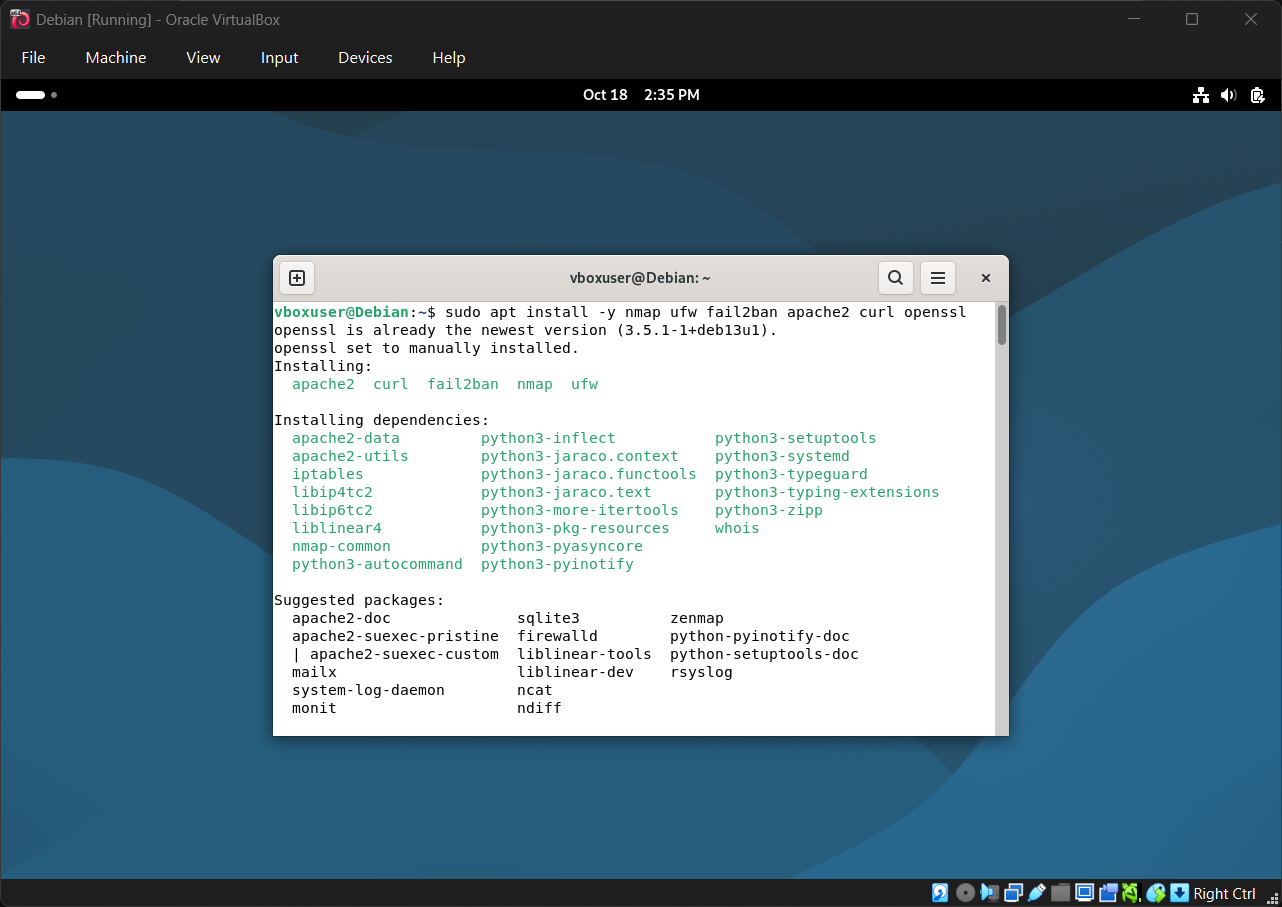
****

* **Actualizar los paquetes.**

**A screenshot of a computer

AI-generated