UNIVERSIDAD INTERNACIONAL DE LA RIOJA

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OSSTMM
www.osstmm.org
Open Source Security Testing Methodology Manual

Seguridad en la Red Informática Mundial

Metodología OSSTMM
Open Source Security Testing Methodology Manual

Semana 7 clases 13 y 14

Mtra. María Noemí Araiza Ramírez

Metodología OSSTMM

Seguridad Inalámbrica

Metodología OSSTMM

Seguridad Inalámbrica

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Radiación Electromagnética (EMR)

Este es un método para verificar la Seguridad de las Emisiones (Emsec) perteneciente a la verificación remota de radiaciones electromagnéticas emitidas por dispositivos de las Tecnologías de la Información.

Se puede capturar la radiación electromagnética de los dispositivos tales como CRTs, LCDs, impresoras, módems, teléfonos móviles, entre otros y utilizarse para reconstruir los datos mostrados en la pantalla, impresos, transmitidos.

Encontrar la fuente correcta de una EMR puede requerir una persona cualificada sentada durante horas. Por esta razón este tipo de verificación se reserva a instalaciones de alta seguridad donde la protección de la propiedad intelectual es absolutamente vital.

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Radiación Electromagnética (EMR)

Protegerse ante este tipo de intrusiones se realiza habitualmente colocando todas las máquinas y periféricos dentro de algún tipo de sala blindada "Tempest" y utilizando únicamente fibra o conexiones filtradas o alámbricas hacia y entre todos los dispositivos internos y desde el exterior, este tipo de protección es muy cara.

Evaluar las Necesidades de Negocio, Prácticas, Políticas y Ubicaciones de las Áreas Sensibles

1. Verificar que la organización disponga de una política de seguridad en uso que trate las EMR.

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Radiación Electromagnética (EMR)

Evaluar el Equipamiento y Ubicación

2. Verificar que todos los dispositivos de las Tecnologías de la Información que deben ser protegidos están ubicados apropiadamente en una habituación blindada de metal.

Evaluar y Verificar el Cableado y Emisiones

3. Verificar que todo el cableado de entradas o salida la sala blindada, donde de ser posible, sean de fibra

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Redes Inalámbricas [802.11]

Este es un método para la verificación del acceso a redes WLAN 802.11, las cuales se están popularizando cada vez más.

Sin embargo existen algunos problemas bastante comunes y alarmantes en la implantación de estas tecnologías.

Se debe principalmente a que estas redes se crean rápida y fácilmente pero las medidas de seguridad no forman parte de la configuración por defecto.

Existen algunas medidas básicas para mejorar la seguridad y algunas más drásticas a aplicar para conseguir unas WLANs bastante seguras.

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Redes Inalámbricas [802.11]

Especificaciones 802.11:

Capa Física	Secuencia Directa en Espectro Ensanchado (DSSS), Saltos de Frecuencia en Espectro Ensanchado (FHSS), infrarrojos (IR)
Cifrado por defecto	Algoritmo de cifrado basado en flujo RC4 para confidencialidad, autenticación, y integridad. Gestión de Claves limitada.
Rango de Operación	Unos 150 pies en interiores y 1500 en exterior.

Implementaciones:

802.11a

- Opera en el rango de frecuencias de 5Ghz
- Incompatibilidad con equipamiento 802.11b o 802.11g
- Máxima velocidad de 54MBps

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Redes Inalámbricas [802.11]

802.11b

- Opera en el rango de frecuencias de 2.4Ghz
- Es la tecnología más extendida actualmente
- Máxima velocidad de 11Mbps

802.11g

- Opera en el rango de frecuencias de 2.4Ghz
- Máxima velocidad estándar de 54MBps
- Se espera compatibilidad con equipamiento 802.11b existente

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Redes Inalámbricas [802.11]

Evaluar las Necesidades de Negocio, Prácticas y Políticas:

- Verificar que la organización disponga de una adecuada política de seguridad en uso que trate la utilización de tecnologías inalámbricas, incluyendo el uso de 802.11

Evaluar Equipamiento, Firmware y Actualizaciones.

