Examen para HE02.

Intento 1.

Pregunta 1

Las redes de tipo OPEN Permiten acceder a la red Wi-Fi sin contraseña, pero ofrecen un cifrado de canal en capa 2 del modelo OSI ¿Verdadero o Falso?:

Seleccione una:

Verdadero
Falso

Pregunta 2

La CA que genera los certificados del Punto de Acceso legítimo se puede desplegar en el cliente mediante el uso de MDM (Mobile Device Management) en sistemas Linux, macOS, Android e iOS. ¿Verdadero o Falso?:

Seleccione una:

Verdadero
Falso

Pregunta 3

Indica cuáles de las siguientes afirmaciones son correctas en el caso de las redes de tipo WEP (Respuesta múltiple):

a. Las redes de tipo WEP NO son vulnerables ante ataques estadísticos para averiguar la clave de acceso.
b. La longitud mínima de la clave de acceso es de 8 caracteres.
c. Las redes de tipo WEP son vulnerables ante ataques estadísticos para averiguar la clave de acceso.
d. La longitud de la clave de acceso es de entre 5 y 13 caracteres.

Pregunta 4

¿Cuáles de las siguientes características de una red inalámbrica se pueden averiguar monitorizando las redes Wi-FI? (Respuesta múltiple):

a. Tipo de red Wi-Fi.
b. Dirección MAC de los Puntos de Acceso.
c. Nombres de las redes Wi-Fi.
d. Canales en los que opera el Punto de Acceso.

Pregunta 5

No existe ningún vector de ataque en las redes de tipo WPA/WPA2-Enterprise. ¿Verdadero o Falso?:

Seleccione una:

Verdadero
Falso

Pregunta 6

Las antenas Omnidireccionales suelen tener menor alcance de señal que las antenas direccionales ¿Verdadero o Falso?:

Seleccione una:

Verdadero
Falso

Pregunta 7

Un Beacon Frame es un paquete de información que envía el Punto de Acceso Wi-FI con información de las características de la red que publica ¿Verdadero o Falso?:

Seleccione una:

Verdadero
Falso

Pregunta 8

La banda de tipo "a" (Banda de 5GHz) utiliza los canales 1-14, ¿Verdadero o Falso?:

Seleccione una:

Verdadero
Falso

Pregunta 9

Las redes de tipo WPA/WPA2-PSK permiten la trazabilidad de los usuarios a nivel de red. ¿Verdadero o Falso?:

Seleccione una:

Verdadero
Falso

Pregunta 10

Indica en cuál de los siguientes supuestos es más común encontrarte con redes de tipo WEP:

a. Para acceder a una red que se considera crítica debido a los datos con los que opera.
b. Para acceder a la red corporativa de la empresa.
c. Redes de Invitados.
d. Sistemas SCADA o equipamiento en fábricas.

Intento 2.

Pregunta 1

¿Cuál de las siguientes herramientas se utiliza para suplantar un portal cautivo?:

a. hostapd-wpe.
b. airodump-ng.
c. Wifiphisher.
d. aireplay-ng.

Pregunta 2

Indica cuáles de las siguientes maneras se pueden utilizar para poner una tarjeta Wi-Fi en modo monitor (Respuesta múltiple):

a. En versiones actuales de la herramienta airodump-ng la tarjeta se pone en modo monitor de manera automática sin necesidad de modificar el modo de operación de la tarjeta previamente.
b. Es el modo de operación por defecto de las tarjetas Wi-Fi, no es necesario realizar ninguna acción adicional.
c. Haciendo uso de la herramienta airmon-ng.
d. Haciendo uso del comando iwconfig.

Pregunta 3

Indica cual es el método utilizado para intentar obtener la clave de acceso de una red WPA/WPA2-PSK en la que no hay conectado ningún cliente:

a. Capturar numerosos vectores de inicialización de la red.
b. Establecer un punto de acceso falso con hostapd-wpe.
c. Capturar el PMKID y realizar un proceso de cracking offline.
d. Capturar el 4-way-handshake y realizar un proceso de cracking offline.

Pregunta 4

Indica cuál de las siguientes afirmaciones es correcta con respecto al ataque en redes tipo WPA/WPA2-Enterprise:

a. El ataque se puede llevar a cabo, aunque los usuarios se autentiquen en la red haciendo uso de un certificado de cliente.
b. El ataque consiste en monitorizar un Punto de Acceso legítimo de la red y esperar los intentos de autenticación de los usuarios legítimos. Estos intentos de autenticación se pueden utilizar para obtener las credenciales de los usuarios mediante un proceso de cracking.
c. El ataque consiste en establecer un Punto de Acceso falso y esperar los intentos de autenticación de los usuarios legítimos. Estos intentos de autenticación se pueden utilizar para obtener las credenciales de los usuarios mediante un proceso de cracking.
d. El ataque se puede llevar a cabo, aunque los usuarios validen los certificados de los Puntos de Acceso.

Pregunta 5

El modo Master de una tarjeta de red sirve para conectarte a una red Wi-Fi como si fueras un dispositivo cliente. ¿Verdadero o Falso?:

Seleccione una:

Verdadero
Falso

Pregunta 6

¿Con qué herramienta podemos realizar una inyección de tramas en la red inalámbrica?:
a. airmon-ng.
b. aircrack-ng.
c. aireplay-ng.
d. airodump-ng.

Pregunta 7

Indica cuál de las siguientes afirmaciones de las redes de tipo OPEN son ciertas (Respuesta múltiple):

a. Cualquier persona puede acceder a la red sin necesidad de conocer la contraseña.
b. Aunque no disponen de contraseña de acceso cifran el canal de comunicaciones.
c. Los clientes suelen tener visibilidad entre ellos pudiendo sufrir ataques de otro equipo de la red.
d. Cualquier usuario que monitorice la red puede acceder a la información transmitida que se haya transmitido a través de HTTP, FTP o telnet entre otros.

Pregunta 8

¿Cuál de los siguientes modos de operación de una tarjeta de red NO se utiliza en las redes de tipo infraestructura?:

a. Master.
b. Adhoc.
c. Monitor.
d. Managed.

Pregunta 9

Indica cual es el método utilizado para intentar obtener la clave de acceso de una red WPA/WPA2-PSK en la que hay conectados clientes legítimos de la red:

a. Capturar el PMKID y realizar un proceso de cracking offline.
b. Capturar el 4-way-handshake y realizar un proceso de cracking offline.
c. Establecer un punto de acceso falso con hostapd-wpe.
d. Capturar numerosos vectores de inicialización de la red.

Pregunta 10

Las redes de tipo WEP se encuentran en desuso. ¿Verdadero o Falso?:

Seleccione una:

Verdadero
Falso

Intento 3.

Pregunta 1

Para ampliar el radio de cobertura de un Punto de Acceso falso se pueden utilizar antenas omnidireccionales externas de mayor potencia:

Seleccione una:

Verdadero
Falso

Pregunta 2

La banda inalámbrica de los 5GHz (Respuesta múltiple):

a. Tiene mayor velocidad de conexión que la banda de 2,4GHZ.
b. Dispone de más canales de frecuencia que la banda de los 2,4GHz.
c. Sufre menos interferencias que la banda de 2,4GHZ.
d. Tiene mayor rango de cobertura que la banda de los 2,4GHz.

Pregunta 3

¿Qué es un paquete de tipo Probe Request?:

a. Un paquete, enviado por un Punto de Acceso, que tiene información de las características de la red inalámbrica.
b. Un paquete, enviado por un Punto de Acceso, para averiguar si existe en su alcance alguna otra red inalámbrica que pueda causar interferencias en la banda en la que opera.
c. Un paquete, enviado por un dispositivo cliente, para averiguar si existe en su alcance alguna otra red inalámbrica de la cuál conoce la clave de acceso.
d. Un paquete, enviado por un dispositivo cliente, que tiene información de las características de la red inalámbrica.

Pregunta 4

En una misma red inalámbrica no puede haber más de un punto de acceso ¿Verdadero o Falso?:

Seleccione una:

Verdadero
Falso

Pregunta 5

La CA que genera los certificados del Punto de Acceso legítimo se puede desplegar en el cliente mediante el uso de GPO (Group Policy Object) en sistemas Microsoft. ¿Verdadero o Falso?:

Seleccione una:

Verdadero
Falso

Pregunta 6

La banda inalámbrica de 2,4GHz soporta mayor velocidad de conexión que la banda de 5GHz ¿Verdadero o Falso?:

Seleccione una:

Verdadero
Falso

Pregunta 7

¿A qué nos referimos cuando hablamos del Basic Set Identifier (BSSID) de una red Wi-Fi?:

a. Al nombre de la red Wi-Fi.
b. Al procedimiento de autenticación en la red Wi-Fi.
c. A la dirección MAC de uno de los Puntos de Acceso de la red Wi-FI.
d. A la dirección MAC de uno de los clientes de la red Wi-FI.