MINISTERIO PÚBLICO

Dirección de Tecnología de la Información y Comunicación

Informe Pericial

ADQUISICIÓN DE HERRAMIENTA PARA ESCANEO DE VULNERABILIDADES

MINISTERIO PÚBLICO
DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN
Santo Domingo, Rep. Dom.

Fecha Agosto 2022

Índice

MINISTERIO PÚBLICO
DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN
Santo Domingo, Rep. Dom.

1. Antecedentes

De acuerdo con los resultados de la encuesta realizada por ESET Latinoamérica para el documento ESET Security Report 2014, la explotación de vulnerabilidades se ha convertido en la mayor preocupación de las empresas en materia de seguridad, seguida de otros incidentes como infección por malware, fraudes, phishing o ataques de denegación de servicio (DoS).

En este sentido, la evaluación cobra relevancia para evitar las incidencias relacionadas con la explotación de las mismas y como un medio para la aplicación de un elemento de la denominada seguridad ofensiva, a través de los escáneres de vulnerabilidades.

Un escaneo de vulnerabilidades es una prueba de alto nivel y automatizada, la cual busca y reporta vulnerabilidades potencialmente identificadas. Cada día hay más vectores y/o factores que pueden influir a la explotación de una brecha de seguridad y que dan mala reputación a la organización. Los escáneres de vulnerabilidades son herramientas de software o hardware que se utilizan para diagnosticar y analizar computadoras conectadas a la red, lo que le permite examinar redes, computadoras y aplicaciones en busca de posibles problemas de seguridad, así como evaluar y corregir vulnerabilidades. A través de los escáneres de vulnerabilidades, se pueden escanear varias aplicaciones de un sistema en busca de posibles debilidades que los atacantes puedan aprovechar. Las herramientas de bajo nivel, como los escáneres de puertos, también se pueden utilizar para identificar y analizar posibles aplicaciones y protocolos que se ejecutan en un sistema. Por lo tanto, los escáneres están destinados a realizar las siguientes tareas: Identificación y análisis de vulnerabilidades Inventario de recursos como sistema operativo, software y dispositivos de red genere informes que describan vulnerabilidades y opciones de reparación.

Una gestión de vulnerabilidades oportuna mitiga el riesgo de que las amenazas impacten la operatividad de la organización.

La gestión eficiente de vulnerabilidades ofrece varios puntos positivos para la organización. Una de ellas es la mejora constante del rendimiento, ya que con la seguridad del sistema los riesgos con ataques maliciosos se reducen significativamente. Otro aspecto que podemos mencionar es la identificación de nuevas soluciones, con actualizaciones y configuraciones más eficientes y adecuadas al entorno interno.

2. Alcance e Importancia

Las herramientas de escaneo de vulnerabilidades nos permiten encontrar las debilidades en las plataformas de software o hardware para solucionar las fallas, antes de que puedan generar un impacto negativo en la organización.

MINISTERIO PÚBLICO
DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN
Santo Domingo, Rep. Dom.

El alcance va dirigido a la detección proactiva de activos, el monitoreo continuo, la mitigación, la corrección y las tácticas de defensa que se necesitan para proteger la superficie de ataque moderna de TI de la organización contra la ciber-exposición.

El Instituto Nacional de Estándares y Tecnología (NIST) recomienda que los análisis de vulnerabilidades se ejecuten al menos trimestralmente, independientemente del tamaño o tipo de red.

Para cualquier organización que confíe en la disponibilidad continua de su red informática para operaciones regulares, los análisis de vulnerabilidad deben ejecutarse al menos una vez al mes e incluso con más frecuencia para las organizaciones que recopilan y/o procesan datos personales o confidenciales.

Un componente importante en la lucha contra un ataque potencial es implementar un escaneo de vulnerabilidades para detectar y clasificar las vulnerabilidades de red, aplicaciones y seguridad. Al identificar fallas conocidas, errores de codificación, anomalías en la construcción de paquetes y configuraciones incorrectas para el acceso potencial a datos confidenciales, los análisis de vulnerabilidades evalúan todo lo que los atacantes podrían aprovechar.