- Realizar un inventario completo de todos los dispositivos inalámbricos de la red.

Evaluar el Control de Acceso, Seguridad Perimetral y Habilidad para Interceptar o Interferir las Comunicaciones:

- Determinar el nivel de control de acceso físico a los puntos de acceso y dispositivos que los controlan (cerrojos, lectores de tarjetas, cámaras…).

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Redes Inalámbricas [802.11]

Evaluar el Acceso Administrativo a los Dispositivos Inalámbricos:

- Determinar si los puntos de acceso son apagados durante los momentos del día en los que no son utilizados.

Evaluar la Configuración, Autenticación y Cifrado de las Redes Inalámbricas:

- Verificar el cambio de los 'Service Set Identifier' (SSID) por defecto de los puntos de acceso.

Evaluar los Clientes Inalámbricos:

- Verificar que todos los clientes inalámbricos poseen un antivirus instalado.

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Redes Bluetooth

Este es un método para la verificación de redes Bluetooth de tipo ad-hoc (piconets), las cuales son populares en las redes inalámbricas de área personal (PANs) pequeñas y de poco ancho de banda.

De igual modo que con otras estrategias inalámbricas, existen vulnerabilidades inherentes que plantean problemas de seguridad significativos.

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Redes Bluetooth

Especificaciones Bluetooth:

Capa Física	Frequency Hopping Spread Spectrum (FHSS)
Banda de Frecuencia	2.4 – 2.45 GHz (ISM band)
Salto de Frecuencia	1,600 hops per second
Tasa Bruta de Transmisión	1Mbps
Ancho de Banda	Hasta 720 Kbps
Seguridad de Datos y Red	• Tres modalidades de seguridad (ninguna, a nivel de enlace y a nivel de servicio) • Dos niveles de confianza de dispositivo y 3 niveles de seguridad del servicio. • Algoritmo de cifrado de flujo para confidencialidad y autenticación. • Claves derivadas del PIN y gestión de claves limitada
Rango de Operación	Sobre 10 metros (30 pies); puede ser ampliado a 100 metros (328 pies).

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Redes Bluetooth

Evaluar las Necesidades de Negocio, Prácticas y Políticas:

- Verificar que existen políticas de seguridad organizativas que traten el uso de la tecnología inalámbrica, incluyendo la tecnología Bluetooth.

Evaluar Equipamiento, Firmware y Actualizaciones.

- Realizar un inventario completo de todos los dispositivos inalámbricos de tipo Bluetooth.

Pruebas de Vulnerabilidades Comunes (especialmente en el Red-M 105AP):

- Realizar ataques de fuerza bruta contra puntos de acceso Bluetooth para comprobar la fortaleza de la contraseña. Verificar que las contraseñas contengan números y caracteres especiales.

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Redes Bluetooth

Los Puntos de Acceso Bluetooth utilizan contraseñas sin diferenciación de mayúsculas lo que facilita a los atacantes la realización de ataques de fuerza bruta al haber un espacio más pequeño de posibles contraseñas por adivinar.

Evaluar el Control de Acceso, la Seguridad Perimetral y la Habilidad para Interceptar o Interferir las Comunicaciones:

- Verificar el perímetro actual de la red Bluetooth.

Evaluar la Configuración de Dispositivo (Autenticación, Contraseñas, Cifrado...):

- Verificar que los dispositivos Bluetooth son configurados con los niveles más bajos de potencia para operar suficientemente y mantener las transmisiones dentro de los límites seguros de la organización.

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Dispositivos de Entrada Inalámbricos

Esta sección trata de los dispositivos de entrada inalámbricos tales como ratones y teclados.

