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**

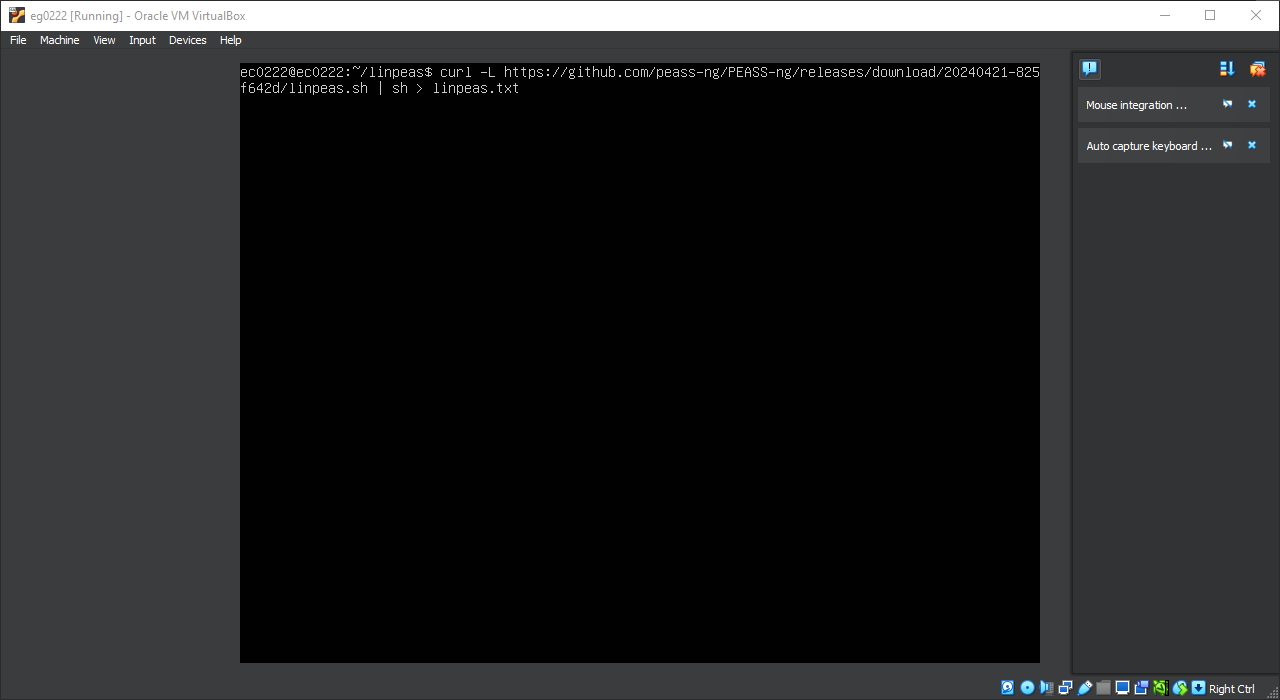
**Alumno:** Gómez Cárdenas, Emmanuel Alberto

