Solución actividad 1.4.5: Identificación de las vulnerabilidades de seguridad más importantes

Objetivos de aprendizaje

Al completar esta actividad, usted podrá:
• Usar el sitio SANS para identificar rápidamente las amenazas de seguridad de Internet.
• Explicar cómo se organizan las amenazas.
• Enumerar varias vulnerabilidades de seguridad recientes.
• Usar los vínculos de SANS para acceder a información adicional relacionada con la seguridad.

Información básica

Uno de los sitios más conocidos y confiables relacionados con la defensa contra las amenazas de seguridad de computadoras y de redes es SANS. SANS proviene de SysAdmin, Audit, Network, Security (Administración del sistema, Auditoría, Red, Seguridad). SANS está formado por varios componentes, cada uno de los cuales contribuye en gran medida con la seguridad de la información. Para obtener información adicional sobre el sitio SANS, consulte http://www.sans.org/ y seleccione los temas en el menú Recursos.

¿Cómo puede un administrador de seguridad corporativa identificar rápidamente las amenazas de seguridad? SANS y el FBI han recopilado una lista de los 20 principales objetivos de ataques de seguridad en Internet en http://www.sans.org/top20/. Esta lista se actualiza periódicamente con información formateada por:

• Sistemas operativos: Windows, Unix/Linux, MAC

• Aplicaciones: interplataforma, incluyendo la Web, base de datos, punto a punto, mensajería instantánea, reproductores de medios, servidores DNS, software para copias de seguridad y servidores de administración

• Dispositivos de red: dispositivos de infraestructura de red (routers, switches, etc.), dispositivos VoIP

• Elementos humanos: políticas de seguridad, conducta humana, temas personales.

• Sección especial: temas de seguridad no relacionados con ninguna de las categorías anteriores.

Escenario

Esta práctica de laboratorio presentará a los estudiantes las vulnerabilidades en los asuntos de Seguridad informática. Se usará el sitio Web de SANS como una herramienta para la identificación, comprensión y defensa de las amenazas de vulnerabilidad.

Tarea 1: Ubicación de los Recursos SANS.

Paso 1: Abrir la Lista SANS de los 20 principales.
Con un navegador Web, vaya al URL http://www.sans.org. En el menú **Recursos**, elija **Lista de los 20 principales**, como se muestra en la Figura 1.

Figura 1. Menú SANS

La lista SANS de los 20 principales objetivos de ataques de seguridad en Internet está organizada por categorías. Una letra indica el tipo de categoría y los números separan los temas de la categoría. Los temas sobre router y switch se encuentran dentro de la categoría Dispositivos de red (Network Devices) **N**.

Hay dos temas principales con hipervínculos:

N1. Servidores y teléfonos VoIP
N2. Debilidades comunes de configuración de dispositivos de red y de otro tipo

Paso 2: Hacer clic en el hipervínculo N2. Debilidades comunes de configuración de dispositivos
de red y de otro tipo, para ingresar en este tema.

Tarea 2: Repaso sobre los Recursos SANS.

Paso 1: Repasar el contenido de N2.2 Temas comunes de configuración predeterminada.
Por ejemplo, N2.2.2 (en enero de 2007) contenía información sobre amenazas relacionadas con cuentas y valores predeterminados. Una búsqueda en Google sobre “contraseñas de router inalámbrico” arroja vínculos a diversos sitios que publican una lista de nombres de cuenta de administrador y contraseñas predeterminadas de routers inalámbricos. La imposibilidad de cambiar la contraseña predeterminada en estos dispositivos puede generar compromiso y vulnerabilidad hacia los atacantes.

Paso 2: Observar las referencias CVE.

La última línea debajo de varios temas se refiere a la Exposición común a la vulnerabilidad (CVE).

El nombre CVE está relacionado con la Base de datos Nacional de Vulnerabilidad (NVD) del Instituto Nacional de Normas y Tecnología (NIST), patrocinado por la División de Seguridad Cibernética Nacional del Departamento de Seguridad Nacional (DHS) y por US-CERT, que contiene información sobre la vulnerabilidad.

Tarea 3: Recolección de datos.

El resto de esta práctica de laboratorio lo guiará a través de la investigación y solución de una vulnerabilidad.

