Práctica de laboratorio: Investigación de amenazas de seguridad de red (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

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.

_____

_____

Reading Room (Sala de lectura), Webcasts (Transmisiones Web), Newsletters (Boletines informativos), Blogs, Top 25 Programming Errors (Los principales 25 errores de programación), Top 20 Critical Controls (Los principales 20 controles críticos), Security Policy Project (Proyecto de política de seguridad)

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.

_____

_____

_____

_____

_____

_____

Las respuestas varían. Critical Control 5: Malware Defenses. (Control crítico 5: Defensas contra malware) Employ automated tools to continuously monitor workstations, servers, and mobile devices. (Utilice herramientas automatizadas para monitorear continuamente estaciones de trabajo, servidores y dispositivos móviles). Employ anti-malware software and signature auto-update features. (Emplee software contra malware y funciones de actualización automática de firmas). Configure network computers to not auto-run content from removable media. (Configure equipos de red para que el contenido de los medios extraíbles no se ejecute automáticamente)

Paso 3: Localizar el menú Newsletter.

Resalte el menú **Resources** y seleccione **Newsletter** (Boletín informativo). Describa brevemente cada uno de los tres boletines disponibles.

_____

_____

_____

_____

_____

_____

SANS NewsBites. Resumen de alto nivel de los artículos periodísticos más importantes sobre la seguridad informática. El boletín se publica dos veces por semana e incluye enlaces para obtener más información.

@RISK: The Consensus Security Alert. Resumen semanal de nuevos ataques y vulnerabilidades de red. El boletín también proporciona detalles sobre la forma en que resultaron los ataques más recientes.

Ouch! Documento para despertar conciencia sobre la seguridad que proporciona a los usuarios finales información sobre cómo pueden ayudar a garantizar la seguridad de su red.

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.

_____

_____

_____

Las respuestas varían. Win.Trojan.Quarian, Win.Trojan.Changeup, Andr.Trojan.SMSsend-1, Java.Exploit.Agent-14, Trojan.ADH.

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.

_____

_____

_____

Las respuestas varían, pero podrían incluir www.mcafee.com/us/mcafee-labs.aspx, www.symantec.com, news.cnet.com/security/, www.sophos.com/en-us/threat-center/, us.norton.com/security_response/.

Enumere algunas de las amenazas de seguridad recientes detalladas en esos sitios Web.

_____

_____

_____

Las respuestas varían. Trojan.Ransomlock, Inostealer.Vskim, Troyano, Fareit, Backdoor.Sorosk, Android.Boxer, W32.Changeup!gen35.

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:	Code Red (Código rojo)
Tipo de ataque:	Gusano
Fechas de ataques:	Julio de 2001

Computadoras/organizaciones afectadas:	Se infectaron unas 359 000 computadoras en un día.
Cómo funciona y qué hizo:	
Nota para el instructor: la mayor parte de lo que sigue se extrajo de la versión en inglés de Wikipedia. El gusano “código rojo” se aprovechó de las vulnerabilidades de desbordamiento del búfer en Microsoft Internet Information Servers sin parches de revisión aplicados. Inició un código troyano en un ataque por negación de servicio contra direcciones IP fijas. El gusano se propagó utilizando un tipo común de vulnerabilidad conocida como desbordamiento del búfer. Utilizó una cadena larga que repetía el carácter “N” para desbordar un búfer, lo que luego permitía que el gusano ejecutara un código arbitrario e infectara la máquina. El contenido del gusano incluía lo siguiente: • Vandalizar el sitio Web afectado con el mensaje: HELLO! Welcome to http://www.worm.com! Hacked By Chinese! (¡HOLA! Bienvenido a http://www.worm.com. Pirateado por los chinos). • Intentó propagarse buscando más servidores IIS en Internet. • Esperó entre 20 y 27 días desde que se instaló para iniciar ataques DoS en varias direcciones IP fijas. Una de ellas fue la dirección IP del servidor Web de la Casa Blanca. • Mientras buscaba máquinas vulnerables, el gusano no revisaba si el servidor en ejecución en una máquina remota ejecutaba una versión vulnerable de IIS o si IIS se ejecutaba.	
Opciones de mitigación:	
Para evitar la explotación de la vulnerabilidad del IIS, las organizaciones necesitaron aplicar el parche de Microsoft para el IIS.	
Referencias y enlaces de información:	
CERT Advisory CA-2001-19 eEye Code Red advisory Code Red II analysis	

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

Reflexión

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

_____

_____

_____

Las respuestas varían, pero podrían incluir: mantener actualizados el sistema operativo y las aplicaciones con parches y paquetes de servicios mediante un firewall personal; configurar contraseñas para acceder al sistema y al BIOS; configurar protectores de pantalla con un tiempo de espera y con solicitud de contraseña; proteger los archivos importantes guardándolos como archivos de solo lectura; encriptar los archivos confidenciales y los archivos de respaldo para mantenerlos seguros.

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

_____

_____

_____

Las respuestas varían, pero podrían incluir: el uso de firewalls, la detección y prevención de intrusiones, la protección de dispositivos de red y de terminales, herramientas de vulnerabilidad de red, educación del usuario y desarrollo de políticas de seguridad.