

Instituto Tecnológico y de Estudios Superiores de Monterrey
Escuela de Ingeniería y Ciencias

Ingeniería en Ciencia de Datos y Matemáticas
Aplicación de criptografía y seguridad

ANÁLISIS FORENSE Y ENDPOINT SECURITY CLOUD

Socio Formador: IPC Services

Karla Andrea Palma Villanueva (A01754270)

Daniela Márquez Campos (A00833345)

Julio Eugenio Guevara Galván (A01704733)

Adrian Pineda Sánchez (A00834710)

David Fernando Armendáriz Torres (A01570813)

Kevin Antonio González Díaz (A01338316)



CONTENIDO

01

Descripción del
problema

02

Desarrollo

03

Resultados

04

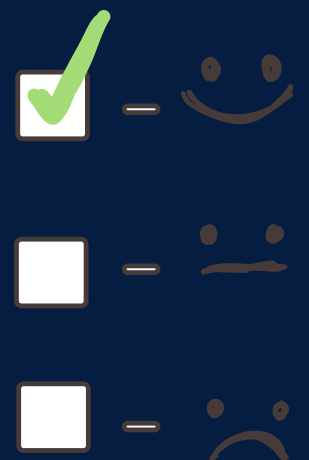
Conclusiones



DESCRIPCIÓN DEL PROBLEMA

El objetivo es evaluar la capacidad del EDR de **Kaspersky** en una máquina virtual, poniéndolo a prueba con diferentes amenazas cibernéticas controladas.

Se busca medir su eficacia en **identificar y neutralizar estas amenazas**, proporcionando información sobre su desempeño en entornos simulados de ataque y entendiendo el funcionamiento específico de los virus seleccionados.





DESARROLLO



CREACIÓN DEL LABORATORIO DE PRUEBAS

Configuración de un entorno controlado para realizar experimentos, pruebas y evaluaciones, sin afectar el sistema principal.

ELEMENTOS PRINCIPALES DEL LABORATORIO

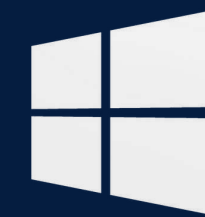


VirtualBox

Plataforma para la ejecución de VMs.
Entorno seguro para realizar pruebas y experimentos sin afectar el sistema operativo principal.

Tres máquinas Windows 11
Enterprise Evaluation 22H2 en
Virtual Box

Windows



PfSense

Funge como *router* para la
conexión de las VMs a internet.

Kaspersky Endpoint Security
Cloud para Windows
versión 12.2.0.462

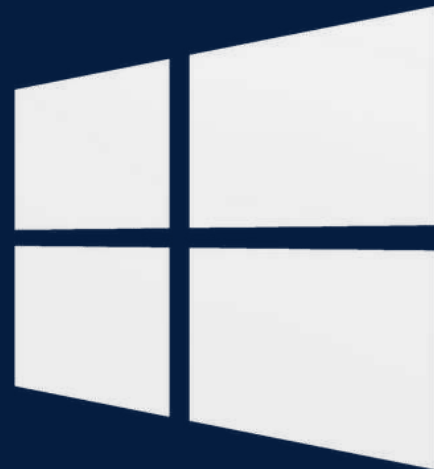
Kaspersky



CONFIGURACIÓN DE WINDOWS Y PFSENSE

Windows

Instalación de imagen de Windows
No password para el usuario
Memoria RAM: 6 Gb



PfSense

Memoria base: 1024 Mb
Adaptador 1 – A través de NAT se establece la conexión a internet.
Adaptador 2 – Se crea una Red Interna a la cual se conectan las VMs



KASPERSKY ENDPOINT SECURITY CLOUD



Creación y Configuración cuenta
(Administrador)

