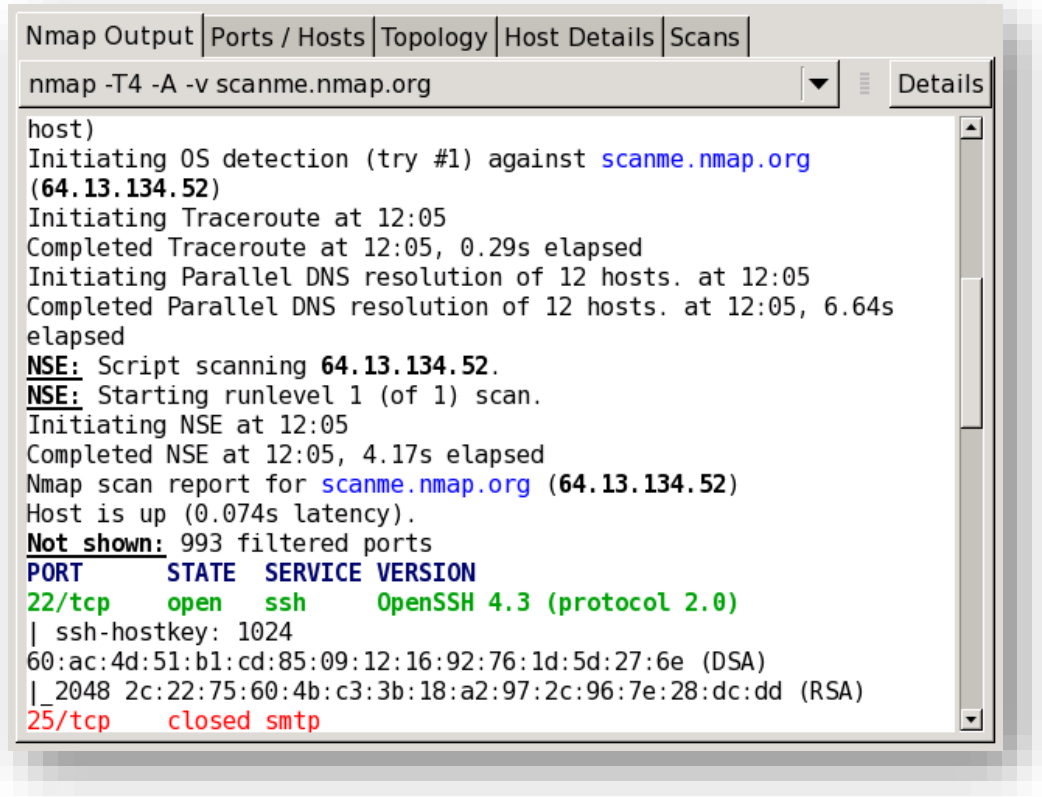
HERRAMIENTAS DE VULNERABILIDADES

MARCOS JAVIER CANCINO HERNÁNDEZ – A200353
ANÁLISIS DE VULNERABILIDADES - 7° "N"

NMAP

- Nmap, que significa "Network Mapper," es una herramienta de código abierto ampliamente utilizada para la exploración y el descubrimiento de redes, así como para el análisis de seguridad en sistemas informáticos.

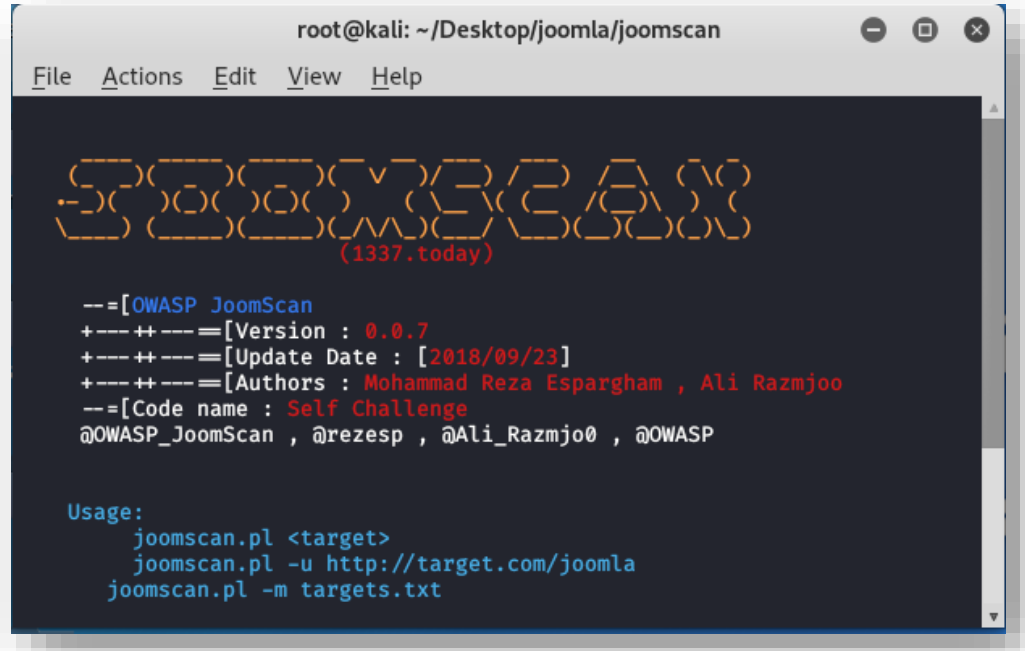
- Fue creado originalmente por Gordon Lyon (conocido por el seudónimo "Fyodor") y es ampliamente utilizado por administradores de sistemas y profesionales de seguridad para evaluar la seguridad de redes y sistemas, así como para llevar a cabo tareas de administración de redes.



JOOMSCAN

- Joomscan es una herramienta de código abierto diseñada específicamente para el escaneo de seguridad de sitios web construidos en el popular sistema de gestión de contenidos Joomla.

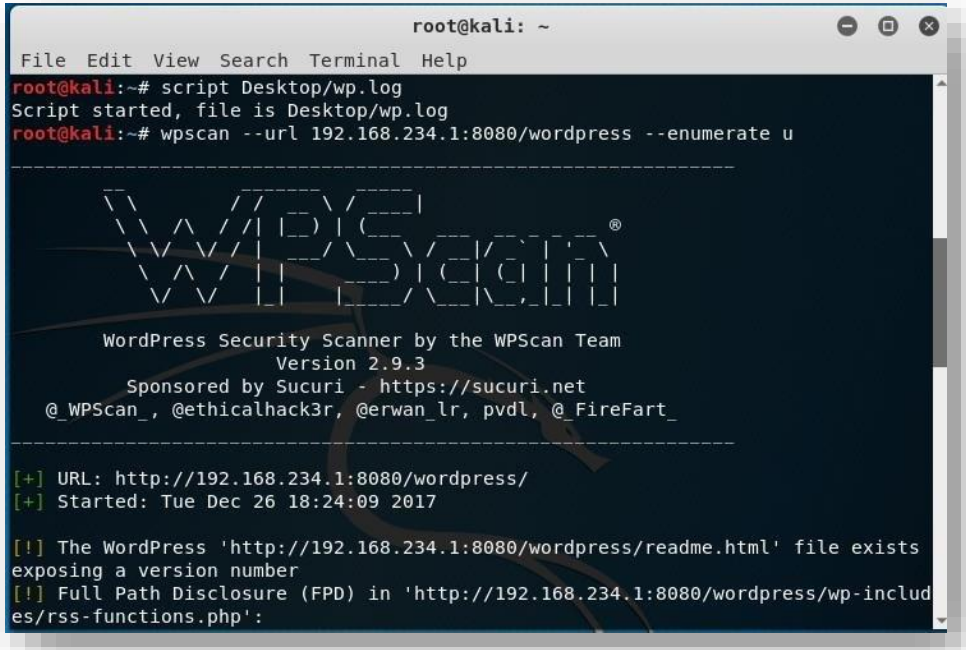
- Al igual que Nmap, Joomscan es utilizado por profesionales de seguridad y administradores de sistemas para identificar posibles vulnerabilidades y debilidades en sitios web Joomla.



WPSCAN

- WPScan es otra herramienta de seguridad de código abierto, pero está diseñada específicamente para el escaneo de seguridad de sitios web construidos en el sistema de gestión de contenidos WordPress.

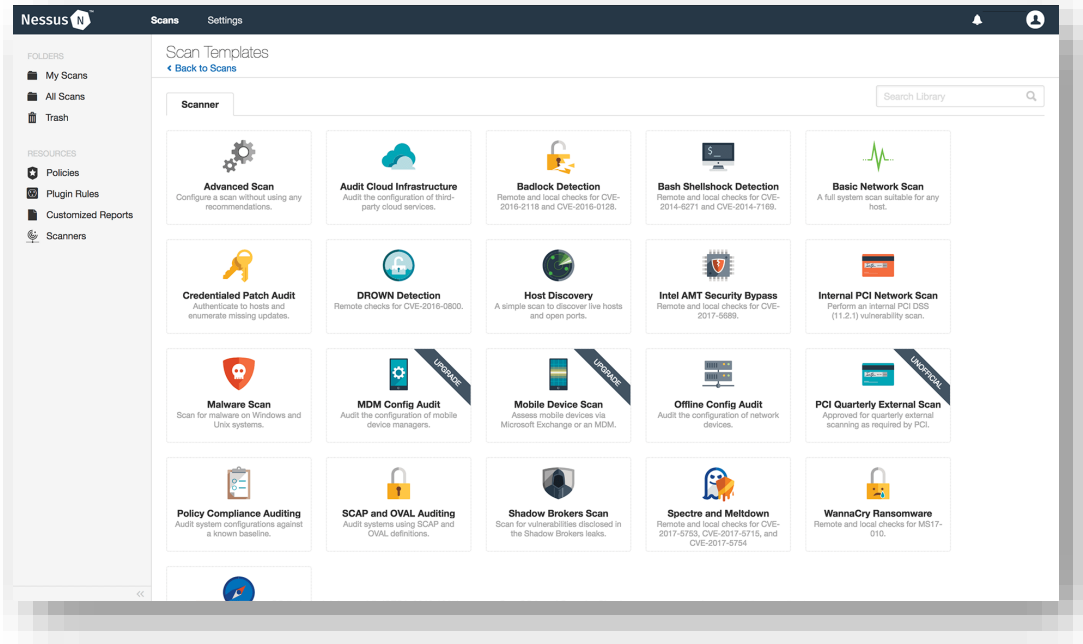
- Al igual que Nmap y Joomscan, WPScan se utiliza para identificar vulnerabilidades y debilidades en sitios web WordPress con el objetivo de mejorar su seguridad.



NESSUS ESSENTIALS

- Nessus Essentials es una versión gratuita y limitada del software de evaluación de vulnerabilidades Nessus, desarrollado por Tenable.

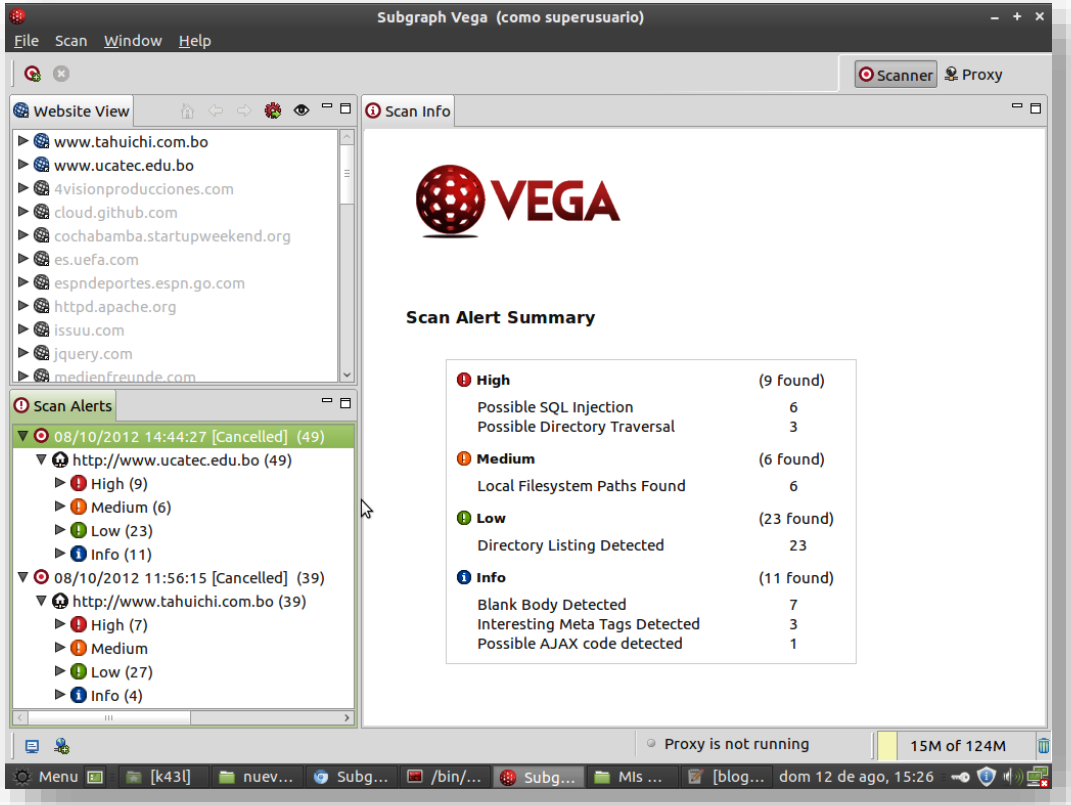
- Nessus es una herramienta de seguridad ampliamente utilizada para identificar vulnerabilidades en sistemas informáticos, redes y aplicaciones. Proporciona un escaneo exhaustivo y automatizado de activos y recursos en busca de debilidades que podrían ser aprovechadas por atacantes.



VEGA

- Vega es otra herramienta de seguridad de código abierto diseñada para la exploración y evaluación de vulnerabilidades en aplicaciones web.

- A diferencia de Nessus, que se enfoca en la evaluación de vulnerabilidades en sistemas y redes, Vega se centra en identificar debilidades específicas en aplicaciones web, incluidos problemas de seguridad en el código, configuraciones incorrectas y posibles riesgos de seguridad.



EL USO DE ESTAS HERRAMIENTAS DEBE SER PARTE DE UNA ESTRATEGIA GENERAL DE SEGURIDAD CIBERNÉTICA Y PRUEBAS DE PENETRACIÓN, Y SE DEBE COMBINAR CON BUENAS PRÁCTICAS DE DESARROLLO SEGURO Y ADMINISTRACIÓN DE SISTEMAS PARA GARANTIZAR LA PROTECCIÓN EFECTIVA DE LAS APLICACIONES Y SISTEMAS.