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

**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. Las actividades opcionales están elaboradas para mejorar la compresión o proporcionar práctica adicional.

1. 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

1. 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.

1. Recursos necesarios

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

1. Explorar el sitio web de SANS

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

* 1. Localizar los recursos de SANS.

Vaya a [www.SANS.org](http://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 25 principales errores de programación), Top 20 Critical Controls (Los 20 principales controles críticos), Security Policy Project (Proyecto de política de seguridad)

* 1. 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.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Las respuestas varían. Control crítico 5: defensas contra malware. Utilizar herramientas automatizadas para supervisar en forma continua las estaciones de trabajo, los servidores y los dispositivos móviles. Utilizar software antimalware y funciones específicas de actualización automática. Configurar los equipos de red para que el contenido de los medios extraíbles no se ejecute automáticamente.

* 1. Localizar el menú Newsletter.

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

SANS NewsBites: un resumen general de los artículos periodísticos más importantes sobre seguridad informática. Este boletín informativo se publica dos veces por semana e incluye enlaces con más información.

@RISK: The Consensus Security Alert: un resumen semanal de los nuevos ataques y vulnerabilidades de red. Este boletín también brinda información sobre el resultado de los ataques más recientes.

Ouch!: un 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.

1. 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.

* 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.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

* 1. 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 podrían ser: 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 que se mencionan en estos sitios web.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

1. 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.

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

|  |  |
| --- | --- |
| Nombre del ataque: | Code Red |
| Tipo de ataque: | Gusano |
| Fecha de los ataques: | Julio de 2001 |
| Equipos/organizaciones afectadas: | Se estima que se infectaron 359 000 equipos en un día. |
| Cómo funciona y qué daños causó: | |
| **Nota para el instructor**: La mayor parte de lo que sigue se extrajo de la versión en inglés de Wikipedia.  El gusano Code Red aprovechó las vulnerabilidades de desbordamiento de búfer en los servidores de Microsoft Internet Information Services sin parches de seguridad. Inició un código troyano en un ataque de denegación de servicio contra direcciones IP fijas. El gusano se propagó usando un tipo de vulnerabilidad común conocida como [desbordamiento de búfer](http://en.wikipedia.org/wiki/Buffer_overflow). 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:   * Reemplazo del sitio web afectado por el mensaje: HELLO! Welcome to http://www.worm.com! Hacked By Chinese! * Intentó propagarse buscando más servidores IIS en Internet. * Esperó entre 20 y 27 días desde que se instaló para iniciar ataques de 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 el aprovechamiento de la vulnerabilidad de IIS, las organizaciones debieron aplicar el parche de Microsoft para IIS. | |
| Referencias y enlaces de información: | |
| Informe CERT Advisory CA-2001-19  Aviso sobre Code Red de eEye  Análisis de Code Red II | |

* 1. Siga las pautas del instructor para completar la presentación.

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Las respuestas varían, pero podrían incluir: mantener actualizados el sistema operativo y las aplicaciones con parches y paquetes de servicios, usar 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, cifrar los archivos confidenciales y los archivos de respaldo para mantenerlos seguros.

* 1. ¿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.