SEGURIDAD EN SISTEMAS OPERATIVOS

Curso Febrero 2020 – Junio 2020

Prueba de Evaluación Continua 2

SECURIZAR SERVIDORES, ANALISIS DE PUERTOS

- Objetivos
- Presentación
- Ejercicios hardening
- Ejercicios intrusión : fingerprinting
- Indicaciones para la PEC
- Evaluación
- Entrega
- Fechas

Objetivos

Los objetivos de esta PEC son:

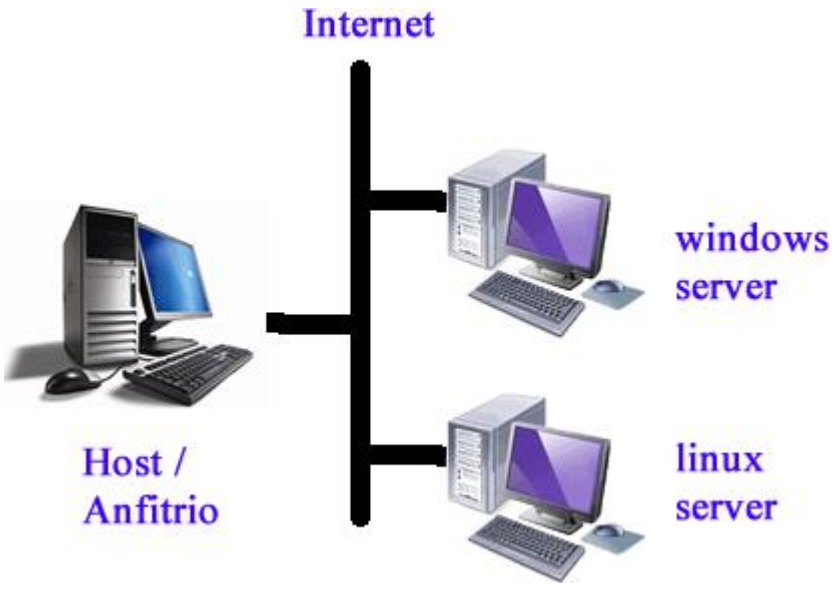
- Uso de herramientas de seguridad Linux
- Fortificación de sistema Linux acceso físico
- Uso de herramientas de seguridad Windows 2019
- Configuración de red virtualizada.
- Análisis de puertos y fingerprinting

Presentación

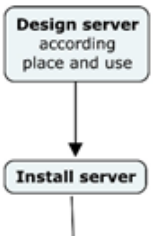
En esta PEC seguiremos con las máquinas virtuales creadas en la PEC anterior. En algún punto de los ejercicios veréis que necesitáis que los dos equipos se puedan comunicar por la red. Necesitaremos, por lo tanto, configurar una red interna en VirtualBox.

Podéis buscar información adicional que os pueda ayudar con la instalación y configuración. Cualquier duda que tengáis podéis exponerla al foro para que sea resuelta.

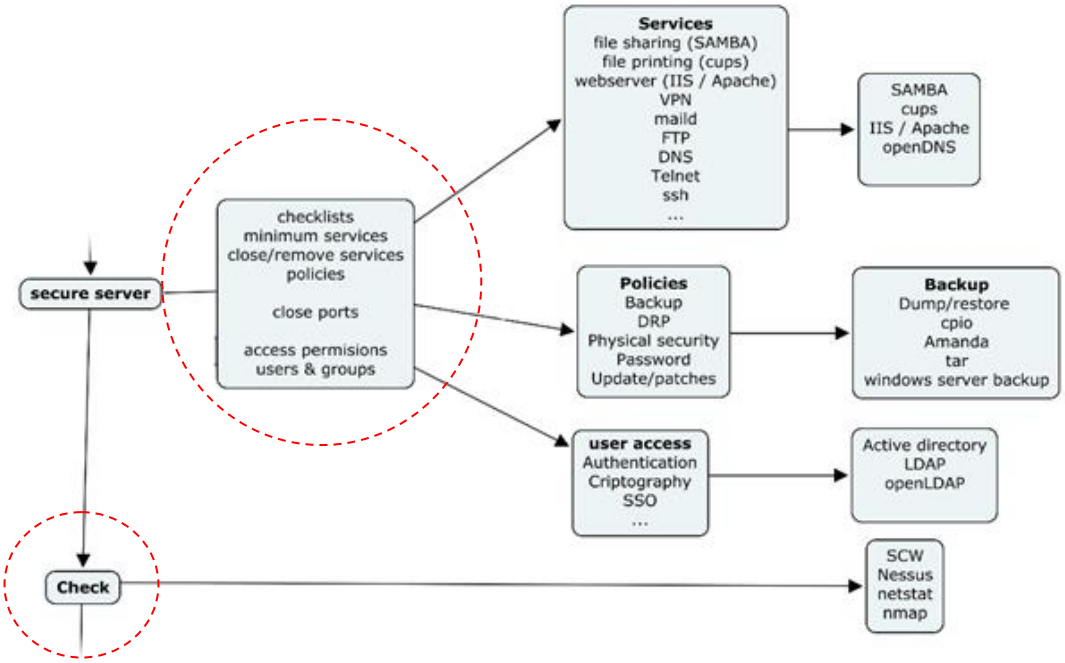
El esquema final de la red que debéis tener debe ser similar al siguiente:



En la pec anterior, hemos hecho las dos primeras etapas de hardening.



En esta nos centraremos en la securizacion de los servidores.



Ejercicios hardening

Para poner en marcha un servidor nuevo, hay que hacer varias acciones. Nosotros las haremos entre los dos equipos para no alargarlo demasiado.

- Eliminar servicios innecesarios
- Cerrar puertos
- Verificar los usuarios, permisos y políticas y comprobar cómo queda el servidor.
- Configurar servicios de forma segura.

Para eliminar los servicios innecesarios, necesitamos herramientas que nos puedan decir qué puertos hay abiertos y qué servicios hay encendidos. Para poderlo saber se utilizan las herramientas nmap, netstat o ss. Instalad nmap en una máquina Linux. Si el anfitrión es una máquina Linux , entonces podéis hacerlo desde la misma. Sino usad el servidor Linux.

LINUX SERVER

a) (0,5 puntos) Mostrar los puertos abiertos e información adicional del daemon de localhost con nmap. Por otro lado, mostrar los puertos en escucha mediante netstat o ss

b) (0,5 puntos) Cerrar todos los servicios excepto el 22, 80 y 443. Los puertos deben seguir cerrados una vez reiniciado el equipo (no filtrados!)

c) (0,5 puntos) Evitar que la máquina virtual responda a ping usando el /proc. Los cambios deben ser persistentes al reinicio

d) (1 punto) Edita el Grub de Debian en el arranque para lograr una Shell. Muestra el proceso que has llevado a cabo para lograr este hecho. Muestra cómo eres root y puedes realizar cualquier acción en el sistema.

e) (1,5 puntos) Protege el Grub de la posible edición. Muestra el proceso para ello. Protege el GRUB del sistema con un superusuario para que no se pueda editar el GRUB y verificar que esto sucede.

WINDOWS SERVER

f) (1,5 puntos) Bajaos la herramienta Policy Viewer y el Security Baseline de Windows Server 2019. Todo esto está incluído en el Microsoft Security Compliance Toolkit:

- https://docs.microsoft.com/es-es/windows/security/threat-protection/security-compliance-toolkit-10
- https://www.microsoft.com/en-us/download/details.aspx?id=55319

Explicad la utilidad de esta herramienta y para qué se puede usar.

Ejecutad la herramienta e importad la política de seguridad del Baseline seleccionando la carpeta GPO. Escoged las políticas correspondientes a Windows Server 2019.

Desde la herramienta de gestión de politicas de grupo haced una copia de seguridad de todas las GPOs del dominio e importadlas en la herramienta Policy Viewer.

Comparad las políticas locales con las recomendadas por el Baseline y la copia de seguridad de las GPOs del dominio, y comentad las diferencias que juzguéis más importantes.

g) (1 punto) Utilizad la herramienta netstat para mostrar los puertos en uso del servidor y que aplicación los está usando. Valorad si todos los servicios son estrictamente necesarios y mostrad algún ejemplo. ¿Quien usa el TCP/88? ¿Se puede desactivar? ¿Por qué?

h) (1 punto) Desde Linux utilizad la herramienta nmap para ver los puertos en escucha en el equipo Windows (o desde nmap para Windows). Comparad los resultados de netstat con nmap. ¿En que situación tiene sentido utilizar nmap y no netstat?

i) (0,5 puntos) Instalar el servidor web con las siguientes características:

- Configurar el servicio para que sea cifrado (HTTPS)
- Configurar el servicio para que escuche HTTP en el puerto 8080
- Comprobar la configuración y funcionamiento mediante un navegador desde el servidor linux

j) (0,5 puntos) Vamos a estudiar el concepto de "Language Mode" en Powershell. Aplicar el modo "Constrained Language" a Powershell. Explicad cómo lo habéis aplicado a nivel de equipo.

- https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_language_modes?view=powershell-7

¿Cómo se puede hacer un bypass de este modo de lenguaje en Powershell?

Ahora vamos a estudiar el concepto de "AMSI". Explicad qué es AMSI y para qué sirve en los sistemas Windows.

Muestra en una captura que AMSI está habilitado en tu Powershell.

Ejercicios de intrusión: fingerprinting

La primera etapa de toda intrusión és el fingerprinting. Es decir, el reconocimiento del equipo al que queremos acceder, los puertos abiertos y los servicios que hay en los puertos abiertos.

k) (1,5 puntos) Desde un ordenador Linux (probablemente vuestro servidor) y usando nmap:

- Hacer un escaneo de la red (la vostra) para determinar que ordenadores/IP estan activos.
- hacer un escaneo "ICMP" de la red "windows" (del servidor).
- hacer un escaneo "SYN TCP" de la red "windows"
- hacer un escaneo "TCP connect" de la red "windows"
- hacer un escaneo "UDP" de la red "windows"
- hacer un escaneo para determinar el sistema operativo
- hacer un escaneo para determinar las versiones de los servicios que están en marcha

Con todos estos análisis, que se puede decir de la máquina analizada?

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).