PRINCIPIOS DE SEGURIDAD INFORMÁTICA

AUTOR: ORLANDO ESPINOZA BARBOZA

NOVIEMBRE: 2020

San Marcos

Introducción

¿Cuáles son las metodologías y herramientas para el análisis de vulnerabilidades?

- Todas las vulnerabilidades deben ser analizadas siguiendo metodologías para ese fin, en este caso se debe seguir los siguientes pasos: acuerdo de confidencialidad, establecimiento de las reglas del juego, recolección de información, análisis inferior, análisis exterior y documentación e informes.
- Por otro lado, existen herramientas especializadas para este análisis, tales como NESSUS, ACUNETIX y GFI LANGUARD.

CONTENIDO

METODOLOGÍAS DE ANÁLISIS DE VULNERABILIDADES

Acuerdo de confidencialidad

Una de las tareas principales que se debe verificar, es la parte del acuerdo de confidencialidad entre ambas partes, donde intervienen la empresa y el analista de seguridad. Es importante realizar un acuerdo de confidencialidad entre las dos partes involucradas en el análisis, debido a que, a lo largo de la búsqueda de vulnerabilidades, se puede obtener alguna información crítica para la organización analizada, por ejemplo, nombres de usuario y contraseñas, algunos agujeros de seguridad, documentos que se encuentran expuestos en la red, etc.

Toda la información que sea obtenida a través del análisis debe ser utilizada sólo para fines informativos, de mejora de servicios y seguridad, no podrá ser divulgada como tal a terceras personas o partes que no sean involucradas en la parte de este análisis. Desde el punto de vista de la organización debe de existir la confianza absoluta por parte del analista en este caso, si se está realizando un test de análisis de caja blanca, se deberá abrir como empresa todas las puertas a la red y ofrecerle toda la información que solicite el especialista.

Desde el punto de vista del analizador, el acuerdo de confidencialidad le ofrece un marco legal sobre el cual trabajar, constituyendo un respaldo formal a la labor realizada.

En conclusión, el acuerdo de confidencialidad debe tener un acuerdo muto entre ambas partes, tanto por la empresa como por el analista de seguridad sobre la información que se va a encontrar en el análisis de vulnerabilidad como, nombres de usuario, contraseñas, agujeros de seguridad, documentos expuestos, información crítica, etc. Toda la información que se encuentre debe ser utilizada para lo siguiente:

- Con fines informáticos
- Mejoras de los servicios y seguridad

Establecimiento de las reglas del juego

Otro de los puntos que se deben de establecer, son las reglas del juego, esto se refiere a todo antes de comenzar con el análisis de vulnerabilidades, ya que es necesario definir cuáles van hacer las tareas que se van a realizar y cuáles serán los límites, permisos y obligaciones que se van a respetar. Es probable que la organización que sea analizada no esté interesada en que sus servicios se suspenden, probablemente por algún ataque de denegación de servicio que sea exitoso por parte del analista. En caso de que esto suceda el experto deberá ser capaz de determinar las vulnerabilidades, durante el análisis se debe de mantener informada a la menor cantidad de personas, de forma de que la utilización de la red por parte del personal sea normal, con la finalidad de evitar cambios en la forma de trabajo de los usuarios de manera regular, ya que, si los usuarios de la red son informados que se va a realizar un cierto análisis, probablemente, lo que van a hacer es modificar algunas prácticas inseguras que normalmente realizan por miedo precisamente a que puedan ser reprendidos, despedidos y si esto sucede el análisis no tendrá el mismo efecto.

En este punto se quiere lograr definir cuáles serán las tareas a realizar, los límites que se deben alcanzar, las obligaciones y permisos que se tienen que cumplir, además se deberá realizar de manera cautelosa el análisis sin informar al personal en lo más mínimo posible para que la utilización de la red fluya de forma normal y realizar un excelente análisis.

