**Informe Auditoría**

****

**Qué es**

*Una auditoría de seguridad informática o auditoría de seguridad de sistemas de información (SI) es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales para identificar, enumerar y posteriormente describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.*

*Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables quienes deberán establecer medidas preventivas de refuerzo y/o corrección siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.*

(Fuente: Wikipedia, https://es.wikipedia.org/wiki/Auditor

%C3%ADa\_de\_seguridad\_de\_sistemas\_de\_informaci%C3%B3n)

**INFORME AUDITORÍA - SMM S.L.**

****

**Índice**

**1. Objetivos**

* Cuál es el grado de exposición a posibles amenazas y ciberataques.
* Qué inconvenientes existen para garantizar la confidencialidad, integridad y disponibilidad de la información.
* Qué tan óptimos son los sistemas y programas instalados.
* Qué tan seguras son las contraseñas utilizadas por el personal de la empresa.
* Cómo se están cumpliendo las políticas y manuales de ciberseguridad implementados.

**2. Resumen ejecutivo**

Realizando muchas pruebas, y exploits, planteamos más adelante todas las vulnerabilidades encontradas en el Sistema Operativo de la empresa. Mayoritariamente todas las vulnerabilidades encontradas son servicios de una máquina de la empresa, y nos parece muy importante que quede documentado cada una de las vulnerabilidades con el fin de mejorar la seguridad de la empresa y de los empleados.

**3. Metodología**

En el proyecto de pruebas hemos empleado una máquina con el Sistema Operativo de Linux (Kali Linux) destinada principalmente al ámbito de la ciberseguridad, en ella tenemos instalado un software dedicado (Metaexploit) a ataques (exploits, payloads, auxiliares, mapeo de red…). Hemos realizado todos los ataques con destino a un equipo remoto de la empresa (Metaexploitable).

**4. Planificación**

**Reconocimiento** (Footprinting y Scanning: elección de máquina a atacar, escaneo de todos sus servicios).

**Preparación** (Máquina metasploitable, softwares…)

**Distribución**

**Explotación** (Exploits, Payload…)

**5. Tareas realizadas**

[PracticaExploit](https://docs.google.com/document/d/1Ic89MWGuLyCqVqPlzdZQZ67aRdpqOxL9bSO2lwi5T8o/edit?usp=sharing)

**6. Tabla de vulnerabilidades encontradas**

| **Equipo** | **SO** | **IP** | **Puerto**  **(TCP/**  **UDP)** | **Aplicación - Versión** | **ID**  **Vulnerabilidad** | **Explotable** | **Nivel de riesgo** | **Observaciones** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| metaexplotable | Linux | 10.110.0.73 | 80 | HTTP | 1111111 | Éxito | Alto | Puerto **tikiwiki** y realizar una conexión al servidor metasploit utilizando **netcat**. |
| metaexplotable | Linux | 10.110.0.73 | 21 | VSFTPD | 222222 | Éxito | Alto | **Backdoor** |
| metaexplotable | linux | 10.110.0.73 | 6667 | UnrealiRCd | 333333 | Éxito | Alto | **Unix Command**  **Shell** |
| metaexplable | linux | 10.110.0.73 | 80 | Apache | 444444 | Sin éxito | Bajo | **Meterpreter:**  **wp\_phpmailer\_host\_header**  **Custom Payload** |

**7. Análisis e informe de resultados**

-Tanto HTTP, VSFTPD, UnrealiRCD son altamente vulnerables: con una tremenda facilidad encontramos acceso como administrador a la máquina. De forma que se puede dañar cualquier cosa.

-Por otro lado, Apache no pudo ser atacado porque el ataque era en función del Wordpress, servicio no instalado en el cliente. Por tanto ya sabemos un servicio al que no se puede atacar porque no se utiliza en la empresa.

**8. Recomendaciones de seguridad y conclusiones**

Bloquear los puertos, cambiar las contraseñas, hacer copias de seguridad, no poner una ip estática para dificultar más el acceso del atacante, . En general configurar de forma exhaustiva el Firewall de cada uno de los clientes de la empresa y de los propios servidores. Tener cuidado con los puertos conocidos ya que parecen ser bastantes vulnerables ya que están en constante pruebas por hackers.

**Consejos**

\* Guardar toda la información del proceso

\* Llevar un cuaderno de bitácora

\* Poner nombre con sentido a las capturas de pantalla…

\* Utilizar herramientas asociativas/colaborativas de recopilación y organización de la información \* Almacenar la información por categorías

\* Utilizar un checklist de elementos a auditar (antes de firmar el acuerdo con el cliente) Seguridad física

Seguridad de redes

Usuarios

Contraseñas

Servicios

Almacenamiento de datos

Aplicaciones

Cumplimiento de la legislación (LOPD, LSSICE, LPI, ...)

Estándares de calidad - ISO27001

…