

Universidad Autónoma de Baja California



Facultad de Ciencias Químicas e Ingeniería

## **GESTIÓN Y SEGURIDAD EN REDES**

### **Meta 4.1**

#### **Auditorias de seguridad informática**

**Docente: ALVAREZ SALGADO, CARLOS FRANCISCO**

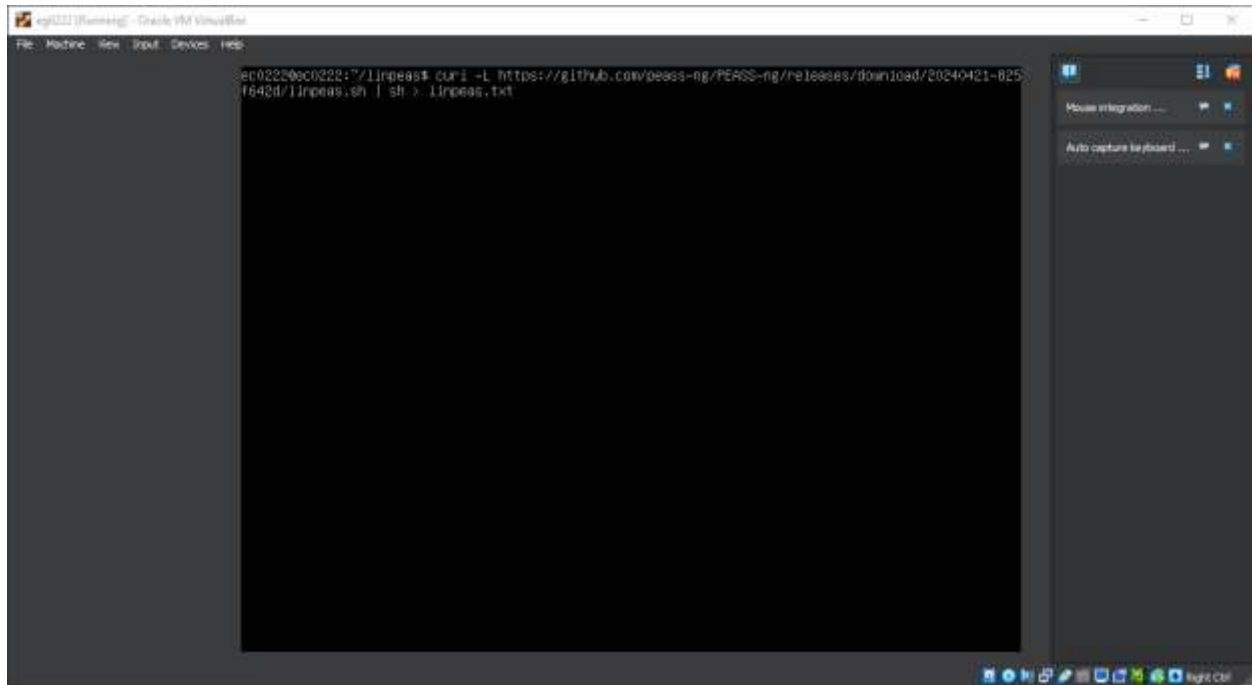
**Alumno: Gómez Cárdenas, Emmanuel Alberto**

**Matricula: 01261509**

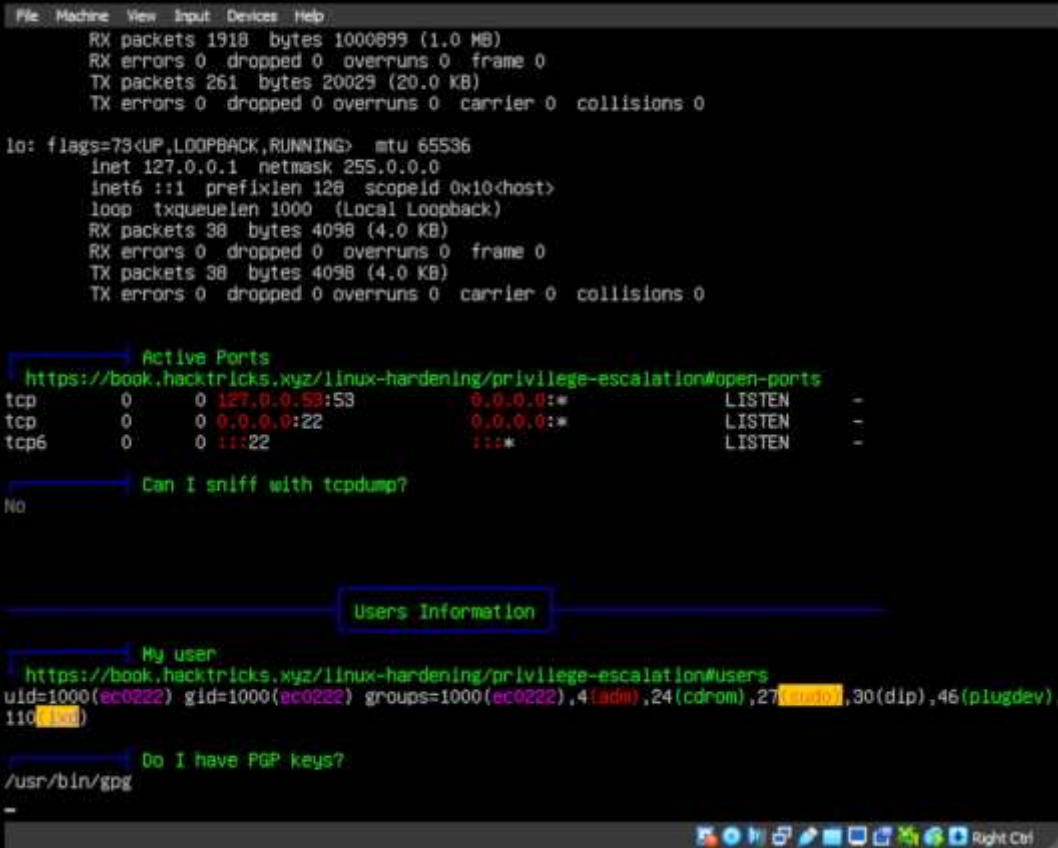
## Reporte de análisis de seguridad usando linPEAS

