SEGURIDAD EN SISTEMAS OPERATIVOS

Curso Febrero 2020 – Junio 2020

Prueba de Evaluación Continua 3

ANÁLISIS DE PUERTOS,VULNERABILIDADES Y PROTOCOLOS

- Objetivos
- Presentación
- Análisis de protocolos
- Análisis de vulnerabilidades
- Indicaciones para la PEC
- Evaluación
- Entrega
- Fechas

Objetivos

Los objetivos de esta PEC son:

- Familiarizarse con las vulnerabilidades inherentes a los sistemas operativos.
- Interpretar los resultados de las herramientas de análisis.
- Comprender como se puede obtener información valiosa a partir de estas herramientas.
- Ver la importancia de un análisis de vulnerabilidades y que es necesario establecer un ciclo de administración de vulnerabilidades para mantener segura la infraestructura de red.

Presentación

En esta PEC seguiremos con las máquinas virtuales creadas en las PEC anteriores. Veréis que necesitáis que los dos equipos se puedan comunicar por red, ya que usaremos las dos máquinas virtuales a la vez.

Podéis buscar información adicional que os pueda ayudar con la instalación y configuración. Cualquier duda que os surja respecto a temas de conectividad, podéis exponerla en el foro para que sea resuelta.

Ejercicios

Los análisis de vulnerabilidades son capaces de descubrir los puntos débiles de la infraestructura de red y constituyen, por tanto, un paso vital para el aseguramiento de la información. El análisis de vulnerabilidades, además, es una de les primeras etapas en un ataque. Realizado por el administrador del sistema, es posible detectar y cerrar los puntos vulnerables haciendo más difícil, por lo tanto, un ataque externo.

Para realizar la PEC, necesitareis los dos servidores funcionando. Como usaremos los dos servidores a la vez, no hemos separado la parte "windows" de la parte "linux" en esta tercera PEC.

Análisis de protocolos

Desde el punto de vista de securización, en este apartado nos centraremos en ver un poco el análisis de protocolos. Esto nos permitirá darnos cuenta de que si un atacante accede a poder ver el tráfico de la red puede conseguir información muy valiosa. Por tanto, ante esta

posibilidad, las herramientas de IDS o análisis de protocolos son muy importantes. El análisis de protocolos nos dice que pasa en la red.

LINUX SERVER

a) (1 punto) Instala snort (las dependencias las podéis instalar con apt-get)

b) (2 puntos) Configura una regla en el snort que detecte el ping desde la maquina host a la máquina virtual. El mensaje en los logs debe ser: "uoc - ping"

c) (2 puntos) Instala el servicio SSH y realiza la siguiente configuración (para cada uno de los puntos explica cómo lo has implementado e incluye capturas de pantallas como sea necesario para mostrar dónde activas la configuración y las diferentes directivas que utilizas en cada caso):

- Indica dónde se encuentra el fichero de configuración.
- Cambia el puerto para que el servicio se ejecute en el puerto 3333.
- Evita que el root pueda conectarse de forma remota.
- Número de intentos máximo en 3.
- Tiempo máximo de Login en 60 segundos (mostrar el mensaje que se obtiene).
- No permitir el login mediante password.
- Configurar el uso de clave pública-privada para poder acceder al servidor.

Análisis de vulnerabilidades

El análisis de vulnerabilidades tanto puede ser usado por un atacante para descubrir los puntos débiles de nuestro servidor como por un administrador de sistemas para descubrir debilidades.

LINUX SERVER

d) (2 puntos) Instala la herramienta nessus en el equipo Linux y úsala para analizar el sistema windows.

A partir de la información obtenida, indicad las vulnerabilidades encontradas. Necesitareis consultar Internet, bases de datos de exploits y de vulnerabilidades. Presentad la información en un formato tabular que incluya al menos la siguiente información:

- Identificación del riesgo de seguridad
- Breve descripción del problema
- Exploits existentes para la vulnerabilidad
- Solución a los problemas detectados

e) (1 punto) Instala la herramienta Lynis en tu servidor. Puedes descargarlo desde su Github: https://github.com/CISOfy/lynis.git. Realiza un chequeo con la herramienta y explica los resultados que obtienes.

WINDOWS SERVER

f) (2 puntos) Investigad y documentad en qué consiste un ataque "pass-the-hash" en Windows y cuáles son las técnicas que pueden emplearse para prevenir y mitigar dichos ataques.

Descargad e instalad la aplicación de Microsoft LAPS en el equipo Windows incluyendo las herramientas "Management Tools". Explora las posibilidades que ofrece la aplicación e investiga su funcionamiento.

¿Para qué sirve esta aplicación? ¿Cómo puede ayudar a prevenir ataques del tipo pass-the-hash?

Indicaciones para la PEC

Existen preguntas que pueden responderse de múltiples formas distintas, simplemente elegid y comentad aquella que se haya utilizado.

Procurad que las respuestas sean lo más concretas posible. No os extendáis.

Las respuestas para ser validas deben contener los pasos para duplicar el resultado.

El documento que enviéis al buzón no debe exceder las 10 páginas máximo (5 para Linux y 5 para Windows). Puede estar en cualquier formato de texto como odt, pdf, doc, docx, sxw, rtf, txt...

Entrega

Depositad las respuestas del enunciado de la PEC en el área destinada a tal fin. Incluid vuestra respuesta en un único documento. En caso de que necesitéis entregar más de un documento, entonces enviadlos dentro de un único fichero comprimido (zip, rar, 7z, tgz…).