CY-302 Programación Avanzada

Entrega 2: Herramientas base

Proyecto: Red Team vs Blue Team en Azure

Docente: Andrés Vargas

Estudiantes:

- Eduardo Jiménez Bonilla
- Andrés Alonso Obando Fallas
- Daniel Vargas
- Victoria Arguedas Chacón
- Fabricio Calderón Medrano
- Jose Castillo

Fecha: 19 de noviembre de 2025

Repositorio: https://github.com/fxbricm/proyecto_ciberseguridad/tree/main

Contenido

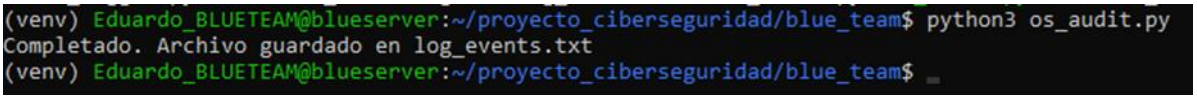
Roles por equipo (Blue / Red)

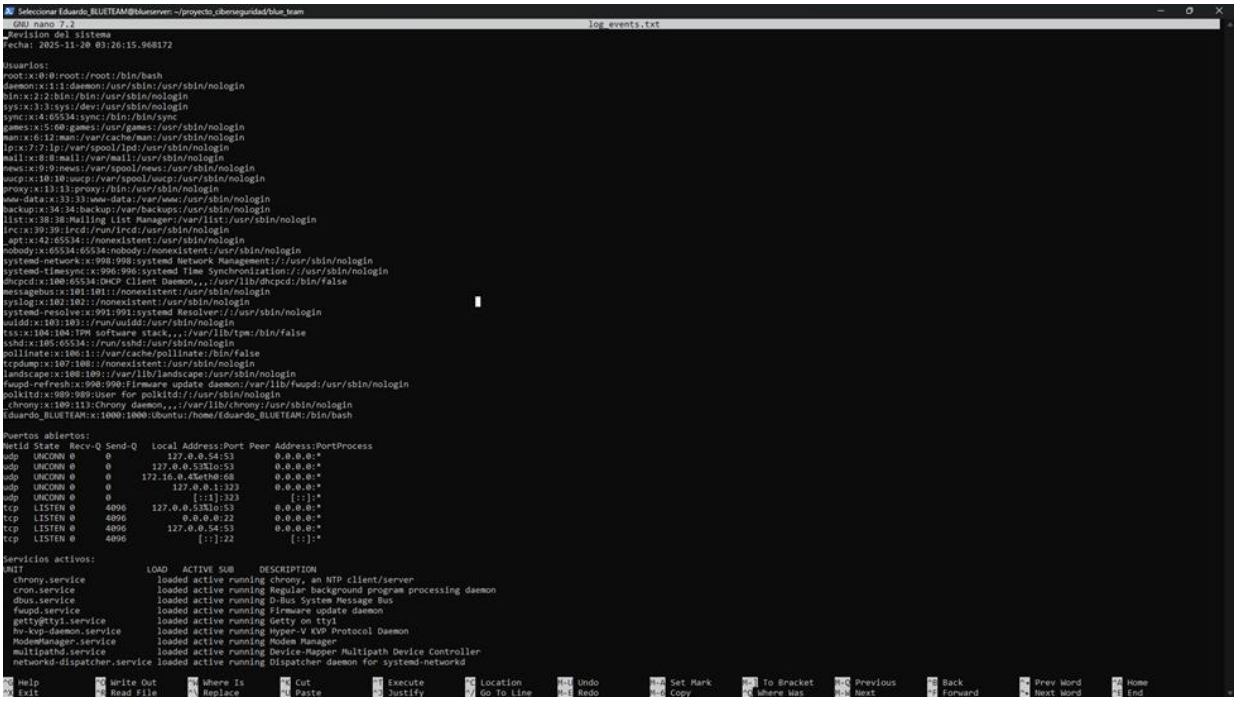
- Red_team/scanner.py (Nmap con flags básicos: -sS, -sV, -Pn) y salida guardada.
- Blue_team/os_audit.py (usuarios, puertos abiertos, servicios) + blue_team/log_events.txt.

