

# **Laboratorio 1: Análisis de Amenazas en Entorno Virtualizado**

Curso: Ciberseguridad / Entornos Virtualizados

Estudiante: \_\_\_\_\_

Fecha: \_\_\_\_\_

Este informe describe el desarrollo del laboratorio 1, cuyo objetivo es analizar el comportamiento de un archivo sospechoso dentro de un entorno virtualizado y documentar los hallazgos utilizando herramientas de monitoreo de procesos, análisis de tráfico de red y servicios de reputación de archivos como VirusTotal.

## 1. Preparación del entorno virtualizado

**Entorno de trabajo.** Se utilizó Oracle VirtualBox en un equipo anfitrión Windows para ejecutar dos máquinas virtuales principales: **Cybersecurity LabVM Workstation 20250409**, basada en Ubuntu 64 bits, utilizada como entorno principal de laboratorio. **Kali Linux 2025.3**, basada en Debian 64 bits, utilizada como entorno adicional de pruebas. En ambos casos se configuró el adaptador de red en modo **NAT**, lo que permite a las máquinas virtuales acceder a Internet a través del host, pero sin ser visibles directamente desde la red local física. Esto aporta aislamiento y reduce la superficie de ataque.

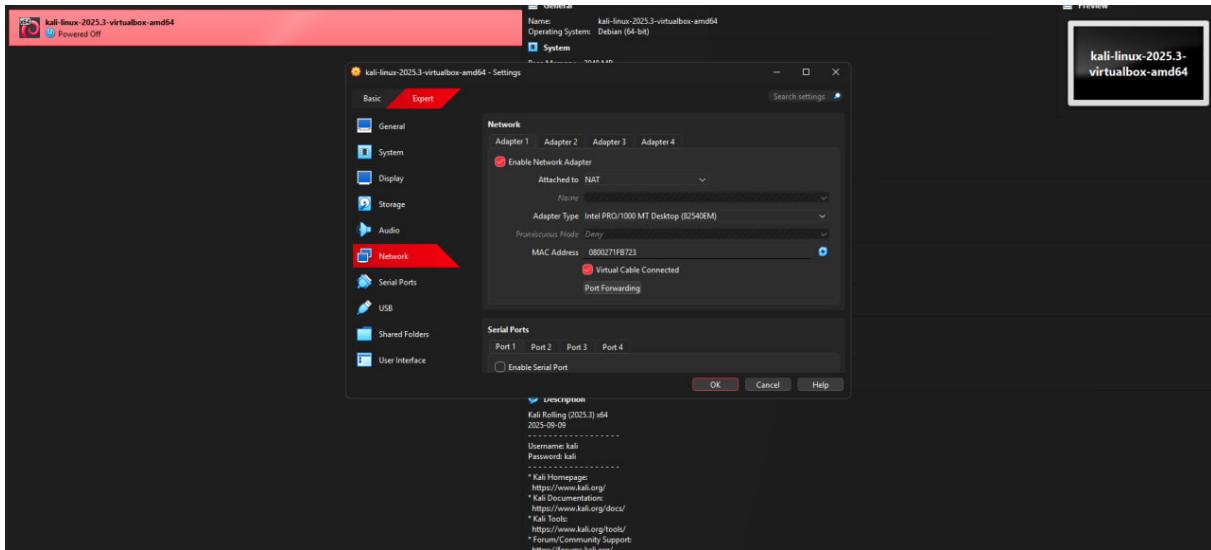


Figura 1. Configuración de red (modo NAT) para la máquina virtual Kali Linux en VirtualBox.

