GOBIERNO DE ESPAÑA | MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES

cide.ad Centro para la Innovación y Desarrollo de la Educación a Distancia

PRIMER APELLIDO	SEGUNDO APELLIDO	NOMBRE DEL ALUMNO/A	DÍA NACIMIENTO	MES NACIMIENTO
V	M	S	22	07

PREGUNTAS DEL TEST DE CONOCIMIENTOS:

1. (Puntuación: 0,25). ¿Cuál es la finalidad principal de las pruebas de seguridad en el hacking ético?
   A) Explotar vulnerabilidades en sistemas informáticos.
   B) Obtener información confidencial.
   C) Comprometer la seguridad de un sistema.
   D) Solventar las vulnerabilidades detectadas para evitar un compromiso del sistema.

2. (Puntuación: 0,25). ¿Cuál es el objetivo principal de un hacker ético durante una auditoría de hacking ético?
   A) Descubrir fallos de seguridad en un sistema informático.
   B) Explotar vulnerabilidades para obtener un beneficio económico.
   C) Dañar la reputación de una empresa o individuo mediante ataques informáticos.
   D) Probar el rendimiento del sistema informático.

3. (Puntuación: 0,25). ¿Cuál es el objetivo del principio de disponibilidad en la seguridad de la informac
   A) Prevenir modificaciones no autorizadas de la información.
   B) Ofrecer los recursos que requieran los usuarios cuando se necesiten.
   C) Mantener la información inalterada ante incidentes o accesos malintencionados.
   D) Ocultar o mantener en secreto determinada información o recursos.

4. (Puntuación: 0,25). ¿Cuál es el objetivo del sistema CVSS?
   A) Detectar vulnerabilidades en sistemas informáticos.
   B) Evaluar la criticidad de las vulnerabilidades identificadas.
   C) Desarrollar parches y soluciones para vulnerabilidades.
   D) Proporcionar herramientas para explotar vulnerabilidades.

5. (Puntuación: 0,25). ¿Cuál es la razón por la que la banda de frecuencia 5 GHz tiene menos interfer que la banda de frecuencia 2,4 GHz?
   A) La banda de 5 GHz ha sido habilitada con posterioridad a las usadas por versiones anteriores.
   B) La banda de 5GHz tiene canales están separados por un mayor espectro de frecuencias.
   C) La frecuencia de la banda de 5 GHz es mayor que la de la banda de 2,4 GHz.
   D) La banda de 5 GHz tiene un alcance menor que la banda de 2,4 GHz.

6. (Puntuación: 0,25). ¿Qué es la dirección MAC en una red Wi-Fi?
   A) Es el identificador único de un dispositivo que ha creado una red Wireless.
   B) Es el nombre amigable asignado a una red wifi para que los usuarios la identifiquen con facilida
   C) Es el procedimiento que se realiza para establecer la comunicación entre el dispositivo Wi-Fi y e de Acceso.
   D) Es la dirección de enlace del dispositivo que identifica de manera inequívoca al dispositivo en l enlace.

PRIMER APELLIDO	SEGUNDO APELLIDO	NOMBRE DEL ALUMNO/A	DÍA NACIMIENTO	MES NACIMIENTO
V	K	S	22	05

7. (Puntuación: 0,25). ¿En qué modo de operación se configura la tarjeta para crear un punto de acceso?
A) Managed.
B) Monitor.
C) Adhoc.
D) Master.

8. (Puntuación: 0,25). ¿Cuál es la principal diferencia entre el reconocimiento pasivo y el reconocimiento activo en una auditoría?
A) El reconocimiento pasivo implica la interacción directa con el objetivo, mientras que el reconocimiento activo no lo hace.
B) El reconocimiento activo implica la interacción directa con el objetivo, mientras que el reconocimiento pasivo no lo hace.
C) Ambos tipos de reconocimiento implican la interacción directa con el objetivo.
D) Ambos tipos de reconocimiento no implican la interacción directa con el objetivo.

9. (Puntuación: 0,25). ¿Qué herramientas o técnicas se utilizan en el reconocimiento pasivo en una auditoría?
A) Escaneo de puertos y crawling.
B) Ping y 3 hand-shake way.
C) Ataques de denegación de servicio (DoS) y phishing.
D) Nmap y Wireshark.

