Prepara tu examen de HE

Introducción

Cada centro, cada año y cada docente, puede plantear al alumnado un modelo de examen concreto que, a su criterio, pueda servir como una correcta evaluación del módulo.

Para ayudar a preparar las evaluaciones, he pensado que podría ser de ayuda crear un archivo único para cada módulo, que pueda crecer cada año con el feedback y apoyo de la comunidad, con cuestionarios de todo tipo, con solucionario o solo los enunciados, pues la intención primera es poder ofrecer una idea de lo que podemos encontrarnos a la hora de una evaluación, poder aprender con ello, y no algo que una persona acabe memorizando, y esperando, sin comprender ni ahondar en la materia, que aparezca mágicamente en el examen.

Este documento, por tanto, no pretende ser una guía única y veraz de exámenes pasados o futuros, pero si una fuente de información sobre la que basar vuestros estudios.

Posibles modelos.

Modelo 1.

Ejemplo para preparación.

PREGUNTAS DEL TEST DE CONOCIMIENTOS:

1. (Puntuación: 0,25). ¿Qué representa la métrica de entorno del sistema CVSS?

A) Las características intrínsecas de la vulnerabilidad.
B) Las características de la vulnerabilidad que pueden cambiar a lo largo del tiempo.
C) Las características propias del entorno en que ha sido encontrada la vulnerabilidad.
D) El impacto global de la vulnerabilidad.

2. (Puntuación: 0,25). ¿Cuál es uno de los problemas de seguridad de las redes de tipo OPEN?

A) No disponen de cifrado de tráfico.
B) Solo permiten la conexión de un número limitado de dispositivos.
C) El acceso a la red solo se realiza mediante autenticación por contraseña.
D) Solo pueden ser utilizadas por usuarios invitados.

3. (Puntuación: 0,25). ¿Qué técnica de escaneo de red suele funcionar únicamente desde una perspectiva de escaneo interna?

A) Wireshark.
B) Arp scan.
C) Nmap.
D) Netdiscover.

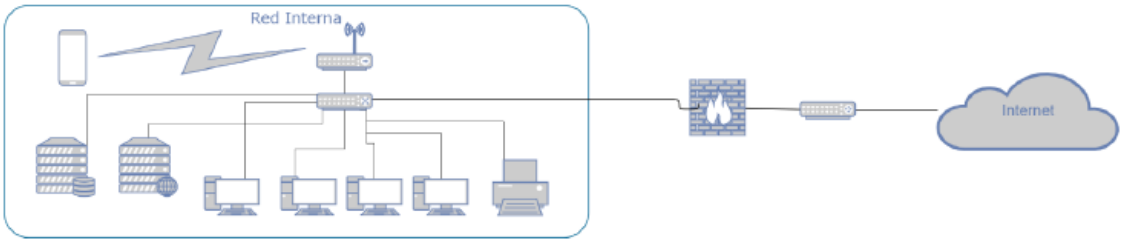
4. ¿Qué son los exploits de escalada de privilegios?

A) Son exploits que se ejecutan de manera local con el objetivo de conseguir un mayor nivel de acceso en el sistema.
B) Son exploits que se ejecutan de manera remota al que no se tiene acceso de manera previa.
C) Son exploits que tienen por objetivo comprometer un servicio que se ejecuta en modo servidor.
D) Son exploits que afectan al software y programas que se ejecutan en el lado del cliente.

PREGUNTAS TEÓRICO-PRÁCTICAS:

PTP1. (2 puntos). Detección de vulnerabilidades.

Dado el siguiente esquema de red:



Datos de la red interna:

- CIDR: 172.16.0.0/16
- Firewall activo en los servidores que bloquea la comunicación ICMP.

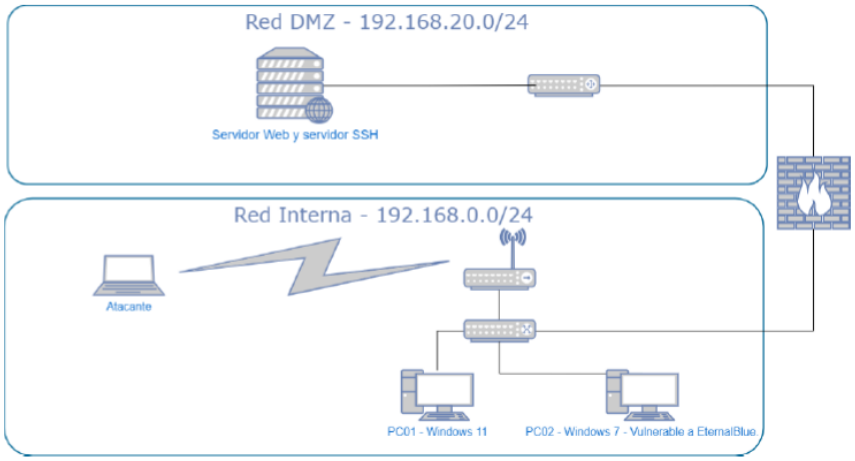
En esta red partimos del caso en que no conocemos ningún equipo de la red y debemos realizar una fase completa de escaneo hasta localizar la vulnerabilidad que se encuentra en el servicio SAMBA (445/TCP).

1. Indica los pasos y los comandos que deberías realizar para poder dar con el servidor SAMBA y su vulnerabilidad, con el uso de nmap. (1,5)

2. Una vez que se ha obtenido la vulnerabilidad, ¿qué herramienta podemos usar para conseguir explotarla? Describe de forma genérica cuál sería el proceso (no es necesario indicar comandos) (0,5)

PTP3. (1 punto). Ataques a sistemas.

Dado el siguiente esquema simplificado de red:



En este esquema, el equipo atacante tiene acceso a la red 192.168.0.0/24. Si nuestro objetivo es el servidor web final que se encuentra en la red 192.168.20.0/24. ¿Qué técnica se podría usar para llegar a tener acceso a esta máquina? Explica el proceso general (no es necesario indicar comandos).

Modelo 2.

Ejemplo pasado por alumnado.

Test

1. ¿Qué es DeepWeb?
2. ¿Qué es la seguridad informática?
3. ¿Qué es un activo en seguridad de la información?
4. ¿Cómo se define una vulnerabilidad zero day?
5. ¿Qué función cumple un router?
6. ¿Qué es el ESSID o SSID en una red Wi-Fi?
7. ¿Cuál es una de las mejoras de seguridad que introduce WPA en comparación con WEP?
8. ¿Cuál es la debilidad principal del protocolo WEP?
9. ¿Cuál de las siguientes herramientas es útil para recopilar información de perfiles de Twitter y Facebook?
10. ¿Qué tipos de información puede obtenerse mediante la enumeración DNS?
11. ¿Cuál es el tipo de escaneo que se ejecuta después de los escaneos de red y de servicios para verificar la presencia de vulnerabilidades en función de la información recopilada?
12. ¿Cuál es la herramienta principal para realizar la enumeración de puertos y servicios?
13. ¿Qué técnica de escaneo si lo envía un segmento TCP con el flag FIN, y puede conocer si un determinado puerto se encuentra abierto, aunque exista un firewall que esté protegiendo las conexiones contra el activo auditado?
14. ¿Qué herramienta utiliza el proyecto Vulscan para buscar posibles vulnerabilidades existentes en los sistemas remotos?
15. ¿Qué herramienta se utiliza para buscar vulnerabilidades y sus correspondientes exploits o pruebas de concepto para aprovecharse de la vulnerabilidad en el sistema remoto?
16. ¿Qué es el mecanismo de las cookies?
17. ¿Qué cabecera de la petición indica el tamaño que ocupa la petición en Bytes?
18. ¿Qué indican los códigos de estado HTTP 5xx?
19. ¿Qué es la autenticación basada en cookies?
20. ¿Qué herramienta es una base de datos online de búsqueda de vulnerabilidades y exploits para poder comprometer un objetivo?

PTP1.Plan de auditorías

Medios de transporte nacionales → establecido un nuevo centro de control de respaldo de su servicio de control de rutas ferroviarias.

2 auditorías que permitan identificar posibles riesgos y vulnerabilidades focalizados en el nuevo centro de control.

Definir un plan de auditorías en el que se recojan las dos auditorías más prioritarias que consideres en este caso. Para cada auditoría se debe especificar:

- Justificación de elección
- Activos incluidos en la auditoría
- Definición del origen, enfoque y el tipo de información proporcionada
- Objetivo perseguido con la auditoría

PTP2. DVWA

Img 1. Intercept
Img 2. Mensaje
Img 3. Vulnerability
(Las imágenes muestran capturas de pantalla del proceso)

1. ¿Qué tipo de ataque se está realizando? ¿Qué se persigue con este?
2. Ordena las 3 imágenes según la secuencia de realización del ataque
3. Explica qué se realiza en cada una de las imágenes para conseguir realizar el ataque
4. Indica qué les sucederá a los futuros visitantes de esta página.

PTP3. Cracking contraseñas

Mediante el uso de la herramienta hashcat se debe realizar el cracking de las siguientes contraseñas:

- Contraseña en la que se le ha obtenido su HASH NetNTLMv4 para el que no se dispone de diccionario, pero se sabe que su clave se compone de tres caracteres alfanuméricos y acaba con un carácter especial.
- Contraseña a la que se le ha obtenido su HASH SHA1 y del que se dispone un diccionario de claves en /usr/share/dictionary.txt