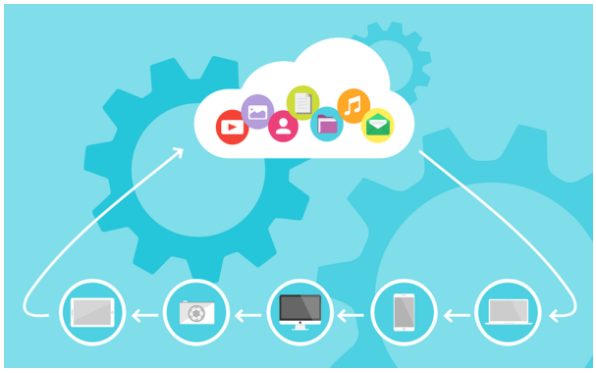
ATAQUES A REDES INALÁMBRICAS MÉTODOS PENETRACIÓN WIFI



SKU: 4247EC

Horas: 50

OBJETIVOS

- Comprender los conceptos básicos en **seguridad informática** como: **WEB**, **WPA**, **SSID** o **LAN**.
- Abordar el proceso de **conexión inalámbrica** y el procedimiento general de seguridad **Wi-fi**.
- Obtener una **visión global de la gestión de la seguridad.**
- Conocer el **Footprinting inalámbrica:** equipamiento, software y mapeo inalámbrico.
- Conocer las diferentes **amenazas** y **vulnerabilidades** a **redes**: pérdida de confidencialidad, de disponibilidad, ataques a usuarios, etc.
- Analizar los **ataques a redes WI – FI**: WEP Y WAP Y WAP2.

DIRIGIDO A

COMPETENCIAS

CONTENIDO

Tema 1. **Introducción y conceptos previos a los métodos de penetración WIFI.**

1. LAN inalámbricas.
2. Evolución de las LAN inalámbricas: una visión general.
3. Una LAN básica wireless.
4. Arquitectura básica de una LAN wireless.
5. Configuraciones LAN inalámbricas.

6. Sistemas de distribución de servicios (DSSS).
7. Estándares de lan inalámbrica existentes.
8. ¿Las LAN inalámbricas tienen riesgos para la salud?
9. Riesgos de seguridad.
10. Historia del IEEE.
11. Estándares inalámbricos IEEE 802.
12. La familia de estándares 802.11.
13. Los detalles del estándard 802.11.
14. Seguridad 802.11.
15. Modos operativos.
16. Las extensiones 802.11.
17. Desventajas de 802.11.
18. Comparación de estándares inalámbricos.

Tema 2. **Parámetros de estudio estructural y topología de Redes Inalámbricas.**

1. Conexiones inalámbricas.
2. Seguridad de los puntos de acceso inalámbricos.
3. SSID.
4. Realización de una encuesta de sitio.
5. Uso de los protocolos de cifrado seguro.
6. La antena.
7. Potencia y portales.
8. Seguridad de la red.
9. Comunicaciones inalámbricas y seguridad.
10. Protocolos de autenticación.
11. Comprender las necesidades de LAN inalámbrica.
12. Realización de la encuesta sobre el sitio.
13. Configuración de requisitos y expectativas.
14. Estimación del hardware y del hardware de la LAN inalámbrica requerida software.

Tema 3. **Equipos inalámbricos WIFI utilizar y realización de rastreos sobre posibles victimas.**

1. Footprinting inalámbrica.
2. Escaneado y enumeración inalámbricos.
3. Identificando defensas de redes inalámbricas y contaminantes.

Tema 4. **Fase de ataque a una red inalámbrica.**

1. Introducción analítica y optimización de resultados.
2. Diferentes amenazas y vulnerabilidades a redes.
3. Ataques sobre redes WI-FI: WEP Y WAP Y WAP2.
4. Ataques y problemas de servicio en la red.
5. Ataques de intrusión: problemas de servicio en la nube.
6. Falsificación de identidades.
7. Software intrusión.
8. Políticas de seguridad.