**Técnicas de enumeración sobre redes, sistemas y comandos en ciberseguridad**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **1**

[**2. Práctica 1-3**](#_ofiic1av8ddq) **2**

[**2.1 Verificación de vulnerabilidad CPU ante Spectre y Meltdown:**](#_5d38uxjyswtl) **2**

[**2.2 Verificación de vulnerabilidad CPU ante MDS y Zombieload (Windows):**](#_msmg75pzfid) **5**

[**2.3 Análisis de seguridad con SFC y DISM (Windows)**](#_blqa1fdl0ps3) **6**

[**2.4 Verificación de integridad contra rootkits con rkhunter y chkrootkit**](#_6psws4hf9ocj) **7**

[**2.5 Pruebas con sar**](#_34qk2krjjjpl) **9**

[**2.6 Pruebas con dmesg**](#_qa4yuv9vkpc) **10**

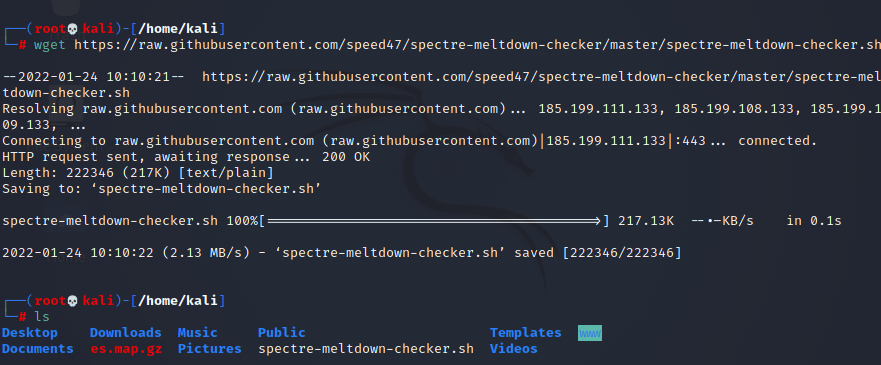
[**2.7 Pruebas con tcpdump**](#_qz7y7v2i3nwp) **12**

# 

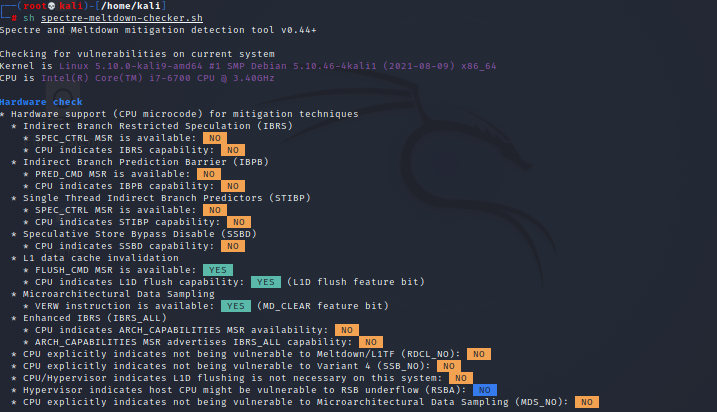
# **2. Práctica 1-3**

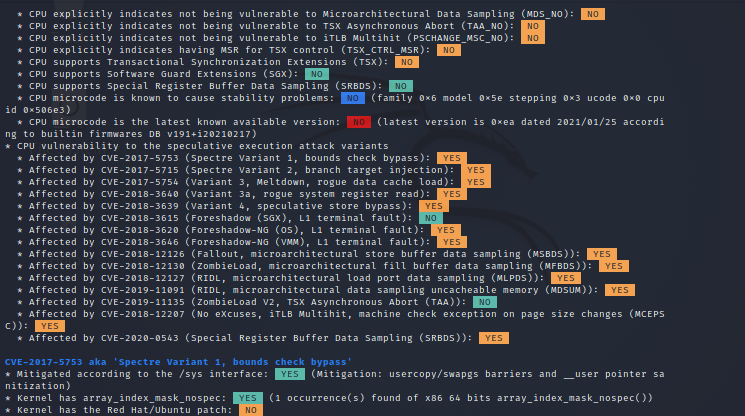
### **2.1 Verificación de vulnerabilidad CPU ante Spectre y Meltdown:**