Cuenta

Empresa

Creación y Configuración de la
empresa

Invitación a Grupo de los
usuarios via e-mail

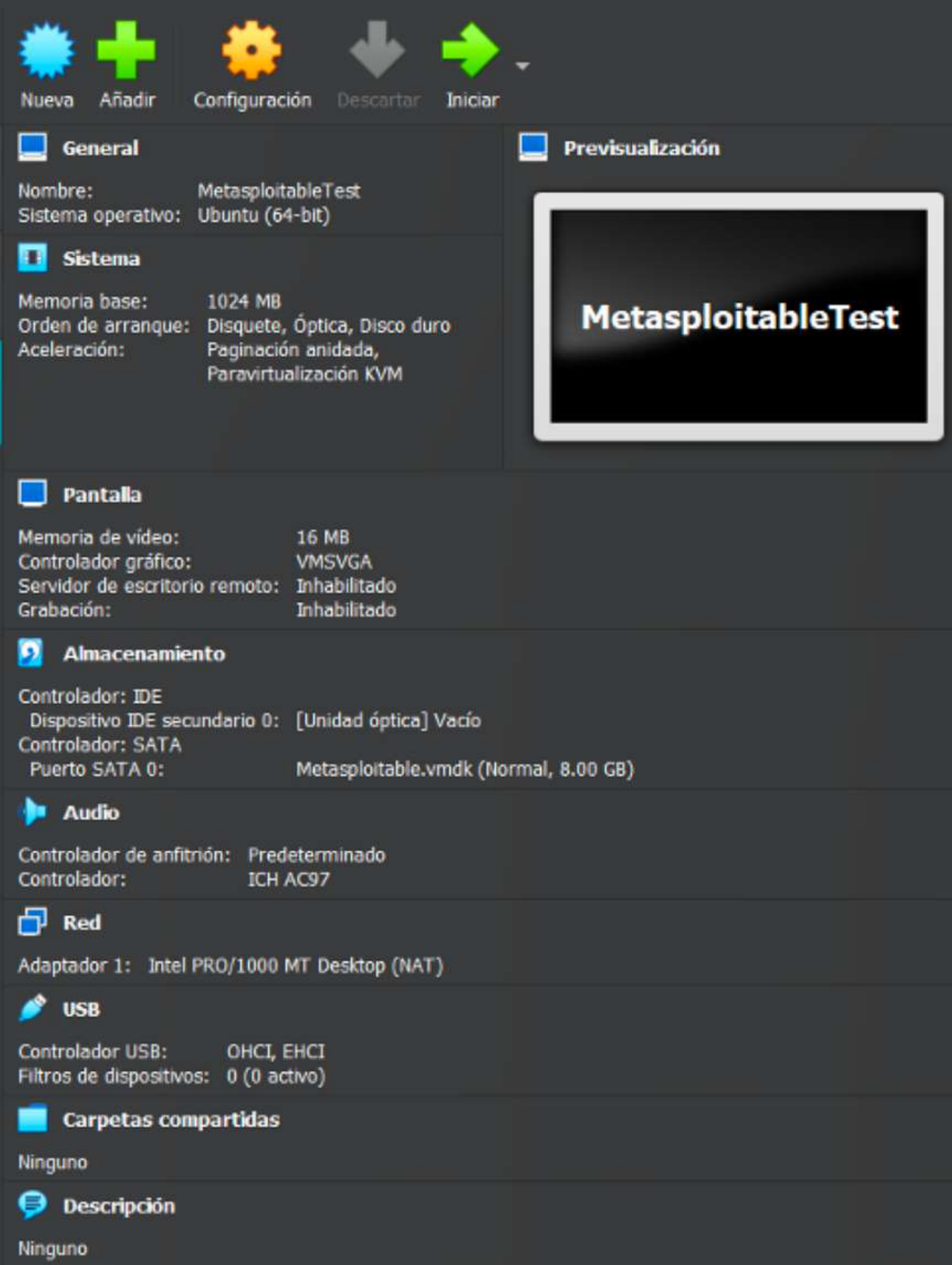
Grupo

**Perfiles de
seguridad**

Configuración del o los perfiles
de seguridad en web, red,
archivos, etc. (Repositorio de los
codigos)

Instalacion del agente Kaspersky
para la detección de amenazas y
cadena de procesos

