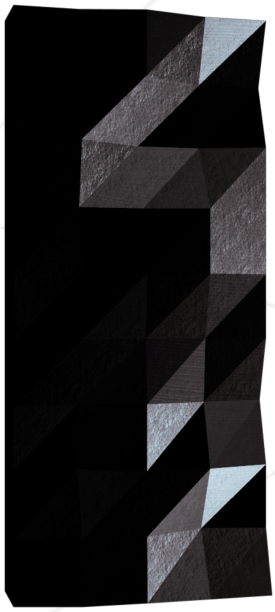

Bootcamp Ciberseguridad | 42 Madrid

Iron Dome

Resumen: Más vale prevenir que curar.

Versión: 1

Índice general

Capítulo I

Introducción

Esta es la segunda parte de los proyectos sobre ransomware. En esta parte, desarrollarás una herramienta específica que detectará actividad anómala monitorizando diferentes parámetros del sistema operativo.

Desgraciadamente, no hay una forma totalmente efectiva de prevenir un ataque de ransomware, pero con este proyecto podrás entender los puntos débiles de un sistema informático de cara a este tipo de infecciones.

Capítulo II

Parte Obligatoria

Crearás un programa llamado `irondome` que cumpla con las siguientes especificaciones.

- El programa se ejecutará en segundo plano como un "daemon.º servicio.
- El programa solo funcionará si es ejecutado por el usuario root.
- El programa monitorizará una zona crítica de manera perpetua. Dicha ruta se deberá indicar como argumento.
- En caso de indicarse más de un argumento, estos corresponderán a las extensiones de archivo a observar. De lo contrario, se monitorizarán todos los archivos.
- El programa detectará abusos en la lectura de disco.
- El programa detectará el uso intensivo de actividad criptográfica.
- El programa detectará cambios en la entropía de los archivos.
- El programa nunca deberá superar los 100 MB de memoria en uso.

Todas las alertas deberán reportarse en el archivo /var/log/irondome/irondome.log.

Capítulo III

Parte Bonus

La evaluación de los bonus se hará `SI Y SOLO SI` la parte obligatoria es `PERFECTA`. De lo contrario, los bonus serán totalmente `IGNORADOS`.

Puedes mejorar tu proyecto con las siguientes características:

- El programa creará una carpeta `backup` en el directorio HOME del usuario y realiza copias de seguridad incrementables en intervalos configurables.

Capítulo IV

Evaluación por pares

Este proyecto será corregido por tus compañeros. Entrega los archivos en el repositorio Git y asegúrate de que todo funciona como se espera.