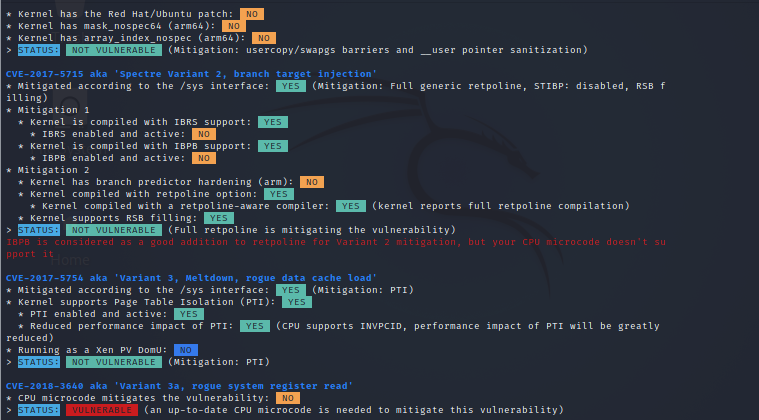
Descargamos el script mediante wget:

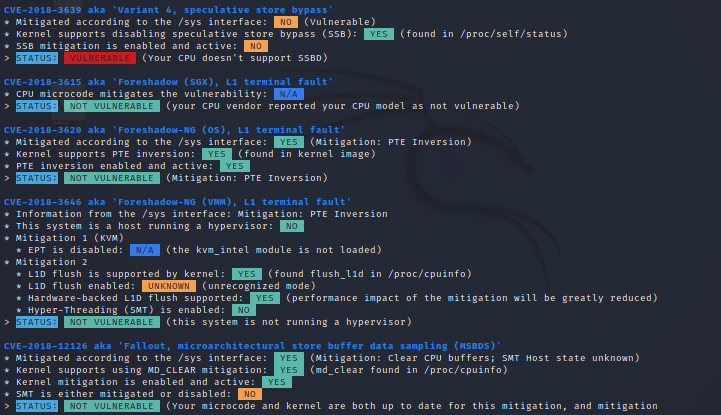


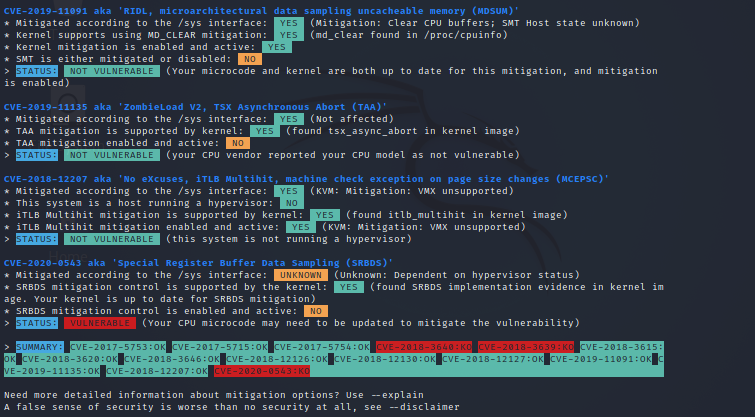
Y lo ejecutamos con sh:





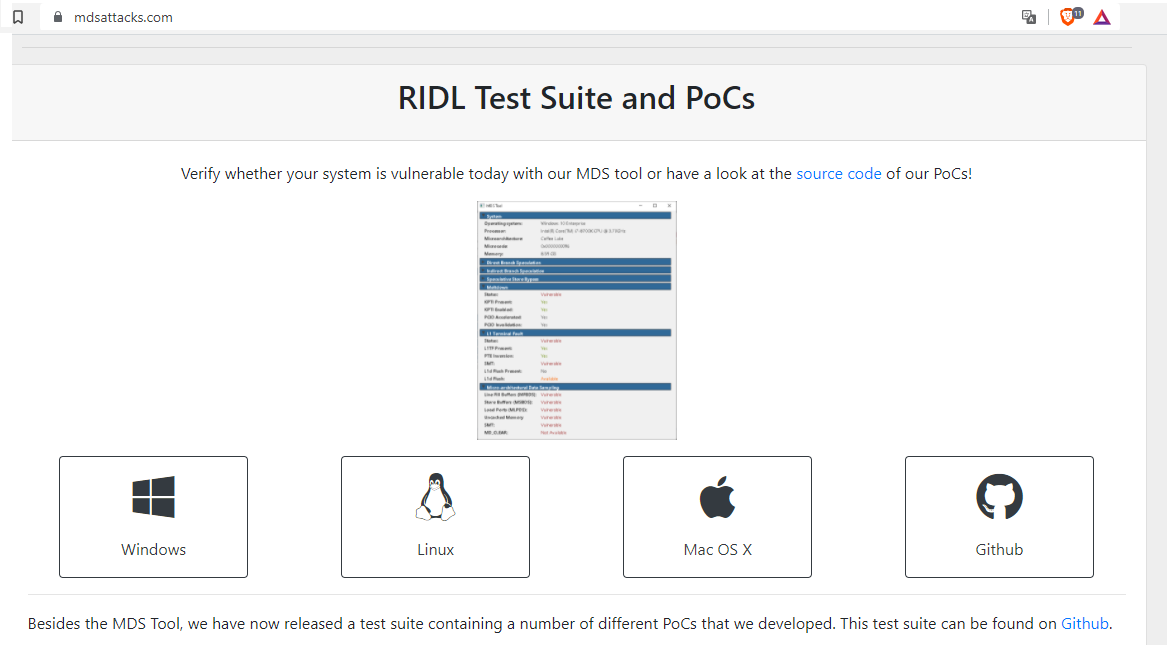


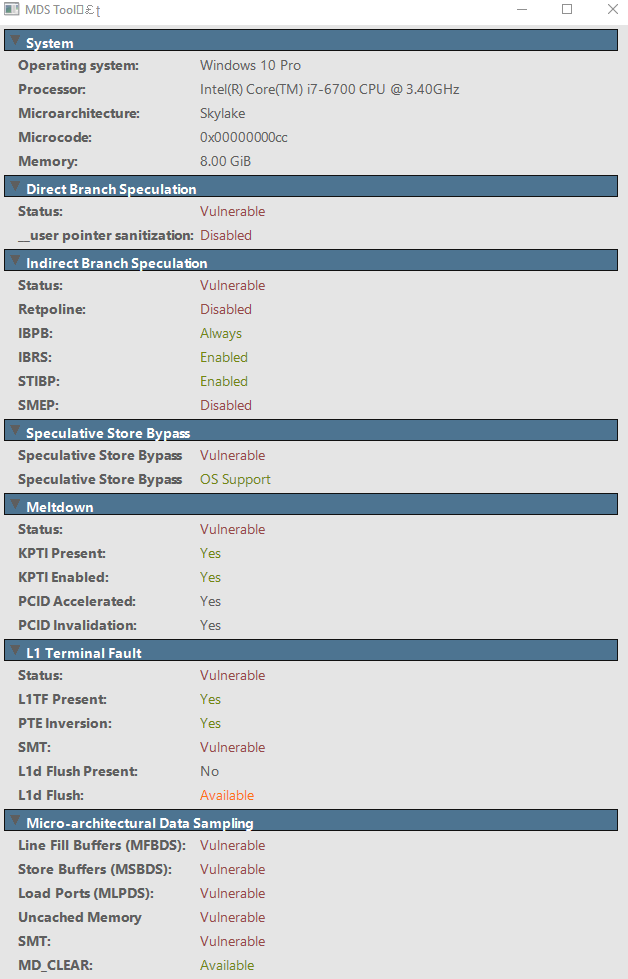




### **2.2 Verificación de vulnerabilidad CPU ante MDS y Zombieload (Windows):**

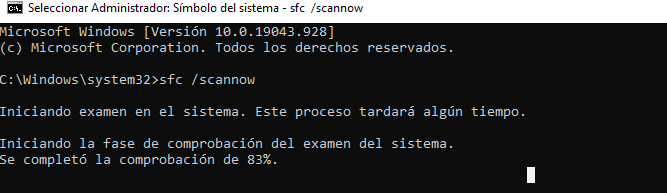
Descargamos la herramienta desde el navegador a través de la página oficial y la ejecutamos.

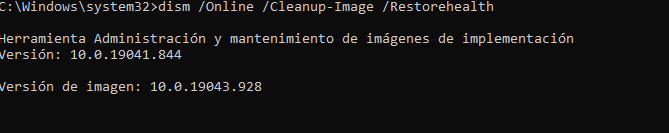




### **2.3 Análisis de seguridad con SFC y DISM (Windows)**

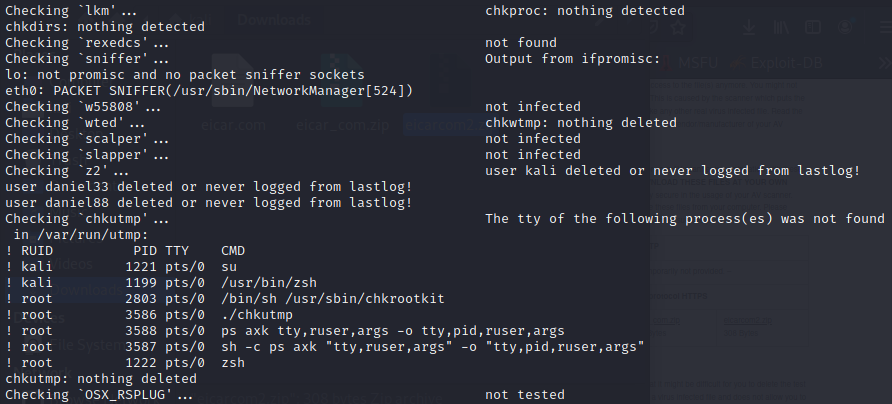
Los comandos vienen instalados por defecto en los sistemas Windows, los ejecutamos:

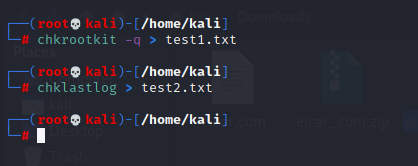


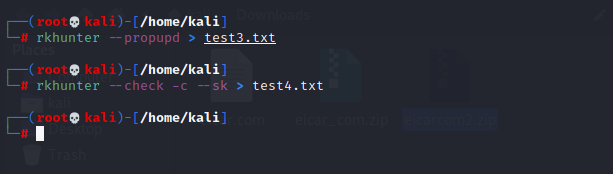


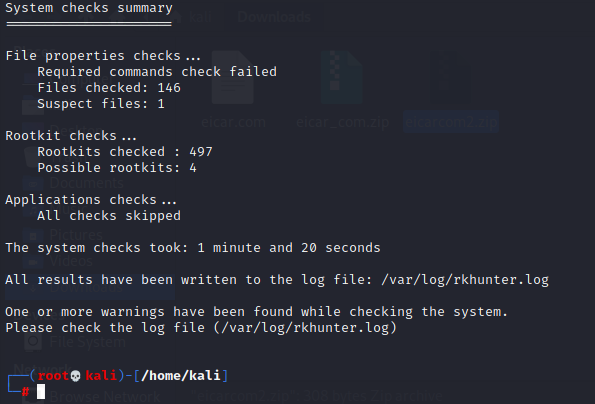
### **2.4 Verificación de integridad contra rootkits con rkhunter y chkrootkit**

Instalamos las herramientas mediante el comando apt install y las ejecutamos, en algunos casos indicando que la salida sea por un archivo de texto:



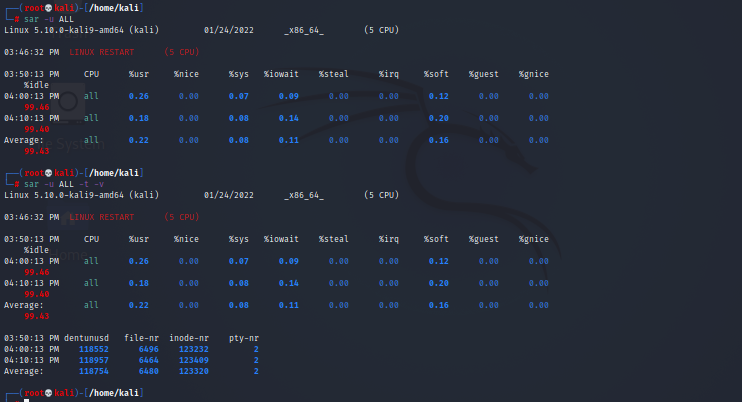


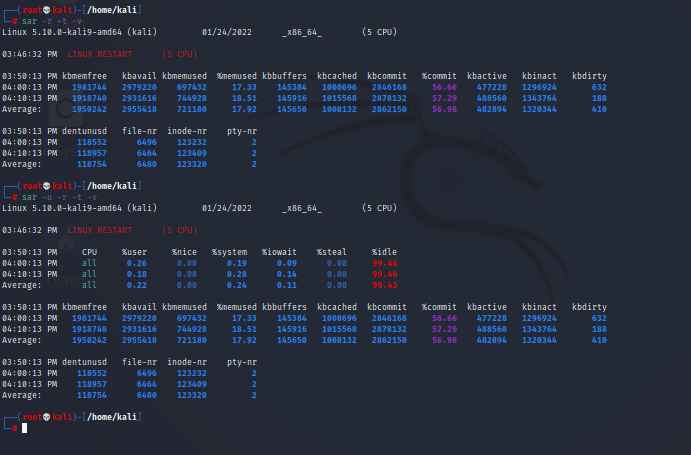


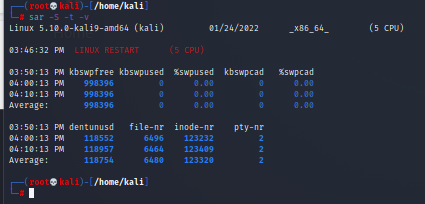


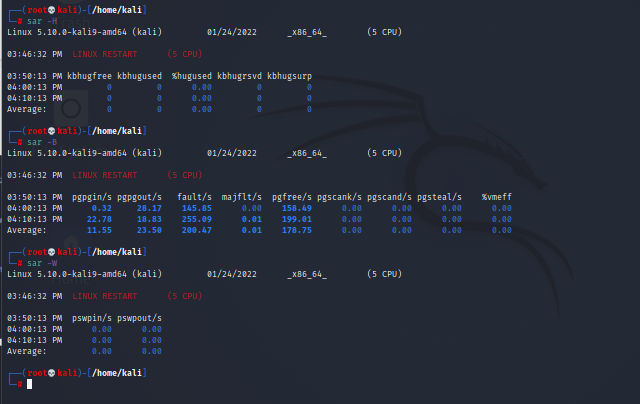
### **2.5 Pruebas con sar**

Realizamos varias pruebas con la herramienta sar, que viene instalada por defecto en los sistemas operativos Linux.