content may be incorrect.**

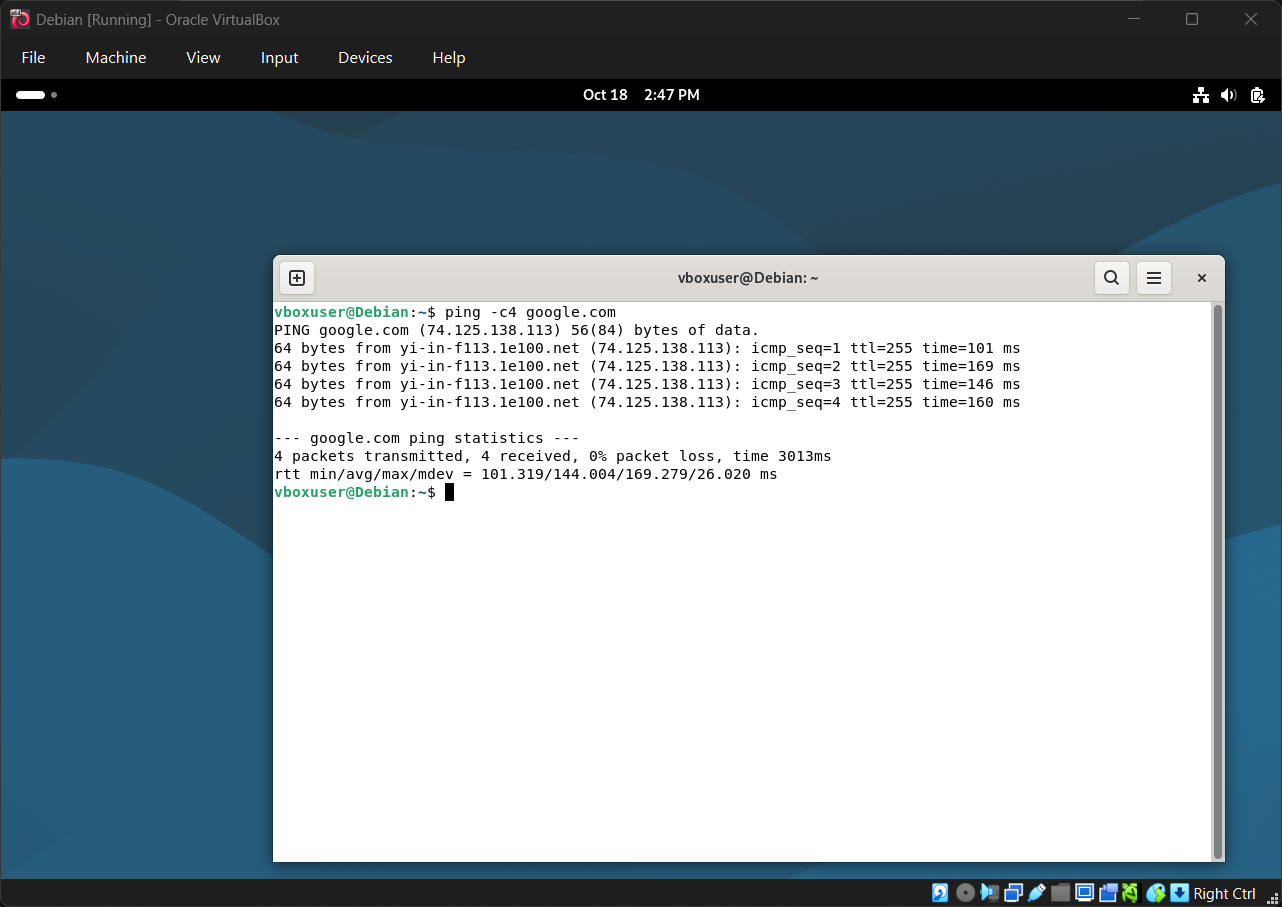
* **Instalación de herramientas necesarias.**

****

* **Configuración de DNS**

**A screenshot of a computer

AI-generated content may be incorrect.**

****

**Paso 1 – Creación de Vulnerabilidades**

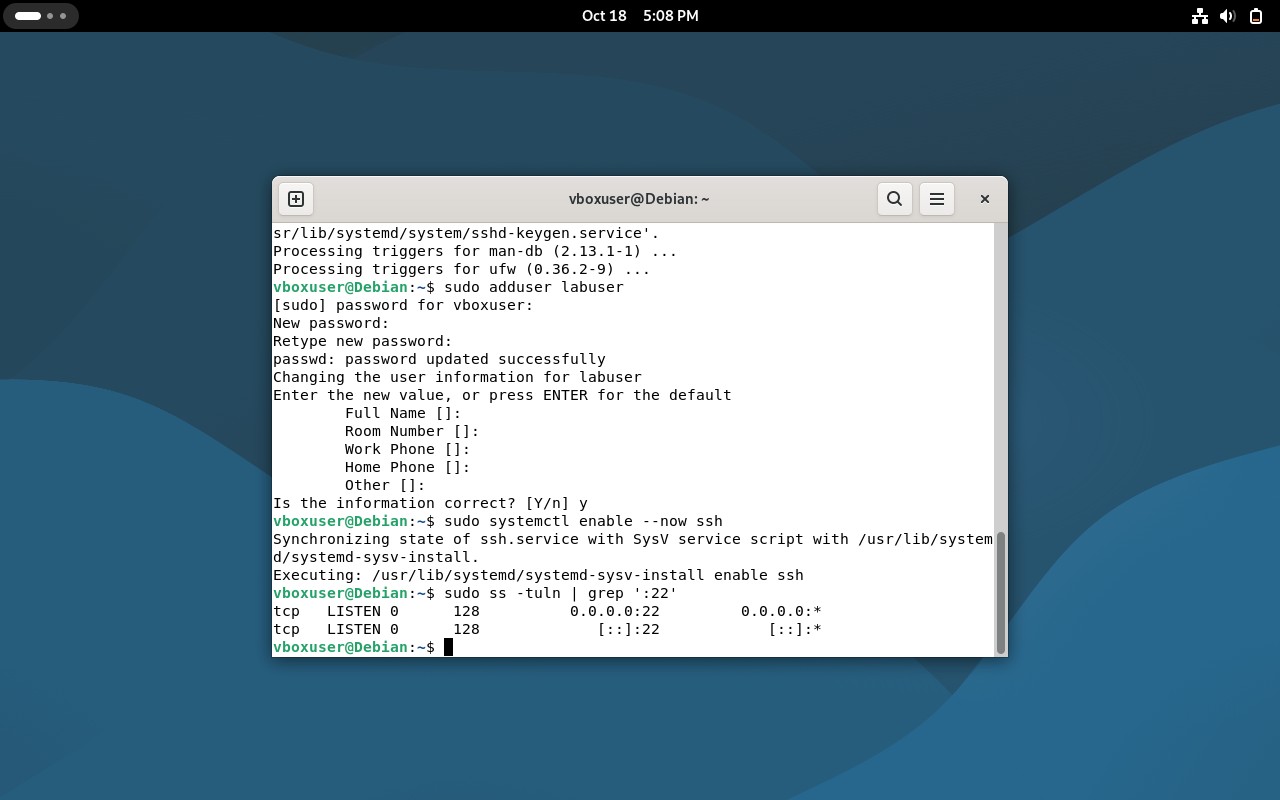
**Vulnerabilidad 1:** SSH expuesto con la contraseña del usuario débil.

A screenshot of a computer

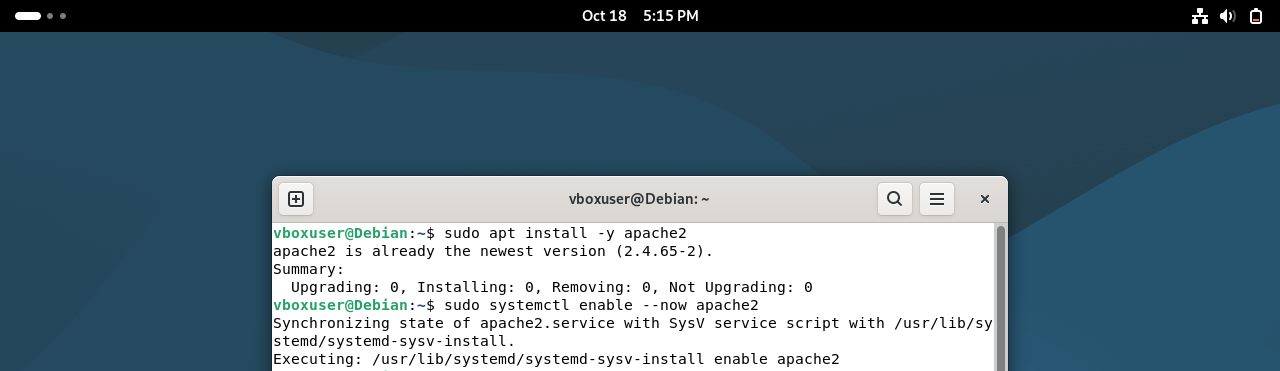
AI-generated content may be incorrect.

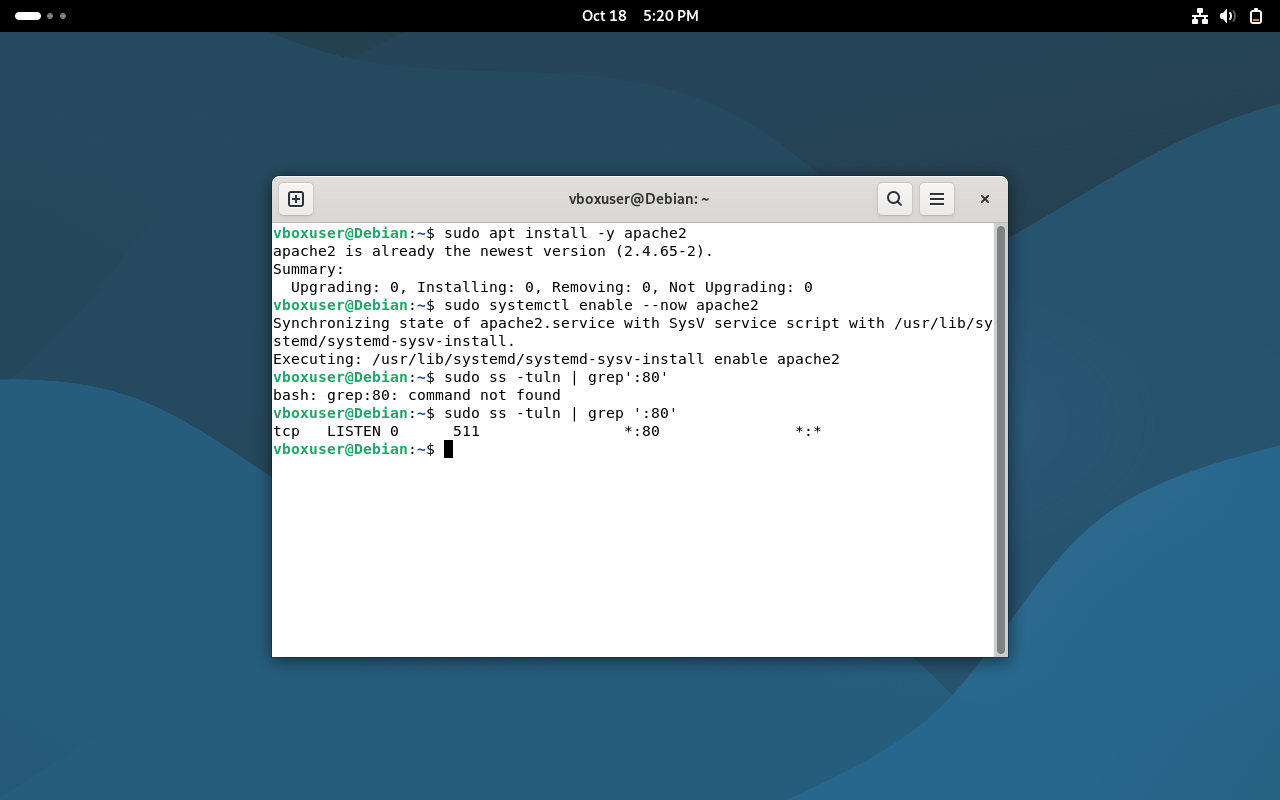
A screenshot of a computer

AI-generated content may be incorrect.



**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").

A screenshot of a computer

AI-generated content may be incorrect.

**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.

A screenshot of a computer

AI-generated content may be incorrect.

