Introducción a la Ciberseguridad - 2025

Trabajo Práctico Integrador

Parte 1 - Hardening utilizando Lynis a nivel de sistema operativo.

Instale lynis, se recomienda utilizar git:

```
cd /tmp
git clone https://github.com/CISOfy/lynis
cd lynis
```

En caso de utilizar windows, debe descargar una máquina virtual o utilizar WSL.

Luego proceda a realizar un escaneo de su máquina a nivel local:

```
sudo ./lynis audit system
```

En caso de que aparezca un mensaje como:

```
... [X] Security check failed

    Why do I see this error?
    ------------------------------
    This is a protection mechanism to prevent the root user from
executing user created files. The files may be altered, or
including malicious pieces of script.

    What can I do?
    --------------------
    Option 1) Check if a trusted user created the files (e.g. due
to using Git, Homebrew or similar).
              If you trust these files, you can decide to continue
this run by pressing ENTER.
```

```
    Option 2) Change ownership of the related files (or full
directory).

       Commands (full directory):
         # cd ..
         # chown -R 0:0 lynis
         # cd lynis
         # ./lynis audit system

[ Press ENTER to continue, or CTRL+C to cancel ]
```

Solo presione la tecla enter.

Copie la salida del resultado en un archivo llamado lynis-resultado-local.txt

Analice la salida y responda:

¿Qué Hardening index obtuvo?
¿Cuántos warnings?
¿Cuántas sugerencias?

Descargue ejercicio1.zip

Entre en el directorio donde lo haya descomprimido y ejecute:

```
chmod +x lab-manager.sh
./lab-manager.sh start
```

IMPORTANTE: NO ejecute el archivo vulnerabilizar en su máquina local.

Realice un escaneo de la “máquina virtual” que se crea.

¿Qué Hardening index obtuvo?
¿Cuántos warnings?
¿Cuántas sugerencias?

Utilizando las referencias que provee lynis, google, etc, intente solucionar los warnings, y algunas sugerencias. Documente detalladamente los comandos utilizados.

Tenga en cuenta de que no se puede apagar el firewall y que debe existir una regla que bloquee las conexiones entrantes de telnet, compruebe que esto sea así, caso contrario cree la regla y fíjese si lynis la marca como solución. ¿Por qué ocurre eso? ¿A algún otro de los warning le pasa lo mismo? ¿Se pueden arreglar todas las sugerencias?

Nota: **NO** puede modificar la imagen.

Documente detalladamente los comandos utilizados. Verifique con escaneos que los problemas desaparecen, se espera que no haya warnings (si es que fuera posible) y un hardening index de al menos 65.

Parte 2 - Analizadores de código estático.

Secrets en el código

Trivy vs. Trufflehog

Instale trivy y trufflehog. Se recomienda docker.

Baje el siguiente .zip.

Nota: NO es necesario hacer un build del docker-compose.yml, ambas herramientas trabajan analizando el código fuente.

Busque **solo secretos** utilizando trivy y trufflehog

¿Cuál encontró más secretos? ¿Cuál le parece que es mejor? Justifique.

Vulnerabilidades en las dependencias

Investigue cómo utilizar trivy, para analizar vulnerabilidades en el archivo requeriments.txt que está en el repositorio. Luego trate de solucionarlas y vuelva a realizar un escaneo, ¿se soluciono todo?

Desarrolle los conceptos de major, minor y bug fix y explique porque no siempre es posible actualizar a la última versión.

Hardening

Investigue cómo utilizar trivy para analizar un Dockerfile, utilícelo en el Dockerfile que hay en el repositorio, si encuentra cosas que no estén bien configuradas,

modifiquelo hasta que no encuentre nada.

Parte 3 - “Pentesting” de un ejecutable

Descargue el archivo: Sap.zip

Dentro del cual hay un ejecutable de windows y el código fuente correspondiente en python. No es malware, pero puede instalar una máquina virtual de windows, para ejecutarlo.

Tareas:

Describir qué hace el programa, ya sea vía la ejecución del archivo o analizando el código fuente. Ignore los mensajes sobre la VPN y la autenticación, tampoco es muy relevante saber qué es y que hace SAP.

Encontrar vulnerabilidades en el ejecutable, que afecten a la máquina donde se está ejecutando y aunque no lo podamos demostrar al servidor.

Utilizando el documento: Informe pentest realizar un informe que documente los hallazgos encontrados.

4. Análisis y reflexión sobre normativas

En este punto deberán recuperar el código **GDPR** **(General Data Protection Regulation – UE)** y realizar un análisis crítico, teniendo en cuenta las siguientes condiciones:

- Identificar y seleccionar **diez artículos** del GDPR que consideren directamente relevantes para el **abordaje y la gestión de la ciberseguridad** en una organización.
- Deberán argumentar detalladamente la elección de cada artículo, explicando cómo su cumplimiento impacta o moldea las políticas y prácticas de seguridad de la información (ej., en relación con el cifrado, el manejo de incidentes o el diseño de sistemas).
- Elaborar una crítica fundamentada sobre los puntos débiles o las limitaciones, que consideren del GDPR en relación con los desafíos actuales de la ciberseguridad (ej., tecnologías emergentes, *big data*, o la aplicación en contextos de ataque avanzado).