METODOLOGIA PARA REALIZAR EL ANÁLISIS DE VULNERABILIDADES O TEST DE INTRUSION

CONTROL DOCUMENTAL

Historia

Versión	Autor	Tipo de Revisión	Descripción	Aprobado por	**Fecha**
1.0	SISTESEG	Creación	Proyecto		

Distribución

Copia	Destinatario	Destino / Dirección
Original	SISTESEG	
Copia	SISTESEG	

Referencias

Ref.	Documento o ítem referenciado

Control de Acceso

Sección	Disponibilidad
Todo	

Tabla de Contenido

1 INTRODUCCION

Este documento busca generar recomendaciones generales relacionadas con el análisis de vulnerabilidades a una muestra de dispositivos tecnológicos, según la metodología diseñada por SISTESEG con el fin de identificar los riesgos a que están sometidos los activos de TI y, de esta manera, mejorar la seguridad de la información siguiendo los lineamientos de las normas ISO 27001:2013 e ISO 27032:2011

Una vulnerabilidad, se puede definir como un estado de un sistema (o conjunto de sistemas) que puede:

- Permitir a un atacante acceder a información confidencial
- Permitir a un atacante modificar información
- Permitir a un atacante negar un servicio

2 RESUMEN

En la actualidad, las organizaciones encaran el doble riesgo de ataques externos a sus activos digitales y el abuso interno de los privilegios de acceso. A pesar de que muchas de sus conexiones a Internet están protegidas por firewalls, IDS/IPS, muchas también no tienen sistemas adecuados de seguridad. Debido a esto, los hackers, y los códigos que éstos programan siguen causando devastación a redes de computadoras, y las consecuentes pérdidas económicas, de imagen y credibilidad de sus víctimas.

Una Prueba de Penetración es una prueba independiente usada para simular posibles acciones de usuarios no autorizados, internos y externos, que se infiltran en los sistemas de cómputo y en los datos confidenciales que ellos almacenan. Con estas acciones se busca identificar vulnerabilidades que existen en una red o en un sistema, utilizando la disciplina de la seguridad de redes llamada Ethical Hacking, la cual se sustenta en el hecho de que la mejor forma que tienen las empresas para estar protegidas contra hackers es conocer cómo operan y cuáles herramientas usan.

3 ALCANCE

La prueba de penetración externa, de acuerdo a los requerimientos se limitan a intentos de acceso a la red y sistemas de información desde un punto externo y para dos sistemas las pruebas serán internas.

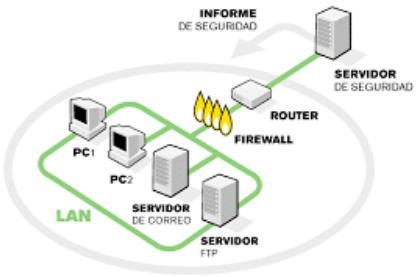
Estos intentos de acceso no son propuestos para que pongan en riesgo la disponibilidad, confidencialidad e integridad de la información.

Las mencionadas pruebas se ejecutarán en los horarios acordados con el cliente si así se requiere. Durante la ejecución de las pruebas se calcula que la probabilidad de generar caídas en los sistemas es menor al 3% según nuestras estimaciones, aunque se recomienda que los sistemas que estarán sujetos a las pruebas tengas copias de respaldo y sean monitoreados por si se presentará algún inconveniente. Se estima generar un tráfico en la red que no incremente la utilización de los enlaces por encima del 5%, este tráfico puede ser TCP o UDP en nivel 4 y HTTP en niveles superiores.

4 METODOLOGIA

El alcance de la prueba de penetración externa, intenta conocer hasta dónde un hacker externo podría penetrar los sistemas. La prueba se debe enfocar en identificar las vulnerabilidades que un hacker competente podría explotar para ganar acceso privilegiado a los sistemas.