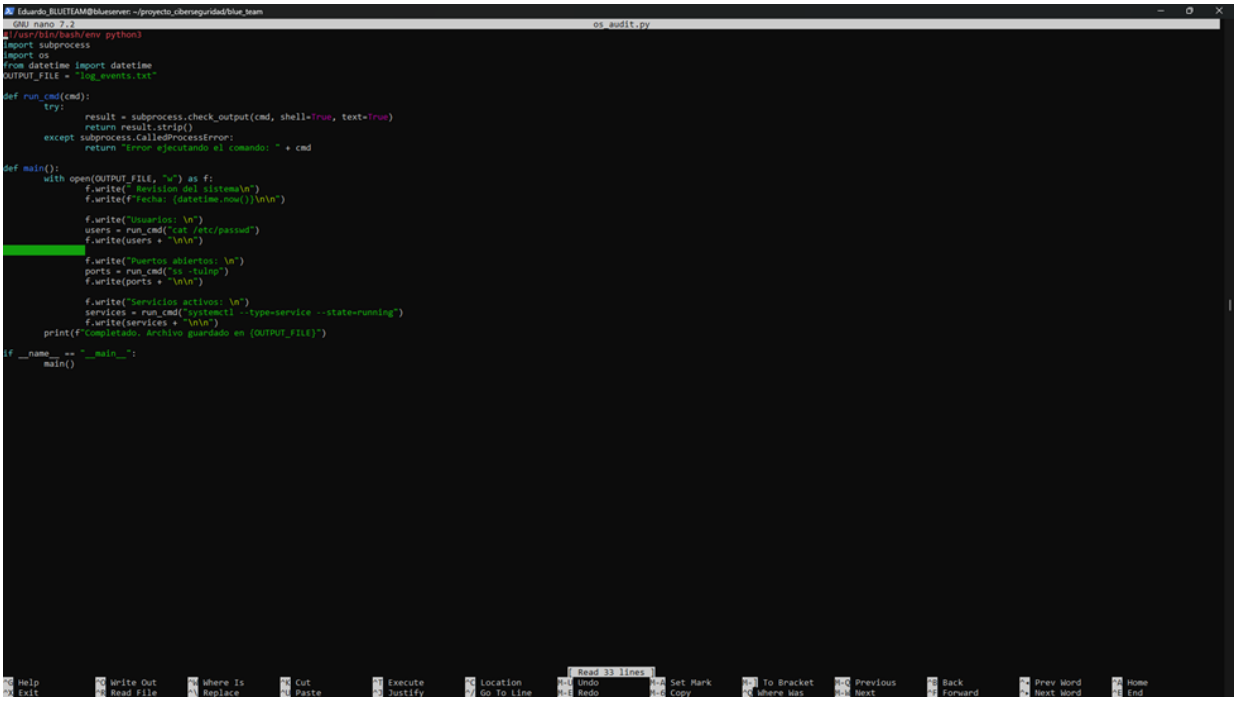
Blue team script

Para ejecutar el script del Blue Team, primero se debe acceder a la máquina virtual en Azure mediante SSH y dirigirse al directorio donde se encuentra la carpeta blue_team. Una vez dentro, se confirma que el archivo os_audit.py esté presente y, se le otorgan permisos de ejecución con chmod +x os_audit.py Luego, el script se ejecuta utilizando el comando python3 os_audit.py, lo que generará automáticamente el archivo log_events.txt dentro del mismo directorio. Finalmente, se revisa el contenido de ese archivo con cat log_events.txt.

Capturas de evidencia Blue_team:







Red team script

Para ejecutar el script del Red Team, es necesario tener instalado Python y Nmap. Para empezar, se abre la terminal del dispositivo en el que se encuentra,. Luego, se dirige al directorio donde esta el documento scanner.py y se ejecuta lo siguiente:

1. En Windows: sudo python scanner.py
2. En MacOs/Linux: sudo python3 scanner.py

- Ambos van a solicitor la contraseña de tu dispositivo, debido a que se esta ejecutando con permisos sudo.

Esto generará una carpeta llamada “results” en la que se encuentran todos los archivos .txt de los escaneos con la fecha y hora incluidas en el nombre del archivo.

Capturas de Evidencia