Tarea online BRS07.

Título de la tarea: Configuración de dispositivos y sistemas informáticos II

Curso de Especialización y módulo: Ciberseguridad en Entornos de las Tecnologías de la Información - Bastionado de Redes y Sistemas.

¿Qué contenidos o resultados de aprendizaje trabajaremos?

Resultados de aprendizaje

- **RA4.** Diseña redes de computadores contemplando los requisitos de seguridad.
- **RA5**. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad.

Contenidos

1.- Seguridad del puesto de trabajo y endpoint fijo y móvil. AntiAPT, antimalware.
2.- Seguridad del correo electrónico.
3.- Herramientas de almacenamiento de logs.
4.- Protección ante ataques de denegación de servicio distribuido (DDoS).
5.- Configuración segura de cortafuegos, enrutadores y proxies.
    5.1.- Firewalls.
        5.1.1.- Medidas de evasión.
    5.2.- Router.
    5.3.- Proxy.
6.- Monitorización de sistemas y dispositivos.
7.- SIEMs.
8.- Soluciones de Centros de Operación de Red, y Centros de Seguridad de Red: NOCs y SOCs.

1.- Descripción de la tarea.

Desde hace unos días no paramos de recibir incidentes de seguridad en el SOC. Tenemos 2 incidentes nuevos que resolver. Uno relacionado con una denegación de servicio distribuido y otro relacionado con un ataque a la web de la compañía.

Nos han enviado la información recopilada en el análisis del incidente de DDoS (Denegación de Servicio Distribuida). Tenemos que ordenar la información para buscar desde qué ISPs viene el ataque para informar a nuestro SOC, y pueda tomar las acciones oportunas con los ISP de país sobre las IPs detectadas, y pueda cortar el ataque desde el origen (fichero - datos conexiones (.dat - 53000 KB)).

Con esta información, además podremos aplicar las contramedidas necesarias y disminuir el impacto del ataque.

Para realizar el análisis del fichero puede utilizar comandos de Linux con una máquina Linux o instalando Cygwin en una máquina Windows: cat, grep, head, tail, sort, cut, awk, netcat o automatizarlo con python.

El ataque se ha producido por UDP y los campos relativos a los logs recibidos tienen el siguiente formato:

Columna	Descripción
1	Fecha
2	Hora
3	Duración
4	Protocolo
5	IP:puerto origen
6	->
7	IP:puerto destino
8	N° paquetes transmitidos
9	N° bytes transmitidos
10	Número de flujo

Héctor Fernández Bardal. *Tabla datos ejercicio* (CC0)

Necesitamos:

- Tener un listado de IPs únicas
- Su geolocalización con un servicio de whois

Relativo al ataque web, debemos identificar (fichero logs.zip (zip - 6,41 KB)):

- Las herramientas ofensivas utilizadas por los atacantes
- Las páginas web sobre las que han realizado el ataque
- Usuarios utilizados en cada uno de los servicios atacados
- Ficheros descargados

Para estas tareas se proporcionarán ficheros de registros (logs) de los que es necesario extraer la información al que se ha hecho referencia anteriormente.

2.- Información de interés.

Recursos necesarios y recomendaciones

Referencias de interés para desarrollar el trabajo:

- https://sqlmap.org/
- https://linuxconfig.org/linux-commands-cheat-sheet
- https://github.com/vanhauser-thc/thc-hydra
- https://whois.cymru.com/
- https://github.com/epi052/feroxbuster
- https://nmap.org/

Indicaciones de entrega

Una vez realizada la tarea, el envío se realizará a través de la plataforma. El archivo se nombrará siguiendo las siguientes pautas:

Apellido1_Apellido2_BRS07_Tarea

Asegúrate que el nombre no contenga la letra ñ, tildes ni caracteres especiales extraños. Así por ejemplo la alumna **Begoña Sánchez Mañas para la séptima unidad del MP de BRS**, debería nombrar esta tarea como...

sanchez_manas_begona_BRS07_Tarea

3.- Evaluación de la tarea.

Criterios de evaluación implicados

Criterios de evaluación RA4

- a)Se ha incrementado el nivel de seguridad de una red local plana segmentándola físicamente y utilizando técnicas y dispositivos de enrutamiento.
- b) Se ha optimizado una red local plana utilizando técnicas de segmentación lógica (VLANs).
- c) Se ha adaptado un segmento de una red local ya operativa utilizando técnicas de subnetting para incrementar su segmentación respetando los direccionamientos existentes.
- d) Se han configurado las medidas de seguridad adecuadas en los dispositivos que dan acceso a una red inalámbrica (routers, puntos de acceso, etc.).
- e) Se ha establecido un túnel seguro de comunicaciones entre dos sedes geográficamente separadas.

Criterios de evaluación RA5

- a)Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.
- b) Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
- c) Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.
- d) Se han implementado contramedidas frente a comportamientos no deseados en una red.
- e) Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.

¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
Apartado 1: Cada pregunta bien contestada del análisis del primer fichero 2,5 puntos. Hay 2 preguntas en dicho apartado. Se evaluarán por separado.	5 punto
Apartado 2: Cada pregunta bien contestada del análisis del segundo fichero 1,25 puntos. Hay 4 preguntas en dicho apartado. Se evaluarán por separado.	5 puntos
Redacción clara y correcta, sin errores ortográficos	Se resta 0,1 puntos por cada error ortográfico o

	expresiones incorrectas.

NOTA IMPORTANTE

Aquellos apartados/subapartados en los que las capturas de pantalla no sean claras o no tengan como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil, no serán corregidos.