El servicio utiliza una metodología propietaria basada en las mejores prácticas de la industria de seguridad de la información, entre otras, la Information Systems Security and Assessment Framework (ISSAF), Open Web Application Security Project (OWASP) y (Open Source Security Testing Methodology Manual) OSSTMM v3.0. La prueba se desarrolla a través de las siguientes fases:



- **Planear prueba**. Durante esta fase se define el alcance de la prueba, los términos contractuales, acuerdo de confidencialidad, los permisos del cliente, los horarios y el término de la prueba son definidos, los cuales son parte de las Reglas de Compromiso (Rules of Engagement).
- **Reconocimiento.** En especial utilizada no sólo para conocer el objetivo, sino también para identificar cuáles podrían ser potenciales vulnerabilidades. Utilizaremos en esta ocasión tanto el reconocimiento pasivo como el activo.
- **Scanning.** Se realizan los rastreos, inventario de direccionamiento y servicios y analizamos los factores que envuelvan a estos elementos en posibles oportunidades de intrusión.
- **Enumeración.** Durante esta etapa se busca descubrir la mayor cantidad de activos de la institución mediante exploraciones directas a las redes, de forma externa. Mediante este inventario de los activos se puede determinar el tamaño de la red y las posibles rutas de intrusión a la misma, además de cuentas de correo, nombres de usuarios y grupos de usuarios entre otras cosas.
- **Análisis de Vulnerabilidades.** Se utilizan herramientas tanto open source como comerciales con Bases de Datos actualizadas de vulnerabilidades para evaluar los sistemas y sus posibles debilidades.
- **Penetración y Escalamiento de Privilegios, (System Hacking).** En esta fase cruzamos el perímetro y mantenemos conexión, para realizar diversas actividades que demuestren el compromiso de los sistemas. La prueba de penetración en sí, según la OSSTMM v.3.0

se refiere generalmente a la meta del proyecto que incluye ganar acceso a privilegios bajo un escenario controlado y acordado.

Una de las preocupaciones más importantes de los profesionales de la seguridad de la información es el aumento en la cantidad de vulnerabilidades encontradas en los sistemas tecnológicos, las cuales son el blanco predilecto de herramientas de software cada vez más poderosas en su capacidad de ocasionar daños a los sistemas de información y la infraestructura que los soporta.

Lo anterior nos lleva a pensar que se necesita contar con una estrategia más coherente y efectiva para mitigar esta inquietante y crítica amenaza, de tal manera, que hemos recopilado una serie de actividades y recomendaciones que le ayudarán a ciertas empresas a realizar un análisis a nivel técnico de las vulnerabilidades de software, asociadas a sus activos de tecnológicos.

5 HERRAMIENTAS RECOMENDADAS

Se detallan a continuación el compendio de herramientas y distribuciones que se podrían utilizar dependiendo del sistema a analizar:

Distribuciones Linux:

- Backtrack 4 R1
- KC Pentrix 2

Herramientas:

- Footprinting: navegadores de internet (Mozilla, Opera), search engines (Google, Yahoo, A9 etc.), mailing list, news groups, maltego, FOCA..
- Scanning: nmap, netcat, zenmap, ike-scan, amap, nikto, wikto, Unicornscan.
- Enumeración: DNS-Brute-Force, dnsenum, gooscan, relay scanner, smtp-vrfy, httprint, snmp-enum, nmbscan, ldapenum, winfingerprint.
- Análisis de Vulnerabilidad: Nessus, xiGUARD (Análisis de Vulnerabilidades propietario de Ximark), Acunetix WVS, Nexpose.
- Explotación de Sistemas: Canvas Framework, Metasploit Framework, Exploit-Db Exploits, Security Forest Exploits, Packet Storm Exploits, Vupen Exploits, Hydra, Xploit-Tree, además de exploits propietarios.
- Explotación de aplicaciones web: Paros-Proxy, Webscarab, Acunetix WVS, Fastrack, Inguma, Hydra, Burpsuite, ASP-Audit, W3AF, Ataques manuales de XSS, XFS, SQL Injection, XSRF, Metacoretex, SQL-Brute, SQL-Ninja, Netsparker, Websecurify, Burp Professional, SQLmap entre otras.

6 METODOLOGIA PARA EL ANALISIS DE VULNERABILIDADES

El análisis de vulnerabilidades el cual complementa el proceso de análisis de riesgo, es una actividad fundamental con el fin de orientarnos hacia un sistema de gestión de la seguridad de la información, el cual debería comprender las siguientes actividades:

7 ENTENDIMIENTO DE LA INFRAESTRUCTURA

En esta fase se busca, identificar cada uno de los dispositivos de hardware o software residentes en la infraestructura que soportan los procesos del negocio. Esta selección debe iniciarse con los servicios prestados, continuar luego con los procesos asociados a estos servicios y de allí, determinar los activos o dispositivos que soportan estos procesos.

A manera de ejemplo, dentro de los posibles elementos de la infraestructura que un momento dado pudieran llegar a albergar vulnerabilidades a nivel de software tenemos los siguientes:

1. Servidores
2. Aplicaciones
3. Estaciones de trabajo
4. Bases de datos
5. Firewalls
6. Enrutadores

8 PRUEBAS

En esta fase se realizará una clasificación de activos o dispositivos con base en la confidencialidad de la información que guardan y la importancia del activo para la continuidad del proceso en estudio.

Por medio del uso de herramientas para la detección de vulnerabilidades preferiblemente comerciales[1] (no software libre) y soportadas debidamente por su fabricante, las cuales pueden ser tanto de software para correr sobre sistemas operativos tradicionales o poseer un hardware especifico (appliances). También se requiere que cuenten con una base de datos actualizada y completa de vulnerabilidades aceptadas por la industria (CERT, SANS) y con un criterio común de clasificación como el CVE[2] (common vulnerabilities and exposure). Se busca por medio del uso de esta herramienta, poder identificar cualquier elemento activo presente en la red, siempre y cuando posea una dirección IP, con el fin de detectar sus vulnerabilidades presentes a nivel de software y evitar futuros incidentes de seguridad.

Una vez seleccionada la herramienta, se debe tomar una decisión costo- beneficio con el fin de determinar el número de IP que deben ser analizadas. Por esta razón, la necesidad de seleccionar un subconjunto de IPs, que sea representativo. Además de esta selección, se pueden crear categorías y agrupar servidores o estaciones de trabajo, siempre y cuando se cuente con la certeza que aquellos seleccionados para esta agrupación, comparten más de un 90 % de similitud en su configuración con los otros que no serán inspeccionados. Si no se tiene esta certeza, necesariamente debemos aumentar el universo de la prueba, hasta que este universo comprenda al menos un elemento de todas las categorías de activos críticos para la operación continua y segura de los procesos.

[1] Algunas de las herramientas comerciales son fabricadas por empresas como: LanGuard y Netclarity.
[2] Otras fuentes de información: CVE vulnerability feeds: security related software flaws, CCE vulnerability feeds: errores de configuración, CPE diccionario de producto.

9 MEDIDAS PREVENTIVAS

Una vez determinado el universo de la prueba se tomarán las medidas preventivas adecuadas para su ejecución, con el fin de prevenir efectos adversos sobre la prestación de los servicios; entre ellas, podemos resaltar:

1. Definir hora adecuada de pruebas
    a. Horas de bajo tráfico
    b. Horarios de no prestación de servicios, si esto fuera posible
2. Realizar un análisis de riesgo cualitativo sobre la prueba
    a. Análisis sobre la no disponibilidad de activos críticos de la prueba
        i. Estimar una probabilidad
        ii. Estimar un impacto
3. Tomar algunas medidas de contingencia
    a. Definir estrategias de contingencia para activos críticos
    b. Involucrar al oficial de seguridad y coordinador BCP, DRP
    c. Realizar respaldos de la información de los activos involucrados
    d. Guardar en formato electrónico y físico configuraciones de equipos involucrados
4. Realizar monitoreo de los servicios durante las pruebas
        i. Tiempos de respuesta excesivos
        ii. Eventos o incidentes de seguridad
5. Se debe informar a operaciones de la realización de las pruebas
6. Se debe monitorear el tráfico de la red
        i. Utilización de los segmentos críticos
        ii. Condiciones de error (CRC, Bad checksum)
        iii. Utilización de CPU en servidores críticos
7. Informar a los dueños de los activos

10 REALIZACIÓN DE LAS PRUEBAS DE VULNERABILIDADES

Es importante considerar que si tenemos redes remotas protegidas por firewall, las cuales también quisieran ser analizadas, el firewall debe permitir pasar el tráfico generado por la herramienta de análisis de vulnerabilidades. Por último, es recomendable contar con una herramienta que tenga la posibilidad de descubrimiento automático de dispositivos de red.

