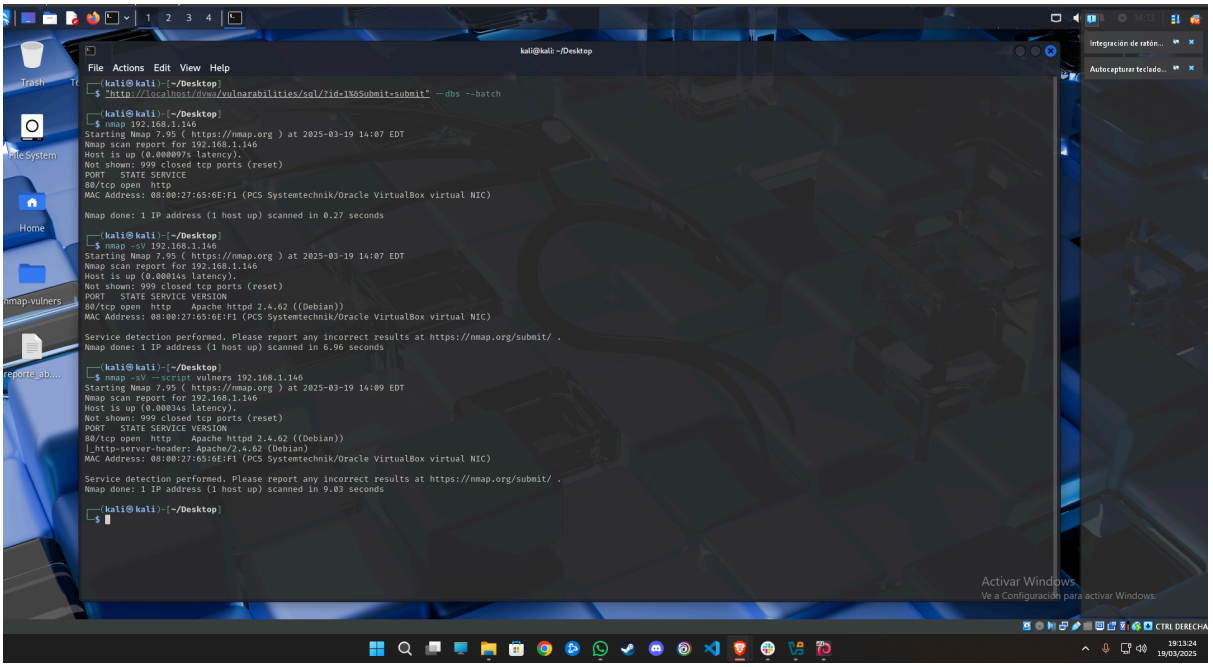
ESCANEO DE PUERTOS DE KALI A DEBIAN

Realizamos un escaneo de puertos:

Nos da que el Debian solo tiene abierto el puerto 80 y que esta funcionando un apache con la versión 2.4.62. Le pasamos también el script vulners para ver si nos encuentra algún CVE asociado a ese puerto con ese apache y aunque no nos arroja ninguno buscamos la información por otro lado investigando en NVD.



Vulnerabilidades asociadas:

Al pasar el vulners desde nmap no nos dice ningún CVE concreto, pero la información que nos da NVD para este puerto y ese servicio son de unas versiones anteriores por lo que en teoría no aplica para esta version de apache porque es la más actual y actualizada y de momento no se encontró ninguna vulnerabilidad o CVE asociado.

1. CVE-2024-38474: Vulnerabilidad de Ejecución Remota de Código en Apache HTTP Server

- **Descripción:** Las versiones de Apache HTTP Server 2.4.59 y anteriores son vulnerables a la divulgación de información, SSRF o ejecución de scripts locales a través de aplicaciones backend cuyas cabeceras de respuesta son maliciosas o explotables.

- **Impacto:** Un atacante podría explotar esta vulnerabilidad para ejecutar código arbitrario en el servidor afectado, comprometiendo su integridad y confidencialidad.

- **Severidad:** Crítica (CVSS v3.1: 9.8)

- **Fecha de Publicación:** 1 de julio de 2024

---

2. CVE-2024-38476: Vulnerabilidad de Denegación de Servicio en mod_proxy de Apache HTTP Server

- **Descripción:** Un fallo de desreferencia de puntero nulo en el módulo mod_proxy de Apache HTTP Server 2.4.59 y versiones anteriores permite a un atacante malicioso enviar una solicitud que provoque la caída del servidor.

- **Impacto:** Un atacante podría causar una denegación de servicio, haciendo que el servidor web deje de responder a nuevas solicitudes.

- **Severidad:** Alta (CVSS v3.1: 7.5)

- **Fecha de Publicación:** 1 de julio de 2024

---

3. CVE-2023-31122: Vulnerabilidad de Ejecución de Scripts No Autorizados en mod_rewrite de Apache HTTP Server

- **Descripción:** Un problema de codificación en sustituciones del módulo mod_rewrite en Apache HTTP Server 2.4.59 y versiones anteriores permite a un atacante ejecutar scripts en directorios permitidos por la configuración pero no directamente accesibles por ninguna URL.

- **Impacto:** Un atacante podría ejecutar scripts no autorizados o acceder a información sensible en el servidor afectado.

- **Severidad:** Crítica (CVSS v3.1: 9.8)

- **Fecha de Publicación:** 1 de julio de 2024

Fuente:

https://nvd.nist.gov/vuln/search/results?cpe_version=cpe%3A%2Fa%3Aapache%3Ahttp_server%3A2.4.6&cves=on&form_type=Advanced