**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

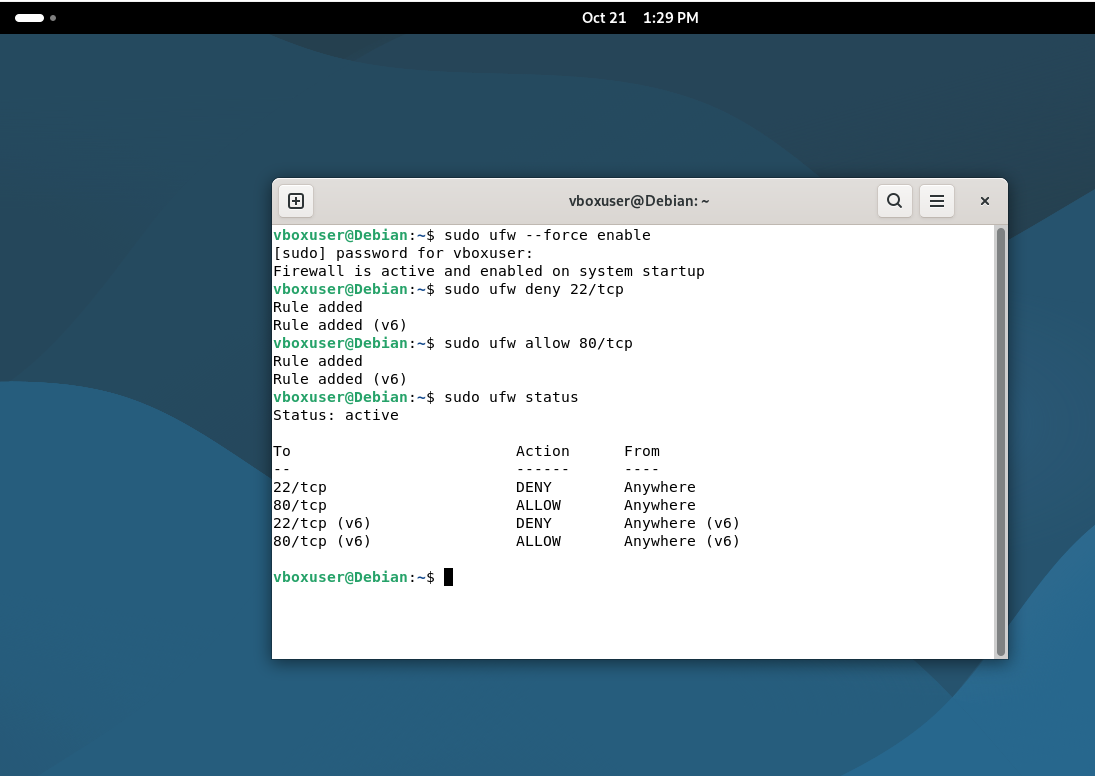
* **Qué copiar al informe:** salida de ls -l mostrando -rwxrwxrwx y contenido del archivo (SECRETO\_DE\_LAB).