Agente Kaspersky

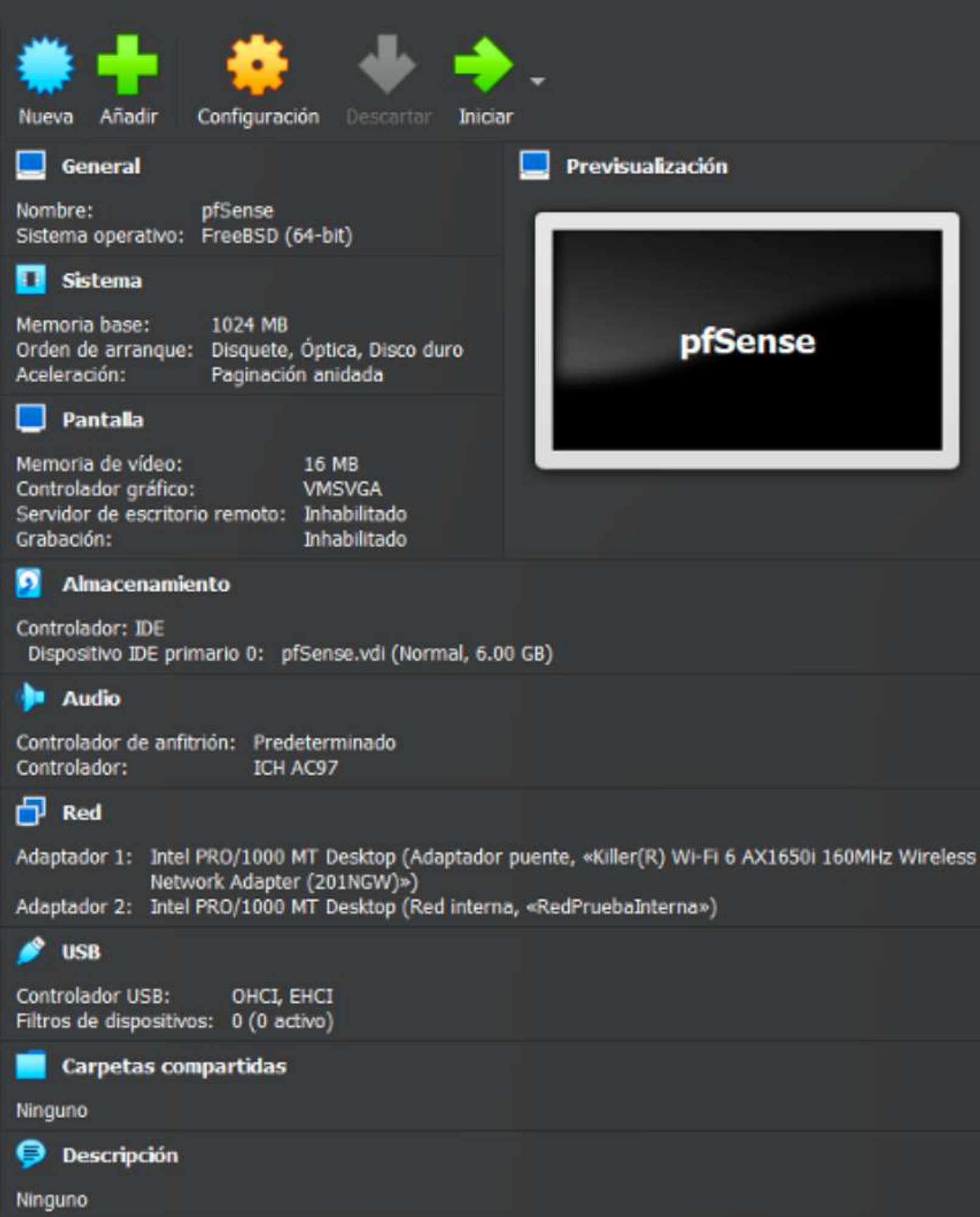


INSTALACIÓN DE MWARE METASPLOITABLE

Nombre	Tipo	Versión
MetasploitableTest	Linux	Ubuntu 64 bits

Memoria	Disco duro virtual existente
1024 MB	imagen Metasploitable.vmdk

Usuario predeterminado: msfadmin
Contraseña predeterminada: msfadmin



INSTALACIÓN DEL ROUTER: PFSENSE

Nombre	Tipo	Imagen iso
pfSenseTest	BSD	LinupfSense-CE-2.6.0-RELEASE-amd64.iso
Memoria	Disco duro virtual	
1024 MB	Se creó un disco duro nuevo de 6 GB	