Estos dispositivos se están popularizando aunque presentan profundas vulnerabilidades y compromisos en privacidad y seguridad

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Dispositivos de Entrada Inalámbricos

Evaluar las Necesidades de Negocio, Prácticas y Políticas:

- Analizar la política de seguridad organizativa que trata el uso de tecnologías inalámbricas tales como la de los dispositivos de entrada inalámbricos.

Evaluar Equipamiento, Firmware y Actualizaciones:

- Realizar un inventario completo de todos los dispositivos de entrada inalámbricos en la red.

Evaluar el Control de Acceso, Seguridad Perimetral y Habilidad para Interceptar o Interferir las Comunicaciones:

- Realizar una inspección del lugar para medir y establecer el alcance de los dispositivos de entrada inalámbricos para la organización.

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Dispositivos de Mano Inalámbricos

Debido a la increíble variedad y ubicuidad de los dispositivos de mano inalámbricos es prácticamente imposible tratar cada tipo.

Los siguientes pasos proporcionan un método de verificación de seguridad en todos los dispositivos.

El aspecto más significativo para verificar estos dispositivos no reside en su configuración sino en la educación del usuario.

La mayoría de estos pasos comprueba los conocimientos del usuario respecto al uso más seguro del dispositivo.

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Dispositivos de Mano Inalámbricos

Evaluar las Necesidades de Negocio, Prácticas y Políticas:

- Verificar que existe una política de seguridad organizativa que trata el uso de los dispositivos de mano.

Evaluar Equipamiento, Firmware y Actualizaciones:

- Realizar un inventario completo de todos los dispositivos inalámbricos de la red.

Evaluar el Control de Acceso, Seguridad Perimetral y Habilidad para Interceptar o Interferir las Comunicaciones:

- Verificar que existe una protección de los limites externos alrededor del perímetro de los edificios o de las redes inalámbricas.

Evaluar la Configuración del Dispositivo (Autenticación, Contraseñas, Cifrado…):

- Verificar que los dispositivos utilizan cifrado fuerte para proteger los ficheros sensibles y las aplicaciones.

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Comunicaciones sin Cable

Este es un método para la verificación de dispositivos de comunicación sin cables que puedan sobrepasar los límites físicos y monitorizados de una organización. Esto incluye la verificación de interferencia entre tipos diferentes o similares de comunicación dentro de una organización y sus organizaciones vecinas.

Evaluar las Necesidades de Negocio, Prácticas y Políticas

- Verificar que la organización disponga de una política de seguridad que trate el uso de tecnologías de comunicación sin cables.

Evaluar Equipamiento, Firmware y Configuración:

- Realizar un inventario de todos los dispositivos de comunicación sin cables.

Evaluar el Control de Acceso, Seguridad Perimetral y Habilidad para Interceptar o Interferir las Comunicaciones:

- Verificar la distancia en la que las comunicaciones sin cables sobrepasa el límite físico de la organización.

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Dispositivos de Vigilancia Inalámbricos

Los dispositivos de vigilancia inalámbricos han empezado recientemente a reemplazar los alámbricos – tales como cámaras, micrófonos, etc.

Estos dispositivos permiten a las compañías instalar equipamiento de monitorización en áreas en las que no era anteriormente factible y a un bajo coste.

Estos equipos de monitoreo están a menudo completamente escondidos ya sea por su pequeño tamaño o bien siendo camuflados por otros objetos tales como alarmas de incendio, cuadros o relojes.

Debido a que gran parte de estos equipos son inalámbricos son más susceptibles a interferencia triviales, intencionadas, monitorización y reproducción que las equivalentes alámbricas.

El verificador de la seguridad debe ser también la última línea de defensa para asegurar que el equipamiento esta instalado y funcionando apropiadamente.

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Dispositivos de Vigilancia Inalámbricos

Evaluación de Necesidades de Negocio, Prácticas y Políticas:

- Verificar que existe una política de compañía que trate efectivamente el equipamiento de vigilancia inalámbrico.

