Descripción servicio CSIRT

Índice

Seguridad y propiedad intelectual

CLASIFICACIÓN	**Confidencial**
ÁREA	**Security Assesment Services**
AUTOR	**OneseQ**
FECHA DE CREACIÓN	**17/01/2022**

1. Análisis de vulnerabilidades

- Objetivo: Analizar y comprender las vulnerabilidades confirmadas.
- Definición:

  El servicio de análisis de vulnerabilidades consiste en funciones destinadas a comprender la vulnerabilidad y sus posibles repercusiones, identificar el problema o fallo subyacente (causa raíz) que permite explotar la vulnerabilidad, y determinar una o más estrategias de reparación o mitigación para evitar o reducir al mínimo la explotación de la vulnerabilidad.

OneseQ aboga por que todos nuestros clientes tengan entornos de trabajo seguros, así como unas directrices de mejora que hagan que el estado de seguridad y tranquilidad sean permanentes, garantizando la integridad, la seguridad y disponibilidad de todos los elementos de valor que componen sus activos ante cualquier situación no deseada.

Considerando el impacto que cualquier vulnerabilidad tiene para el desarrollo del negocio de nuestros clientes, se considera oportuno la ejecución de ciber-ejercicios de evaluación para medir el nivel de exposición al riesgo y vulnerabilidades, evaluar el estado de las medidas y controles de seguridad implementados y aportar las mejoras y soluciones adecuadas para cada vulnerabilidad detectada en este proceso.

De esta manera se garantiza que se pueda trabajar de una manera eficaz y autónoma, con la confianza de que la seguridad y disponibilidad de las infraestructuras y servicios expuestos esté garantizada siempre o en el peor de los casos que se pueda dar una rápida respuesta ante eventos que supongan un riesgo para la continuidad del negocio de nuestros clientes.

OneseQ propone la realización de test de vulnerabilidades automatizados, la evaluación y análisis de los resultados aportando las recomendaciones de medidas a tener en cuenta y los controles de seguridad que mitiguen las deficiencias localizadas.

Mediante la aplicación de las pruebas del test de vulnerabilidad y el análisis del nivel de exposición al riesgo, se pretende:

- Identificar las vulnerabilidades para poder mitigar los riesgos asociados a estas.
- Establecer los mecanismos reales y aplicables necesarios para corregir las vulnerabilidades detectadas en los análisis realizados.
- Realizar otros tipos de pruebas de intrusión que pudieran ser aplicables de acuerdo a los resultados de los test de vulnerabilidades y la experiencia del equipo de OneseQ.

1.1. Paso 1: Análisis y recopilación de información

Consiste en obtener la mayor información posible de los sistemas realizando un análisis del entorno contando con el apoyo de diferentes herramientas que cumplen este propósito.

Así se buscarán nombres de dominio, direcciones IP, posibles nombres de usuario, bases de datos públicas, etc.

Se analizarán los sistemas que se tengan como objetivo para identificar servicios activos, máquinas disponibles, mapeo de red, sistemas operativos, y cualquier elemento de configuración sobre los que vayamos a realizar el escaneo de vulnerabilidades.

1.2. Paso 2: Test de vulnerabilidades

Se realizan las pruebas y test ejecutados por autómatas para identificar recursos específicos y características concretas. Se buscan las versiones de los sistemas operativos y los servicios, los parches de seguridad, cuentas de usuario válidas. Se intenta localizar las posibles y potenciales vulnerabilidades tanto en la arquitectura de soporte, como en el sistema en sí.

1.3. Paso 3: Explotación

Es un conjunto de técnicas, para realizar una evaluación integral de las debilidades detectadas en las plataformas de soporte. Este modelo reproducirá intentos de acceso a los servicios web y servicios perimetrales, simulando un intruso potencial, de forma remota.

Permitirá detectar la potencial vulnerabilidad y los puntos débiles de la seguridad de la arquitectura que soporta las aplicaciones relativas a los servicios expuestos.

Nos permite definir otros objetivos secundarios sobre los que realizar pruebas dirigidas hacia otros servicios o sistemas tecnológicos.

Se realizarán ejercicios manuales de comprobación de las vulnerabilidades por el equipo técnico especialista. La explotación y la ejecución no se realizará a menos que hayan sido autorizados

1.4. Paso 4: Generación de informes

Esta fase es considerada la más importante del test y es en la que se informará sobre cada una de las acciones y pruebas que se han realizado. Se incluye una descripción de las técnicas y herramientas utilizadas en la realización de los test, así como las vulnerabilidades descubiertas y el nivel de gravedad que estas suponen.

Se elaboran los entregables finales, que cómo mínimo incluye:

- Informes técnicos
    - Mapa de arquitectura de seguridad actual
    - Mapa propuesto para mejorar la arquitectura de seguridad
    - Normas de seguridad y buenas prácticas
- Informe ejecutivo
- Recomendaciones de seguridad
    - Recomendaciones tecnológicas para la protección y defensa
    - Recomendaciones de soluciones y servicios

2. Metodología de trabajo

La metodología empleada por OneseQ está basada en el modelo OSSTMM (Open Source Security Testing Methodologies) y OWASP que cumplen lo especificado en la LOPD y la norma ISO 17799/27000 entre otras, con lo que se procede al análisis exhaustivo no sólo de las vulnerabilidades sino de los procedimientos y modos de actuación:

- **Test de Acierto**: análisis externo de seguridad ejecutado desde el SOC por autómatas en busca de vulnerabilidades en los servicios de cara a Internet y fallos de configuración de aplicaciones/servicios Web, servidores, routers, comms y firewalls, etc.
- **Análisis Interno**: evaluación de la seguridad interna del aplicativo en busca de vulnerabilidades en los servicios y fallos de configuración de aplicaciones/servicios web del alcance.

La gestión de los procesos de gestión del proyecto seguirá la metodología ITILv3 para garantizar la estandarización y calidad del proyecto.

3. Esquema de gestión

El método de trabajo del técnico especialista pasará por las siguientes etapas:

- Definición de Alcance y Objetivos del ciber-ejercicio de Test de intrusión del sistema en producción para la detección de posibles vulnerabilidades
- Estudio inicial del entorno a evaluar
- Determinación de las características y granularidad que se aplicará al ciber-ejercicio de test de intrusión
- Elaboración de la planificación y esquemas del ciber-ejercicio
- Actividades automatizadas y planificadas propias del ciber-ejercicio de test de intrusión

Elaboración de los entregables finales del proyecto.

4. Premisas de seguridad

Se debe determinar cómo se considerará el nivel de riesgo estimado (Alto/Medio/Bajo/Tolerable) que se utilizará como parámetro para la calificación de las vulnerabilidades.

- No se ejecutará simultáneamente más de una herramienta de ataque por objetivo de test, para evitar o minimizar la explotación accidental de vulnerabilidades que generen impacto en la capacidad y/o disponibilidad sobre las plataformas tecnológicas o dispositivos de conexión.
- Una misma prueba o fase se podrá ejecutar sobre los Servidores Objetivo más de una vez, pero con distinta herramienta, para propósitos de comparación y optimización de resultados.
- Se debe llevar un registro y documentación de la evidencia y vulnerabilidades identificadas por cada objetivo del ciber-ejercicio.
- Las pruebas de vulnerabilidad se deberán realizarán con absoluto consentimiento y aprobación del comité de cambios para evitar caídas o fallos en los servidores, ciclos inactivos o cualquier otro incidente causado de manera inadvertida por las actividades de escaneo. Para lo cual el ciber-ejercicio automatizado deberá previamente determinar que se requiere para ejecutar las pruebas en un ambiente controlado.
- Por ningún motivo y bajo ningún concepto se autoriza al equipo de trabajo integro a divulgar información que se obtenga en el desarrollo de los ejercicios.
- Los ciber-ejercicios deben garantizar el cumplimiento de la política de gestión que este ya integrada en el CLIENTE, sus procedimientos, instructivos y manuales.
- El ciber-ejercicio automatizado deberá estar directa y constantemente vinculado con la ejecución del objeto del proyecto, de acuerdo con el plan de características y cargas de trabajo, durante el proceso y realización de cada escenario del test.
- El equipo de trabajo debe contar como mínimo con una persona de CLIENTE, con cargo y perfil de autoridad para despejar posibles contratiempos en las fases de provisión de los requerimientos del test. Sólo se requiere un Jefe de Proyecto y un especialista para las pruebas del ciber-ejercicio de test de vulnerabilidad.