Recolección de información

Otro de los puntos que se debe de verificar, es la parte de la recolección información, así como anteriormente se ha analizado los test de caja negra y caja blanca, el análisis de vulnerabilidades comienza con la obtención de información del objetivo, si se está seleccionando un test de caja negra, el proceso de análisis será muy similar al proceso seguido por un atacante, si se realiza el proceso de caja blanca, este es el momento para recopilar la mayor cantidad de información de acceso a servicios, información y todo lo que se considere necesario al momento de realizar el análisis. Por ejemplo, si se está realizando un test de caja blanca probablemente lo que hay que obtener son direcciones de servidores, nombres de usuarios, contraseñas, servicios que se llegan a brindar, esquemas de redireccionamiento, topologías de red, niveles de privilegios, etc.

Si se realiza un test de caja negra se puede obtener probablemente alguna dirección, nombres de dominio, correos

electrónicos, etc. Cuando se realiza este tipo de análisis para recolectar la información uno de las técnicas de análisis para levantar la información es el llamado OSINT,

Análisis interior

Antes de continuar con el análisis de vulnerabilidad, se debe verificar varios tipos de test, un análisis interior trata de mostrar o demostrar hasta dónde se puede llegar con los privilegios de un usuario típico dentro de la organización, para poder realizarlo se requiere que la organización provea una computadora con un nombre de usuario y una clave de acceso normal de un usuario específico.

Este tipo de test se compone normalmente de varias pruebas entre las cuales se puede mencionar a las siguientes:

La revisión de la privacidad: aquí simple y sencillamente el analista se centra en cómo se gestiona desde el punto de vista ético y legal el almacenamiento, transmisión y control de la información que todos los usuarios típicos o los empleados utilizan día a día.

Testeo de aplicaciones de internet: La parte del análisis de aplicaciones de internet o de aplicaciones web, este estudio se emplea de manera diferente, por ejemplo, se realizan técnicas de análisis de software para encontrar fallas de seguridad en aplicaciones que sean cliente servidor de un sistema desde internet. Cómo se está realizando un análisis interno, se deben probar las aplicaciones que son accedidas por los usuarios dentro de la red.

Testeo de sistema de detección de intrusos: En este tipo de análisis, normalmente se enfoca en la parte del rendimiento de los sistemas de identificación de intrusos, la mayor parte de este análisis normalmente no se puede llevar a cabo de manera adecuada, si no, accediendo a los registros del sistema de identificación de intrusos.

Testeo de medidas de contingencia: En este tipo de análisis se debe medir el mínimo de recursos necesarios que se necesitan en el subsistema, para realizar las tareas y verificar la detección de medidas presentes para la detección de intentos de acceso o recursos protegidos.

Descifrado de contraseñas: Descifrar las contraseñas es el proceso de validar cuan robusta puede ser una clave, a través del uso de herramientas de recuperación de contraseñas de manera automática, dejando normalmente al descubierto las aplicaciones de algoritmos criptográficos débiles y mal implementados o contraseñas débiles debido a factores humanos ya que las personas no se encuentran preparadas lo suficiente como para poder registrar una buena clave de seguridad.

Testeo de denegación de servicios: La denegación de servicio es una situación, donde una circunstancia sea intencional o de manera accidental previene a el sistema de que llegue a funcionar de manera exactamente como se dice lo diseñó. Normalmente se realiza en base alguna carga excesiva, algún alcance que no se llegue a cubrir o que los mismos usuarios abusen de los recursos del sistema, es muy importante que los test o análisis de denegación de servicios reciban ayuda adicional de la organización ya sea a monitorizar a nivel privado o de algunos otros usuarios que también sean analistas de seguridad.

Evaluación de políticas de seguridad: En la evaluación de políticas, la reducción de riesgos en una organización con la utilización de tipos de específicos de tecnologías, por ejemplo Cisco, existen dos funciones a llevar a cabo, lo primero es el análisis de lo escrito contra el estado actual de las conexiones y segundo asegurar que la política esté incluida dentro de las justificaciones del negocio de la organización, en especial en lo que hace referencia a la parte de una política que está incluida dentro de las justificaciones de negocio, esta se refiere a que esta política vaya ajustada hacia los objetivos, debido a que si se pone una política, por ejemplo de que no se puede utilizar internet y resulta que la empresa para sus ventas hace uso de este recurso la política no tendría sentido, por eso es importante realizar un análisis acerca de las políticas de seguridad que más le benefician a la organización.