Evaluación de Dispositivos y Ubicación:

- Verificar que los equipos de vigilancia están realmente camuflados o no visibles, si es una de las cosas que pretende el equipamiento.

Evaluación del Control de Acceso, Seguridad Perimetral y Habilidad de Interceptar y Interferir las Comunicaciones:

- Verificar el perímetro actual de la transmisión del dispositivo de vigilancia inalámbrico.

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Dispositivos de Transacción Inalámbricos

Instalados en numerosas tiendas. Este equipamiento se esta utilizando para proporcionar conexión con cajas registradoras y otros dispositivos de punto de venta a lo largo de los comercios.

Esta tecnología ha demostrado un tremendo beneficio de negocio para las compañías aunque algunas veces se instalan sin tener en cuenta la seguridad y protección de la información confidencial.

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Dispositivos de Transacción Inalámbricos

Evaluar las Necesidades de Negocio, Prácticas y Políticas:

- Verificar que existe una política corporativa que trate efectivamente el equipamiento de transacción inalámbrico.

Evaluar Equipamiento, Firmware y Actualizaciones:

- Realizar un inventario completo de todos los dispositivos de transacción inalámbricos.

Evaluar la Configuración de Dispositivo:

- Verificar que los datos enviados sean cifrados y el nivel utilizado.

Evaluar el Control de Acceso, Seguridad Perimetral y Habilidad para Interceptar o Interferir con las Comunicaciones:

- Determinar la habilidad de un tercero no intencionado de interceptar los datos transmitidos.

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de RFID

Las etiquetas de RFID (Radio Frequency Identifier) se componen de un circuito integrado (IC), a menudo del tamaño de medio grano de arena, y una antena – habitualmente una espiral de cables. La información está almacenada en el IC y se transmite mediante la antena. Las etiquetas RFID pueden ser pasivas (sin batería utilizando la transmisión de energía del lector de etiquetas RF) o activa (autoalimentadas por batería).

Las etiquetas RFID no requieren línea directa de visión para ser leídas y pueden trabajar bajo diversas condiciones ambientales – algunas son resistentes al agua y lavables. Cada etiqueta contiene un identificador único de 64 bits y una cantidad variable de memoria – gran parte de ellas 1024 bits. Por esta razón pueden proporcionar un alto nivel de funcionalidad e integridad de datos.

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de RFID

Algunas de ellas proporcionan medidas de seguridad. Gran parte de las que utilizan cifrado tienen una clave secreta escondida de 40 bits. Algunos transponedores integran firma digital y protocolo de cifrado que incluye una autenticación de desafío/respuesta. Dependiendo del diseño de la etiqueta RFID y del transpondedor, la autenticación puede ser de una o dos caras.

Sin embargo también se necesita asegurar que las etiquetas RFID no pueden ser desactivadas por aquellos que intentan robar los artículos. Por esta razón la desactivación de la etiqueta de RFID sólo debería poder ser realizada en la caja registradora y cualquier otro lugar especifico requerido por el negocio.

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de RFID

Evaluación de Necesidades de Negocio, Prácticas y Políticas:

- Verificar que la organización tiene una política de seguridad que trata adecuadamente el uso de RFIDs inalámbricas.

Evaluar los Atributos RFID (Autenticación, Cifrado, Propiedades…):

- Verificar que el número de serie en la etiqueta ID no puede ser cambiado.

Evaluar la Ubicación, Scanners y Equipamiento de Seguimiento:

- Para un seguimiento completo de los productos etiquetados en un almacén o en un medio de almacenamiento, hay que asegurar la ubicación de lectores de etiquetas en todas las entradas y salidas, no solo en las zonas de llegada y salida de cargas. Esto ayudará a reducir el robo causado por empleados.

Evaluar el Control de Accesos, Seguridad Perimetral y Habilidad para Interceptar o Interferir las Comunicaciones:

- Verificar que las etiquetas RFID y los transmisiones con los lectores no interfieren las redes inalámbricas y los equipos de comunicaciones.

