Generando un Reporte de Pentest

www.lnxnetwork.com

Recopilación de información en las Fases del Pentest

De donde recopilar información?

1. **Recopilación de información preliminar**
2. **Enumeración de la red**
3. **Exploración de los sistemas**
4. **Extracción de información**
5. **Acceso no autorizado a información sensible**
6. **Auditoría de las aplicaciones web**
7. **Elaboración de informespreliminares**
8. **Informe final**

Generando un Reporte de Pentest

Cuál es el objetivo del Informe de Pentest o de un hacking ético (ethical hacking)?

El objetivo es encontrar las vulnerabilidades y plantear paliaciones para mitigar dichas vulnerabilidades

Generando un Reporte de Pentest

Informe de vulnerabilidades

Teniendo claro que nuestro público objetivo será distinto del que explicaba para el resumen ejecutivo podemos enfocarnos en los aspectos técnicos de nuestro ethical hacking.

Generando un Reporte de Pentest

En este apartado de nuestro reporte tenemos que dejar en claro varios aspectos:

- **Las vulnerabilidades encontradas.**
- **Cómo fueron explotadas; es decir metodología, pasos para reproducirla, exploit utilizados.**
- **Qué máquinas o recursos fueron vulnerados.**

Generando un Reporte de Pentest

Todo esto lo podemos organizar desde 2 puntos de vista, dependiendo del tamaño y complejidad de nuestro pentest:

- **Vulnerabilidades por tipo**
- **Vulnerabilidades por objetivo**

Generando un Reporte de Pentest

Vulnerabilidades por tipo

Enfocado mayormente en un ethical hacking a una empresa mediana a grande, con una cantidad considerable de activos y donde se identifican ciertas vulnerabilidades que se repiten y que permiten agrupar estos recursos enfocándonos más en la vulnerabilidad en cuestión y no en los activos involucrados.

Generando un Reporte de Pentest

Para cada vulnerabilidad encontrada y explotada, se debe identificar su:

- **Nombre**
- **Descripción breve**
- **Impacto en la organización**
- **Clasificación**
- **ID único en caso que corresponda**

Generando un Reporte de Pentest

Además, se debe describir de manera explícita cuáles fueron los objetivos afectados por esta vulnerabilidad, ya sea una IP + puerto, Aplicación, URL o incluso podemos llegar a agrupar por departamento dentro de la organización (Informática, Ventas, Atención al Cliente, Directorio etc.).

Generando un Reporte de Pentest

Finalmente, para cada una de estas vulnerabilidades se debe proporcionar una prueba de concepto que valide la explotación, ya sea con el código utilizado (payload) o con screenshots de pantalla con el resultado obtenido.

Generando un Reporte de Pentest

Vulnerabilidades por objetivo

A diferencia del anterior formato de presentación, se utiliza la identificación por objetivo en el caso de vulnerabilidades muy heterogéneas o en que el alcance del pentest sea pequeño en cuanto a activos o recursos explotados.

Se debe proporcionar la siguiente información:

- **El objetivo alcanzado**
- **Un listado de las vulnerabilidades**

  (cada una con su propia descripción similar en contenido a la explicada anteriormente para las vulnerabilidades por tipo).

Generando un Reporte de Pentest

Las acciones de remediación

Dentro de todo reporte de pentest, es fundamental poder definir los pasos a seguir para corregir los problemas identificados. Debemos considerar lo siguiente:

- **Priorizar**
- **Medidas a tomar**

Generando un Reporte de Pentest

Priorizar

Según el impacto que puedan tener las vulnerabilidades encontradas, existirán algunas medidas que deberán ser necesarias tomar a corto plazo para minimizar el riesgo al que se encuentra expuesta la organización.

En caso que algunas medidas además sean relativamente fáciles de implementar y con un costo bajo, también podrán priorizarse en el roadmap de acciones de remediación. Sin embargo existirán otras acciones que son más a largo plazo ya sea por su complejidad y costos. Para poder llegar a hacer este análisis se debe entender bien a la empresa que se está testeando y por supuesto validar con ellos las capacidades y condiciones con las que cuentan.

Generando un Reporte de Pentest

Medidas a tomar

En esta parte del reporte se define un listado de acciones que se recomienda al cliente de realizar, desde un punto de vista general y donde se consideran por ejemplo la aplicación de parches de seguridad y actualización.

Un punto aparte se debe entregar para el caso de una organización que no cuenta con un manual de buenas prácticas de seguridad en sus procesos tecnológicos y será necesario apoyar al cliente en el proceso de adopción de estas recomendaciones.

Generando un Reporte de Pentest

El registro de logs

Finalmente, todo reporte debe contener el registro detallado de las acciones realizadas durante las pruebas, identificando específicamente:

- **Fecha del test**
- **Objetivo atacado**
- **Tipo de prueba**
- **IP de origen**
- **Herramientas utilizadas (opcional)**
- **Pentester a cargo**

Generando un Reporte de Pentest

Ya se tiene en claro todas las secciones que debe contener nuestro reporte técnico de un pentest.

Como última consideración es recomendar que al momento de realizar un ethical hacking, uno de los aspectos más importantes a realizar (sino el más) es tomar notas de todos los procesos que se realizan. Esto facilitará enormemente la etapa final de generación del reporte y sobre todo facilitará el orden de toda la información recopilada.

Generando un Reporte de Pentest

(Ver ejemplo)

Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

Preguntas?

Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

LNXnetwork
SOLUCIONES ALTERNATIVAS

Centro de Ethical Hacking & Security