Análisis exterior

En el punto anterior se hizo un análisis interno, también existe el análisis externo, el principal objetivo de este tipo de análisis, es acceder en forma remota a los servidores de la organización y sobre todo obtener privilegios o permisos que no deberían estar disponibles. Este test puede comenzar con técnicas ya sea aplicando ingeniería social para poder obtener alguna información y luego se podría utilizar en algún intento de acceso. Los pasos de este tipo de análisis consisten en los siguientes puntos:

Revisión de la inteligencia competitiva: Esta parte se basa en toda la información recolectada a partir de la presencia en internet de la organización.

Revisión de la privacidad: Esta etapa se basa en un punto de vista legal y ético del almacenamiento, transmisión y control de los datos basados en la privacidad del cliente. Por ejemplo, se hace una imaginación que dicha empresa no tiene el control suficiente como para hacer que toda la información o los datos que están manejando los empleados se queden dentro de la organización, lo que pueda a conllevar a que probablemente alguno de los empleados se pueda llevar dicha información.

Análisis de solicitud: Éste es el método para obtener privilegios de acceso a una organización y sus activos, preguntando sencillamente al personal de entrada usando las comunicaciones como algún teléfono, correo, chat, etc., desde una posición privilegiada o de una forma fraudulenta que tiende a ser simplemente un análisis basado en ingeniería social.

Análisis de sugerencia dirigida: Aquí en este método, se intenta lograr que un integrante de la organización ingrese a un sitio o reciba un correo electrónico en este sitio o el correo se podría agregar a herramientas que luego serían utilizadas en el intento de acceso. Técnicamente sería tener un cómplice dentro de la organización que ayude a instalar ciertas herramientas y posteriormente el atacante podría crear una sesión, ya sea con alguna herramienta que le permita gestionar sesiones desde el exterior.

Una vez que se recopila esta información se procede a realizar algunas de las siguientes pruebas que se muestran a continuación:

1. **Sondeo de red**: Sirve como Introducción a los sistemas a ser analizados, aquí se analizan nombres de dominio, nombres de servidores, direcciones IP, mapas de red, información del proveedor de internet, propietarios de sistema y servicios.
2. **Identificación de los servicios de sistemas**: En esta prueba se deben enumerar los servicios de internet activos o sobretodo accesibles, así como, traspasar el firewall con el objetivo de encontrar más máquinas activas, luego es necesario llevar adelante un análisis de la aplicación que escucha, tras dicho servicio. Tras la identificación de los servicios el siguiente paso simplemente es identificar al sistema con el fin de obtener respuestas que pueden dirigir el sistema operativo y su versión, técnicamente realizar un análisis de Fingerprint.
3. **Búsqueda y verificación de vulnerabilidades**: Esta prueba se basa en la identificación, comprensión y verificación de las vulnerabilidades o debilidades, errores de configuración dentro de un servidor o en una red. La búsqueda de vulnerabilidades se realiza mediante herramientas automáticas para determinar agujeros de seguridad existente y niveles de parcheado de los sistemas, pero se debe tener en cuenta nuevas vulnerabilidades que se publican en sitios donde normalmente todavía no incluyen las herramientas automáticas.
4. **Testeo de aplicaciones de internet**: Aquí se emplean diferentes técnicas de análisis de software para encontrar fallos de seguridad en aplicaciones cliente, como se está realizando un análisis externo, se pueden utilizar en este módulo los test de caja negra.
5. **Testeo de relaciones de confianza**: La parte de enrutamiento técnicamente está diseñado para asegurar que sólo aquellos que deben ser expresamente permitidos puede ser aceptado en la red.
6. **Verificación de redes inalámbricas**: Aquí en este caso se menciona la parte del estándar 802.11, que es un método para la verificación del Wireless que normalmente se basa en la parte de la cobertura y el acceso de los Access Point por red ad hoc.