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Sistemas Infrarrojos

Este es el método de verificación de dispositivos de comunicaciones infrarrojas que pudieran sobrepasar los limites físicos y monitoreados de la organización.
Las comunicaciones infrarrojas son mucho menos accesibles desde el exterior de la organización en comparación con 802.11 y Bluetooth. Sin embargo la seguridad en los dispositivos infrarrojos suele descuidarse debido a su relativa inaccesibilidad.

Evaluar las Necesidades de Negocio, Prácticas, Políticas y Ubicaciones de las Áreas Sensibles:

- Verificar que la organización dispone de una política de seguridad que trata el uso de las tecnologías inalámbricas tales como dispositivos infrarrojos.

Evaluar Equipamiento, Firmware y Actualizaciones:

- Realizar una auditoria completa de todos los dispositivos con capacidad infrarroja.

Metodología OSSTMM

Seguridad Inalámbrica

Verificación de Sistemas Infrarrojos

Evaluar el Control de Acceso, Seguridad Perimetral y Habilidad para Interceptar o Interferir con las Comunicaciones:

- Verificar la distancia sobrepasada en las comunicaciones infrarrojas más allá de los límites físicos de la organización.

Evaluar la Configuración de Dispositivo (Autenticación, Contraseñas, Cifrado..):

- Verificar el método de autenticación de los clientes.

Metodología OSSTMM

Seguridad Inalámbrica

Revisión de Privacidad

La privacidad de los dispositivos de comunicación inalámbricos pueden sobrepasar los limites físicos y monitoreados de una organización. La revisión de la privacidad es el punto central, desde un punto de vista legal y ético, del almacenamiento, transmisión y control de los datos en base a la privacidad de empleados y clientes.

El uso de estos datos es una inquietud para bastantes particulares y la legislación está mostrando reglas especificas respecto a la privacidad.

Aunque algunas de estas leyes son locales, todas aplican a la Internet y por tanto afectan internacionalmente a todos los auditores de seguridad.