Por otro lado, las pruebas se pueden realizar suministrando información al responsable (por ejemplo direcciones IP) de su ejecución o se pueden realizar también sin suministrar esta información. También estas pruebas se pueden clasificar según si se hacen en la red interna o se intentan ataques desde fuera de la red, es decir, intentar llegar a la red interna desde por ejemplo Internet, pasando por el firewall o algún otro dispositivo de frontera.

1. Internas
    a. Sin conocimiento
    b. Con conocimiento
2. Externas

a. Sin conocimiento
b. Con conocimiento

11 PRUEBAS DE EXPLOTACIÓN DE LAS VULNERABILIDADES

Una vez clasificadas las vulnerabilidades más críticas, se debe realizar una prueba sobre ellas con el fin de realizar su explotación. En la medida en que la herramienta sea más inteligente y estructurada el proceso será más corto y no requerirá un perfil tan sofisticado. Estimamos que el tiempo de explotación de 15 vulnerabilidades debe estar del orden de 3 horas, incluyendo la realización del informe. El proceso de explotación debe incluir el escalar privilegios (tomar control del dispositivo como administrador) con el fin de tomar control total de los sistemas y de esta manera seguir de manera estricta la forma en que se llevan a cabo los ataques en la vida real.

12 ANALISIS DE RESULTADOS

Una vez realizadas las pruebas contando con las anteriores recomendaciones, se debe con base en la información obtenida realizar una reunión técnica para informar de estos resultados y realizar una revisión general de las vulnerabilidades encontradas y la clasificación realizada por la herramienta.

En esta reunión deben participar:

1. Oficial de seguridad
2. Dueños de procesos
3. Gerente del área
4. Comité de seguridad
5. Dueños de activos
6. Coordinador del plan de contingencias

13 PLAN DE REMEDIACIÓN DE VULNERABILIDADES

A continuación, se debe proponer un plan de remediación específico para las vulnerabilidades, el cual podría ser parte del plan de tratamiento general de riesgos, una vez claro está, se haya hecho un análisis formal y detallado de los resultados obtenidos tanto de la prueba de vulnerabilidades como de las de explotación. Este plan de remediación, clasifica con ayuda de la herramienta de vulnerabilidades y de explotación, la criticidad de cada una de las vulnerabilidades encontradas y sugiere cuales deben ser solucionadas en el corto, mediano o largo plazo. Esta decisión sobre el tiempo a implantar el control respectivo a la vulnerabilidad también debe contemplar costo del control, capacidad, administración y facilidad de implementación.

14 CONCLUSIONES

Se recomienda que se utilice una herramienta de análisis de vulnerabilidades que cuente con un soporte adecuado de su fabricante y cuente también con una base de datos muy completa en

cuanto a vulnerabilidades, lo mismo se recomienda con la herramienta de prueba de las vulnerabilidades, adicionándole que en lo posible sea un herramienta automatizada para mejorar la efectividad de este proceso. Es importante considerar la efectividad del plan de remediación, que como tal es la salida principal de todo este proceso de análisis de vulnerabilidad, y en últimas lo que garantizará la confiabilidad de los procesos y servicios ofrecidos por SISTESEG.

15 BIBLIOGRAFÍA

Business Continuity Institute (2013) *Good Practice Guidelines: A guide to global good practice in business continuity*, Business Continuity Institute, Caversham.

Disaster Recovery Institute International (DRII) (2012) *Professional Practices for Business Continuity Practitioners*, DRII, New York.

ISO 22301 (2012) – Societal security – Business continuity management systems – Requirements

ISO 22301 (2012) – Societal security – Business continuity management systems – Guidance

ISO 22301 (2012) – Societal security – Terminology

ISO 27001:2013 Information security.

www.sans.org