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.

Sala de lectura, transmisiones web, boletines informativos, blogs, 25 errores de software principales, 20 controles críticos, políticas de seguridad.

### 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.

Las respuestas pueden variar. Control crítico 5: Defensas contra malware. Utilice herramientas automatizadas para supervisar en forma continua las estaciones de trabajo, los servidores y los dispositivos móviles. Utilice software antimalware y funciones específicas de actualización automática. Configure las computadoras de la red para que no ejecuten automáticamente contenido de medios extraíbles.

### 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 semestral de alto nivel de los artículos de noticias más importantes que se han publicado sobre seguridad informática durante la última semana. Cada noticia se resume muy brevemente e incluye una referencia en la web para obtener información detallada, si es posible.  
@RISK proporciona un resumen semanal fiable de (1) vectores de ataque recién descubiertos, (2) vulnerabilidades con nuevos exploits activos, (3) explicaciones detalladas de cómo funcionaron los ataques recientes y otros datos valiosos  
OUCH! es el boletín de noticias de seguridad gratuito líder mundial diseñado para el usuario común de la computadora. Publicada cada mes y en varios idiomas, cada edición es cuidadosamente investigada y desarrollada por el equipo SANS Securing The Human, los expertos en materia de instructor SANS y los miembros del equipo de la comunidad. Cada número se centra en un tema específico y explica los pasos que las personas pueden tomar para protegerse a sí mismas, a su familia y a su organización.

## 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.

Las respuestas pueden variar.

### 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.

Las respuestas pueden variar.

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

Las respuestas pueden variar.

## 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:** | WannaCry ransomware |
| **Tipo de ataque:** | CryptoWorm |
| **Fecha de los ataques:** | July 2001May 2017 |
| **Equipos/organizaciones afectadas:** | Estimación de 200.000 computadoras en 150 países |
| **Cómo funciona y qué daños causó:** | |
| ***Desde Wikipedia: WannaCry es un criptoworm de ransomware, que se dirige a los ordenadores que ejecutan el sistema operativo Microsoft Windows mediante el cifrado de datos y la exigencia de pagos de rescate en Bitcoincryptocurrency. El gusano también es conocido como WannaCrypt, Wana Decrypt0R 2.0, WanaCrypt0R 2.0 y Wanna Decryptor. Se considera un gusano de red porque también incluye un mecanismo de «transporte» para propagarse automáticamente. Este código de transporte busca sistemas vulnerables, luego utiliza el exploit EternalBlue para obtener acceso, y la herramienta DoublePulsar para instalar y ejecutar una copia de sí mismo. Las versiones 0, 1 y 2 de WannaCry se crearon con Microsoft Visual C++ 6.0. EternalBlue es un exploit del protocolo de bloque de mensajes de servidor (SMB) de Windows lanzado por The Shadow Brokers. Gran parte de la atención y los comentarios en torno al evento fueron causados por el hecho de que la Agencia de Seguridad Nacional de los Estados Unidos (NSA) (de quien probablemente fue robado el exploit) ya había descubierto la vulnerabilidad, pero la utilizó para crear un exploit para su propio trabajo ofensivo, en lugar de denunciarlo a Microsoft. Microsoft finalmente descubrió la vulnerabilidad y, el martes 14 de marzo de 2017, publicaron el boletín de seguridad MS17-010, que detallaba el error y anunciaba que se habían lanzado parches para todas las versiones de Windows compatibles actualmente en ese momento, como Windows Vista, Windows 7, Windows 8.1. Windows 10, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 y Windows Server 2016. Cuando se ejecuta, el malware WannaCry primero comprueba el nombre de dominio «switch kill»; si no se encuentra, entonces el ransomware cifra los datos del equipo, luego intenta aprovechar la vulnerabilidad de SMB para extenderse a equipos aleatorios en Internet, y «lateralmente» a equipos en la misma red. Al igual que con otros ransomware modernos, la carga útil muestra un mensaje informando al usuario que los archivos han sido encriptados, y exige un pago de alrededor de US$300 en bitcoin dentro de tres días, o US$600 en siete días. Tres direcciones de bitcoin codificadas, o «billeteras», se utilizan para recibir los pagos de las víctimas. Al igual que con todas estas carteras, sus transacciones y saldos son de acceso público a pesar de que los propietarios de billeteras de criptomonedas permanecen desconocidos.*** | |
| **Opciones de mitigación:** | |
| ***Aplique parches emitidos por Microsoft para el sistema operativo Windows*** | |
| **Referencias y enlaces de información:** | |
| ***Wikipedia OSC en línea*** | |

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

# Preguntas de reflexión

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

Las respuestas variarán, pero podrían incluir mantener actualizado el sistema operativo y las aplicaciones con parches y paquetes de servicio, usar un firewall personal, configurar contraseñas para acceder al sistema y la BIOS, configurar protectores de pantalla para que se agote el tiempo de espera y solicitar una contraseña, proteger archivos importantes al hacerlos solo lectura y encriptación de archivos confidenciales y archivos de respaldo para su custodia

* 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.***