Metodología OSSTMM

Seguridad Inalámbrica

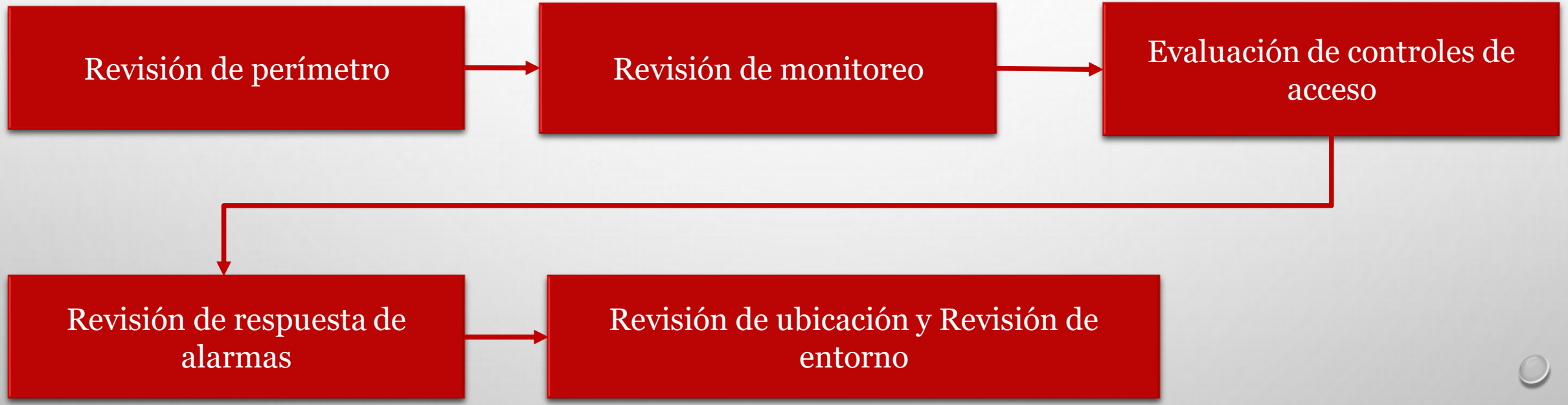
Revisión de Privacidad

Resultados Esperados:	Enumerar cualquier revelación Enumerar las anomalías en el cumplimiento entre la política pública y la práctica actual Enumerar las comunicaciones inalámbricas involucradas en la obtención de datos Enumerar las técnicas de obtención de datos Enumerar los datos obtenidos

Verificar el método de autenticación de los clientes
2. Verificar si están en uso de forma apropiada contraseñas robustas
3. Verificar que existe una política de expiración de contraseñas
4. Verificar si el cifrado está en uso y correctamente configurado
5. Verificar que los clientes no pueden ser forzados a volver al modo sin cifrado
6. Comparar la política públicamente accesible a la práctica actual
7. Compara la práctica actual a las leyes u obediencias regionales de fraude y privacidad
8. Identificar el tipo y tamaño de la base de datos para almacenar información
9. Identificar la información recogida por la organización
10. Identificar la ubicación de la información almacenada
11. Identificar los momentos de expiración de la información

OSSTMM

Seguridad Física



Metodología OSSTMM

Seguridad Física

Revisión de Perímetro

Este es un método para evaluar la seguridad física de una organización y sus bienes, verificando las medidas de seguridad de su perímetro físico.

Resultados Esperados:	Mapa del perímetro físico Tipos de medidas de protección física Lista de áreas desprotegidas o insuficientemente protegidas

1. Trazar mapa del perímetro físico
2. Trazar mapa de las medidas de protección físicas (cercas, puertas, luces, etc.)
3. Trazar mapa de las rutas de acceso y/o métodos físicos
4. Trazar mapa de las áreas no monitoreadas

Metodología OSSTMM

Seguridad Física

Revisión de monitoreo

Este es un método para descubrir puntos de acceso monitoreados, a una organización y sus bienes, por medio del descubrimiento de custodia y monitoreo electrónico.

Resultados Esperados:	Lista de puntos de acceso monitoreados Tipos de monitoreo Lista de puntos de acceso estándar y privilegiados, no monitoreados Lista de disparadores de alarmas

1 Enumerar los dispositivos de monitoreo
2. Trazar mapa de sitios protegidos y rutas recorridas
3. Trazar mapa de áreas monitoreadas y no monitoreadas
4. Examinar los dispositivos de monitoreo en búsqueda de limitaciones y vulnerabilidades
5. Examinar posibles ataques de denegación de servicio sobre los dispositivos de monitoreo

Metodología OSSTMM

Seguridad Física

Evaluación de Controles de Acceso

Este es un método para evaluar los privilegios de acceso a una organización y a sus bienes a través de puntos de acceso físicos.

Resultados Esperados:	Lista de puntos de acceso físicos Tipos de autenticación Tipos de sistemas de alarmas Lista de disparadores de alarmas

1. Enumerar áreas de control de acceso
2. Examinar dispositivos y tipos de control de acceso
3. Examinar tipos de alarmas
4. Determinar el nivel de complejidad en un dispositivo de control de acceso
5. Determinar el nivel de privacidad en un dispositivo de control de acceso
6. Examinar los dispositivos de control de acceso en búsqueda de puntos débiles y vulnerabilidades
7. Examinar posibles ataques de denegación de servicio sobre los dispositivos de control de acceso

Metodología OSSTMM

Seguridad Física

Revisión de Respuesta de Alarmas

Este es un método para descubrir procedimientos y equipos de alarmas en una organización por medio del descubrimiento de custodia y monitoreo electrónico.