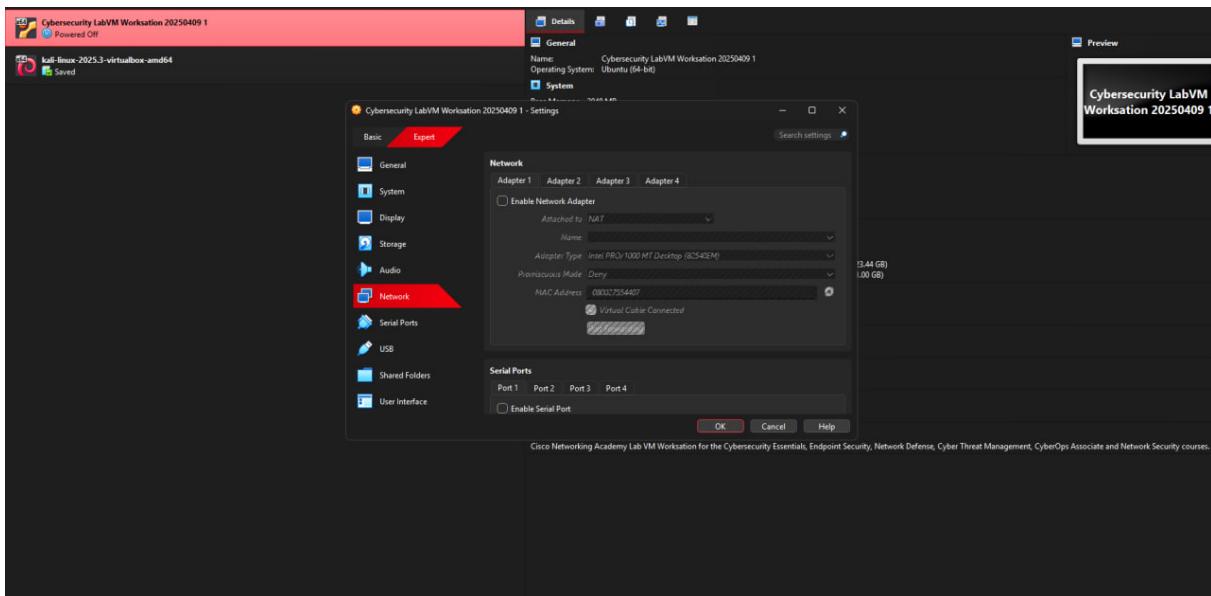


Figura 2. Configuración de red (modo NAT) para la Cybersecurity LabVM Workstation.

**Firewall del sistema operativo.** En la Cybersecurity LabVM se verificó el estado del firewall **UFW** (Uncomplicated Firewall) y se habilitó para que permaneciera activo de forma permanente. Esto asegura que todo el tráfico de red que entra o sale de la máquina pase por las reglas de filtrado correspondientes.

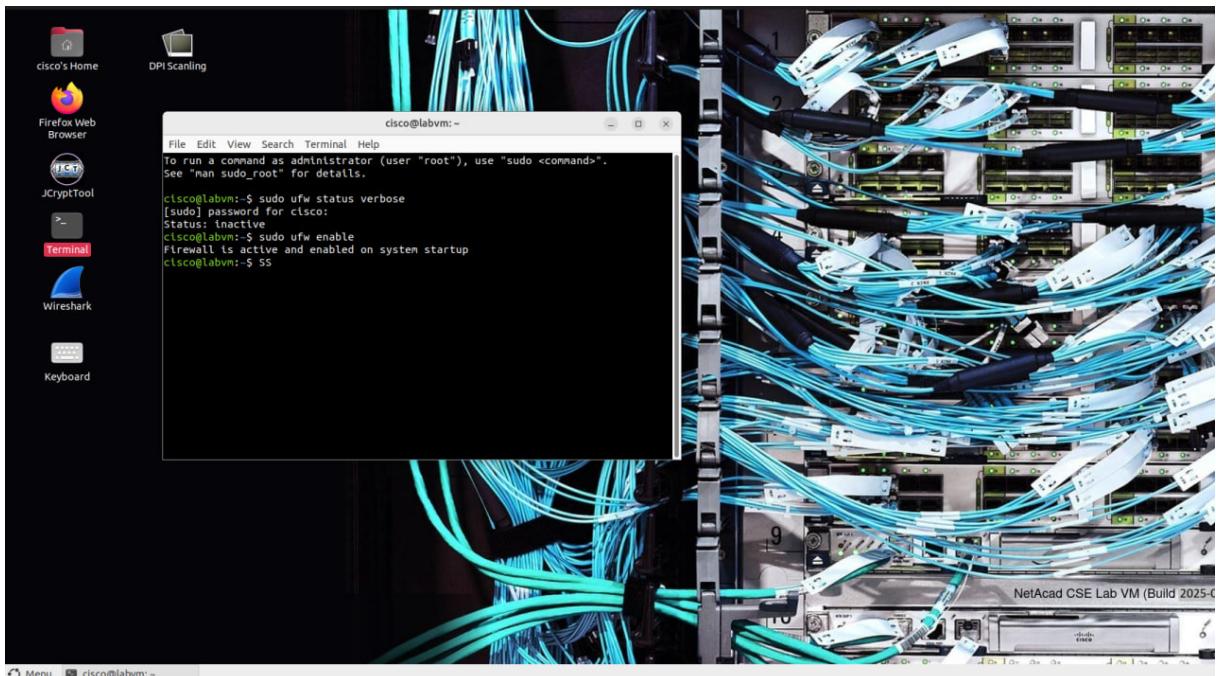


Figura 3. Activación del firewall UFW en la Cybersecurity LabVM.

## 2. Obtención y análisis del archivo sospechoso

Para evitar riesgos reales se utilizó el archivo de prueba **EICAR**, diseñado específicamente para comprobar el correcto funcionamiento de soluciones antivirus. Este archivo contiene una cadena de texto que los motores de seguridad reconocen como si fuera malware, aunque en realidad es completamente inofensivo.

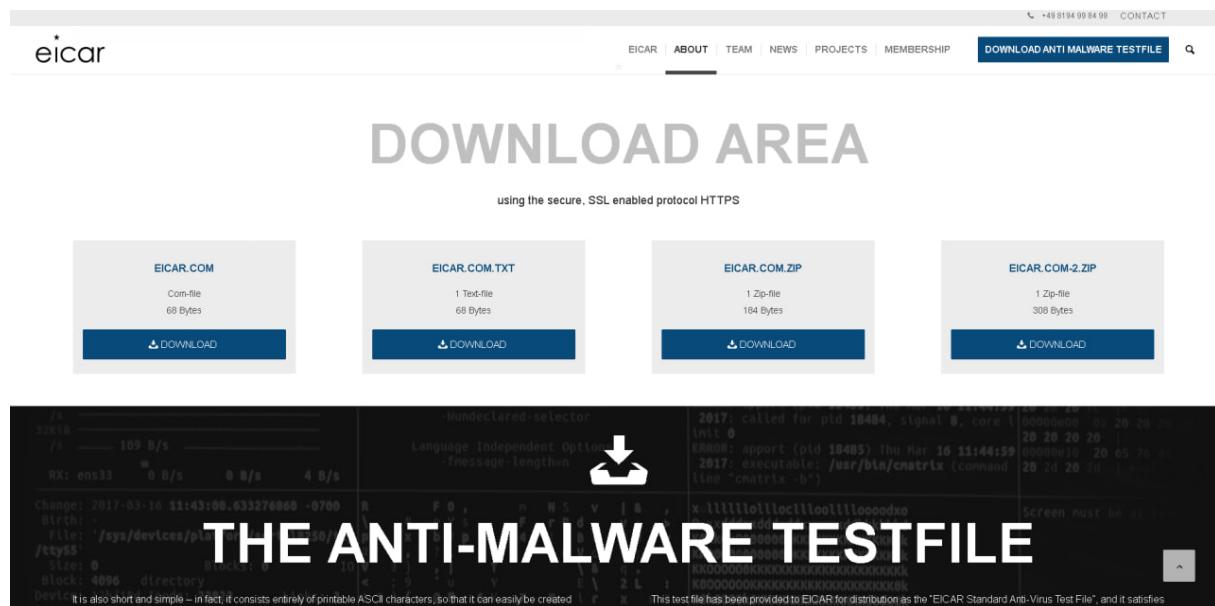


Figura 4. Página oficial de EICAR con los archivos de prueba disponibles para descarga.

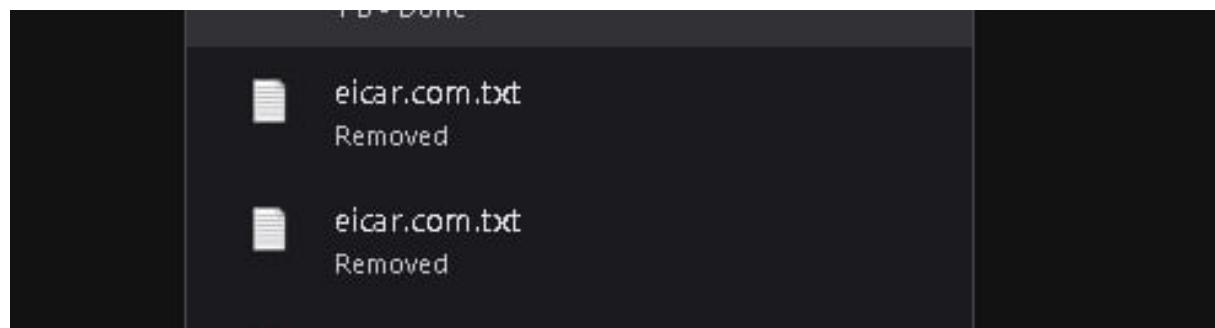


Figura 5. El navegador indica que el archivo eicar.com.txt fue eliminado automáticamente por la protección de seguridad.

El archivo *eicar.com.txt* se descargó desde la máquina virtual y posteriormente se analizó desde el host mediante el servicio **VirusTotal**, que envía la muestra a decenas de motores antivirus diferentes y consolida el resultado en un único informe.

The screenshot shows the VirusTotal analysis page for the file eicar.com.txt. The top navigation bar includes links for 'File distributed by Offensive Security' and 'Reanalyze'. Below the header, the file's SHA-1 hash is listed as 275a021bbfb5489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f. The file size is 68 B and it was last analyzed 9 minutes ago. A 'Community Score' of 65/69 is displayed, with 3702 users having analyzed it. The file is categorized under 'powershell', 'direct-cpu-clockaccess', 'idle', 'known-distributor', 'detected-debug-environment', 'long-sleeps', 'visitor', and 'attachment'. The 'DETECTION' tab is selected, showing a green banner encouraging community participation. Below the banner, there is a section titled 'Code insights' with a note that EICAR is a test string used to detect and test antivirus software. It states that EICAR is harmless and cannot infect your computer. A 'Show more' link is present. The 'Popular threat label' is 'virus.eicar/test'. Threat categories include 'virus' and 'trojan'. Family labels include 'eicar', 'test', and 'file'. The 'Security vendors' analysis' table lists 21 different antivirus engines and their results. The table has four columns: vendor name, detection result, company name, and threat label. Some detections are marked with a warning icon (yellow circle with a red exclamation mark). The table includes entries for AhnLab-V3, AiCloud, Anty-AVL, Avast, AVG, Baidu, Bkav Pro, CMC, Cynet, Elastic, eScan, Fortinet, Google, and Huorong.

Figura 6. Resultado general en VirusTotal para el archivo eicar.com.txt (65 de 69 motores lo marcan como malicioso).

AhnLab-V3	① Virus/EICAR_Test_File	Alibaba	① Virus:Win32/EICAR.A
AiCloud	① EngtestMulti/Eicar	ALYac	① Misc.Eicar-Test-File
Anty-AVL	① TestFile/Win32.EICAR	Arcabit	① EICAR-Test-File (not A Virus)
Avast	① EICAR Test-NOT Virus!!!	Avast-Mobile	① Eicar
AVG	① EICAR Test-NOT Virus!!!	Avira (no cloud)	① Eicar-Test-Signature
Baidu	① Win32.Test.Eicar.a	BitDefender	① EICAR-Test-File (not A Virus)
Bkav Pro	① W32.EicarTest.Trojan	ClamAV	① Win.Test.EICAR_HDB-1
CMC	① Eicartest.file	CTX	① Txt.virus.eicar
Cynet	① Malicious (score: 99)	DrWeb	① EICAR Test File (NOT A Virus!)
Elastic	① Eicar	Emsisoft	① EICAR-Test-File (A)
eScan	① EICAR-Test-File	ESET-NOD32	① Eicar Test File
Fortinet	① EICAR_TEST_FILE	GData	① EICAR_TEST_FILE
Google	① Detected	Gridinsoft (no cloud)	① Trojan.U.EICAR_Test_File.dd
Huorong	① TEST/AVEngTestFile/EICAR	Ikarus	① EICAR-Test-File

Figura 7. Detalle de algunos de los motores antivirus que clasifican la muestra como archivo de prueba EICAR o virus de prueba.

En los resultados se observa que la mayoría de soluciones la identifican explícitamente como *EICAR Test File* o variantes similares, e incluso algunos motores indican en la propia descripción que se trata de un archivo de prueba y no de un virus real. Esto confirma que los mecanismos de detección funcionan correctamente.

### 3. Análisis de tráfico de red con Wireshark

Para observar el tráfico generado durante la navegación y el uso del archivo de prueba se utilizó **Wireshark** en la máquina virtual Linux, capturando paquetes sobre la interfaz *enp0s3*, que corresponde al adaptador de red NAT de VirtualBox.

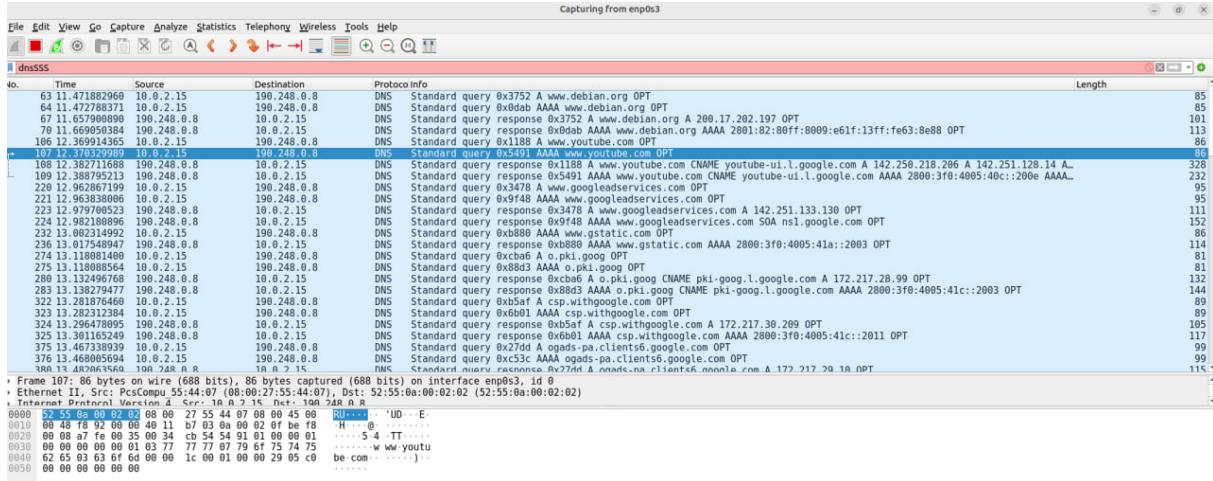


Figura 8. Captura de tráfico en Wireshark mostrando consultas DNS a distintos dominios.

Aplicando el filtro dns fue posible centrarse en las consultas y respuestas de resolución de nombres. Entre ellas se identificaron peticiones hacia *www.debian.org*, dominios de servicios de Google y, de forma particular, *www.youtube.com* al reproducir un vídeo en la máquina virtual.

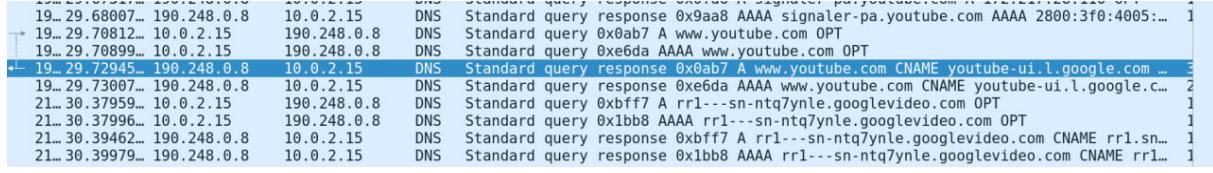


Figura 9. Respuesta DNS para www.youtube.com; se observa un CNAME a youtube-ui.l.google.com y múltiples direcciones IP asociadas.

En la respuesta DNS de *www.youtube.com* se aprecia un alias (*CNAME*) hacia *youtube-ui.l.google.com* y un conjunto de direcciones IPv4 asociadas. La presencia de múltiples IP para un mismo nombre de dominio refleja el uso de redes de distribución de contenido (CDN) y balanceo de carga por parte de Google/YouTube.

Filtrando posteriormente el tráfico con expresiones del tipo ip.addr in { ... } se pudo aislar el flujo de paquetes TCP/TLS/QUIC entre la máquina virtual (10.0.2.15) y los servidores de YouTube, lo que permite analizar de forma más precisa el comportamiento de la aplicación.

#### **4. Conclusiones**

1. El uso de máquinas virtuales con adaptadores en modo NAT, junto con el firewall UFW habilitado en la VM de laboratorio, proporciona un entorno razonablemente aislado para experimentar con archivos potencialmente peligrosos sin exponer la red local.
2. El archivo empleado, *eicar.com.txt*, es un archivo de prueba estándar reconocido por prácticamente todos los motores de antivirus. VirusTotal confirmó que más de 60 motores clasifican la muestra como maliciosa, aunque muchos de ellos indican explícitamente que se trata de un fichero de prueba EICAR y no de una amenaza real.
3. El monitoreo de procesos en la máquina virtual no mostró comportamientos sospechosos ni procesos persistentes asociados al archivo de prueba, lo cual es coherente con su naturaleza puramente textual en este entorno.
4. El análisis de tráfico con Wireshark permitió identificar tanto el tráfico legítimo hacia los sitios visitados (EICAR, YouTube, dominios de Google) como la resolución de nombres que realiza el sistema mediante DNS. El estudio detallado de las respuestas para *www.youtube.com* ilustra cómo grandes servicios en la nube distribuyen su carga entre múltiples servidores.

En conjunto, el laboratorio permitió practicar el uso combinado de entornos virtualizados, firewall, herramientas de captura de tráfico y servicios de reputación de archivos para analizar un supuesto archivo malicioso de forma segura y controlada.