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

1.Explore el sitio web de SANS

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

1.Localice los recursos de SANS

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

Indique tres recursos disponibles.

2.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.

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

Control seleccionado: CSC 8 - Malware Defenses

Se sugiere que:

- Se mantenga actualizado el antivirus en todos los equipos
- Configurar escaneos automáticos y análisis en tiempo real
- Bloquear archivos ejecutables desde medios externos cuestionables

3.Localice el menú Newsletter

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

@RISK: Reporte semanal que resume vulnerabilidades nuevas, campañas activas de ataque y malware en circulación

NewsBites: Boletín corto y directo con noticias relevantes sobre la ciberseguridad, dirigido a ejecutivos y responsables de seguridad

OUCH!: Boletín orientado a usuarios finales con consejos simples sobre como mantenerse seguro en internet

2.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.

1.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**

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

1. Vulnerabilidad Zero-Day en navegadores Chromium utilizada para ejecución remota.
2. Explotación de puertas traseras en servidores Exchange para robo de correos.
3. Ataques ransomware tipo LockBit contra infraestructura hospitalaria.
4. Campañas de phishing dirigidas usando dominios falsificados.

2.Identifique 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.

MITRE ATTACK: Base de datos de tácticas y técnicas de atacantes

The Hacker News: Noticias de ciberseguridad y ataques nuevos

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

3.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.

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

Nombre del ataque:	WannaCry Ramsomware
Tipo de ataque:	Ramsomware de auto-propagación
Fecha de los ataques:	Mayo de 2017
Equipos/organizaciones afectadas:	Hospitales, telefonica, Renault, FedEx, universidads y servicion publicos
Cómo funciona y qué daños causó:	
Aprovechó la vulnerabilidad EternalBlue (SMBv1) en Windows para propagarse automáticamente en redes sin parches. Encriptó archivos y exigió pago en Bitcoin, deteniendo operaciones críticas (incluyendo servicios médicos).	
Opciones de mitigación:	
Aplicar parches de seguridad en el sistemam mantener un respaldo del sistema y segmentar redes internas	
Referencias y enlaces de información:	
https://en.wikipedia.org/wiki/WannaCry_ransomware_attack	

2.Siga las pautas del instructor para completar la presentación

Preguntas de reflexión

1. ¿Qué medidas puede tomar para proteger su PC?
    1. Mantener el sistema y software actualizados
    2. Usar antivirus/EDR y activarlo en tiempo real
    3. No abrir archivos adjuntos sospechosos
    4. Usar contraseñas fuertes y activar autenticación en dos pasos
    5. Realizar respaldos periódicos

2. ¿Cuáles son algunas medidas importantes que las organizaciones pueden seguir para proteger sus recursos?
    1. Políticas claras de seguridad y capacitación de usuarios.
    2. Implementar firewalls y segmentación de red.
    3. Monitoreo continuo y respuesta a incidentes.
    4. Copias de seguridad verificadas y planes de recuperación.