Resultados Esperados:	Lista de tipos de alarmas Lista de disparadores de alarmas Mapa de procedimiento en caso de alarma Lista de personas involucradas en el procedimiento en caso de alarma Lista de medidas de contención y precauciones de seguridad activadas por alarmas

1. Enumerar áreas de control de acceso
2. Examinar dispositivos y tipos de control de acceso
3. Examinar tipos de alarmas
4. Determinar el nivel de complejidad en un dispositivo de control de acceso
5. Determinar el nivel de privacidad en un dispositivo de control de acceso
6. Examinar los dispositivos de control de acceso en búsqueda de puntos débiles y vulnerabilidades
7. Examinar posibles ataques de denegación de servicio sobre los dispositivos de control de acceso

Metodología OSSTMM

Seguridad Física

Revisión de Ubicación

Este es un método para obtener acceso a una organización o a sus bienes, a través de puntos débiles en su ubicación y en su protección contra elementos externos.

Resultados Esperados:	Mapa de ubicación física de los bienes Lista de ubicación física de los puntos de acceso Lista de puntos de acceso vulnerables en la ubicación Lista de la ubicación de los accesos de terceras partes

1. Enumerar las áreas de la organización que son visibles (Línea de visión)
2. Enumerar las áreas dentro de la organización que son audibles (Escuchas electrónicas, con láser y otros dispositivos)
3. Examinar las áreas de la ubicación referentes a las entradas por abastecimiento en búsqueda de puntos débiles y vulnerabilidades
4. Listar las empresas y empleados de abastecimiento
5. Listar las empresas y empleados de limpieza
6. Listar días y horarios de los ciclos de entregas
7. Listar días y horarios de los ciclos de visitantes

Metodología OSSTMM

Seguridad Física

Revisión de Entorno

Este es un método para ganar acceso o dañar a una organización o sus bienes, a través de puntos débiles en su entorno.

Resultados Esperados:	Mapa físico de bienes en cada ubicación Lista de ubicaciones vulnerables Lista de leyes, costumbres, y ética locales Lista de leyes, costumbres, y ética operativas.

1. Examinar las condiciones de la región respecto de los desastres naturales
2. Examinar las condiciones del entorno político
3. Examinar los procedimientos de resguardo y recuperación
4. Identificar puntos débiles y vulnerabilidades en los procedimientos de resguardo y recuperación
5. Identificar posibles ataques de denegación de servicio en los procedimientos de resguardo y recuperación
6. Examinar impedimentos físicos y electrónicos frente a distintas condiciones climáticas
7. Comparar procedimientos operacionales con las leyes, costumbres y ética regional

OSSTMM

Plantillas

Las siguientes plantillas son un ejemplo de los requisitos que deben cumplir los informes de cada una de las partes de la seguridad que se revisa.

Se indica la información que debe contenerse en el informe para que sea calificado dentro de la metodología OSSTMM

OSSTMM

Plantilla de Perfil de Red

Rangos de IP que serán testeados y detalle de dichos rangos

Información de los dominios y su configuración

Información destacada de la transferencia de zonas

LISTA DE SERVIDORES

Dirección IP	Nombre(s) de dominio	Sistema operativo

OSSTMM

Plantilla de Datos del Servidor

Dirección IP	Nombre de dominio

Puerto	Protocolo	Servicio	Detalles del servicio

MENSAJES DE BIENVENIDA:

Puerto	Protocolo	Mensaje de bienvenida

SECUENCIAS TCP:

Predicción de secuencia TCP:
Números de secuencia ISN TCP:
Generación de secuencias IPID:
Tiempo operacional

PREOCUPACIONES Y VULNERABILIDADES:

Preocupación o Vulnerabilidad
Ejemplo
Solución

Referencias:

Herzog, P. (23 de agosto de 2003). Manual de la Metodología Abierta de Testeo de Seguridad. OSSTMM 2.1. (M. Barceló, G. O. Zabal, & G. Crivelli, Trads.) Recuperado el 19 de mayo de 2018.