INSTALACIÓN DEL ROUTER: PFSENSE

Iniciar la maquina virtual

Red en modo bridge el
adaptador 1

Vaciar el disco

Apagar la maquina virtual

Crear red de prueba

Iniciar la maquina virtual y
abrir la terminal

Identificar ip

CONFIGURACIÓN Y CONEXIÓN A INTERNET

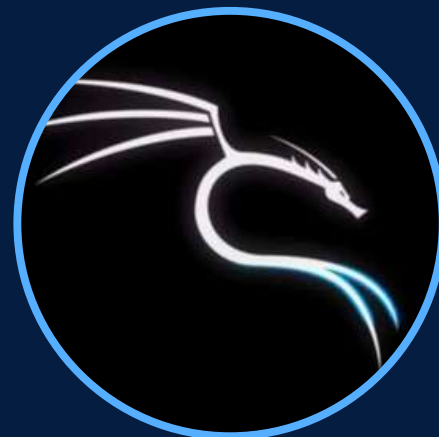
Configuración

Red

Adaptador 1

Red Interna

RedPruebaInternaTes



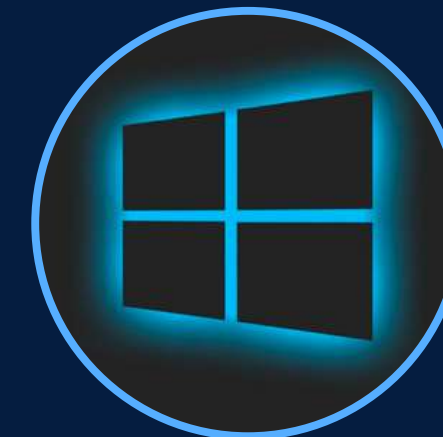
Kali Linux



Ubuntu
Linux



MWare
Metasploitable



Windows

CÓDIGOS MALICIOSOS PROBADOS

Eicar



Fuente: Página
Oficial de EICAR

MyDoom



Fuente:
Repositorio de
Github The Zoo

DOUBLE FANTASY



Fuente:
Repositorio de
Github The Zoo

Satana



Fuente:
Repositorio de
Github The Zoo

Vipasana



Fuente:
Repositorio de
Github The Zoo



RESULTADOS

EICAR TEST FILE

- Código que si bien no ejecuta ninguna acción en el dispositivo, suele ser detectado como amenaza.
- Diseñado por el *European Institute for Computer Anti-Virus Research*

Detalle del alerta

Archivo:

<http://www.eicar.org/download/eicar.com>

Código malicioso:

