

Seguridad y Auditoría Informática

# Unidad 4 - Gestión de Malware y Respuesta a Incidentes

Guia de trabajos prácticos 4

| Ing. Fernando Boiero | Año 2024 |
| --- | --- |

Tabla de Contenidos

[**Unidad 4 - Gestión de Malware y Respuesta a Incidentes 1**](#_heading=h.cfqubuy74qsf)

[**Unidad 4 - Gestión de Malware y Respuesta a Incidentes 3**](#_heading=h.309bl4l03l1t)

[Objetivos Generales 3](#_heading=h.4dbwm3gd23zv)

[Actividades Prácticas 3](#_heading=h.qyixno17mzwi)

[Actividad 1: Identificación y Clasificación de Malware 3](#_heading=h.bi2si74lvh26)

[Respuestas Actividad 1: 5](#_heading=h.2vm84o4dp7vq)

[Tipos de malware 5](#_heading=h.2t9u8za5xy38)

[Recomendaciones de mitigación 6](#_heading=h.i1x50ujsjzo5)

[Informe 8](#_heading=h.kj10kx2v3a7k)

[Actividad 2: Análisis de Malware y Respuesta a Incidentes 9](#_heading=h.x2g6niev62r9)

[Objetivos 9](#_heading=h.nvorxt1ijp52)

[Paso 1: Preparación del Entorno de Análisis 9](#_heading=h.pnx05nxt0hu7)

[Paso 2: Simulación de Ataques 9](#_heading=h.5rg9vx4j6dsm)

[Paso 3: Respuesta a Incidentes 10](#_heading=h.a7u55ih308ze)

[Paso 4: Documentación 10](#_heading=h.6fo318fc3e29)

[Respuestas Actividad 2: 12](#_heading=h.9krvayt27s47)

[Informe 12](#_heading=h.cpnqnfuwjkh7)

[Actividad 3: Evaluación de Herramientas de Monitoreo y Detección de Intrusiones 18](#_heading=h.55d2iuaaarc)

[Objetivos 18](#_heading=h.77tkcr9ee0qm)

[Paso 1: Investigación de Herramientas 18](#_heading=h.wef9awv91rvt)

[Paso 2: Pruebas Prácticas 18](#_heading=h.8zjbrzoc7iha)

[Paso 3: Análisis y Comparación 19](#_heading=h.ar95r4xyk89x)

[Paso 4: Informe Final 19](#_heading=h.hrht8lyoap20)

[Informe 20](#_heading=h.bqxcjwsxcn5l)

[**Referencias Bibliográficas y Recursos 26**](#_heading=h.hq99sre375nw)

[Actividad 1: Identificación y Clasificación de Malware 26](#_heading=h.n34hr8cytv6r)

[Materiales Necesarios 26](#_heading=h.6v04nmha9cj2)

[Recursos Adicionales 26](#_heading=h.af7d7xe4kcz6)

[Actividad 2: Análisis de Malware y Respuesta a Incidentes 26](#_heading=h.e95hno3vj5wr)

[Materiales Necesarios 26](#_heading=h.9i1qoxk9z4lr)

[Recursos Adicionales 26](#_heading=h.vwf6s26hippm)

[Actividad 3: Evaluación de Herramientas de Monitoreo y Detección de Intrusiones 27](#_heading=h.gv1ou7wmehdb)

[Materiales Necesarios 27](#_heading=h.mv6lwuzi71iv)

[Recursos Adicionales 27](#_heading=h.y9jvnv48m8y0)

[**Documento Teórico: Definición y Tipos de Malware 27**](#_heading=h.gjdgxs)

[Introducción 28](#_heading=h.qa455lgehqz7)

[Definición de Malware 28](#_heading=h.nnasdyuiyb8u)

[Tipos de Malware 28](#_heading=h.eq5g4g4ce3lw)

[1. Virus 28](#_heading=h.7bcqhi8g5c3d)

[2. Gusanos 28](#_heading=h.hsbnfrq5eocv)

[3. Troyanos 29](#_heading=h.8eg6f4ehruov)

[4. Ransomware 29](#_heading=h.z9r28s32hy1m)

[5. Spyware 29](#_heading=h.wbr074y2udql)

[6. Rootkits 29](#_heading=h.3m0aampkv6rt)

Guía de Trabajos Prácticos 4

# Unidad 4 - Gestión de Malware y Respuesta a Incidentes

## Objetivos Generales

1. Identificar y clasificar diferentes tipos de malware para comprender mejor su impacto en la seguridad de los sistemas informáticos.
2. Aplicar técnicas de análisis de malware para investigar y entender su comportamiento, lo que ayuda en la creación de estrategias de mitigación efectivas.
3. Evaluar y utilizar herramientas de monitoreo y detección de intrusiones para fortalecer las defensas de las infraestructuras de TI.

## Actividades Prácticas

## Actividad 1: Identificación y Clasificación de Malware

#### Objetivos Específicos

* Aprender a identificar diferentes tipos de malware, incluyendo virus, troyanos, ransomware y rootkits, que son los más comunes y perjudiciales en el ámbito de la seguridad informática.
* Comprender las características distintivas y los métodos de propagación de cada tipo de malware para mejorar las tácticas de prevención y respuesta.

#### Pasos Detallados

1. Estudio Teórico:
   * Objetivo: Adquirir conocimientos fundamentales sobre los diferentes tipos de malware y sus mecanismos de acción mediante la lectura de material académico específico.
   * Recursos: Se recomienda leer los capítulos 1 y 2 de "Practical Malware Analysis" de Michael Sikorski y Andrew Honig. Estos capítulos proporcionan una introducción exhaustiva a los conceptos básicos de malware, incluyendo definiciones, categorías, y ejemplos prácticos de código malicioso.
   * Actividad: Tomar notas detalladas sobre las características y tácticas de cada tipo de malware discutido en los capítulos para usar en el análisis posterior.
2. Análisis de Muestras:
   * Objetivo: Aplicar el conocimiento teórico en un entorno práctico mediante la análisis de muestras reales de malware.
   * Herramientas:
     + VirusTotal: Un servicio en línea que analiza archivos sospechosos y URLs facilitando la identificación rápida de virus, gusanos, troyanos y todo tipo de malware detectado por motores antivirus. [VirusTotal](https://www.virustotal.com/)
     + Cuckoo Sandbox: Una solución automatizada que ejecuta y analiza archivos sospechosos en un entorno seguro para observar su comportamiento y las interacciones con el sistema. [Cuckoo Sandbox](https://cuckoosandbox.org/)
   * Actividad: Seleccionar y descargar muestras de malware de repositorios reconocidos o utilizar ejemplos proporcionados en el laboratorio. Analizar estas muestras utilizando las herramientas mencionadas, observando cómo se comportan y qué sistemas o archivos intentan modificar o dañar.
3. Reporte:
   * Objetivo: Documentar y clasificar las muestras de malware analizadas, proporcionando una referencia útil para futuras investigaciones o para mejorar las políticas de seguridad.
   * Contenido del Reporte:
     + Descripción detallada de cada muestra de malware, incluyendo el tipo, mecanismo de infección, comportamiento observado y potencial impacto en los sistemas.
     + Capturas de pantalla del proceso de análisis y los resultados de las herramientas de análisis.
     + Conclusiones sobre el riesgo que representa cada tipo de malware y recomendaciones para su mitigación.
   * Formato: El reporte debe ser estructurado, claro y conciso, adecuado para ser compartido con colegas o como parte de una presentación académica.

## Respuestas Actividad 1

### Tipos de malware

**Backdoor:** Código malicioso que se instala en un ordenador para permitir el acceso al atacante. Las puertas traseras suelen permitir al atacante conectarse al ordenador con poca o ninguna autenticación y ejecutar comandos en el sistema local.

**Botnet**: Similar a un backdoor, en el sentido de que permite al atacante acceder al sistema, pero todos los ordenadores infectados con el mismo botnet reciben las mismas instrucciones de un único servidor de comando y control.

**Downloader:** Código malicioso que sólo existe para descargar otro código malicioso. Los atacantes suelen instalar los descargadores cuando acceden por primera vez a un sistema. El programa descargador descargará e instalará código malicioso adicional.