10. (Puntuación: 0,25). ¿Qué buscador es el mayor indexador de contenidos de internet?
A) Bing.
B) DuckDuckGo.
C) Shodan.
D) Google.

11. (Puntuación: 0,25). ¿Cuál de las siguientes herramientas se utiliza para la enumeración de SMB?
A) Nmap.
B) Hydra.
C) Metasploit.
D) Dirbuster.

12. (Puntuación: 0,25). ¿Qué técnica se utiliza para comprobar si un determinado puerto UDP se encue
abierto en el sistema remoto?
A) Stealth scan (Half open scan).
B) FIN Scan (Inverse TCP flag scan).
C) XMAS scan (All TCP flag scan).
D) UDP scan.

GOBIERNO DE ESPAÑA | MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES

cidead

PRIMER APELLIDO	SEGUNDO APELLIDO	NOMBRE DEL ALUMNO/A	DÍA NACIMIENTO	MES NACIMIENTO
V	H	S	22	05

13. (Puntuación: 0,25). ¿Cuál es la técnica de escaneo de puertos por defecto en nmap que intenta realizar una conexión completa mediante el establecimiento del "three way handshake"?
A) Stealth scan (Half open scan).
B) NULL scan (null TCP flag scan).
C) UDP scan.
D) TCP Connect (Full open scan).

14. (Puntuación: 0,25). ¿Qué herramienta se utiliza para localizar vulnerabilidades de versión y defectos en la configuración de portales basados en el framework Joomla?
A) Testssl.
B) CMSMap.
C) JoomScan.
D) OWASP.

15. (Puntuación: 0,25). ¿Cómo se pueden utilizar scripts en nmap?
A) Con el operador -sS.
B) Con el operador -A.
C) Con el operador --script.
D) Con el operador -v.

16. (Puntuación: 0,25). ¿Qué es el Modelo-Vista-Controlador (MVC)?
A) Una capa que se encarga de recoger y gestionar los datos de los usuarios.
B) Una estructura que divide un aplicativo web en tres capas: Controlador, Modelo y Vista.
C) Un lenguaje de programación para aplicativos web.
D) Un protocolo de comunicación para intercambiar información en la web.

17. (Puntuación: 0,25). ¿Qué método de HTTP se utiliza para hacer una actualización de información en el servidor?
A) GET.
B) HOST.
C) PUT.
D) DELETE.

18. (Puntuación: 0,25). ¿Qué parte de la dirección URL indica la ruta dentro del dominio al que se quiere acceder?
A) Protocolo.
B) Dominio.
C) Path.
D) Parámetros.

GOBIERNO DE ESPAÑA

MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES

cideo
Centro para la Innovación y D... de la Educación a Distan...

PRIMER APELLIDO	SEGUNDO APELLIDO	NOMBRE DEL ALUMNO/A	DÍA NACIMIENTO	MES NACIMIE...
V	M	S	22	07

19. (Puntuación: 0,25). ¿Qué es la autenticación basada en credenciales?
A) Es el proceso de identificar a un usuario en una aplicación web mediante su dirección IP.
B) Es el proceso de identificar a un usuario en una aplicación web mediante cookies.
C) Es el proceso de identificar a un usuario en una aplicación web mediante su nombre de usuario y contraseña.
D) Es el proceso de identificar a un usuario en una aplicación web mediante su dirección de correo electrónico.

20. ¿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 ac... 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.

GOBIERNO DE ESPAÑA | MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES

cidead
Centro para la Innovación y Desarrollo de la Educación a Distancia

PRIMER APELLIDO	SEGUNDO APELLIDO	NOMBRE DEL ALUMNO/A	DÍA NACIMIENTO	MES NACIMIENTO
V	H	S	22	07

PREGUNTAS TEÓRICO-PRÁCTICAS:

PTP1. (2 puntos). Plan de auditorías.

La empresa "SISE Transporte" (Servicios Informáticos de Seguridad del Estado), dedicada a ofrecer servicios informáticos seguros en el sector de los medios de transporte nacionales ha establecido un nuevo centro de control de respaldo de su servicio de control de rutas ferroviarias. Para garantizar la seguridad de este servicio, se han solicitado dos auditorías que permitan identificar posibles riesgos y vulnerabilidades focalizados en el nuevo centro de control.

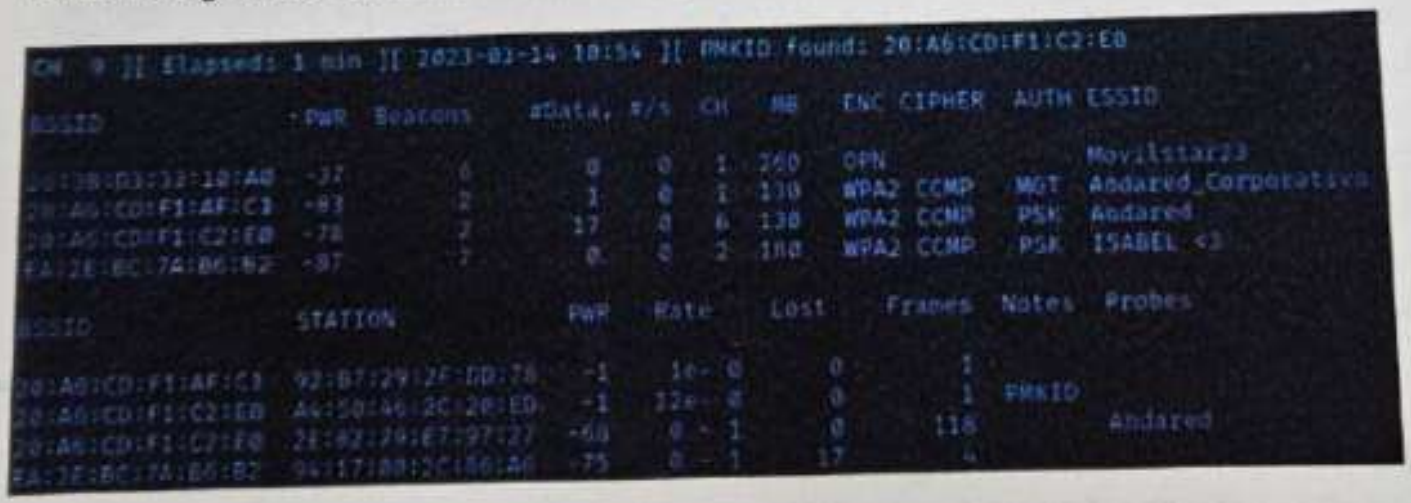
Se solicita:

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

a) Justificación de elección. (0,5)
b) Activos incluidos en la auditoría. (0,5)
c) Definición del origen, enfoque y el tipo de información proporcionada. (0,5)
d) Objetivo perseguido con la auditoría. (0,5)

PTP2. (2 puntos). Monitorización y análisis de datos.

Dada la siguiente captura de "airodump-ng":



Responde a las siguientes cuestiones:

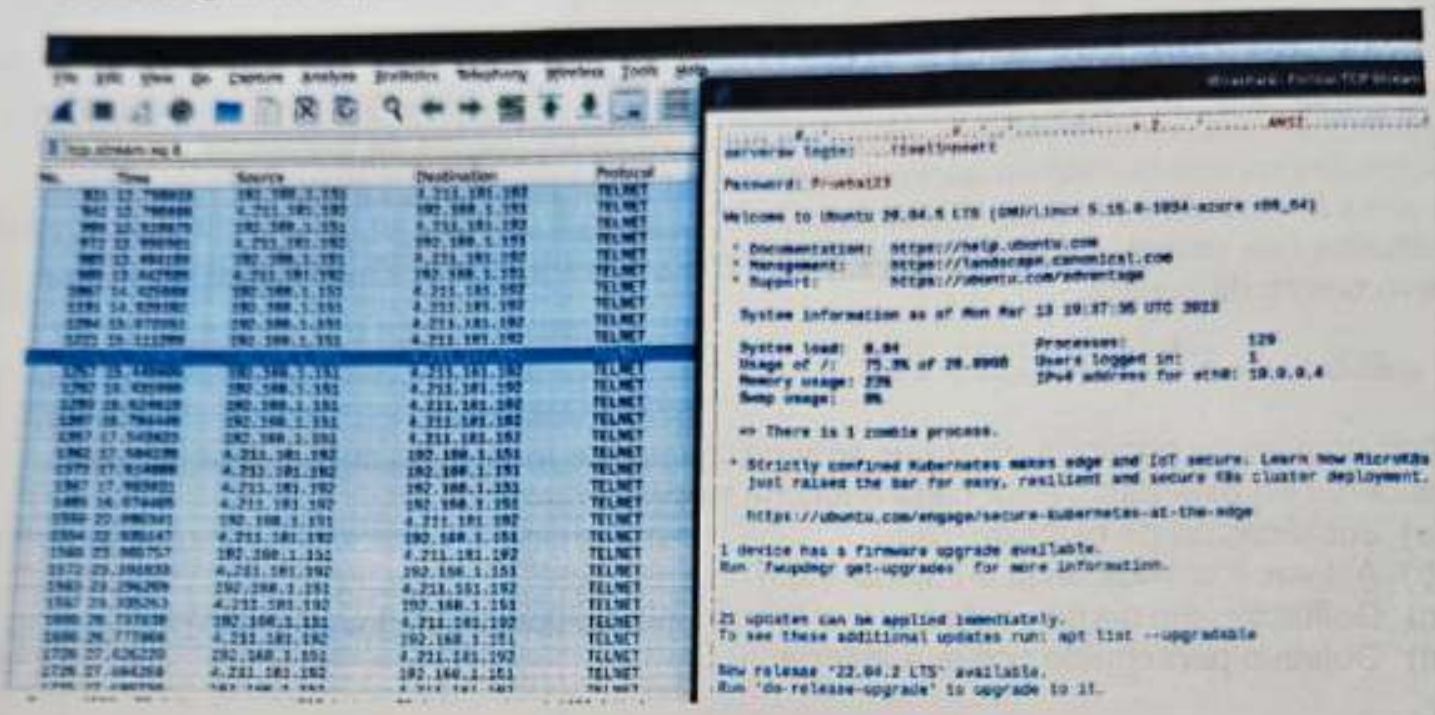
a) Indica el ESSID del Punto de Acceso con dirección MAC: 20:A6:CD:F1:C2:E0.(
b) Indica en qué bandas de frecuencia y en que canales opera la red MovilStar23. (
c) Indica un dispositivo que esté conectado a la red ISABEL <3. (0,25)
d) Indica el tipo de protocolo de seguridad inalámbrica (tipo de proceso de autentica de la red Andared_Corporativo. (0,25)

GOBIERNO DE ESPAÑA	MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES

cidead
Centro para la Innovación y Desarrollo de la Educación a Distancia

PRIMER APELLIDO	SEGUNDO APELLIDO	NOMBRE DEL ALUMNO/A	DÍA NACIMIENTO	MES NACIMIENTO
V	H	S	22	05

Dada la siguiente captura de Wireshark:



Responde a las siguientes preguntas:

1. ¿Sobre qué red de la lista de la primera captura de pantalla se ha podido realizar captura de red para obtener esta información en claro? Justifica la respuesta. (0,2
2. ¿Qué filtro de airodump se ha podido establecer para solamente recoger los datos de esta captura en un fichero llamado "capturaOpen-01.pcap"? (0,25)
3. ¿Qué información de autenticación se ha podido conseguir en claro y de qué protocolo? (0,25)
4. ¿Se podría haber obtenido la información de la navegación HTTPS? Justifica la respuesta. (0,25)

PTP3. (2 puntos). Realiza las siguientes cuatro búsquedas utilizando técnicas de Google Dorking: (1 punto)

a) Busque archivos PDF que contengan la palabra "manual" en el dominio example.com.
b) Busque URLs que contengan la ruta "/admin/" pero que excluyan aquellas que incluyan "/secure/".
c) Busque páginas cuyo título incluya la frase "index of" y la palabra "backup".
d) Busque páginas que en su contenido incluyan las palabras "confidencial" e "informe", excluyendo aquellas provenientes del dominio "cidead.es".