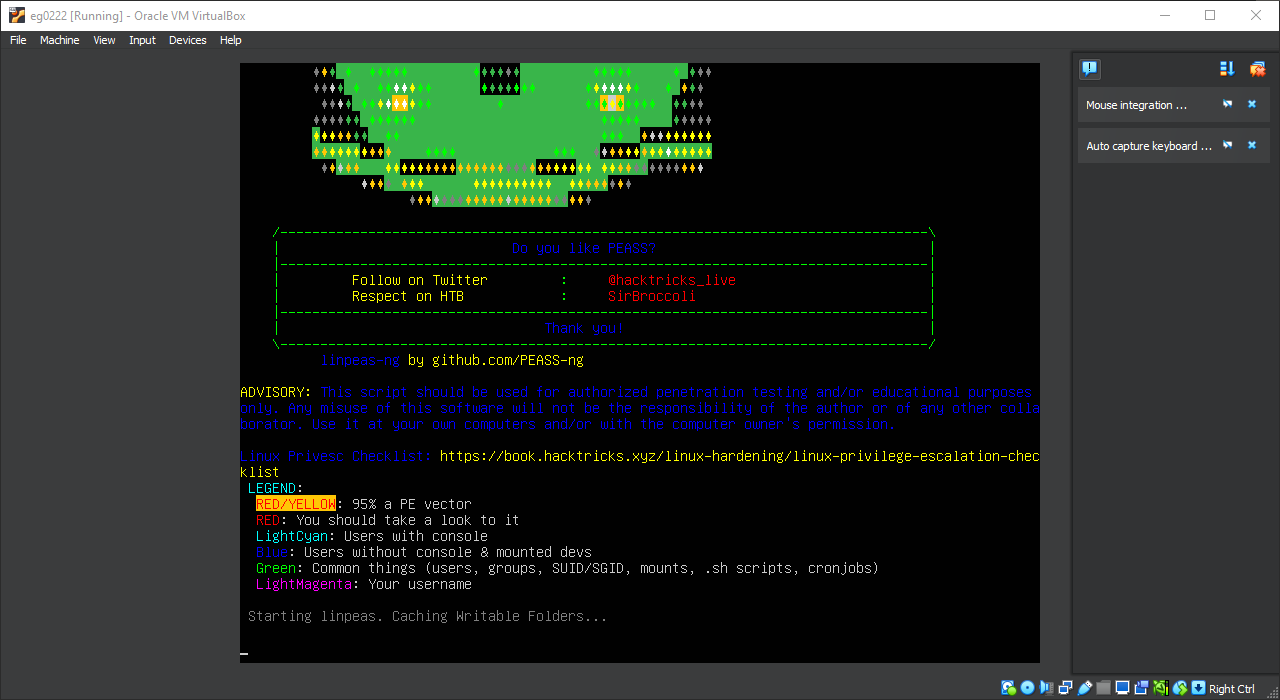
**Matricula:** 01261509

## Reporte de análisis de seguridad usando linPEAS

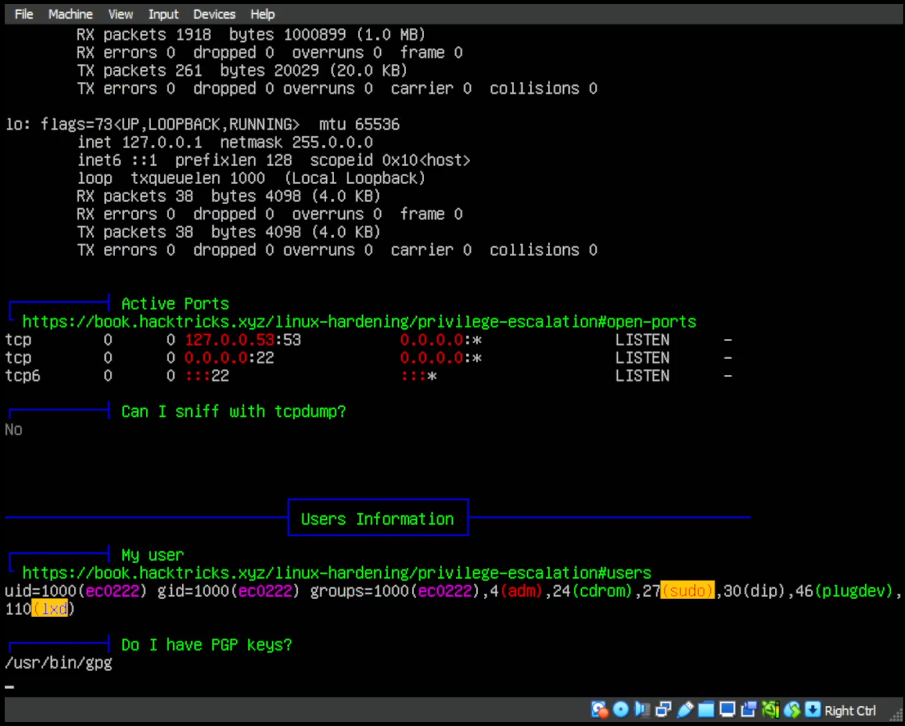
Como el comando para descargar y correr latest no funciono, tuve que usar curl indicándole el enlace para descargar él .sh de GitHub

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



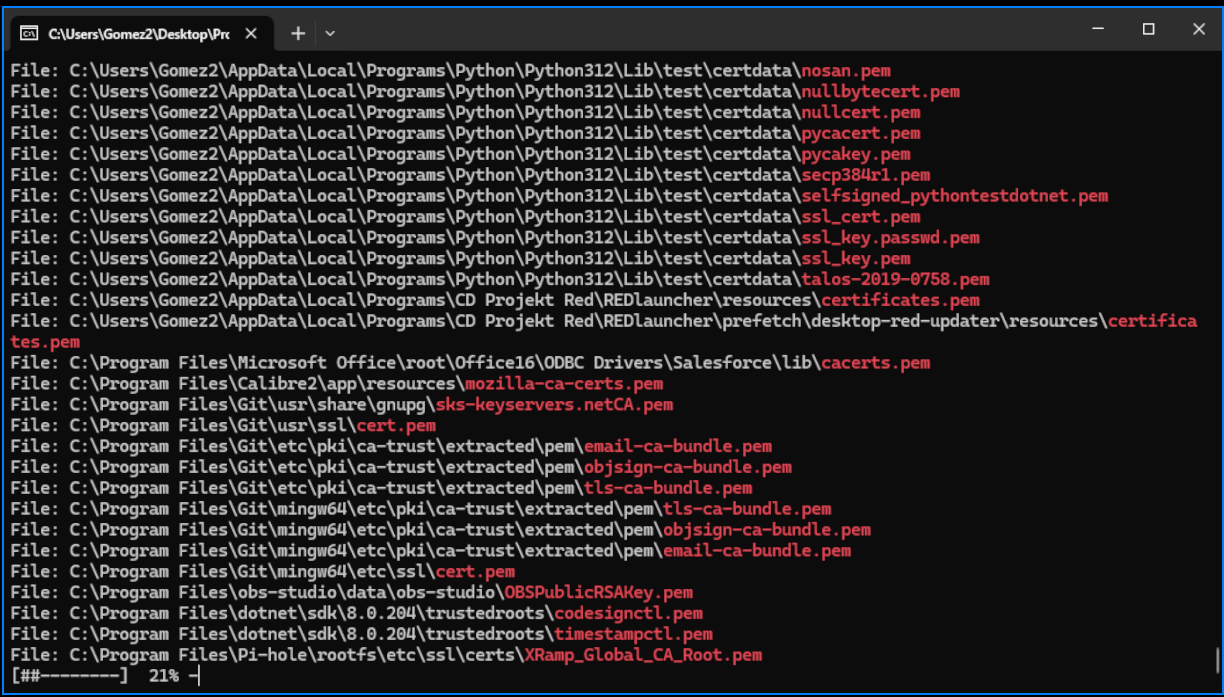


Después de correr el comando podemos observar las partes donde tenemos vulnerabilidades y todo tipo de información importante, desde simple información del sistema (Si es una máquina virtual) hasta si hay puertos abiertos y demás.



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.



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.