**Information-stealing malware:** Malware que recopila información del ordenador de la víctima y normalmente la envía al atacante. Algunos ejemplos son los sniffers, los capturadores de contraseñas y los keyloggers. Este malware suele utilizarse para obtener acceso a cuentas en línea, como las de correo electrónico o banca electrónica.

**Launcher:** Programa malicioso utilizado para lanzar otros programas maliciosos. Normalmente, los lanzadores utilizan técnicas no tradicionales para lanzar otros programas maliciosos con el fin de garantizar el sigilo o un mayor acceso a un sistema.

**Rootkit** Código malicioso diseñado para ocultar la existencia de otro código. Los rootkits suelen ir acompañados de otro malware, como una puerta trasera, para permitir el acceso remoto al atacante y dificultar la detección del código por parte de la víctima.

**Scareware** Malware diseñado para asustar al usuario infectado para que compre algo. Suele tener una interfaz de usuario que lo hace parecer un antivirus u otro programa de seguridad. Informa a los usuarios de que hay código malicioso en su sistema y que la única forma de deshacerse de él es comprar su "software", cuando en realidad el software que vende no hace más que eliminar el scareware.

**Spam-sending malware:** Malware que infecta la máquina de un usuario y luego la utiliza para enviar spam. Este malware genera ingresos para los atacantes al permitirles vender servicios de envío de spam.

**Worm or virus:** Código malicioso que puede copiarse a sí mismo e infectar otros ordenadores.

### Recomendaciones de mitigación

**Backdoor**

* Instalar y mantener actualizado un software antivirus y antimalware.
* Implementar firewalls para bloquear accesos no autorizados.
* Usar sistemas de detección de intrusos para identificar y bloquear actividades sospechosas.
* Limitar los privilegios de usuario en las máquinas para reducir el alcance de lo que puede hacer un atacante.
* Realizar auditorías de seguridad regulares para detectar posibles puertas traseras.

**Botnet**

* Utilizar soluciones de seguridad que puedan identificar y bloquear tráfico relacionado con botnets.
* Mantener los sistemas operativos y aplicaciones actualizados para evitar vulnerabilidades.
* Capacitar a los usuarios sobre los riesgos de hacer clic en enlaces o descargar archivos de fuentes desconocidas.
* Monitorear continuamente el tráfico de red para detectar patrones inusuales que puedan indicar actividad de botnet.

**Downloader**

* Implementar soluciones de seguridad con capacidad para detectar y bloquear descargas maliciosas en tiempo real.
* Restringir el acceso a sitios web sospechosos o no seguros mediante el uso de filtros web.
* Asegurarse de que todos los software estén actualizados, incluidos los navegadores y sus plugins.

**Information-stealing malware**

* Utilizar soluciones de seguridad que ofrezcan protección contra programas de robo de información.
* Encriptar los datos sensibles almacenados en los dispositivos para minimizar el daño en caso de robo.
* Capacitar a los usuarios sobre la importancia de usar contraseñas fuertes y no repetirlas en diferentes servicios.

**Launcher**

* Usar software de seguridad que pueda detectar y bloquear actividades sospechosas, incluidos los lanzadores de malware.
* Aplicar el principio de menor privilegio a todas las cuentas de usuario para limitar qué programas pueden ejecutar.
* Verificar regularmente la integridad de los archivos del sistema para detectar cambios no autorizados.

**Rootkit**

* Utilizar herramientas específicas para la detección de rootkits, las cuales pueden identificar modificaciones a nivel del sistema operativo.
* Realizar escaneos de seguridad regulares, especialmente con herramientas capaces de arrancar desde medios externos y escanear el sistema sin iniciar el sistema operativo comprometido.
* Mantener los sistemas actualizados y aplicar parches de seguridad tan pronto como estén disponibles.

**Scareware**

* Educar a los usuarios para que reconozcan las tácticas de intimidación típicas de los scareware.
* Instalar y mantener actualizado un software antivirus legítimo.
* Ignorar y cerrar pop-ups que afirmen haber detectado malware y que soliciten pagos para la limpieza.

**Spam-sending malware**

* Utilizar software antimalware que incluya protección contra malware que envía spam.
* Configurar el servidor de correo electrónico para bloquear la salida de correos masivos no autorizados.
* Monitorizar las cuentas de correo para detectar envíos anormales de correos.

**Worm or virus**

* Implementar soluciones antivirus y antimalware con protección en tiempo real.
* Usar firewalls personales y de red para bloquear conexiones no autorizadas.
* Realizar copias de seguridad regulares de los datos para poder restaurar los sistemas en caso de infección.

### 

### Informe

Datos del malware

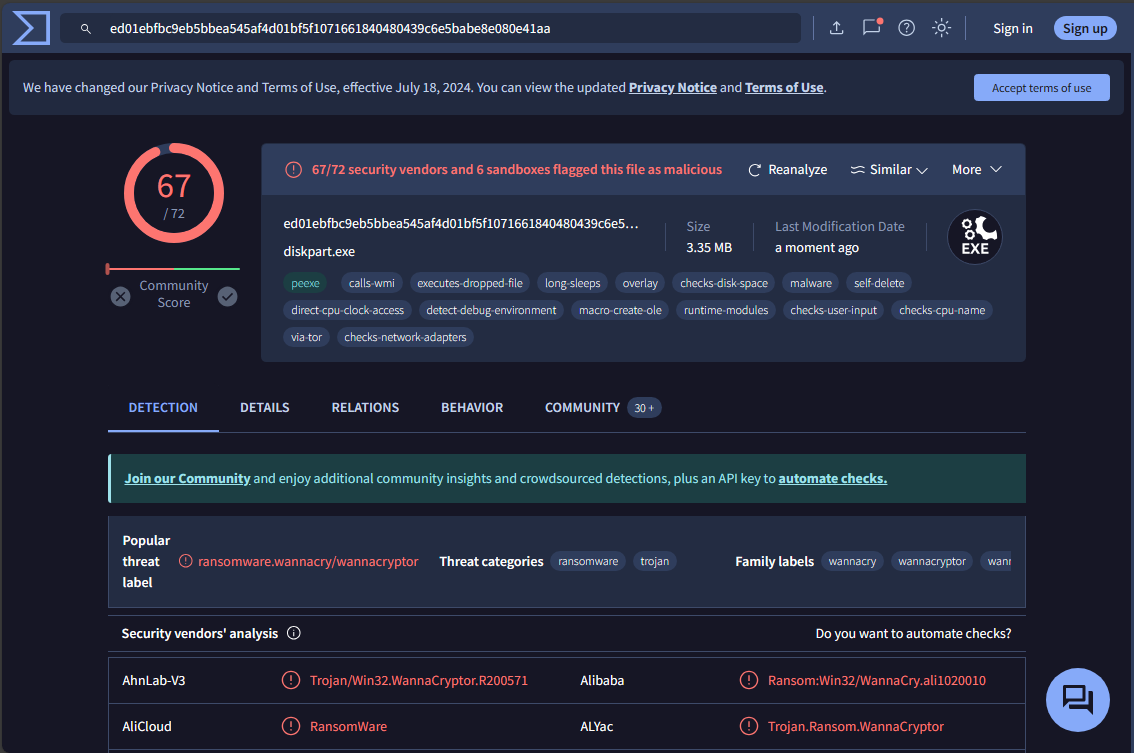
* Nombre del archivo: WannaCry
* Tipo de malware: Ransomware
* Sistema operativo: Windows
* <https://github.com/limiteci/WannaCry/blob/main/WannaCry.EXE>

Objetivo

El objetivo de este malware “WannaCry” es encriptar tus archivos y pedir un rescate para desencriptarlos. Una vez ejecutado el “.exe” podremos observar que el fondo de pantalla cambia dando un aviso, a tus archivos se le agrega una extensión “.wnry” y luego te abrirá una ventana con una dirección para transferir 300 USD en BTC para el rescate.

Proceso

Primero descargamos el malware. Posteriormente analizaremos el malware con VirusTotal.



Podemos ver que 67 de 72 proveedores de seguridad detectaron este archivo como un malware de tipo RansomWare. Es decir 5 no sirven.

## Actividad 2: Análisis de Malware y Respuesta a Incidentes

### Objetivos

* Desarrollar habilidades avanzadas en el análisis técnico de malware.
* Aprender a implementar procedimientos de respuesta a incidentes de manera efectiva para mitigar amenazas y restaurar la seguridad.

### Paso 1: Preparación del Entorno de Análisis

#### Objetivos Específicos

* Configurar un entorno controlado y seguro que permita analizar el malware sin riesgo para los sistemas de red o de producción real.

#### Actividades

1. Selección de la Herramienta de Virtualización:
   * Elegir entre VMware y VirtualBox como plataforma para crear máquinas virtuales (VMs). Ambas herramientas son robustas y soportan múltiples configuraciones de red y de sistema.
   * Instalar y configurar el software de virtualización en una máquina host segura.
2. Configuración de la Máquina Virtual:
   * Instalar un sistema operativo adecuado en la VM, como Windows o Linux, dependiendo de la compatibilidad con el malware a analizar.
   * Asegurarse de que la VM esté aislada de la red corporativa o personal para evitar la propagación del malware.
3. Preparación de Herramientas de Análisis:
   * Instalar y configurar herramientas de análisis de malware como OllyDbg, X64Dbg, y Wireshark en la VM.
   * Configurar snapshots o puntos de restauración en la VM para facilitar la recuperación rápida del sistema entre análisis.

### Paso 2: Simulación de Ataques

#### Objetivos Específicos

* Observar cómo interactúa el malware con el sistema operativo y otros programas instalados.
* Identificar las técnicas y vectores de ataque utilizados por el malware.

#### Actividades

1. Introducción de Malware:
   * Obtener muestras de malware de fuentes confiables y seguras como repositorios académicos o bases de datos de análisis de malware.
   * Ejecutar el malware en la VM bajo condiciones controladas.
2. Monitoreo y Análisis:
   * Utilizar OllyDbg o X64Dbg para monitorear el comportamiento del malware en tiempo real, observando cambios en archivos, registros del sistema y comunicaciones de red.
   * Aplicar técnicas de análisis dinámico para ver cómo el malware interactúa con el sistema operativo, cómo se manejan las excepciones y cómo se realizan las llamadas al sistema.

### Paso 3: Respuesta a Incidentes

#### Objetivos Específicos

* Aplicar un protocolo efectivo de respuesta a incidentes para contener y mitigar el malware.
* Restaurar el sistema a un estado seguro y operativo.

#### Actividades

1. Implementación de Procedimientos de Respuesta:
   * Seguir las guías del NIST y otros estándares relevantes para contener la infección y evitar su propagación.
   * Utilizar herramientas de remoción de malware y técnicas de aislamiento de red para eliminar o neutralizar el impacto del malware.
2. Recuperación y Mitigación:
   * Restaurar los sistemas afectados utilizando los snapshots creados anteriormente.
   * Evaluar la necesidad de fortalecer las políticas de seguridad y actualizar las soluciones de antivirus y anti-malware.

### Paso 4: Documentación

#### Objetivos Específicos

* Registrar todas las observaciones, acciones y resultados para mejorar las futuras respuestas a incidentes.

#### Actividades

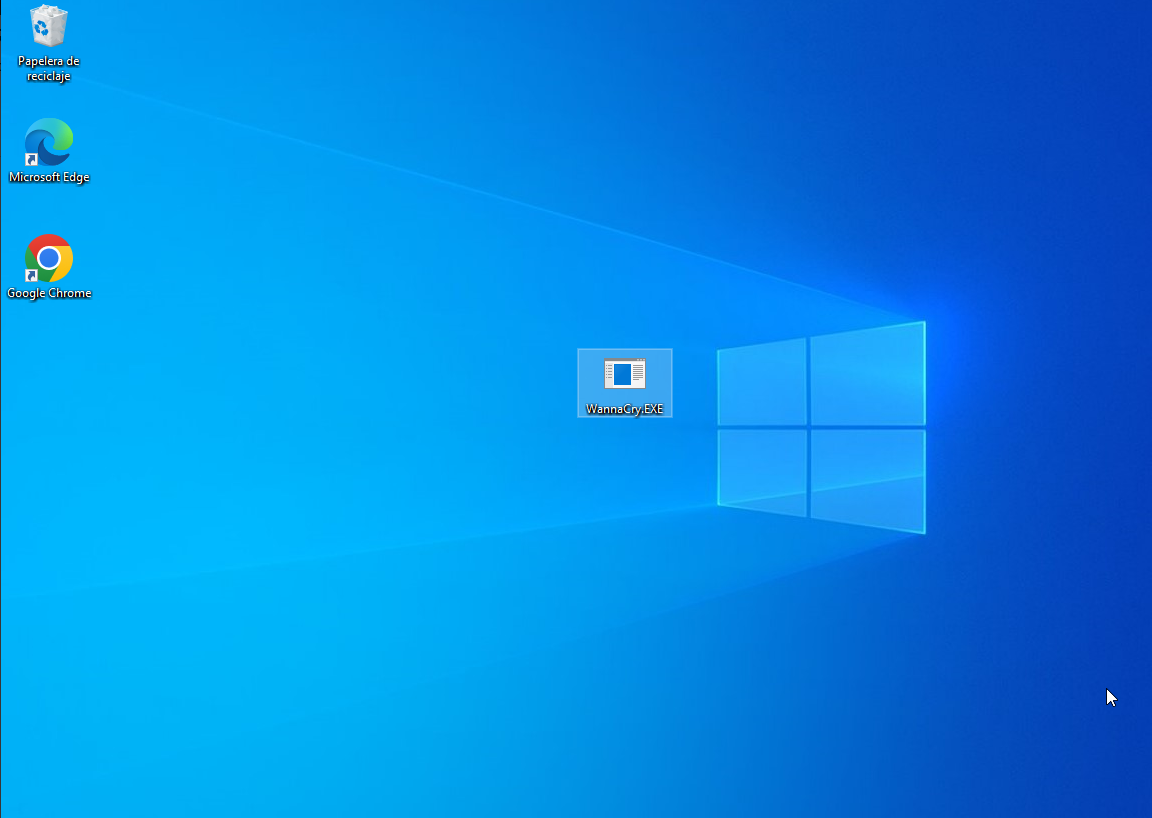
1. Redacción de un Informe Detallado:
   * Documentar el proceso de análisis, los hallazgos, las acciones tomadas y las lecciones aprendidas.
   * Incluir detalles técnicos y recomendaciones para prevenir futuros incidentes similares.
2. Revisión y Aprendizaje:
   * Revisar el informe con supervisores o colegas para obtener feedback.
   * Implementar mejoras en las prácticas de seguridad basadas en las conclusiones del informe.