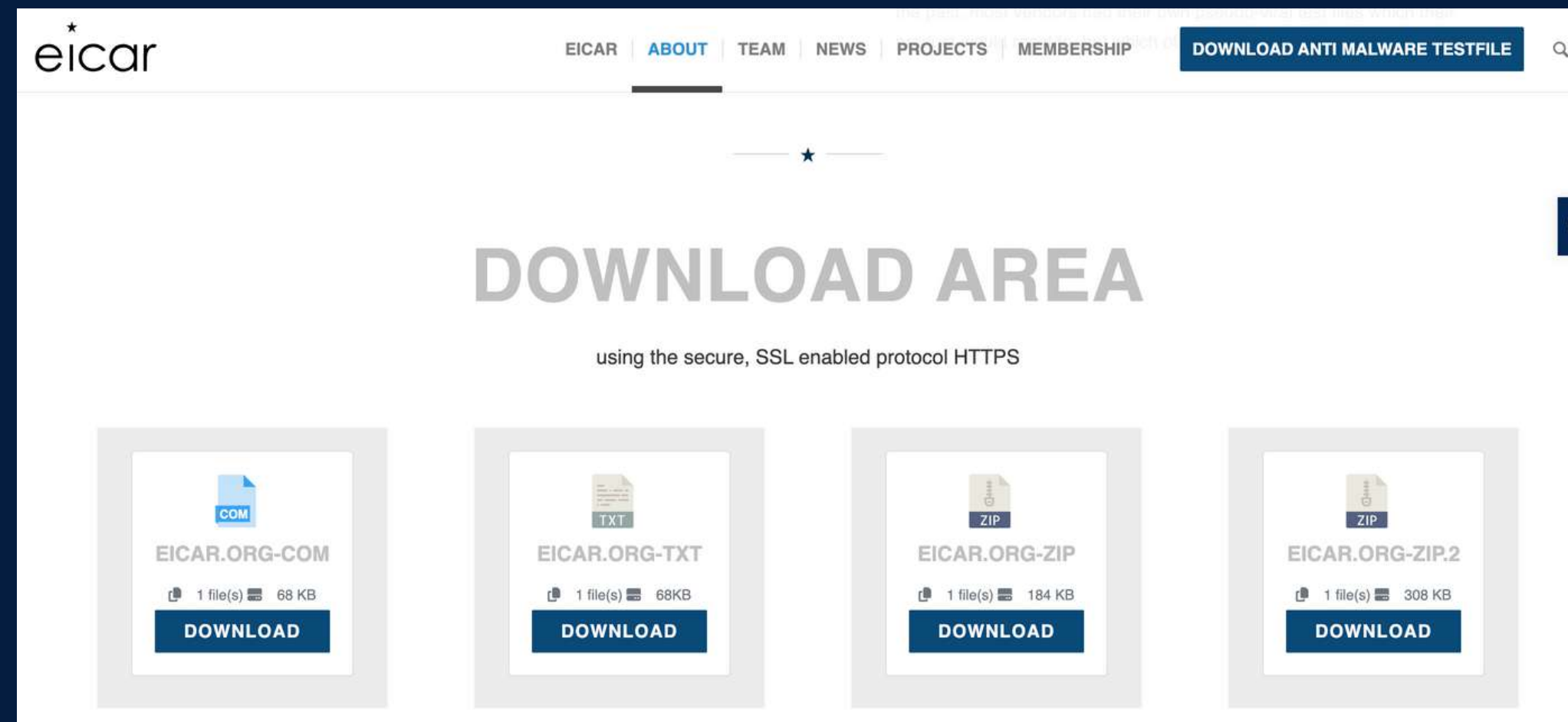
Eicar Archivo de prueba

Descripción:

El objeto contiene una amenaza para su ordenador.

EICAR TEST FILE: EDR

- Posterior a la descarga y descompresión, lo identifica como un archivo malicioso y bloquea su ejecución
- Amenaza eliminada: EICAR-Test-File



MYDOOM

- *Gusano Informático para Windows*
- *Distribución extremadamente rápida mediante e-mail attachment.*
- *Origen: desconocido*
- *Target: SCO Group & Microsoft*
- *Ejecuta un ataque DDoS*
- *Crea una backdoor en el puerto 3127/tcp*



MYDOOM: EDR

- Se ejecutan búsquedas de archivos en command prompt.
 - Búsqueda de contactos
 - Falso negativo
- Web Spoofing
 - .htm, .css, .gif
 - "nav_bar", "main_menu"
- Objetivo DDoS: www.sco.com
- Amenaza eliminada: Email-Worm.Win32.Mydoom.a

DOUBLEFANTASY

- Creado por *Equation Group*, un sofisticado *thread actor*.
- *Target*: Empresas y organizaciones
- Troyano que recopila información esencial del dispositivo y la transfiere al C&C.
- Puede introducir *malware* adicional en el sistema:
 - GRAYFISH
 - EQUATIONDRUG

DOUBLEFANTASY: EDR

- Proceso Sospechoso:
 - Archivo de bases de datos almacenado dentro del directorio de Caches de Windows (extensión .db)
 - Sugiere la recopilación de datos para su transferencia al C&C
- Amenaza eliminada:
Trojan.Win32.DoubleFantasy.gen



SATANA

- Troyano que analiza los discos y la red en busca de archivos y los cifra
- Impide el inicio normal de Windows
- Cambia el nombre de los archivos encriptados, añadiendo un correo al inicio
- De esta manera se realiza el *ransomware*