Documentación e informes

En los puntos anteriores se analizó la parte del análisis interno y externo, ahora se debe realizar un análisis acerca de la parte de la documentación y los informes. Como en la parte de la finalización del análisis de vulnerabilidades se debe presentar un informe, donde se detalle cada uno de los test que se han realizado y los resultados de los mismos. Este informe debe especificar la lista de vulnerabilidades que han sido probadas, las vulnerabilidades detectadas, lista de servicios y dispositivos vulnerables, el riesgo o el nivel de riesgo que involucra cada vulnerabilidad que ha sido encontrada

en cada servicio y dispositivo, como tal se debe incluir los resultados de los programas utilizados

HERRAMIENTAS PARA EL ANÁLISIS DE VULNERABILIDADES

Nessus

Actualmente existen muchas herramientas para el análisis de fallos e inseguridades en el mercado, una de estas aplicaciones tipo escáner más populares es Nessus, esta solución es un escáner de vulnerabilidades desarrollado por la empresa Tenable Network Security, en la actualidad ofrece distintas soluciones no solo de escaneos de redes para encontrar fallos, sino, aplicaciones más completas como **Nessus Security Center** el cual evalúa las vulnerabilidades de una organización o empresa categorizando estas deficiencias de acuerdo al riesgo, incluso proporciona reportes continuos, datos estadísticos y posee un plugin que genera alertas y notificaciones, también apoya a la organización en el cumplimiento de estándares regulatorios y es posible integrarla con otras soluciones, esto constituye una de las grandes ventajas que tiene esta herramienta.

El **Nessus Cloud** permite realizar escaneos de una manera externa como interna, permite realizar múltiples escaneos personalizando las políticas y delegar los resultados a los posibles responsables de la administración de la infraestructura o del desarrollo, apoya también en el cumplimiento de estándares internacionales y una de sus grandes ventajas es el escaneo por medio de agentes, esto reduce el tiempo en el escaneo y permite reducir los costos y los riesgos.

Nessus Manager, esta versión permite realizar escaneos, gestión de políticas con respecto a reportes y estadísticas de las vulnerabilidades que se hayan detectado en la organización y en la infraestructura. Esta herramienta se actualiza constantemente para trabajar sobre las amenazas avanzadas, vulnerabilidades de día cero y nuevos requisitos en el cumplimiento de estándares. Permite realizar integraciones por medio de su Api con algunos datos de infraestructura de seguridad perimetral como los firewalls, sistemas de virtualización.

Acunetix

Es un escáner de vulnerabilidades web que se orienta principalmente en el OWASP TOP TEN, en las principales fallas o falencias que hay, la cual es una organización que desarrolla y apoya la investigación y a partir de allí están publicando los Exploits en su herramienta.

Acunetix también trabaja con vulnerabilidades que pueden tener un impacto muy grande las cuales están integradas en su escáner, esta herramienta que tiene varias posibilidades de trabajo para su utilización, se instala y se trabaja de manera local o se realiza los escaneo en línea.

Esta aplicación de manera muy general es una herramienta que tiene una interfaz gráfica vía web, diseñada para encontrar agujeros de seguridad en todas las aplicaciones de internet o de forma local implementadas en una organización con el objetivo de descubrir dichas vulnerabilidades, para que el atacante no ingrese al sistema y robe información del mismo. Entre esas vulnerabilidades puede encontrar ataques de SQL Injection, Cross Site Scripting, Password débiles.

De manera muy general en esta herramienta se puede seleccionar a un objetivo y con ello se puede realizar un escaneo para detectar vulnerabilidades, con esto, se puede seleccionar un rango determinado de direcciones IP y comenzar la detección de las posibles fallas dentro de la empresa. Entre los diferentes tipos de escaneo más usuales que se puede aplicar dentro de la organización, se tiene a los escaneos completos o los personalizados.