La implementación de un programa de gestión de vulnerabilidades ayuda a las organizaciones a evaluar y proteger sus redes. Incluye la detección, evaluación y mitigación de vulnerabilidades de seguridad de sistemas y software, y el factor clave es la detección.

Este programa de gestión de vulnerabilidades debe ir acompañado de capacitaciones relativas al particular. Tal es el caso de CompTIA Security+. Una certificación para prácticas y funciones básicas de seguridad. La Asociación de la Industria de la Tecnología Informática (CompTIA) refiere que esta certificación de seguridad es una de las primeras certificaciones basadas en la seguridad que deben obtener los profesionales de la tecnología de la información.

ALCANCE DE LA CERTIFICACIÓN.

Amenazas, ataques y vulnerabilidades. Ser capaz de identificar y analizar cualquier indicador de compromiso.

Gestión de acceso e identidad (SOY). Ser capaz de implementar controles IAM y controles de gestión de cuentas.

Criptografía. Ser capaz de identificar e implementar conceptos básicos de criptografía.

Gestión de riesgos. Ser capaz de identificar la importancia de las políticas, planes y procedimientos en seguridad.

Tecnologías y herramientas. Ser capaz de solucionar problemas de seguridad comunes con herramientas de software. Arquitectura y Diseño. Ser capaz de resumir los conceptos detrás

MINISTERIO PÚBLICO
DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN
Santo Domingo, Rep. Dom.

del desarrollo y la implementación de aplicaciones seguras, así como los conceptos detrás de la protección de las nubes y la virtualización.

3. Especificaciones y características del servicio.

1. **HERRAMIENTA DE ESCANEO DE VULNERABILIDADES**

Ver anexo términos de referencia

2. **CERTIFICACION DE COMPTIA SECURITY +**

- Centro de Entrenamiento Autorizado por el fabricante mediante carta vigente.
- Uso de materiales oficiales
- Instructor avalado por el proveedor del material mediante certificación o carta del proveedor, con al menos 5 años de experiencia CompTIA.
- El instructor debe tener las certificaciones de la ruta de Ciberseguridad según diagrama anexo para que pueda manejar temas abiertos y no limitarse al silabario de este curso.
- El instructor debe tener amplia experiencia como instructor, tanto en el material de CompTIA como en formaciones de EC-Council e ISC2, para que pueda complementar la experiencia según los contenidos más reconocidos de la industria de ciberseguridad,
- Cupones de examen incluidos y apoyo para el proceso de certificación.
- Laboratorios oficiales incluidos.
- Modalidad presencial

4. Análisis técnico de la solución propuesta.

1. **Estimación Presupuestal**

HERRAMIENTA ESCANEO DE VULNERABILIDADES			
CANTIDAD	**MONTO USD$**	**DESCRIPCION**	**TOTAL USD$**
1		Herramienta para escaneo de vulnerabilidades en la red.	20,000.00

CERTIFICACION DE COMPTIA SECURITY +			
CANTIDAD	**MONTO USD$**	**DESCRIPCION**	**TOTAL USD$**
6	1900.00	Certificación para prácticas y funciones básicas de seguridad	11,400.00

MINISTERIO PÚBLICO
DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN
Santo Domingo, Rep. Dom.

4. Conclusión.

Con base en lo antes expuesto, entendemos procedente que el Comité de Compras y Contrataciones del MP pondere los argumentos expuestos en el presente informe pericial a la luz de las disposiciones de la Ley 340-06 sobre Compras y Contrataciones, sus modificaciones por la ley no. 449-06 y el reglamento vigente de aplicación. 543-12 y, si lo entendiese oportuno al interés institucional, autorice a celebrar un proceso la modalidad correspondiente para llamar al concurso de la adquisición de herramientas de escaneo de vulnerabilidades y certificación de COMPTIA Security +.

MINISTERIO PÚBLICO
DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN
Santo Domingo, Rep. Dom.

Atentamente,

Armando José Díaz Díaz
Director Interino de Tecnología
de la Información y Comunicación

Reynaldo Rossi
Encargado Departamento de
Seguridad y Monitoreo TIC