SATANA: EDR

- Procesos Sospechosos:
 - winlogon.exe
 - Explotar privilegios
 - Persistencia post-reinicio
 - Operación sin detección
 - userinit.exe
 - Explotar privilegios
- Técnicas antiforenses: timestamp

```
ng of all your files in a
<!SATANA!>
E-mail: matusik11@techemail
065AE31E707FFE019711 and pay
7XABd4TJANXtQXGCacNUG total
the software will be sent to y
. All changes in hardware con
ryption of your files absolut
ossible only on your PC!
days, after which the program
signature from a public certi
which you can find as yet in the
rypted files, as well as in th
ot appreciate your files we reco
l the system. Read carefully thi
artup of the computer. We remind
the configuration of your compute
l.com - this is our mail
707FFE019711 this is code; you mu
JANXtQXGCacNUG here need to pay 0,
wallet you can easily find on the
obtained by E-mail here and press "
load on your computer. Good luck! M
<!SATANA!>
```


VIPASANA

- Cifra sus archivos con la clave pública mezclando cifrado simétrico y asimétrico.
- Envía la clave privada necesaria para el descifrado al servidor del extorsionador.
- Devuelve esta clave después de pagar el rescate



VIPASANA: EDR



- Proceso sospechoso
 - Archivo de bases de datos almacenado dentro del directorio de Caches de Windows
- No hay conexión a internet
- Amenaza eliminada:
UDS:DangerousObject.Multi.Generic

RECOMENDACIONES

Firewall

Antivirus

Actualizaciones
de Software

Identificar
datos críticos

Copias de
seguridad

Control
de acceso

Revisiones
constantes

Concientización
del Personal



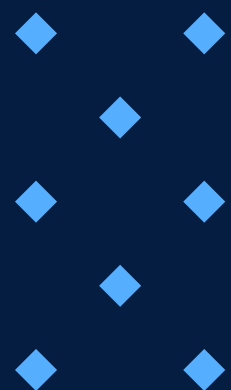


CONCLUSIONES

Con este proyecto pudimos ver la importancia de tener disponibles herramientas efectivas para la mitigación de amenazas y cómo Kaspersky simplifica la configuración y supervisión de entornos virtuales y proporciona protección contra amenazas informáticas.

Después de ponerla a prueba frente a diferentes códigos maliciosos, como EICAR, MyDoom, Satana, DOUBLEFANTASY y Vipasana, pudimos notar su capacidad para identificar y bloquear archivos maliciosos, proporcionando detalles sobre el origen de la amenaza, el desarrollo de la misma y los indicadores de compromiso asociados, por lo que podemos decir que demostró una respuesta eficiente ante este tipo de amenazas.

Estas medidas, junto con la educación en seguridad cibernética, son cruciales para mantener un entorno seguro.



REFERENCIAS

1. Graham, D. G. (2021) Ethical Hacking : A Hands-on Introduction to Breaking In. No Starch Press.
2. Acerca del virus de prueba EICAR. (n.d.). <https://support.kaspersky.com/KESS/3.0/es-MX/147734.htm>
3. Titova, V. (2020, July 3). Satana: el ransomware del infierno. Kaspersky. Retrieved November 30, 2023, from <https://latam.kaspersky.com/blog/satana-ransomware/7362/>
4. CCN-CERT – Publicados cinco nuevos Informes de Código Dañino. 2015, October 22). <https://www.ccn-cert.cni.es/es/comunicacion-eventos/comunicados-ccn-cert/3094-publicados-cinco-nuevos-informes-de-codigo-danino.html>
5. A close look at ransomware by the example of Vipasana – I. (2016, October 7). <https://www.boxcryptor.com/en/blog/post/a-close-look-at-ransomware-vipasana-part-i/>
6. Endpoint Security para Windows | Kaspersky. (2018). Kaspersky.com. <https://latam.kaspersky.com/small-to-medium-business-security/endpoint-windows>
7. Kaspersky Lab HQ. (2015). EQUATION GROUP: QUESTIONS AND ANSWERS. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf