Report RedHat Linux 7.2 (apache-1.3.20-16)

Análisis de Vulnerabilidades

Informe Técnico

Resumen

El día 03/03/2021 se entregó el informe de Análisis de Vulnerabilidades del proyecto llamado Report RedHat Linux 7.2 (apache-1.3.20-16) en la cual se han encontrado 2 vulnerabilidades y 0 informativa incluyendo 2 vulnerabilidades de riesgo alto, 0 vulnerabilidades de riesgo medio y 0 vulnerabilidades de riesgo bajo. En cada detalle de las vulnerabilidades se brinda una posible solución de las mismas.

Metodología de Trabajo

Nuestro trabajo se llevó a cabo basándonos en la utilización de la metodología "OSSTMM", la Metodología Abierta de Testeo de la Seguridad.

La metodología OSSTMM (Metodología Abierta de Testeo de la Seguridad), creada por la organización ISECOM, el Instituto para la Seguridad y las Metodologías Abiertas, es uno de los estándares profesionales más completos y comúnmente utilizados en Auditorías de Seguridad para revisar la Seguridad de los Sistemas desde Internet. Incluye un marco de trabajo que describe las fases que habría de realizar para la ejecución de la auditoría.

OSSTMM se centra en los detalles técnicos de los elementos que necesitan ser comprobados, qué hacer antes, durante y después de las pruebas de seguridad, así como evaluar los resultados obtenidos.

Si bien se trata de un proceso mayoritariamente manual, durante el mismo se utilizarán una serie de herramientas que permiten disminuir los tiempos necesarios para la finalización de las tareas, como así también permiten la manipulación del tráfico enviado a los servicios web analizados.

Debajo damos a conocer algunas de las herramientas utilizadas durante las pruebas:

• Acunetix

o Scanner de vulnerabilidades web utilizado para detectar problemas globales de seguridad en aplicaciones web.

• Nessus Vulnerability Scanner / OpenVAS

o Herramienta de identificación de vulnerabilidades, basada en el escaneo de un rango de direcciones IP. La misma posee miles de pruebas de intrusión apuntadas a detectar vulnerabilidades de redes basadas en servicios TCP/UDP.

• Qualys

o Scanner de vulnerabilidades utilizado para la detección de parches faltantes, errores de configuración y configuraciones por defecto en el sistema operativo y servicios que corren en los servidores analizados.

• Nmap

o Scanner de puertos y servicios. Permite determinar los puertos abiertos que posee un equipo y el tipo y versión de los servicios que corren en los mismos.

• Burp Suite

o Proxy local que permite efectuar la manipulación de peticiones enviadas a un servidor.

• Wireshark

o Analizador de protocolos utilizado para detectar falencias en el desarrollo de sistemas.

• Kali

o Es una distribución de Linux pensada y diseñada para la auditoría de seguridad informática, enfocada en pruebas de intrusión.

• Metasploit

o Es un framework para la ejecución de scripts de explotación sobre vulnerabilidades conocidas.

• Cain & Abel

o Herramienta utilizada para la recuperación de contraseñas en plataformas Microsoft, entre otras.

• John the Ripper

o Herramienta utilizada para crackear hashes de contraseña de diferentes plataformas.

• Netcat

o Herramienta utilizada para abrir puertos, forzar conexiones TCP/UDP y establecer una línea de comandos remota en los sistemas afectados.

• Programas internos

o Scripts desarrollados por el área de Seguridad Informática del Grupo Telecom para efectuar el análisis de determinadas configuraciones.

Clasificación de Riesgo

A continuación se detalla la descripción de los riesgos:

Riesgo Crítico

Se refiere a vulnerabilidades en las cuales su explotación puede derivar en un compromiso total de la confidencialidad, integridad y/o disponibilidad del dispositivo en sí y eventualmente de otros componentes conectados.

Riesgo Alto

Se refiere a vulnerabilidades en las cuales su explotación puede derivar en un compromiso de la confidencialidad, integridad y/o disponibilidad del dispositivo en sí.

Riesgo Medio

Se refiere a vulnerabilidades cuya explotación puede derivar en el compromiso de algún atributo de seguridad, pudiendo afectar tanto a recursos críticos como no críticos de la infraestructura.

Riesgo Bajo

Se refiere a vulnerabilidades menores, por ej. Divulgación de información no sensitiva.

Riesgo Informativo

Se refiere a vulnerabilidades que, dada su baja probabilidad de ocurrencia y escaso impacto, se informan como informativas, sin requerir una acción directa.

Vulnerabilidades detectadas

Se han detectado las siguientes vulnerabilidades Web:

Se han identificado la cantidad de 2 vulnerabilidades y 0 informativa incluyendo 2 vulnerabilidades de riesgo alto, 0 vulnerabilidades de riesgo medio y 0 vulnerabilidades de riesgo bajo.

Detalle de las vulnerabilidades

A continuación van los detalles de las vulnerabilidades:

|  |
| --- |
| EOL/Obsolete Software: Samba 4.x Detected - Riesgo: Alto |
|  |

|  |
| --- |
| OpenSSL Multiple Vulnerabilities - Riesgo: Alto |
|  |

Resumen Ejecutivo

Se recomienda realizar un plan de acción pare resolver los puntos expuestos en el presente informe.



Anexo

A continuación van los anexos de cada vulnerabilidad.