Como el comando para descargar y correr latest no funciono, tuve que usar curl indicándole el enlace para descargar él .sh de GitHub

```
curl -L https://github.com/peass-ng/PEASS-ng/releases/download/20240421-825f642d/linpeas.sh | sh
```



Después de correr el comando podemos observar las partes donde tenemos vulnerabilidades y todo tipo de información importante, desde simple información del sistema (Si es una máquina virtual) hasta si hay puertos abiertos y demás.



```
File Machine View Input Devices Help
RX packets 1918 bytes 1000899 (1.0 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 261 bytes 20029 (20.0 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 38 bytes 4098 (4.0 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 38 bytes 4098 (4.0 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Active Ports
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp 0 0 127.0.0.1:53 0.0.0.0:* LISTEN -
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN -
tcp6 0 0 :::22 :::* LISTEN -

Can I sniff with tcpdump?
No

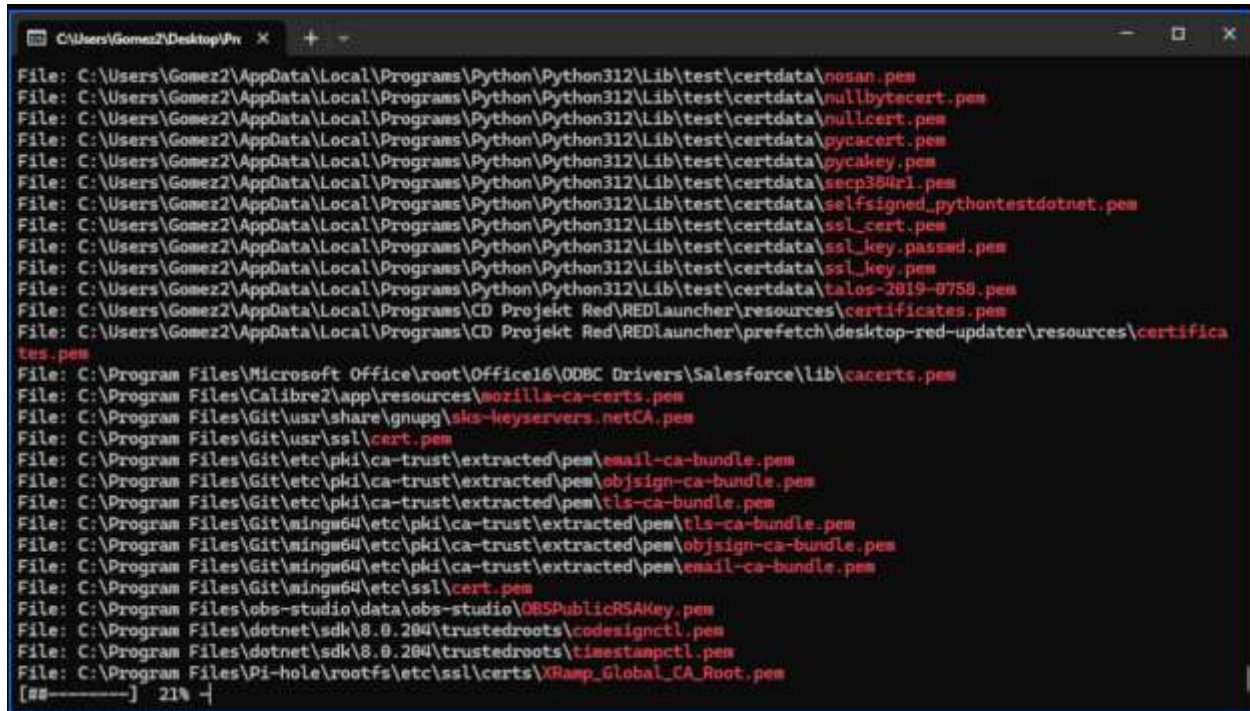
Users Information

My user
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#users
uid=1000(ec0222) gid=1000(ec0222) groups=1000(ec0222),4(admin),24(cdrom),27(audio),30(dip),46(plugdev),110(lxd)

Do I have PGP keys?
/usr/bin/gpg
```

En el caso de la máquina virtual me pude dar cuenta de todas las vulnerabilidades que presenta a pesar de no tener la gran cantidad de programas / servicios instalados.