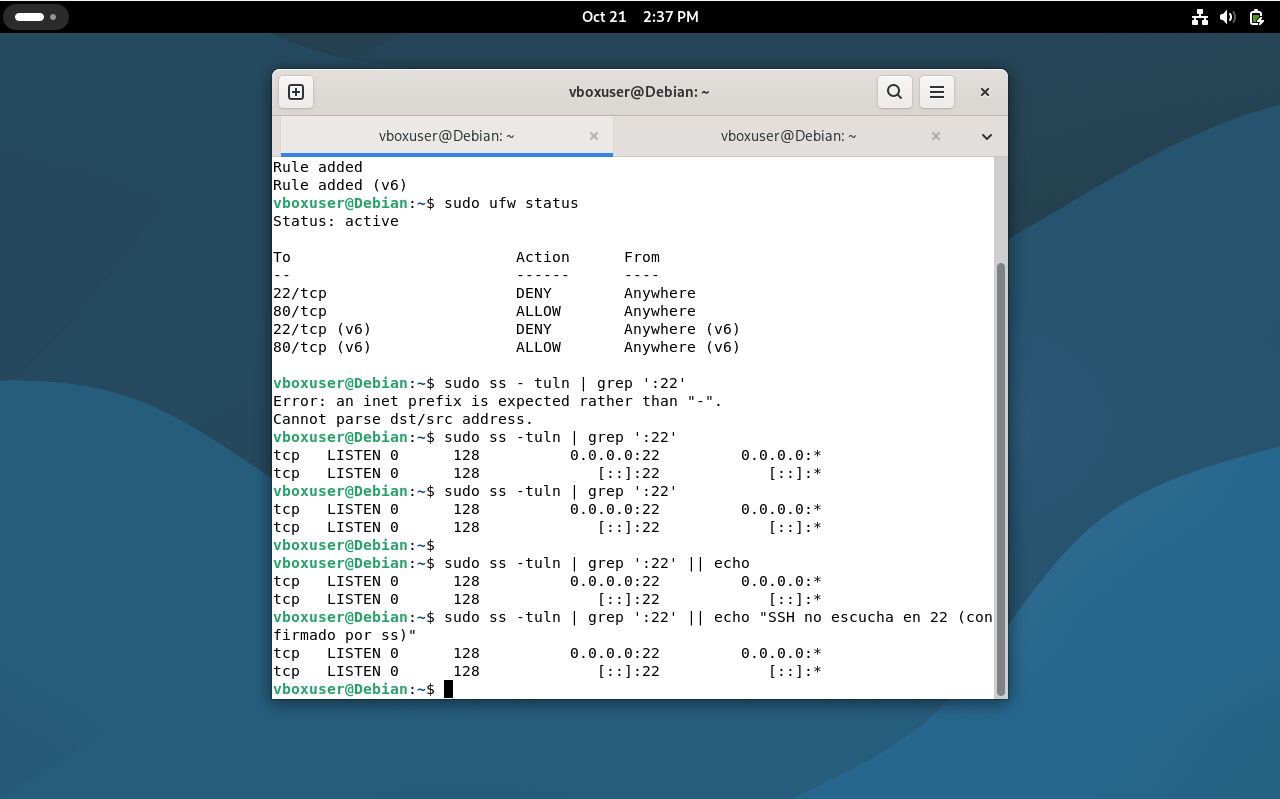
A screenshot of a computer

AI-generated content may be incorrect.

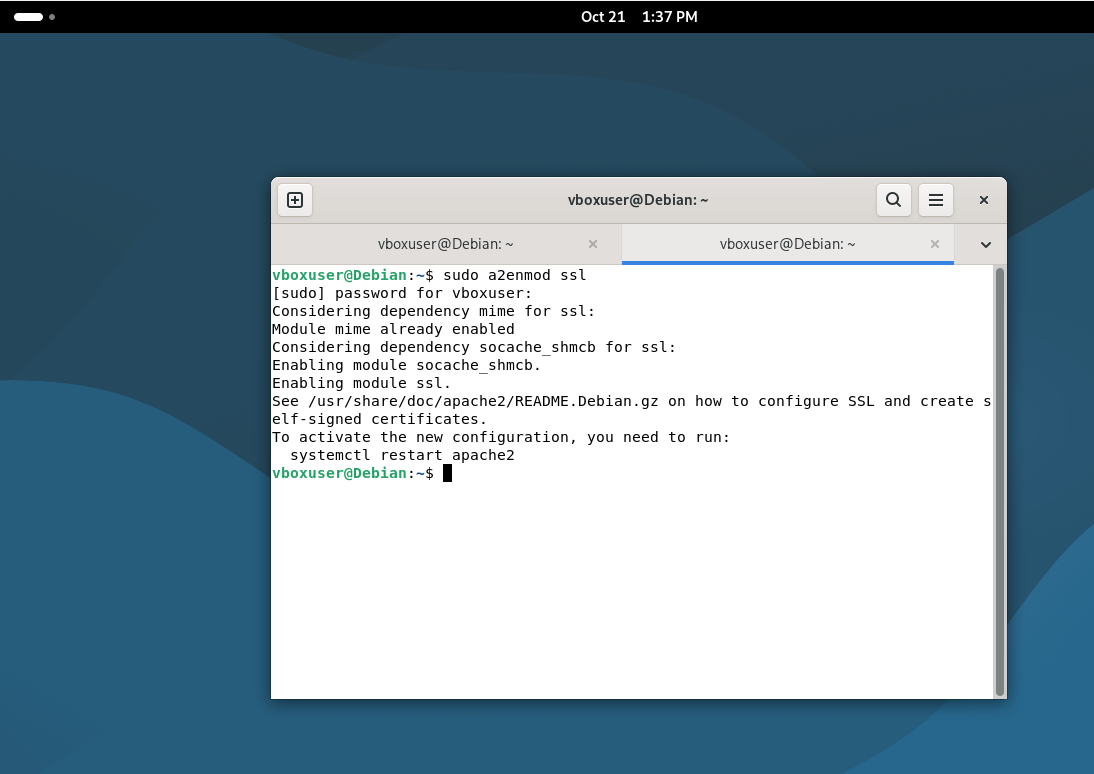
**Parte 3: Mitigación de las Vulnerabilidades**

