BRS05. Tarea online

Título de la tarea: Diseño de redes de computadores seguras

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.

Contenidos

1.- Seguridad en redes inalámbricas.
    1.1.- Conceptos básicos.
    1.2.- Debilidades de las redes wifi.
    1.3.- Vulnerabilidades en los protocolos wifi.
    1.4.- Ataques a redes wifi.
2.- Soluciones DLP (Data Loss Prevention)
3.- Redes privadas virtuales (VPNs)
4.- Herramientas de monitorización.
    4.1.- Tecnologías.

1.- Descripción de la tarea.

Caso práctico

A lo largo de esta unidad, el alumno tendrá que llevar a cabo dos prácticas relacionadas con los temas que se tratan en esta unidad.

Wifi

El alumno tendrá que configurar en la seguridad wifi de su router el filtrado MAC y añadir a la lista una MAC de un dispositivo que esté a su alcance (móvil, portátil, etc.).

A continuación, desde una distribución Kali u otra linux, virtualizada o nativa, se hará pasar por el dispositivo autorizado modificando su MAC con la aplicación correspondiente y comprobando que se puede conectar. El alumno evidenciará con capturas que ha conseguido conectarse a la red wifi suplantando a un cliente.

IDS

El alumno llevará a cabo un trabajo de investigación que consistirá en desplegar una solución de IDS opensource como SNORT y tras configurarlo, realizará un escaneo con nmap que trate de identificar los servicios para ver cómo se comporta la herramienta.

Para ello necesitará una máquina de ataque que puede ser Kali, y otra máquina para desplegar Snort (puede ser otra distribución Linux o un Windows). Tras desplegar la herramienta, el alumno tendrá que saber dónde se almacenan los logs del IDS para que, una vez lanzado el ataque con nmap, pueda interpretar los resultados.

Recursos:

Nmap: https://nmap.org/
Snort: https://www.snort.org/downloads
Adicionalmente puede instalar la interfaz gráfica snorby para tener un dashboard gráfico: https://github.com/Snorby/snorby

¿Qué te pedimos que hagas?

- **Apartado 1: seguridad wifi**
  El alumno tendrá que configurar en la seguridad wifi de su router el filtrado MAC y añadir a la lista una MAC de un dispositivo que esté a su alcance (móvil, portátil, etc.). A continuación, desde una distribución Kali u otro linux, virtualizada o nativa, se hará pasar por el dispositivo

autorizado modificando su MAC con la aplicación correspondiente y comprobando que se puede conectar.

- **Apartado 2: implementación IDS**

El alumno llevará a cabo un trabajo de investigación que consistirá en desplegar una solución de IDS opensource como SNORT y tras configurarla, realizará un escaneo con nmap que trate de identificar los servicios para ver cómo se comporta la herramienta. Para ello necesitará una máquina de ataque que puede ser Kali, y otra máquina para desplegar Snort (puede ser otra distribución Linux o un Windows). Tras desplegar la herramienta, el alumno tendrá que saber dónde se almacenan los logs del IDS para que, una vez lanzado el ataque con nmap, pueda interpretar los resultados.

NOTA IMPORTANTE

Para todos los apartados es necesario entregar las capturas de pantalla de los principales pasos realizados, explicando el proceso seguido en cada uno de ellos. Las capturas de pantalla realizadas deben tener como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil. Aquellos apartados/subapartados que no cumplan esta condición no serán corregidos.

2.- Información de interés.

Recursos necesarios y recomendaciones

Recursos necesarios

- Ordenador personal con, al menos, 4 Gigabytes de memoria RAM
- Conexión a Internet para consultar la Unidad 3.
- Sistemas Operativos Windows 10, Ubuntu 18.04, Ubuntu 20.04
- Navegador web.
- Software para comprimir los archivos de la tarea.

Otros:

Nmap:https://nmap.org/
Snort: https://www.snort.org/downloads
Adicionalmente puede instalar la interfaz gráfica snorby para tener un dashboard gráfico: https://github.com/Snorby/snorby

Recomendaciones

- Antes de abordar la tarea:
- lee con detenimiento la unidad, consulta los enlaces para saber más, examina el material proporcionado por el profesor y aclara las dudas que te surjan con él.
- Realiza el examen online de la unidad, y consulta nuevamente las dudas que te surjan. Solo cuando lo tengas todo claro, debes abordar la realización de la tarea.
- No olvides elaborar el documento explicativo.

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_BRS05_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 quinta unidad del MP de BRS**, debería nombrar esta tarea como...

sanchez_manas_begona_BRS05_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.

¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
Se ha demostrado que el filtrado a través de la MAC en las redes wifi es ineficaz.	5 puntos
Ha implementado un IDS y verificado que es capaz de detectar ataques de red.	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.

BRS05. Foro

Problema de acceso a configuración router para tarea

Re: Problema de acceso a configuración router para tarea
de Bruno Béjar Abalde - miércoles, 3 de enero de 2024, 00:35

Buenas noches.
Para aquellos alumnos que no dispongan de un router WiFi en el que podáis modificar la configurar de seguridad para implementar el filtrado por MAC. Podéis hacer lo siguiente. Creáis una MV con Linux, vale cualquier distribución. Y en esa MV activáis el servidor SSH. Ahora deberéis configurar las ip-tables para permitir la conexión en el puesto 22 de una MAC en concreto, la sintaxis general de ip-tables es:
iptables -I "CHAIN-NAME" -m mac --mac-source "MAC-ADDRESS" -j "ACTION"
Una vez permitís esa conexión debéis denegar el resto de conexiones, con la siguiente instrucción:
iptables -P FORWARD DROP

Tener en cuenta el orden, primero se permite y por último se deniega todas las demás conexiones. Si lo hacéis al revés no funcionara la regla que permite la conexión.

Una vez configurada la MV que hará el filtrado solo queda comprobar que la MAC que le hemos dado establece la conexión. Cuando hayáis probado esa conexión. Probar con otra MV y ver que no se os permite. Ahora en esa misma MV cambiar la MAC a la MAC que se le permite conexión y comprobar que ahora si es posible.

En la entrega se debe ver de forma clara como es permitida la conexión desde la MV que tiene la MAC que habéis autorizado. Como se rechaza desde otra MV cuya interfaz de red tiene otra MAC, mostrar la MAC y después intentar la conexión. Por último, como cambiáis la MAC de esta MV y ahora si os permite la conexión.

En unos días os cambiaré la rubrica de corrección para que no quede duda que es posible hacerlo o bien por la red WiFi si se dispone de router o bien mediante el filtrado con ip-tables para aquellos que no podías hacer mediante un router WiFi.

Espero que os haya servido de ayuda. Un saludo y Feliz Año.