GFI Languard

Languard es un escáner de vulnerabilidades que tiene algunas ventajas sobre otras herramientas, ya que permite escaneos de forma local y en red, para los escaneos se pueden necesitar algunos datos como pueden ser las credenciales de un usuario ya sea estándar, el cual puede ser administrador local o administrador de dominio y a partir de ahí se puede ir realizando los análisis. Entre las múltiples ventajas de esta herramienta se puede mencionar:

- Automatizar la actualización de múltiples SO
- Buscar vulnerabilidades

- Auditar hardware y software
- Realizar informes de cumplimiento

Prácticamente esta herramienta se basa en la automatización de las actualizaciones sin importar el tipo de sistema operativo, las brechas de seguridad de la red son comúnmente causadas por la falta de actualizaciones, generalmente actualizaciones generales o actualizaciones de seguridad y LanGuard escanea y detecta estas vulnerabilidades en la red antes de que queden expuestas de acuerdo a las políticas de cada organización, esto ayuda a reducir el tiempo para actualizar los equipos en la red, cuando detecta que un sistema operativo no tiene una actualización podría enviar una alerta.

También busca las vulnerabilidades en más de 60000 evaluaciones de vulnerabilidades que se realizan a través de las redes LanGuard, esto incluye entornos virtuales, dispositivos móviles y datos de la red, tanto de infraestructura como CISCO, TRICOM, datos de sistemas operativos como Windows, Linux, Mac, entre otras. Generalmente escanea los sistemas operativos en entornos virtuales, aplicaciones instaladas mediante las bases de datos de comprobación como puede ser la OVAL (Open Vulnerability And Assessment Language). A diferencia de otras herramientas como Acunetix y Nessus no se tiene un OWASP TOP TEN porque no se está haciendo un escaneo a una página web, sin embargo, tiene otros tipos de cumplimiento.

También esta herramienta realiza auditoría de hardware y de software, la cual proporciona un análisis detallado del estado de la red, este análisis incluye las aplicaciones o configuraciones ya sean de una manera general o por defecto y el riesgo que pueden generar para la seguridad de la organización, también proporciona una imagen completa de las aplicaciones instaladas, el hardware de la red, los dispositivos móviles que se conectan a un servidor entre otras cosas. Se podría si un determinado usuario ha instalado aplicaciones que están o no están dentro de las autorizadas en la organización y de ahí se podría generar los reportes.

La diferencia entre Nessus y Languard es que Nessus necesita tener la herramienta instalada en el equipo y de ahí lanzar los escaneos y LanGuard se basa más en las auditorías de red donde se va a tener un equipo con ciertas características que van a ir de acuerdo al número de nodos que se vaya a auditar

Los precios de este analizador de vulnerabilidades son muy bajos comparados con otras herramientas, porque prácticamente es para una red, no está orientado a la parte de consultoría como otras aplicaciones como Nessus y Acunetix, sin embargo, también se puede instalar en el equipo la herramienta, ejecutarlo y a partir de ahí ir trabajando. Esta herramienta es bastante utilizada por los precios, soporte y actualizaciones constantes.

Nexpose

Esta herramienta es utilizada para la explotación de las vulnerabilidades, la cual va a trabajar sobre la parte web y de red. Entre las ventajas que tiene esta aplicación sobre otras, es que puede interactuar directamente con Metasploit para la explotación de las vulnerabilidades, la herramienta se la puede descargar directamente del sitio web www.rapid7.com.

Esta herramienta trabaja directamente sobre una consola web, se inician los servicios y se puede trabajar con Metasploit directamente una vez que ya se identifican las vulnerabilidades, la herramienta va a indicar si existen Exploits o no, ya sea en Metasploit solamente o halla que descargar algún código directamente de la página web. En esta aplicación se pueden generar algunos reportes los cuales van a permitir trabajar con reportes tipos ejecutivos o técnicos.

Conclusiones y recomendaciones

Que el estudiante sea capaz de identificar las principales metodologías y herramientas para el análisis de vulnerabilidades.
Se recomienda reforzar estos conocimientos con investigación propia en páginas públicas del internet.

Referencias bibliográficas

1. Romero, M,. Figueroa, G.,Vera, D., Álava, J., Parrales, G., Álava, C., Murillo, Á., Castillo, M. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. Editorial Área de Innovación y Desarrollo, S.L. Recuperado de https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica