Test de Intrusión

Una de las labores fundamentales, antes de poner un servidor en producción, es que pase un *test de intrusión* o, si los recursos existentes lo permiten, una auditoría de seguridad. Para ello, se contratará a un especialista en detectar y realizar pruebas de intrusión en un sistema informático, para evaluar el impacto que las malas configuraciones o vulnerabilidades encontradas puedan tener sobre el sistema.

Al especialista en realizar estas pruebas ofensivas en el sistema informático se le conoce como auditor de sistemas o [*pentester*](https://es.infosecaddicts.com/career-path/por-que-y-como-convertirse-en-un-tester-de-penetracion/#:~:text=De%20acuerdo%20con%20PayScale%2C%20un,alrededor%20de%20%24%20117.398%20por%20a%C3%B1o.): persona que realiza test de intrusión en un sistema informático para detectar vulnerabilidades, medir el impacto de éstas y hacer que las vulnerabilidades sean corregidas.

Para ello, el *pentester*, entregará un documento donde recoja todas las pruebas realizadas y cuáles han sido los resultados obtenidos en cada una de las pruebas realizadas.

**Enunciado**

El objetivo de este trabajo es realizar un test de intrusión [sobre el activo (máquina virtual en el rango de IPs 192.168.4.0-254) proporcionado](https://centrodonbosco-my.sharepoint.com/:u:/g/personal/amador_centrodonbosco_es/EVSJV1pFZdFGmA1TUT4J17oBvBPVv513TcWFVk63Cj5mOQ?e=bficQg). La metodología a seguir será la siguiente:

1. Comprobar la comunicación a nivel de red con la máquina objetivo del test de intrusión.
2. Comprobar el estado de todos los puertos TCP/UDP la máquina objetivo del test de intrusión.
   1. Para cada uno de los puertos TCP/UDP descubiertos, ver qué servicios se ejecutan en ellos y si estos presentan [vulnerabilidades conocidas](https://www.exploit-db.com/).
   2. En función de las versión de los servicios que se ejecutan en los puertos TCP/UDP descubiertos, consultar en una base de conocimientos si existe algún *exploit* útil para explotar la vulnerabilidad conocida.
3. Comprobar el comportamiento de los servicios que se ejecutan en cada uno de los puertos TCP/UDP descubiertos.
4. En caso de tener acceso a la máquina, es interesante intentar obtener todos los privilegios administrativos en la máquina (escalada de privilegios), o incluso poder lograr tener persistencia dentro del sistema, por ejemplo, a través de la instalación de una puerta trasera, *backdoor*, creación de usuarios con privilegios administrativos, etcétera.

**Propuesta de Trabajo**

Se propone realizar un test de intrusión sobre el activo proporcionado por el profesor siguiendo los pasos anteriores y utilizando, al manos, las técnicas y las herramientas vistas en esta asignatura.

Las pruebas y los resultados obtenidos se documentarán en un **Informe de Auditoría** que constará de los siguientes apartados:

1. Descubrimiento de la dirección IP del activo a auditar.
2. Prueba de comunicación a nivel de red con la máquina objetivo.
3. Descubrimiento de los servicios presentes en los puertos TCP/UDP de los activos.
   1. Estado de los puertos TCP/UDP.
   2. Versiones de los servicios presentes en los puertos anteriores.
   3. Búsqueda de vulnerabilidades conocidas en los servicios anteriores.
4. Pruebas de fuerza bruta basada en diccionario sobre los servicios de red que necesiten autenticación de usuarios.
5. Para los aplicativos web descubiertos.
   1. Pruebas de las vulnerabilidades propias de aplicaciones web.
   2. Pruebas de inyección de código SQL sobre los parámetros GET/POST de las peticiones HTTP.
   3. Manipulación de parámetros presentes en la peticiones HTTP.
6. Una vez que se han conseguido credenciales de usuarios:
   1. Intento de lectura y extracción de los usuarios locales y sus contraseñas.
   2. Intento de acceso a través de los usuarios administrativos *root* (escalada de privilegios).
   3. Ejecución de comandos para la creación de un nuevo usuario para lograr la persistencia en el sistema (persistencia en el sistema).