Paso 1: Seleccionar un tema para investigar y hacer clic en un hipervínculo CVE de ejemplo.

Nota: Debido a que la lista CVE cambia, la lista actual puede no contener las mismas vulnerabilidades que en enero de 2007.

El vínculo debe abrir un nuevo explorador Web conectado a http://nvd.nist.gov/ y la página resumen de vulnerabilidades de CVE.

Tratamos la vulnerabilidad CVE-2006-5382

Pasó 2: Completar la información sobre la vulnerabilidad:
Fecha de lanzamiento original: 25 de octubre de 2006
Última revisión: 8 de marzo de 2011
Fuente: US-CERT/NIST

Descripción general:

3Com Switch SS3 4400 switches, firmware 5.11, 6.00 and 6.10 y anteriores, podría permitir a un atacante remoto obtener información sensible causado por un manejo inadecuado de los paquetes de gestión. Un atacante remoto podría enviar una solicitud especialmente diseñada para causar una respuesta a devolver que contiene el SNMP de lectura y escritura de Community strings (SNMP es un protocolo muy utilizado para administrar la red a traves de internet, su uso esta muy extendido, y las Community strings son las contraseñas de los elementos de la red). Un atacante remoto podría explotar esta vulnerabilidad para obtener información sensible, deshabilitar ciertos puertos, o volver a configurar VLAN.

En Impacto hay varios valores. Se muestra la severidad del Sistema de puntaje de vulnerabilidades comunes (CVSS), que contiene un valor entre 1 y 10.

Pasó 3: Completar la información sobre el impacto de vulnerabilidad:

Severidad CVSS: versión 2.0 actualizada de la v1.0
Rango: 7,5 (HIGH) (AV: N / AC: L / Au: N / C: P / I: P / D: P)
Autenticación: no se requiere
Tipo de impacto: Proporciona acceso no autorizado, permite la confidencialidad parcial, integridad y disponibilidad de violación, permite la divulgación no autorizada de la información, permite la interrupción del servicio.

El próximo encabezado contiene vínculos con información sobre la vulnerabilidad y las posibles soluciones.

Pasó 4: Con la ayuda de los hipervínculos, escribir una breve descripción sobre la solución encontrada en esas páginas.

Una vez detectada la vulnerabilidad, como solución los fabricantes, realizaron un parche para solucionarla, comentar que muchos de los links ya no están disponibles, debido a que una vez aplicado el parche no se ha vuelto a detectar ningún tipo de vulnerabilidad.

Tarea 4: Reflexión

La cantidad de vulnerabilidades para las computadoras, redes y datos sigue creciendo. Los gobiernos han dedicado importantes recursos para coordinar y difundir información sobre las vulnerabilidades y las posibles soluciones. Sigue siendo responsabilidad del usuario final la implementación de la solución. Piense de qué manera pueden los usuarios ayudar a fortalecer la seguridad. Piense qué hábitos de los usuarios crean riesgos en la seguridad.

Una de las formas seria en no acceder a paginas web de dudosa reputación o que muestren desconfianza (un ejemplo a paginas que contengan cracks, etc,). Utilizar contraseñas seguras (difíciles de descubrir), etc. Y también como prevención tener un buen antivirus, no guardar en archivos de texto dentro de los mismos ordenadores las contraseñas que se utilizan, no descargar nada que no sea conocido de internet (aplicaciones). Tener siempre en el sistema operativo dos tipos de usuario el administrador para instalaciones y el nivel usuario para navegar por internet y trabajar, ya que de esta manera si alguna aplicación intenta instalarse necesitara los permisos del administrador y nos daremos cuenta que se esta intentando instalar algo desconocido.

Tarea 5: Desafío

Intente identificar una organización que se pueda reunir con nosotros para explicarnos cómo se rastrean las vulnerabilidades y se aplican las soluciones. Encontrar una organización dispuesta a hacer esto puede ser difícil, por razones de seguridad, pero ayudará a los estudiantes a aprender cómo se logra mitigar las vulnerabilidades en el mundo. También les dará a los representantes de las organizaciones la oportunidad de conocer a los estudiantes y realizar entrevistas informales.

- http://www.360sec.com

-http://www.tb-security.com