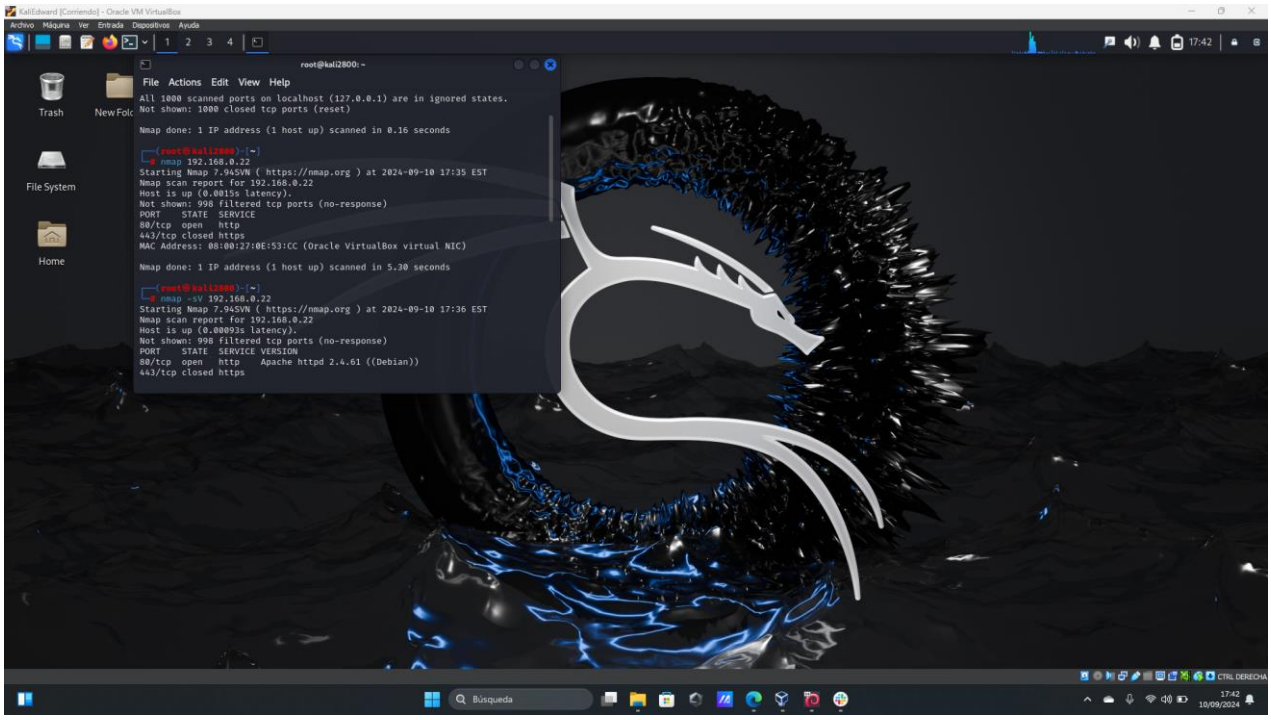
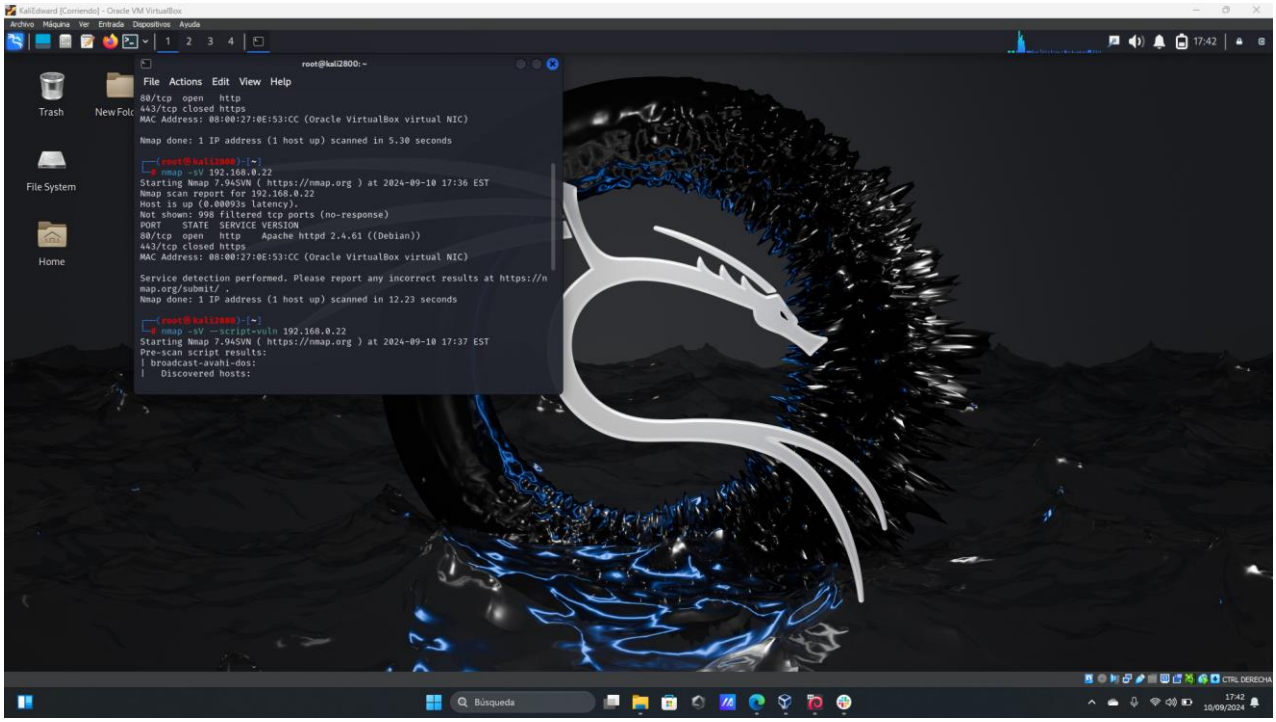
Reporte Escaneo de puertos con NMAP

