Práctica de laboratorio: Investigación de amenazas de seguridad de red

Objetivos

Parte 1: Explorar el sitio Web de SANS

- Navegar hasta el sitio Web de SANS e identifique los recursos.

Parte 2: Identificar amenazas de seguridad de red recientes

- Identificar diversas amenazas de seguridad de red recientes mediante el sitio de SANS.
- Identificar otros sitios, además de SANS, que proporcionen información sobre amenazas de seguridad de red.

Parte 3: Detallar una amenaza de seguridad de red específica

- Seleccionar y detallar una amenaza de red específica reciente.
- Presentar la información a la clase.

Información básica/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 SANS (SysAdministration, Audit, Networking and Security). El sitio de SANS proporciona varios recursos, incluida una lista de los 20 principales controles de seguridad críticos 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 recursos de SANS.

Con un explorador Web, navegue hasta 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), incluido en el sitio Web de SANS, es el resultado de una asociación pública y privada entre el Departamento de Defensa de los EE. UU. (DoD), 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 seguridad cibernética 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 **Newsletter** (Boletín informativo). 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 informativo @Risk: Consensus Security Alert.

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

Enumere algunos ataques recientes. Examine varios boletines informativos recientes, si es 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 detalladas en esos sitios Web.

Parte 3: Detallar un ataque de seguridad de red específico

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: Completar el siguiente formulario para el ataque de red seleccionado.

Nombre del ataque:	
Tipo de ataque:	
Fechas de ataques:	
Computadoras/organizaciones afectadas:	
Cómo funciona y qué hizo:	
Opciones de mitigación:	
Referencias y enlaces de información:	

Paso 2: Siga las pautas para instructores para completar la presentación.

Reflexión

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

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