En el caso de usar Windows, el programa a ejecutar se llama WinPeas, que funciona con el mismo principio que linPEAS, pero para Windows.



```
C:\Users\Gomez2\Desktop\WinPeas>
File: C:\Users\Gomez2\AppData\Local\Programs\Python\Python312\Lib\test\certdata\nosan.pem
File: C:\Users\Gomez2\AppData\Local\Programs\Python\Python312\Lib\test\certdata\nullbytecert.pem
File: C:\Users\Gomez2\AppData\Local\Programs\Python\Python312\Lib\test\certdata\nullicert.pem
File: C:\Users\Gomez2\AppData\Local\Programs\Python\Python312\Lib\test\certdata\pycacert.pem
File: C:\Users\Gomez2\AppData\Local\Programs\Python\Python312\Lib\test\certdata\pycaker.pem
File: C:\Users\Gomez2\AppData\Local\Programs\Python\Python312\Lib\test\certdata\secp384r1.pem
File: C:\Users\Gomez2\AppData\Local\Programs\Python\Python312\Lib\test\certdata\selfsigned_pythontestdotnet.pem
File: C:\Users\Gomez2\AppData\Local\Programs\Python\Python312\Lib\test\certdata\ssl_cert.pem
File: C:\Users\Gomez2\AppData\Local\Programs\Python\Python312\Lib\test\certdata\ssl_key.passed.pem
File: C:\Users\Gomez2\AppData\Local\Programs\Python\Python312\Lib\test\certdata\ssl_key.pem
File: C:\Users\Gomez2\AppData\Local\Programs\Python\Python312\Lib\test\certdata\talos-2019-0750.pem
File: C:\Users\Gomez2\AppData\Local\Programs\CD Projekt Red\REDLauncher\resources\certificates.pem
File: C:\Users\Gomez2\AppData\Local\Programs\CD Projekt Red\REDLauncher\prefetch\desktop-red-updater\resources\certificates.pem
File: C:\Program Files\Microsoft Office\root\Office16\ODBC Drivers\Salesforce\Lib\cacerts.pem
File: C:\Program Files\Calibre2\app\resources\mozilla-ca-certs.pem
File: C:\Program Files\Git\usr\share\gnupg\skis-keyservers.netCA.pem
File: C:\Program Files\Git\usr\ssl\cert.pem
File: C:\Program Files\Git\etc\pki\ca-trust\extracted\pem\email-ca-bundle.pem
File: C:\Program Files\Git\etc\pki\ca-trust\extracted\pem\objsign-ca-bundle.pem
File: C:\Program Files\Git\etc\pki\ca-trust\extracted\pem\tls-ca-bundle.pem
File: C:\Program Files\Git\mingw64\etc\pki\ca-trust\extracted\pem\tls-ca-bundle.pem
File: C:\Program Files\Git\mingw64\etc\pki\ca-trust\extracted\pem\objsign-ca-bundle.pem
File: C:\Program Files\Git\mingw64\etc\pki\ca-trust\extracted\pem\email-ca-bundle.pem
File: C:\Program Files\Git\mingw64\etc\ssl\cert.pem
File: C:\Program Files\obs-studio\data\obs-studio\OBSPublicRSAKey.pem
File: C:\Program Files\dotnet\sdk\8.0.204\trustedroots\codesignctl.pem
File: C:\Program Files\dotnet\sdk\8.0.204\trustedroots\timestampctl.pem
File: C:\Program Files\Pi-hole\rootfs\etc\ssl\certs\XRamp_Global_CA_Root.pem
[##-----] 21% -
```

En el caso de Windows se puede observar que como hay una mayor cantidad de programas / servicios instalados. Existe un mayor número de vulnerabilidades, especialmente los puertos abiertos.

Ya que distintos programas utilizan y necesitan tener los puertos abiertos para comunicación externa, estos conllevan un riesgo al permitir cualquier tipo de conexión desde cualquier maquina remota. Como se muestra en la siguiente imagen

### Conclusión:

Realizar auditorías constantemente ayuda a mantener o hasta a aumentar la seguridad dentro de un sistema de red al garantizar que las defensas estén completamente actualizadas y sean efectivas contra amenazas emergentes, así como a detectar todo tipo de vulneraciones y riesgos especiales en una etapa temprana.