5. Contexto del ciber-ejercicio

Cada escenario deberá desarrollarse siguiendo las fases establecidas en el plan de trabajo y presentando toda la documentación a satisfacción de conformidad con la planificación de entregables.

OneseQ y cualquier CLIENTE ajustarán las fechas de inicio y fin de cada una de las actividades contenidas en el plan de trabajo y además establecerán el criterio de seguimiento y control de los resultados esperados.

OneseQ y el CLIENTE deben realizar como primera etapa del proyecto la identificación y evaluación de riesgo de la ejecución de las pruebas de vulnerabilidad, que contenga mínimo la siguiente información:

- Descripción de la Actividad
- Amenaza
- Vulnerabilidad
- Descripción del Riesgo
- Probabilidad de Ocurrencia
- Impacto
- Nivel de riesgo
- Recomendaciones y/o actividades que lo mitigan

En esta fase, para la aplicación del segundo escenario de pruebas y análisis del nivel de exposición al riesgo, se deberá tomar la información encontrada y generada del primer escenario, para realizar un comparativo del estado de identificación y evaluación de riesgo.

Para las pruebas contra los activos de información únicamente se necesitará las direcciones IPs y los servicios asociados.

Dependiendo de la información obtenida durante el levantamiento de información el especialista establecerá la o las herramientas necesarias para la aplicación de las pruebas de vulnerabilidad.

Por cada ciclo de análisis de vulnerabilidades realizado y finalizado el especialista entregará un informe ejecutivo que contenga como mínimo los siguientes elementos:

- Descripción de las pruebas realizadas.
- Metodología utilizada.
- Listado de vulnerabilidades encontradas en los elementos de la plataforma tecnológica.
- Puertos y servicios habilitados.
- Evidencias de la información a la que se tuvo acceso dentro del dispositivo.
- Las acciones que se pudieron realizar.
- Identificación de amenazas hacia la información (Pérdida, Modificación, Fuga u otro).
- Posible solución o recomendación para la corrección de vulnerabilidades que sea de naturaleza realista y ejecutable, indicando las acciones a seguir.

En esta fase, para la aplicación del segundo escenario de pruebas, deberá tomar la información encontrada y generada del primer escenario, para realizar un comparativo del análisis de vulnerabilidades.

6. Requerimientos

Para llevar a cabo el servicio, será necesaria una carta de autorización para poder realizar las pruebas relativas al test de intrusión; un acuerdo de confidencialidad estará conformado como anexo a la aprobación del plan de trabajo. Asimismo, todos los test estarán documentados y esquematizados por escrito con anterioridad, de forma que haya una conformidad por las dos partes afectadas.

Como resultado del test de intrusión se obtiene un informe descriptor del estado actual de vulnerabilidades externas de los sistemas testeados. Incluirá todas las actividades realizadas, las vulnerabilidades y problemas de seguridad detectados y las recomendaciones de las soluciones a implementar para la corrección de los mismos.

Para el caso de la auditoría interna, se deberá proporcionar acceso al equipo Auditor mediante VPN, para los sistemas operativos Linux y Windows, y se dará soporte ante cualquier incidencia relativa a la conexión VPN, y otros imprevistos Internos que puedan surgir con respecto al enrutado de la Red. El enrutado es un punto clave, puesto que se debe llegar a todos los activos incluidos en el alcance de manera directa, sin interferencias de IPS/IDS, a no ser que sea requerido expresamente, lo que modificará el coste y esfuerzo requerido.

Se deberá proporcionar todos los datos requeridos, credenciales y tecnologías, así de un mapeo de Red que permita que todos los activos requeridos sean perfectamente auditados.

Se deberá proporcionar un contacto técnico, que apoye en todo momento el buen desarrollo del ejercicio.

7. Pruebas

7.1. Pruebas de servicios

- Escaneo Automático de Vulnerabilidades
- Medir la organización objetivo contra las herramientas populares de escaneo.
- Determinar las vulnerabilidades de los sistemas por tipo de servicio.
- Intentar emparejar las vulnerabilidades con las aplicaciones.
- Intentar determinar el tipo de aplicación y servicio por vulnerabilidad.
- Realizar un test redundante con al menos dos escáneres automáticos de vulnerabilidades.

Análisis de la información obtenida mediante las tecnologías y herramientas automatizadas:

- Identificar todas las vulnerabilidades de acuerdo a los sistemas operativos.
- Identificar todas las vulnerabilidades de sistemas similares que pueden también afectar a los sistemas objetivo.
- Verificación y comprobación manual de vulnerabilidades
- Verificar todas las vulnerabilidades encontradas durante la fase del desarrollo de exploits en busca de falsos positivos.
- Verificar todos los positivos altos y críticos
- Verificar la robustez y seguridad de los servicios SSL
- Realizar ataques de fuerza bruta sobre las plataformas que lo posibiliten
- Análisis del tráfico de Red en busca de anomalías.
- Descripción detallada del proceso de generación y presentación del Informe de auditoría final

La función del ciber-ejercicio se materializa exclusivamente por escrito. Por lo tanto, la elaboración final es el exponente de su calidad y el resultado de todas las operaciones realizadas.

En el desarrollo de esta fase el especialista y el jefe del proyecto realizaran un análisis de los resultados obtenidos para determinar si los efectos de las pruebas realizadas han cumplido el objetivo esperado, dependiendo de esta evaluación el especialista podrá reprogramar las pruebas que sean necesarias previo acuerdo con CLIENTE y luego terminará de preparar los informes y presentación correspondiente

8. Entregables

Estas pruebas de test de vulnerabilidades proporcionarán al área de seguridad TIC los siguientes entregables:

- Informe técnico de vulnerabilidades elaborado a través de la identificación automatizada de debilidades provocadas por una mala configuración de las aplicaciones.
- Análisis y categorización de las debilidades explotadas por los autómatas del SOC de OneseQ, con base al impacto potencial y la posibilidad de que la amenaza se convierta en realidad.
- Recomendaciones en base a las prioridades establecidas para mitigar y eliminar las vulnerabilidades y así reducir el riesgo de ocurrencia de cualquier evento desfavorable.
- Resumen ejecutivo del proyecto orientado a la alta dirección.

OneseQ entregará tanto en medio digital, como impreso, junto con el mismo informe escaneado cuando traiga firmas o en los formatos que sean compatibles con las herramientas de visualización de Documentos.

Al finalizar los dos escenarios de las pruebas del test de vulnerabilidades y análisis del nivel de explosión al riesgo, el jefe de proyecto elaborará el acta de cierre del proyecto y finalización del ciber-ejercicio.

Por cada ciclo de prueba finalizado y a petición específica del supervisor del proyecto asignado, el especialista podrá entregar un informe parcial de resultados que contenga como mínimo los siguientes elementos:

- Descripción del trabajo realizado
- Resumen de las actividades realizadas
- Descripción de principales hallazgos
- Conclusiones
- Recomendaciones