Práctica de laboratorio: Investigación de amenazas de seguridad de red

Objetivos

Parte 1: Explorar el sitio web de SANS

Parte 2: Identificar amenazas de seguridad de la red recientes

Parte 3: Describir con detalle una amenaza específica de seguridad de la red

Aspectos básicos/situación

Para defender una red contra ataques, el administrador debe identificar las amenazas externas que representan un peligro para la red. Pueden usarse sitios web de seguridad para identificar amenazas emergentes y para proporcionar opciones de mitigación para defender una red.

Uno de los sitios más populares y confiables para la defensa contra amenazas de seguridad informática y de redes es el de SysAdministration, Audit, Networking and Security (SANS). El sitio de SANS proporciona varios recursos, como una lista de los 20 principales controles de seguridad fundamentales para una defensa cibernética eficaz y el boletín informativo semanal "@Risk: The Consensus Security Alert". Este boletín detalla nuevos ataques y vulnerabilidades de red.

En esta práctica de laboratorio, navegará hasta el sitio de SANS, lo explorará y lo utilizará para identificar amenazas de seguridad de red recientes, investigará otros sitios web que identifican amenazas, e investigará y presentará detalles acerca de un ataque de red específico.

Recursos necesarios

- Dispositivo con acceso a Internet
- PC para la presentación con PowerPoint u otro software de presentación instalado

Parte 1: Explorar el sitio web de SANS

En la parte 1, navegue hasta el sitio web de SANS y explore los recursos disponibles.

Paso 1: Localizar los recursos de SANS.

Vaya a www.SANS.org. En la página de inicio, resalte el menú **Resources** (Recursos).

Indique tres recursos disponibles.

Paso 2: Localizar el recurso Top 20 Critical Controls.

El documento **Twenty Critical Security Controls for Effective Cyber Defense** (Los 20 controles de seguridad críticos para una defensa cibernética eficaz) que aparece en el sitio web de SANS es el resultado de una asociación de carácter público-privado entre el Departamento de Defensa de los EE. UU. (DoD, Department of Defense), la National Security Association, el Center for Internet Security (CIS) y el instituto SANS. La lista se desarrolló para establecer el orden de prioridades de los controles de ciberseguridad y los gastos para el DoD y se convirtió en la pieza central de programas de seguridad eficaces para el gobierno de los Estados Unidos. En el menú **Resources**, seleccione **Top 20 Critical Controls** (Los principales 20 controles críticos).

Seleccione uno de los 20 controles críticos e indique tres de las sugerencias de implementación para ese control.

Paso 3: Localizar el menú Newsletter.

Resalte el menú **Resources** y seleccione **Newsletters** (Boletines informativos). Describa brevemente cada uno de los tres boletines disponibles.

Parte 2: Identificar amenazas de seguridad de red recientes

En la parte 2, investigará las amenazas de seguridad de red recientes mediante el sitio de SANS e identificará otros sitios que contienen información de amenazas de seguridad.

Paso 1: Localizar el archivo del boletín @Risk: Consensus Security Alert.

En la página **Newsletters**, seleccione **Archive** (Archivo) para acceder a @RISK: The Consensus Security Alert. Desplácese hacia abajo hasta **Archives Volumes** (Volúmenes de archivo) y seleccione un boletín informativo semanal reciente. Revise las secciones **Notable Recent Security Issues and Most Popular Malware Files** (Problemas de seguridad recientes destacados y Archivos de malware más populares).

Enumere algunos de los ataques recientes. Explore varios boletines informativos recientes, si fuera necesario.

Paso 2: Identificar sitios que proporcionen información sobre amenazas de seguridad recientes.

Además del sitio de SANS, identifique otros sitios web que proporcionen información sobre amenazas de seguridad recientes.

Enumere algunas de las amenazas de seguridad recientes que se mencionan en estos sitios web.

Parte 3: Describir con detalle un ataque específico de seguridad de la red

En la parte 3, investigará un ataque de red específico que haya ocurrido y creará una presentación basada en sus conclusiones. Complete el formulario que se encuentra a continuación con sus conclusiones.

Paso 1: Complete el formulario a continuación según el ataque de red seleccionado.

Nombre del ataque:	
Tipo de ataque:	
Fecha de los ataques:	
Equipos/organizaciones afectadas:	
Cómo funciona y qué daños causó:	
Opciones de mitigación:	
Referencias y enlaces de información:	

Paso 2: Siga las pautas del instructor para completar la presentación.

Reflexión

1. ¿Qué medidas puede tomar para proteger su PC?

2. ¿Cuáles son algunas medidas importantes que las organizaciones pueden seguir para proteger sus recursos?