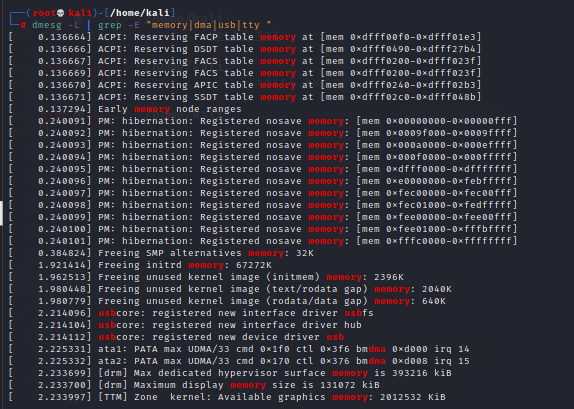


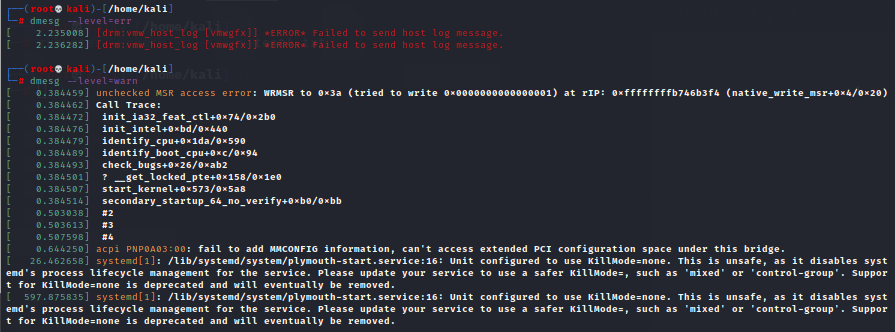


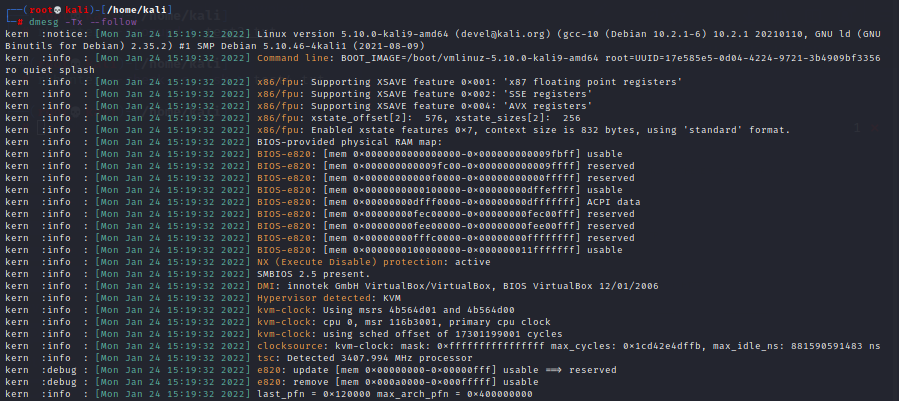


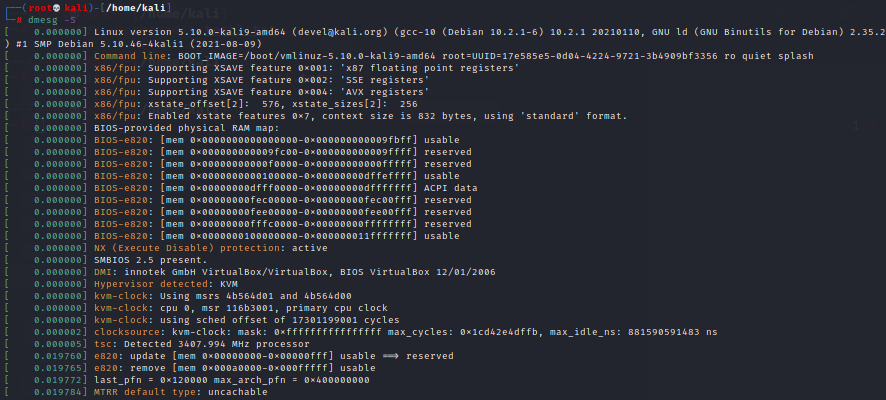
### **2.6 Pruebas con dmesg**

Utilizamos el comando dmesg para realizar pruebas y comprobar sus parámetros:









### **2.7 Pruebas con tcpdump**

Utilizaremos la herramienta tcpdump para capturar el tráfico de la red.