## Respuestas Actividad 2

### Informe

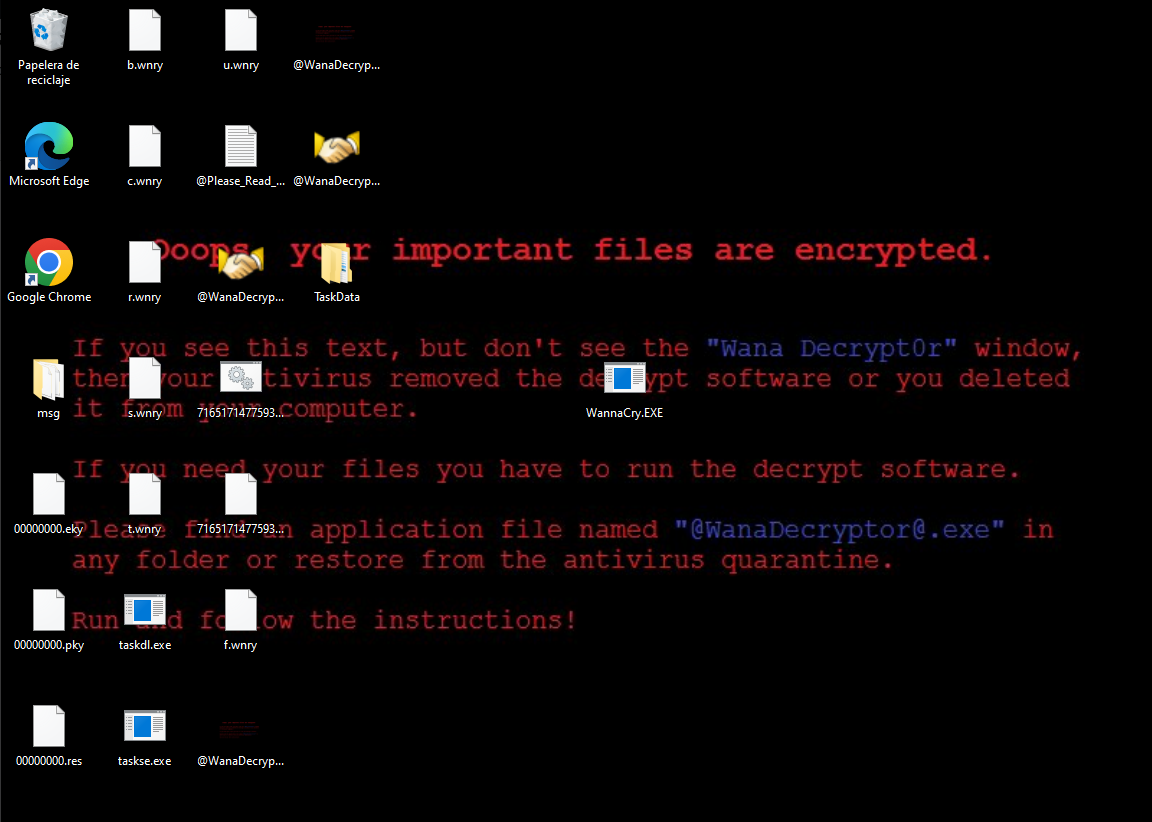
Descarga del malware

Para esta actividad utilizaremos el mismo malware utilizado en la actividad anterior, “Wannacry”. Para poder instalarlo tuvimos que desactivar las opciones de seguridad del navegador, debido a que estos lo detectan como un malware y no permiten su descarga.



Ejecución

Para ejecutar este ransomware tuvimos que desactivar las funciones de seguridad de windows, ya que estos detectaban el archivo como malicioso y no permitian su ejecución.



Analisis

Después de la activación del ransomware, el fondo de pantalla se modifica para mostrar un mensaje de advertencia. Además, todos tus archivos se renombran con la extensión ".wnry", lo que indica que han sido cifrados. Para recuperar el acceso, se abre automáticamente una ventana que persiste incluso después de ser cerrada repetidamente. Esta ventana proporciona instrucciones para pagar un rescate de 300 USD en Bitcoin (BTC). Este comportamiento del malware impide el acceso a cualquier archivo afectado, haciendo que la interacción normal con el sistema sea prácticamente imposible.

Adicionalmente, es importante destacar que pagar el rescate no garantiza la recuperación de los datos; los expertos en ciberseguridad y las autoridades suelen recomendar no cumplir con las demandas de los atacantes.

Recuperación y Mitigación

El Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos ofrece una serie de pautas y mejores prácticas para mitigar y responder a incidentes de ransomware. Aquí te detallo algunos de los principales pasos y estrategias recomendadas por NIST para la mitigación de ransomware:

* Preparación y prevención:

1. Actualizaciones de software: Mantener todos los sistemas operativos y aplicaciones actualizados es crucial para protegerse contra vulnerabilidades que los atacantes pueden explotar para instalar ransomware.
2. Control de acceso: Limitar los permisos de usuario solo a los necesarios para realizar tareas específicas puede prevenir la propagación de ransomware si un sistema se ve comprometido.
3. Segmentación de redes: Dividir las redes en segmentos para controlar mejor el acceso y limitar cómo el ransomware puede propagarse a través de la red.
4. Formación y concienciación de los empleados: Educar a los empleados sobre cómo reconocer intentos de phishing y otras tácticas comunes utilizadas para desplegar ransomware.

* Protección a través de soluciones tecnológicas:

1. Copia de seguridad de datos: Realizar copias de seguridad regulares y asegurarse de que estén almacenadas de manera segura, preferiblemente desconectadas de la red, para que no sean accesibles para el ransomware.
2. Antivirus y antimalware: Usar software de seguridad que incluya protección contra ransomware y configurar para actualizaciones automáticas y escaneos regulares.
3. Bloqueo de anuncios y gestión de macros: Desactivar las macros de documentos de Office y bloquear anuncios maliciosos puede reducir los vectores de ataque.

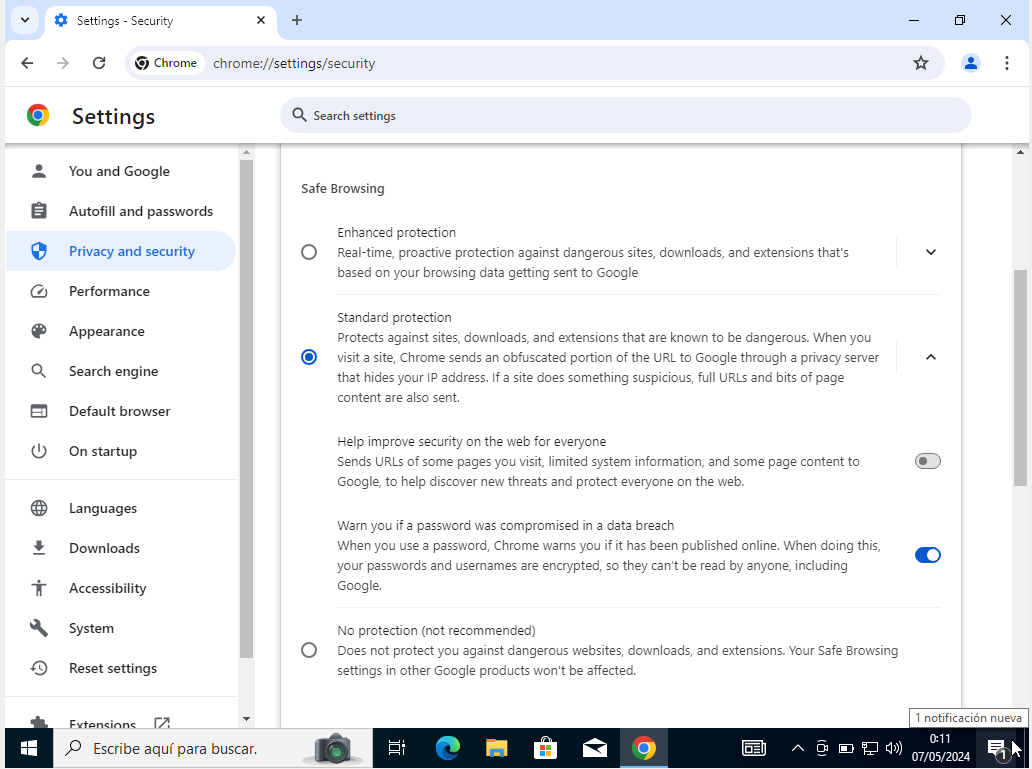
* Detección y respuesta:

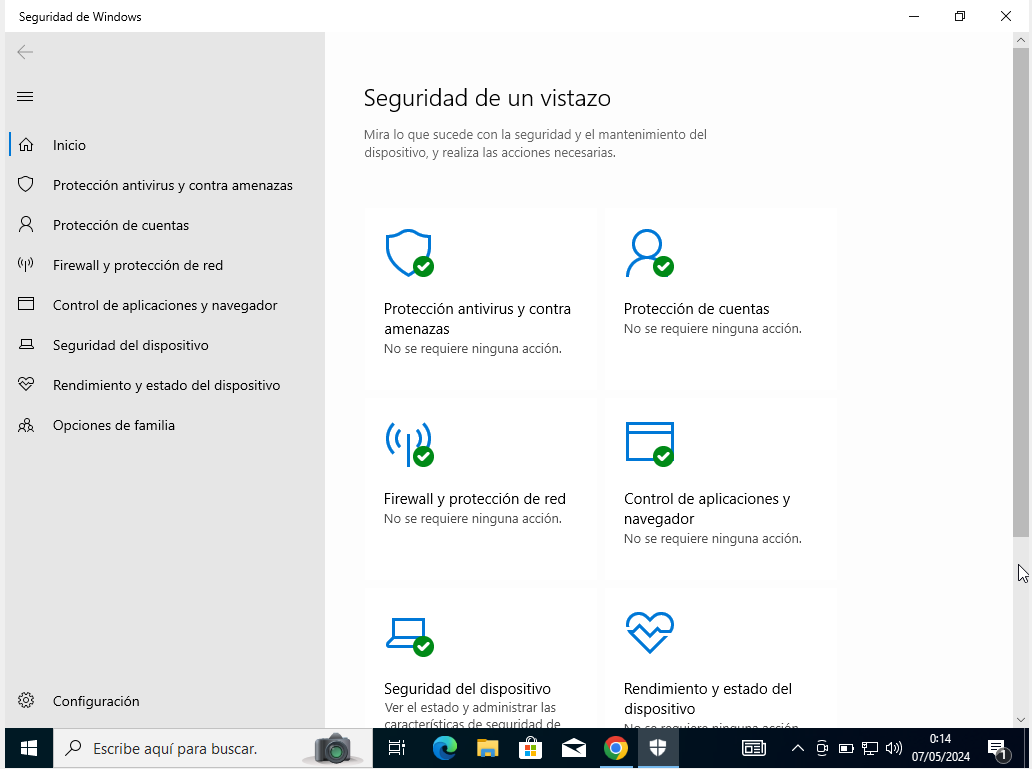
1. Herramientas de detección de intrusiones y comportamiento anómalo: Utilizar software que pueda detectar cambios inusuales en los archivos y comportamientos sospechosos en la red para alertar tempranamente sobre una posible infección de ransomware.
2. Planes de respuesta a incidentes: Desarrollar y ensayar un plan de respuesta a incidentes que incluya escenarios específicos de ransomware, asegurando que todos los actores clave conozcan sus roles y responsabilidades.