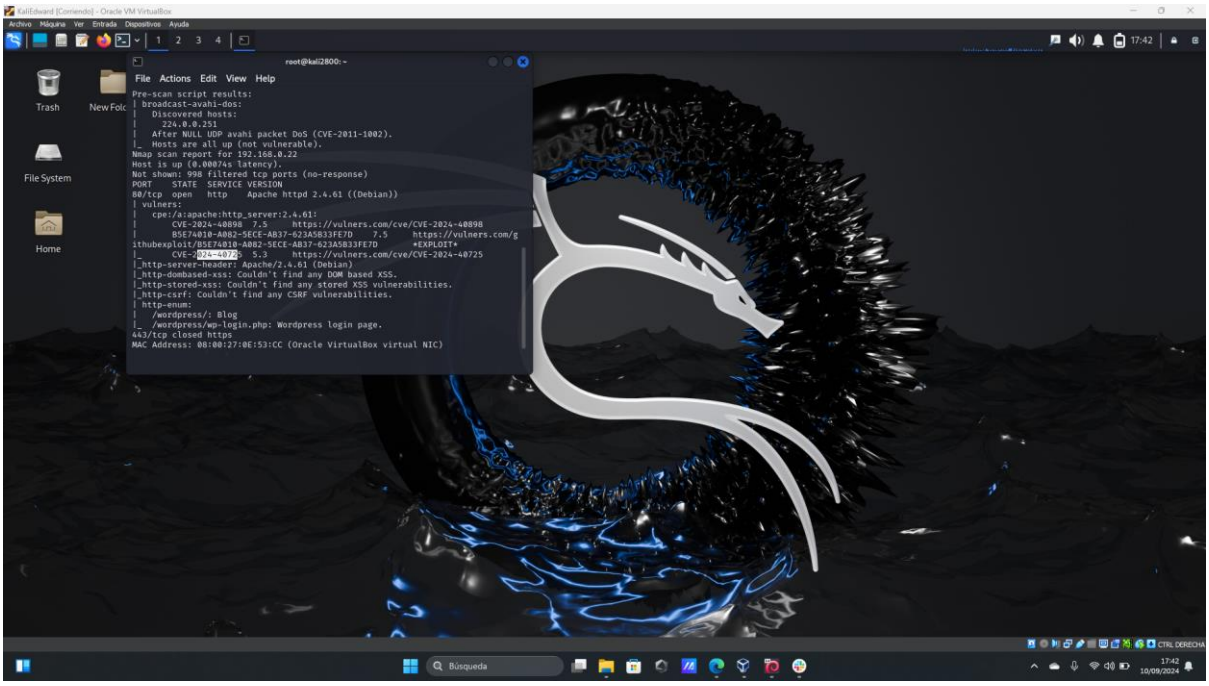
- Escaneo básico de un objetivo.



- Escaneo de puertos y servicios.



- Escaneo detallado y búsqueda de vulnerabilidades.



Nota de los servicios y sus versiones a partir del escaneo con NMAP.

- Puerto: 80/tcp, Estado: Abierto, Servicio: HTTP, Versión: Apache httdp 2.4.61 .
- Puerto: 443/tcp, Estado: Cerrado, Servicio: HTTP.

Vulnerabilidades.

- CVE-2024-4075 Vulnerabilidad en Servidor Apache HTTP.

Descripción: Una solución parcial para CVE-2024-39884 en el núcleo de Apache HTTP Server 2.4.61 ignora parte del uso de la configuración de controladores heredada basada en el tipo de contenido. "AddType" y configuraciones similares, en algunas circunstancias en las que los archivos se solicitan indirectamente, dan como resultado la divulgación del código fuente del contenido local. Por ejemplo, los scripts PHP pueden servirse en lugar de interpretarse. Se recomienda a los usuarios actualizar a la versión 2.4.62, que soluciona este problema.

- CVE-2024-40898 Vulnerabilidad en Servidor Apache HTTP 2.4.61

Descripción: Servidor HTTP Apache: SSRF con mod_rewrite en contexto de servidor/vhost en Windows (CVE-2024-40898) SSRF en el servidor HTTP Apache en Windows con mod_rewrite en contexto de servidor/vhost, permite filtrar potencialmente hashes NTLM a un servidor malicioso a través de SSRF y solicitudes maliciosas. Se recomienda a los usuarios actualizar a la versión 2.4.62, que soluciona este problema.