**Informe Ejecutivo – Proceso de Pentesting**

**Laboratorio de Seguridad Ofensiva – Kali Linux/Windows7**

## 1) Objetivo del Pentesting

Identificación y explotación de vulnerabilidades existentes en un sistema operativo Windows 7, en un ambiente de máquinas virtuales.

## 2) Alcance y Activos del Pentesting

El alcance se compone de un ambiente controlado de máquinas virtuales, habiendo sido el principal objetivo de pruebas una máquina virtual con S.O. Windows 7, con el fin de encontrar y analizar vulnerabilidades del sistema.

* **Tipo de auditoría:** Canal de seguridad de redes de datos. (COMSEC)
* **Tipo de prueba de penetración:** Test de caja blanca o doble caja gris.
* **Activos identificados:** Máquina virtual S.O. Windows 7.
* **Vectores de ataque:** Sniffing, Spoofing, DoS, Exploits.
* **Elementos de detección activa:** Firewall y Windows Defender.
* **Puertos testeados del host:** 135, 137, 139, 445, 554, 2069, 5357, 10243.
* **Puertos testeados del DNS:** 53**.**

## 3) Resumen de Vulnerabilidades y Amenazas Posibles

* Escalabilidad de privilegios por parte de usuarios externos o posibles atacantes.
* Obtención de accesos no autorizados mediante exploits.
* Denegación de servicios a puertos del host y suplantación de IP origen.
* Denegación de servicios a puertos del DNS y suplantación de IP origen.
* Ataques de fuerza bruta desde puertos abiertos.
* Interceptación, lectura, inserción y modificación de mensajes mediante ataques Man in the Middle en puertos abiertos.
* Ataque al sistema desde puertos abiertos con troyanos, gusanos y virus.

## 4) Recomendaciones y métodos de protección posibles a adoptar

* 1. Se recomienda comprender el alto riesgo a la que está expuesta la maquina víctima. Estas vulnerabilidades se pueden materializar en amenazas y al tener una seguridad mínima, esta red puede ser víctima de ataques de gran magnitud e impacto.
  2. Se recomienda la actualización constante del sistema evaluado, considerando que algunos de los ataques de denegación de servicio tienen su origen en sistemas desactualizados.
  3. Se recomienda realizar regularmente una limpieza de la máquina virtual víctima para descartar que tengan rastros de virus.
  4. Se recomienda implementar un sistema de detección y prevención de intrusiones (IDS/IPS) que monitorice las conexiones y nos alerte si detecta intentos de acceso no autorizados o mal uso de protocolos.
  5. Se recomienda reducir la superficie de ataque lo máximo posible, por lo que cualquier servicio que no sea estrictamente necesario para el correcto funcionamiento del sistema debe ser desinstalado. Cuanto menor sea la superficie de ataque, menor será la posibilidad de sufrir un daño.
  6. Se recomienda realizar respaldos periódicos de la información contenida en el sistema.
  7. Se recomienda considerar el cierre de los puertos más críticos del host, en caso de persistir los problemas relativos a puertos abiertos, teniendo en cuenta que sus servicios y protocolos asociados no se encontrarán disponibles para otros servicios.
  8. Se recomienda cambiar los nombres de usuarios predeterminados. (Ej: “Admin” por uno único o cifrado)
  9. Se recomienda evitar ingresar a redes públicas o de baja confianza en Internet, así como posiblemente adoptar el uso de servicios VPN para mejorar la seguridad de la máquina testeada.