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





**Mitigación 2** — Apache: habilitar HTTPS (certificado autofirmado)

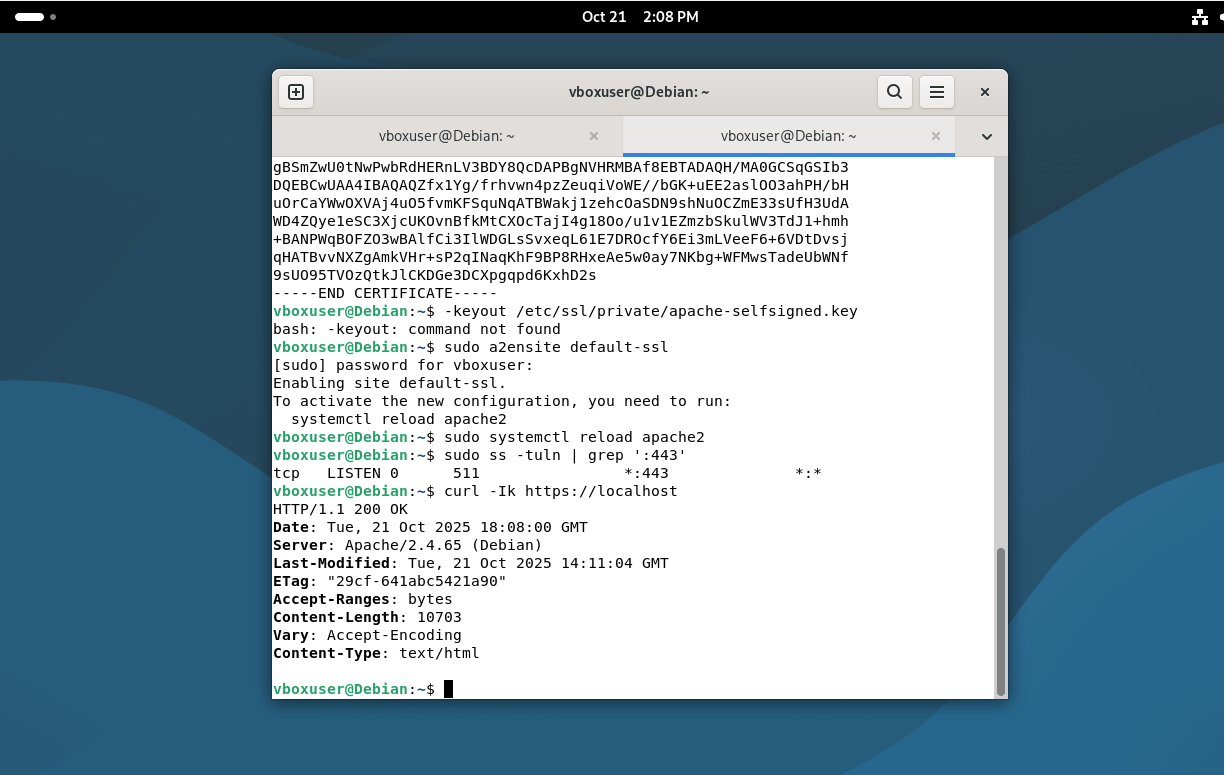


A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.



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

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**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% |