Laboratorio - Investigación de amenazas de seguridad de red Objetivos

Parte 1: Explorar el sitio web de SANS

Parte 2: Identificar amenazas de seguridad de 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: La alerta de seguridad consensuada”. 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

# Instrucciones

## Explore el sitio web de SANS

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

### Localice los recursos de SANS

Busque SANS en Internet. En la página de inicio de SANS, haga clic en **Recursos** GRATIS.

#### Pregunta:

Indique tres recursos disponibles. Transmisiones web, blogs, 25 errores de software principales.

Escriba sus respuestas aquí.

### Localice el enlace a los controles de seguridad críticos de CIS.

Los **controles críticos de seguridad de CIS** vinculados en el sitio web de SANS son la culminación de una asociación público-privada que involucra al Departamento de Defensa (DoD), la Asociación de Seguridad Nacional, el Centro de Seguridad de Internet (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. Del menú **Resources**, seleccione **Critical Security Controls**, o similar. El documento de Controles de seguridad críticos de CIS está alojado en el sitio web del Centro de seguridad de Internet (CIS) y requiere un registro gratuito para acceder. Hay un enlace en la página de controles de seguridad de CIS en SANS para descargar el póster de controles de seguridad críticos de SANS 2014, que proporciona una breve descripción de cada control.

#### Pregunta:

Seleccione uno de los controles y enumere las sugerencias de implementación para este control.

Control critico: Se recomienda usar herramientas automatizadas para supervisar las estaciones de trabajo.

Escriba sus respuestas aquí.

### Localice el menú Newsletter

#### Pregunta:

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

SANS NewsBites es un resumen ejecutivo semanal que destaca las noticias más importantes sobre seguridad informática. Proporciona resúmenes breves de cada noticia y referencias web para obtener más información detallada.

@RISK es un resumen semanal confiable que cubre nuevos vectores de ataque, vulnerabilidades con exploits activos y explicaciones detalladas de ataques recientes, ofreciendo datos valiosos para la seguridad informática.

OUCH! es un boletín de noticias gratuito líder en seguridad informática dirigido al usuario común de computadoras. Publicado mensualmente en varios idiomas, cada edición es cuidadosamente investigada y desarrollada por expertos de SANS Securing The Human, instructores SANS y miembros de la comunidad. Se enfoca en temas específicos y proporciona pasos para que las personas protejan a sí mismas, a sus familias y a sus organizaciones.

Escriba sus respuestas aquí.

## Identifique 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.

### Localice el archivo del boletín @Risk: Alerta de seguridad consensuada

En la página **Newsletters**, seleccione **Archive**  para acceder a @RISK: La alerta de consenso de seguridad. Desplácese hacia abajo hasta **Archives Volumes** y seleccione un boletín informativo semanal reciente. Revise las secciones **Notable Recent Security Issues and Most Popular Malware Files**

#### Pregunta:

Enumere algunas vulnerabilidades recientes. Explore varios boletines informativos recientes, si fuera necesario.

Vulnerabilidades en sistemas operativos: Como Windows, macOS o Linux. Estas vulnerabilidades pueden permitir a los atacantes ejecutar código malicioso, obtener privilegios elevados o comprometer la integridad del sistema.

Vulnerabilidades en aplicaciones populares: Incluyen navegadores web, lectores de PDF, reproductores multimedia u otros programas ampliamente utilizados. Estas vulnerabilidades pueden permitir la ejecución de código malicioso o la obtención de información confidencial.

Vulnerabilidades en dispositivos IoT: Los dispositivos de Internet de las cosas a menudo tienen deficiencias de seguridad, como contraseñas débiles o falta de actualizaciones de seguridad. Esto puede permitir a los atacantes acceder a los dispositivos y comprometer la privacidad o seguridad de los usuarios.

Escriba sus respuestas aquí.

### Identifique sitios que proporcionen información sobre amenazas de seguridad recientes

#### Preguntas:

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.

National Vulnerability Database (NVD) - El NVD, administrado por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos, es una base de datos exhaustiva de vulnerabilidades de software conocidas. Proporciona información detallada sobre vulnerabilidades, incluyendo descripciones, referencias y puntuaciones de gravedad.

## Describa 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.

### Complete el formulario a continuación según el ataque de red seleccionado

|  |  |
| --- | --- |
| **Nombre del ataque:** | Sony |
| **Tipo de ataque:** | Ataque cibernético , intrusión en su red de juegos en línea. |
| **Fecha de los ataques:** | Abril 2011 |
| **Equipos/organizaciones afectadas:** | PlaySatation, Sony |
| **Cómo funciona y qué daños causó:** | |
| En abril de 2011, Sony anunció que había sufrido una intrusión en su red de juegos en línea, PlayStation Network. El ataque resultó en el robo de información personal de aproximadamente 77 millones de cuentas de usuarios, incluyendo nombres, direcciones de correo electrónico, fechas de nacimiento y contraseñas. Además, se informó que los detalles de tarjetas de crédito de algunos usuarios también podrían haber sido comprometidos, aunque Sony declaró que los datos estaban encriptados y no se habían encontrado pruebas de uso fraudulento. Se estima que la perdida fue de 247 mil millones de pesos | |
| **Opciones de mitigación:** | |
| Sony tuvo que cerrar PlayStation Network durante varios días mientras investigaba el incidente y mejoraba su seguridad. También se llevaron a cabo auditorías y se implementaron medidas adicionales para proteger la red y la información de los usuarios | |
| **Referencias y enlaces de información:** | |
| https://www.unocero.com/videojuegos/gaming/ataque-playstation-network-2011/ | |

### Siga las pautas del instructor para completar la presentación

# Preguntas de reflexión

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

Hacerle caso al antivirus, proteger las cuentas, tener contraseñas distintas y seguras.

Escriba sus respuestas aquí.

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

Fin del documento