* Recuperación:

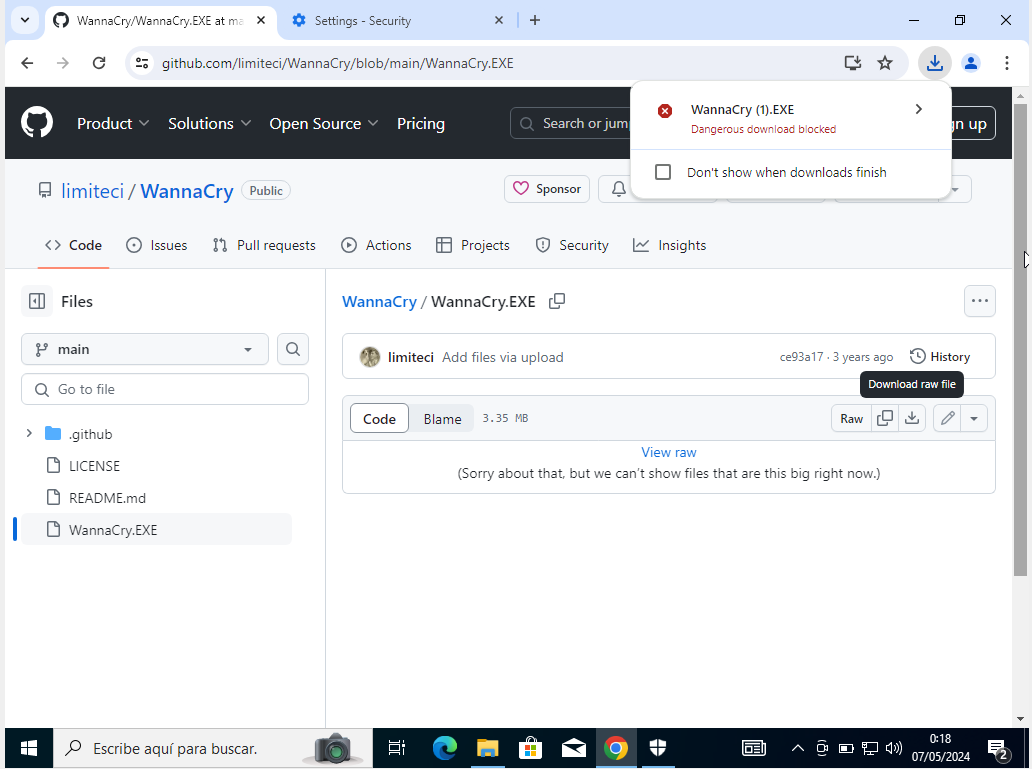
1. Restauración de datos: Utilizar las copias de seguridad para restaurar los datos cifrados sin necesidad de pagar el rescate.
2. Comunicación: Mantener líneas de comunicación claras tanto internamente como con clientes y partes externas para gestionar la percepción y las consecuencias del ataque.
3. Análisis post-incidente: Revisar y analizar el incidente para mejorar las medidas de seguridad y la respuesta a incidentes futuros.

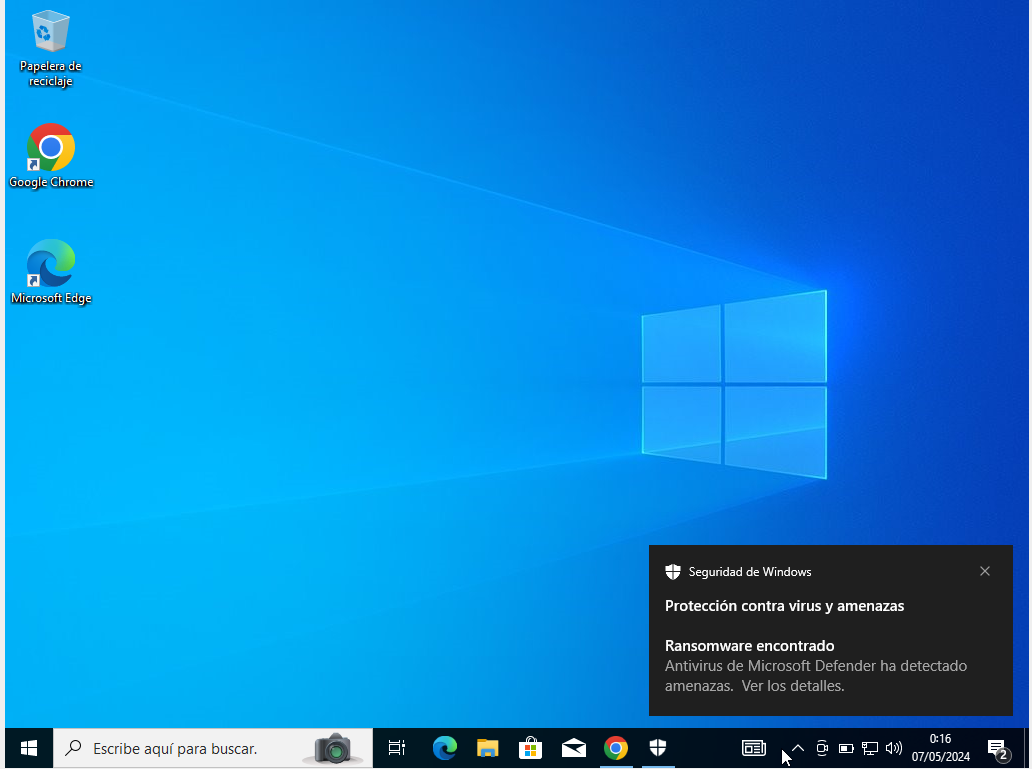
Antes de que se ejecutara el malware, habíamos creado una copia de seguridad en forma de snapshot. A partir de este punto de restauración, procedemos a reiniciar el sistema. Para prevenir cualquier propagación adicional del malware, hemos reactivado las medidas de seguridad de Windows y del navegador. Esto incluye la actualización y el fortalecimiento de los ajustes de seguridad para bloquear vulnerabilidades potenciales y evitar que el malware se reactive o se disemine.





Ahora podemos observar que tanto el navegador como windows no nos permiten descargar este archivo debido a que lo detectan como malware.





## Actividad 3: Evaluación de Herramientas de Monitoreo y Detección de Intrusiones

### Objetivos

* Profundizar en el conocimiento y manejo de diversas herramientas de monitoreo y detección de intrusiones.
* Evaluar la eficacia de estas herramientas para detectar y responder a actividades maliciosas en un entorno de red.

### Paso 1: Investigación de Herramientas

#### Objetivos Específicos

* Identificar y seleccionar herramientas relevantes que se utilizan comúnmente en la industria para la detección de intrusiones y el monitoreo de red.

#### Actividades

1. Revisión de Opciones:
   * Estudiar herramientas de detección de intrusiones de red (NIDS) como Snort, que analizan el tráfico de red en busca de patrones conocidos de comportamiento malicioso.
   * Investigar herramientas de detección de intrusiones basadas en host (HIDS) como OSSEC, que monitorean cambios en los archivos del sistema y los logs para detectar actividad sospechosa.
   * Explorar herramientas de análisis de protocolos como Wireshark, que permiten capturar y analizar paquetes de red en tiempo real.
2. Compilación de Recursos:
   * Recolectar documentación técnica, tutoriales, casos de uso y revisiones de cada herramienta para comprender mejor sus capacidades y limitaciones.
   * Contactar con expertos o participar en foros y seminarios web para recabar opiniones y experiencias de otros usuarios.

### Paso 2: Pruebas Prácticas

#### Objetivos Específicos

* Configurar y utilizar las herramientas seleccionadas en un entorno de prueba para evaluar su efectividad en la detección de actividades maliciosas.

#### Actividades

1. Configuración de la Red de Laboratorio:
   * Establecer una red de laboratorio que imite un entorno de red empresarial, incluyendo servidores, estaciones de trabajo y dispositivos de red.
   * Asegurar que la red esté aislada de la red principal para evitar interferencias y riesgos durante las pruebas.
2. Implementación de Herramientas:
   * Instalar y configurar cada herramienta en la red de laboratorio. Esto puede incluir la configuración de sensores Snort en puntos estratégicos de la red o la instalación de OSSEC en servidores y estaciones de trabajo.
3. Simulación de Ataques:
   * Generar tráfico de red malicioso, como escaneos de puertos, ataques de fuerza bruta o tráfico de malware, utilizando herramientas como Metasploit o scripts personalizados.
   * Monitorizar la respuesta de cada herramienta a estas intrusiones simuladas.

### Paso 3: Análisis y Comparación

#### Objetivos Específicos

* Analizar los datos recogidos durante las pruebas y comparar la efectividad de las herramientas en términos de precisión, tiempo de respuesta y facilidad de uso.

#### Actividades

1. Recopilación de Datos:
   * Recolectar logs y alertas generadas por las herramientas durante las simulaciones de ataque.
   * Documentar cualquier incidente de falso positivo o falso negativo, así como la capacidad de cada herramienta para identificar correctamente el tráfico malicioso.
2. Evaluación de Rendimiento:
   * Comparar cómo cada herramienta manejó los diferentes tipos de ataques en términos de rapidez de detección y precisión.
   * Evaluar la usabilidad y la gestión de configuraciones de cada herramienta para determinar su adecuación en un entorno empresarial.

### Paso 4: Informe Final

#### Objetivos Específicos

* Consolidar y presentar los hallazgos de la evaluación en un formato claro y profesional que pueda servir como referencia para decisiones futuras sobre herramientas de seguridad.

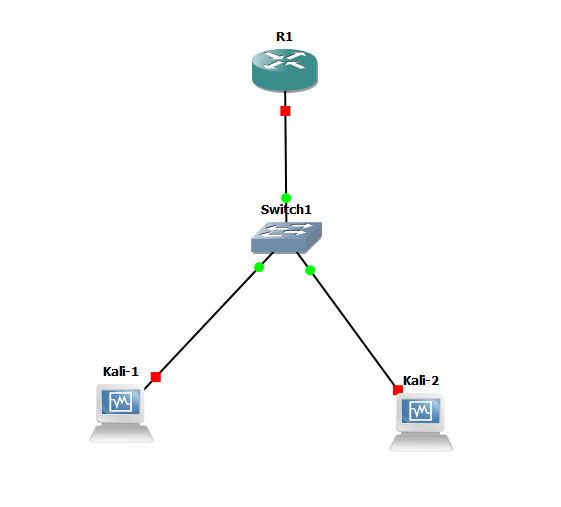
#### Actividades

1. Redacción del Informe:
   * Describir en detalle los procedimientos de configuración, las pruebas realizadas, los datos recopilados y los análisis realizados.
   * Presentar una comparación detallada que incluya las fortalezas y debilidades de cada herramienta, así como recomendaciones para su implementación.
2. Revisión y Mejoras:
   * Permitir que expertos en seguridad revisen el informe para obtener retroalimentación.
   * Ajustar el informe basándose en los comentarios recibidos para mejorar la claridad y la precisión.

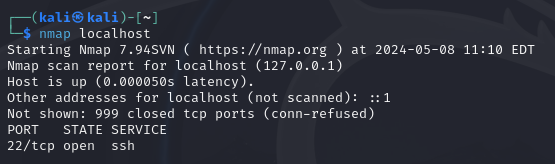
## Respuestas Actividad 3

Snort

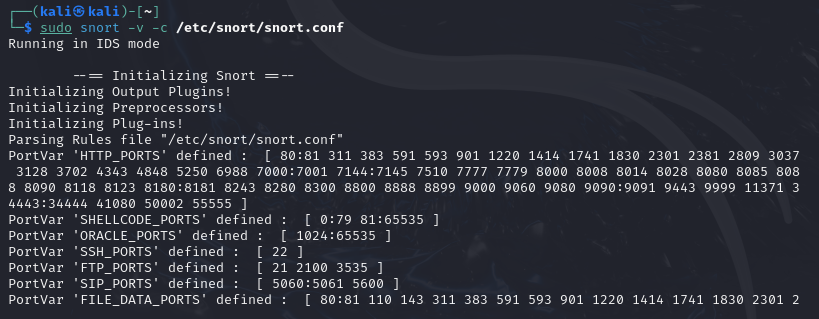
Red utilizada.



Primero levantamos un servicio ssh en el puerto 22 de la máquina virtual Kali-1.

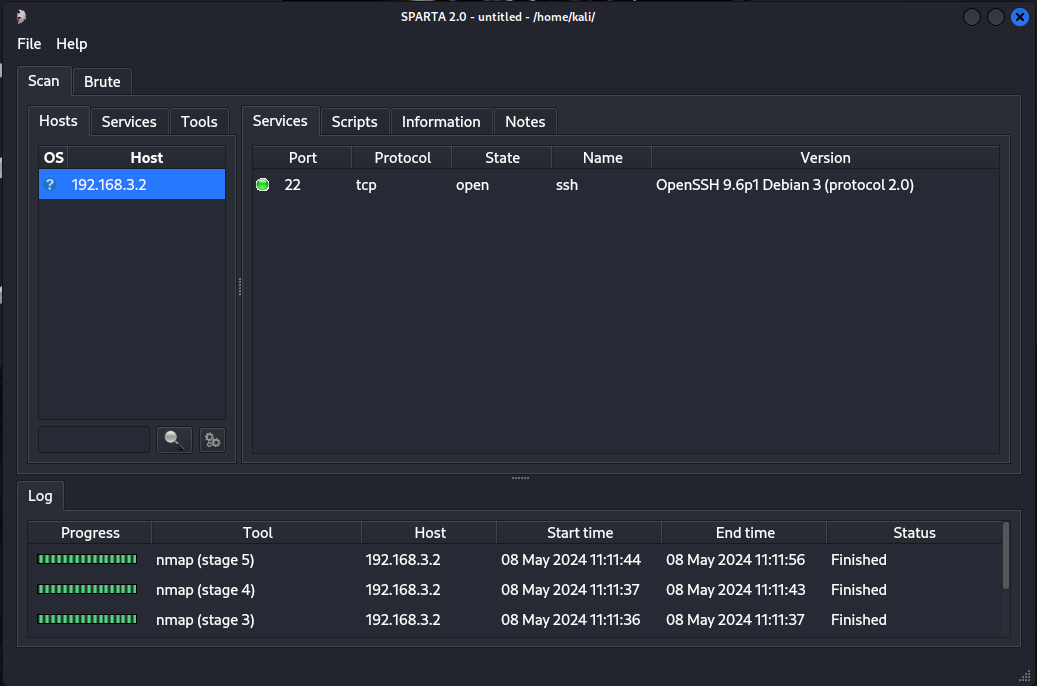


Posteriormente iniciaremos Snort con las configuraciones guardadas en “/etc/snort/snort.conf”

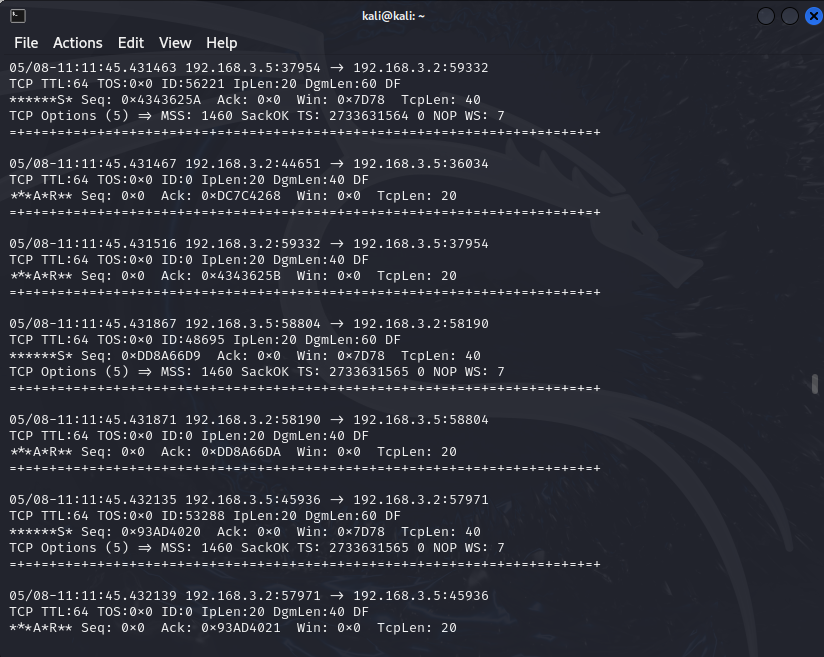


En la máquina virtual Kali-2 utilizaremos Sparta. Con esta herramienta analizaremos los puertos de Kali-1. Podemos observar que en el puerto 22 se encuentra levantado un servicio ssh como mencionamos anteriormente.

Sparta: Sparta en Kali Linux es una herramienta integral para la evaluación de seguridad de redes, que ayuda a los profesionales de seguridad a identificar y abordar vulnerabilidades potenciales en sistemas y redes. Integra Hydra y Nmap.



Podremos observar que Snort, desde Kali-1, ha detectado todas las solicitudes realizadas por Sparta para escanear los puertos. Esto podría indicar la presencia de un tercero que intenta analizar los puertos y los servicios levantados, posiblemente con intenciones de llevar a cabo un ataque.



También hemos empleado la funcionalidad Brute, que nos permite llevar a cabo ataques para evaluar la seguridad de contraseñas. Con esta herramienta, es posible enviar extensas listas de usuarios y contraseñas para su prueba, utilizando múltiples hilos simultáneamente. Para verificar si Snort lo detecta, hemos realizado una prueba directa utilizando las credenciales correctas.

# 

Podemos notar que Snort ha detectado las solicitudes al puerto 22, correspondiente al servicio SSH, lo que sugiere que alguien ha accedido al servicio. En este caso, la IP registrada es 192.168.3.5.

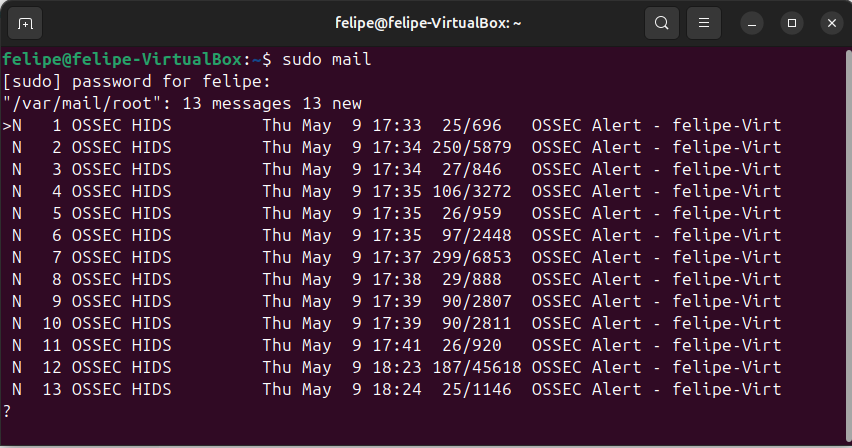
# 

OSSEC

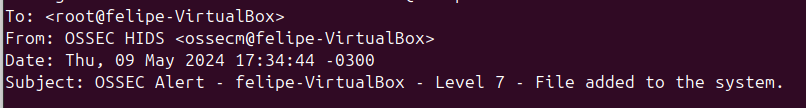
Instalamos y configuramos OSSEC.

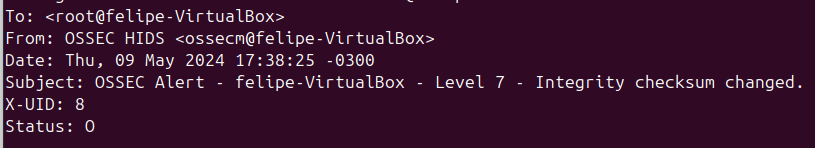
Una vez levantado el servicio de manera **local**, procedemos a modificar y/o borrar archivos que estén dentro del rango de directorios en el que está configurado el monitor de OSSEC.

Luego revisamos la casilla local de mailing, ya que configuramos OSSEC para que envíe las alertas por mail.



Abrimos dos de nivel 7 (nivel configurado para detectar alertas de tipo File Addition, Removal or Modification).

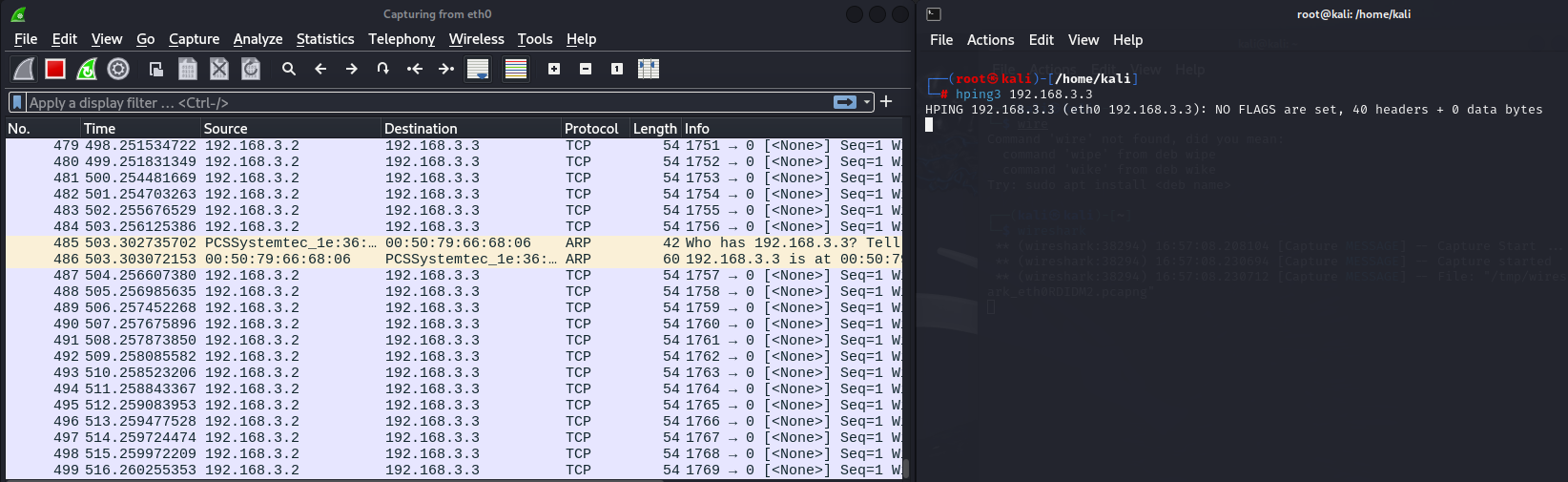




Como podemos ver OSSEC fue capaz de capturar un archivo nuevo agregado al sistema y que la integridad de un archivo cambió, es decir, que un archivo fue modificado.

Wireshark

Detección de un ataque DoS sin enmascaramiento de IP en tiempo real.



Comparación de herramientas

**Snort** es una de las herramientas más rápidas y precisas para la detección de ataques que implican tráfico de red específico. Gracias a su capacidad para analizar y reaccionar al tráfico en tiempo real, Snort es muy eficiente en la identificación de patrones de ataques, como intentos de intrusiones, anomalías en los protocolos, y otros comportamientos maliciosos que cruzan la red.

Esta herramienta utiliza un conjunto robusto de reglas que se actualizan constantemente para reconocer las últimas amenazas y vulnerabilidades, permitiendo a los administradores y sistemas de seguridad implementar respuestas casi inmediatas a actividades potencialmente dañinas. Además, Snort es flexible y puede ser configurado para funcionar en diversos entornos y escenarios, desde pequeñas redes hasta grandes infraestructuras corporativas.

**OSSEC** se utiliza primordialmente para monitorear y detectar cambios y actividades sospechosas directamente en los hosts. Se enfoca en la integridad de archivos, la detección de rootkits, y el análisis de registros, esto lo hace útil para identificar modificaciones no autorizadas y comportamientos anómalos en los sistemas. Es capaz de proporcionar una vigilancia detallada y continua de los sistemas operativos, aplicando comprobaciones de integridad que alertan a los administradores sobre cualquier alteración en los archivos críticos.

Esta herramienta también es muy efectiva en la monitorización de logs, permitiendo detectar patrones de ataques, como fuerza bruta contra servicios SSH o anormalidades en las autenticaciones de usuarios. Su capacidad para automatizar respuestas ante eventos detectados ayuda a mitigar rápidamente el impacto de los ataques, manteniendo así la seguridad y estabilidad del sistema. Su naturaleza de código abierto permite una personalización extensa para adaptarse a las necesidades específicas de cada entorno.

**Wireshark** ofrece una gran precisión en el análisis detallado del tráfico de red, proporcionando una visión en profundidad de cada paquete que atraviesa la red. Esta herramienta es fundamental para los analistas de seguridad y los administradores de red que necesitan realizar diagnósticos complejos o investigar actividades sospechosas a nivel de paquete.

Permite desglosar el tráfico a nivel de bits, ofreciendo una visibilidad completa de los protocolos y las conversaciones de red. Sin embargo, esta precisión tiene como contraparte la necesidad de un análisis manual intensivo, lo que puede ser un desafío en situaciones que requieren respuestas rápidas y automáticas. A pesar de esto, Wireshark es muy útil para el desarrollo y prueba de protocolos de red, donde la capacidad de inspeccionar detalladamente cada interacción en la red es crucial.

# 

# Referencias Bibliográficas y Recursos

## Actividad 1: Identificación y Clasificación de Malware

### Materiales Necesarios

* Software de Análisis:
  + VirusTotal (Acceso online gratuito): [VirusTotal](https://www.virustotal.com/)
  + Cuckoo Sandbox (Software de código abierto para análisis automático): [Cuckoo Sandbox](https://cuckoosandbox.org/)
* Lectura Recomendada:
  + Sikorski, M., Honig, A. (2012). "Practical Malware Analysis". Capítulos 1 y 2. Proporciona una base sólida sobre los tipos de malware y sus características.
  + <https://github.com/adwait1-g/Practical-Malware-Analysis>

### Recursos Adicionales

* Artículos y Guías:
  + "Types of Malware and How They Work" - [Un artículo detallado sobre diferentes formas de malware, disponible en múltiples sitios de ciberseguridad.](https://its.uri.edu/itsec/viruses-trojans-and-malware/#:~:text=TYPES%20OF%20MALWARE%20AND%20HOW%20THEY%20WORK&text=Adware%20%E2%80%93%20Software%20that%20is%20financially,transmits%20it%20to%20interested%20parties.)

## Actividad 2: Análisis de Malware y Respuesta a Incidentes

### Materiales Necesarios

* Herramientas de Análisis de Malware:
  + OllyDbg: [OllyDbg](http://www.ollydbg.de/)
  + X64Dbg: [X64Dbg](https://x64dbg.com/)
* Entornos Virtuales:
  + VMware: [VMware](https://www.vmware.com/)
  + VirtualBox: [VirtualBox](https://www.virtualbox.org/)
* Lectura Recomendada:
  + Sikorski, M., Honig, A. (2012). "Practical Malware Analysis". Capítulo 7. Detalla técnicas avanzadas para el análisis de malware.

### Recursos Adicionales

* Guías del NIST sobre respuesta a incidentes:
  + NIST Special Publication 800-61, "Computer Security Incident Handling Guide": [NIST SP 800-61](https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final)

## Actividad 3: Evaluación de Herramientas de Monitoreo y Detección de Intrusiones

### Materiales Necesarios

* Herramientas de Monitoreo y Detección:
  + Snort: [Snort](https://www.snort.org/)
  + Wireshark: [Wireshark](https://www.wireshark.org/)
  + OSSEC: [OSSEC](https://www.ossec.net/)
* Red de Laboratorio:
  + Equipos y dispositivos necesarios para configurar una red de laboratorio que simule un entorno empresarial.

### Recursos Adicionales

* Documentación y Tutoriales de cada herramienta para facilitar la configuración y el uso eficaz en entornos de prueba.
  + Snort User Manual: Proporciona una guía detallada para configurar y utilizar Snort.
  + Wireshark User Guide: Ofrece instrucciones detalladas sobre cómo capturar y analizar paquetes con Wireshark.
  + OSSEC Documentation: Explica cómo implementar y configurar OSSEC para la detección de intrusiones basada en host.

# Documento Teórico: Definición y Tipos de Malware

## Introducción

El término malware —contracción de "malicious software" (software malicioso)— engloba una variedad de programas diseñados específicamente para dañar, perturbar o infiltrarse ilegalmente en sistemas de computación. El conocimiento de los diferentes tipos de malware es fundamental para la ciberseguridad, ya que permite a los profesionales y usuarios identificar amenazas potenciales y tomar medidas adecuadas para proteger sus sistemas y datos.

## Definición de Malware

El malware es cualquier tipo de software que se instala en un sistema sin el consentimiento del usuario y lleva a cabo actividades no deseadas y potencialmente dañinas. Estas actividades pueden incluir el robo de información, la corrupción de datos, el secuestro de recursos del sistema y la alteración del funcionamiento normal del sistema.

## Tipos de Malware

A continuación, se describen los tipos más comunes de malware, cada uno con sus propias características y métodos de ataque.

### 1. Virus

* Características: Un virus informático es un tipo de malware que se replica a sí mismo al modificar otros programas de computadora e insertar su propio código. Cuando este código se ejecuta, se replica y puede infectar otros programas o archivos.
* Impacto: Puede dañar el sistema operativo, borrar archivos o reprogramar el sistema para realizar tareas no deseadas.
* Más información: Virus Informáticos - Kaspersky

### 2. Gusanos

* Características: Los gusanos son programas que se replican a sí mismos de una computadora a otra sin necesidad de intervención humana, a menudo a través de redes.
* Impacto: Consumen ancho de banda y pueden sobrecargar los sistemas, haciendo que estos se vuelvan inestables o dejen de funcionar.
* Más información: Gusanos Informáticos - Symantec

### 3. Troyanos

* Características: Un troyano es un tipo de malware que se disfraza de software legítimo. Los usuarios son engañados para cargar y ejecutar troyanos en sus sistemas, después de lo cual pueden llevar a cabo sus acciones maliciosas.
* Impacto: Desde espiar hasta robar datos sensibles, interrumpir el sistema, abrir puertas traseras a otros malware, etc.
* Más información: Troyanos - Trend Micro

### 4. Ransomware

* Características: Este tipo de malware restringe el acceso al sistema infectado y exige un rescate al usuario para que el acceso pueda ser restablecido.
* Impacto: Bloquea archivos personales y datos del usuario, a menudo cifrándolos, y pide dinero a cambio de la clave de descifrado.
* Más información: [Ransomware - Microsoft](https://www.microsoft.com/security/blog/2021/07/22/ransomware/)

### 5. Spyware

* Características: El spyware es un software que recopila información de un ordenador y transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.
* Impacto: Robo de información personal, hábitos de navegación, credenciales de acceso y otros datos sensibles.
* Más información: Spyware - Malwarebytes

### 6. Rootkits

* Características: Los rootkits son un conjunto de programas y herramientas que permiten a un tercero mantener el control remoto del sistema informático sin ser detectado.
* Impacto: Ocultación de otros malware, facilitación de accesos no autorizados al sistema y manipulación de sistemas operativos.
* Más información: Rootkits - McAfee

# 