openwebinars.net/cert/jO63

OpenWebinars

Gracias a

OpenWebinars certifica que

Nacho Pérez Asenjo

Ha superado con éxito

Ciberseguridad en la Empresa

CEO de OpenWebinars

Manuel Agudo

Duración de la ruta

57 horas

Fecha de expedición

10 abril 2023

Contenido

Ciberseguridad en la Empresa

1. Curso de Onboarding en Ciberseguridad: Bienvenid@ a bordo

1. Introducción

Presentación

'Lo aplicado en la oficina me vale para mi vida personal'

2. Términos que debemos conocer

Vulnerabilidad

Amenaza

Ingeniería social

3. Dispositivos ¿Qué debemos conocer de ellos?

¿Qué son los dispositivos?

Sistemas Operativos: ¿Qué tengo que conocer de ellos?

Software y Apps: ¿Son lo mismo?

Contraseñas fuertes

4. Dispositivos corporativos vs BYOD

¿A qué denominamos dispositivo corporativo?

¿Qué significa la denominación BYOD?¿Qué impacto tiene?

5. Usuarios y Contraseñas

¿Qué es un usuario?¿Qué función realiza?

¿Por qué debemos utilizar usuarios y contraseñas?

Gestores de contraseñas

6. Políticas de Contraseñas

¿Por qué me obligan a cambiar mi contraseña cada cierto tiempo?

Beneficios de las políticas de contraseñas y adaptación a ellas

7. Copias de seguridad (Backup)

Copias de seguridad

8. Carpetas compartidas

Carpetas compartidas

9. Navegación segura

¿Qué es un navegador?

Navegadores seguros

Actualizaciones de navegadores

Extensiones en navegadores

¿Qué es una URL o dirección de Internet?

Reconociendo URLs seguras e inseguras

Códigos QR

Certificados

10. Correo electrónico seguro

Entendiendo el correo electrónico

¿Qué es el Phishing?

Documentos adjuntos en el email

11. Descarga desde Internet

¿A qué consideramos descarga desde Internet?

¿Es segura la descarga de ficheros desde Internet?

Precauciones a tener en cuenta de la descarga desde Internet

12. Bloqueo de sesión

Bloqueo de sesión

13. Datos sensibles

Datos sensibles

14. Notificación de incidentes de Ciberseguridad

¿Qué es un incidente de Ciberseguridad?

¿Cómo notificamos un incidente de Ciberseguridad?

15. Desconexión cuando no se está utilizando la red

Desconexión cuando no se está utilizando la red

16. Cierre de sesiones

Cierres de sesiones

17. Apagado del dispositivo

Apagado del dispositivo

18. Conclusiones

Conclusiones

2. Curso de análisis y gestión del riesgo

1. Introducción

Presentación

Introducción a los riegos de seguridad de la información

Gobierno, Riesgo y Cumplimiento

Test autoevaluación Introducción

2. Definición del marco de gestión del riesgo

Marco de gestión ISO 27005 y Estándares NIST 800-39 y 800-30

Establecimiento del marco de gestión del riesgo

Alineación con el negocio

Roles y responsabilidades

Registro del riesgo

Test autoevaluación Definición del marco de gestión del riesgo

3. Evaluación del riesgo

Métodos y herramientas para el análisis del riesgo

Análisis de impacto del negocio (BIA)

Identificación de activos

Amenazas y vulnerabilidades

Valoración del riesgo

Modelos de valoración de activos y del riesgo

Escenarios de riesgo, modelado de amenazas y metodologías de análisis del riesgo

Informe de evaluación del riesgo

Test autoevaluación Evaluación del riesgo

4. Mitigación del riesgo

Introducción a la mitigación del riesgo

Evaluación y opciones de tratamiento del riesgo

Requisitos de un programa de ciberseguridad

Informe de tratamiento del riesgo

Frameworks de seguridad

5. Controles de mitigación: Seguridad administrativa y física

Gobierno de la ciberseguridad

Políticas, procedimientos y guías

Organización de la seguridad de la información

Dispositivos móviles y teletrabajo y Seguridad en RRHH

Gestión de activos

Seguridad física

6. Controles de mitigación: Seguridad lógica

Terminología y requisitos del negocio para el control de acceso

Gestión de acceso de usuarios

Aplicaciones para la gestión de identidades

Principios de criptografía

Protección de información

Seguridad operacional (Parte I)

Seguridad operacional (Parte II)

Seguridad de las comunicaciones

Seguridad en la adquisición, desarrollo y mantenimiento de Sistemas de Información

Continuidad de negocio y recuperación ante desastres

Gestión de incidentes

Test autoevaluación Mitigación del riesgo

7. Monitorización del riesgo

Introducción y requisitos para la monitorización del riesgo

Actividades para la monitorización, reporte y comunicación del riesgo

Indicadores Clave del Riesgo (KRI)

Herramientas para monitorización del riesgo

Test autoevaluación Monitorización del riesgo

3. OSINT para fuga de datos empresariales

1. Taller

OSINT para fuga de datos empresariales

4. Criptografía Simétrica y Asimétrica en la práctica

1. Taller

Criptografía Simétrica y Asimétrica en la práctica

5. Curso de Seguridad de red en el ámbito corporativo: Capa 2 del modelo OSI

1. Introducción

Presentación

Las redes y la seguridad hoy en día

Modelo OSI y modelo TCP/IP

2. Aseguramiento básico de dispositivos

Formas de acceso a los dispositivos

Modos de acceso CLI

Configuración del dispositivo y aseguramiento del acceso local

Aseguramiento de las líneas de acceso remoto

Ejemplo de configuración en Packet Tracer

3. Introducción a la Capa 2

Capa 2

4. ARP

Funcionamiento de ARP

Fallo de seguridad de ARP

Configuración segura de ARP

5. STP

Funcionamiento de STP

Ejemplo de configuración en Packet Tracer

Fallo de seguridad de STP

Configuración segura de STP

6. CDP

Funcionamiento de CDP

Fallo de seguridad de CDP

Configuración segura de CDP

7. VLAN

Concepto de VLAN y tipos

Etiquetado y configuración de VLAN

Ejemplo de configuración en Packet Tracer

Fallo de seguridad de VLAN

Configuración segura de VLAN

8. DTP

Funcionamiento de DTP

Fallo de seguridad de DTP

Configuración segura de DTP

9. VTP

Funcionamiento de VTP

Ejemplo de configuración Packet Tracer

Fallo de seguridad de VTP

Configuración segura de VTP

6. Curso de Seguridad de red en el ámbito corporativo: Capas 3 y 7 del modelo OSI

1. Introducción

Presentación

Las redes y la seguridad hoy en día

Modelo OSI y modelo TCP/IP

2. Introducción a la Capa 3

Capa 3 (Modelo OSI)

Tipos de enrutamiento

Tabla de enrutamiento y elección de la mejor ruta

Reenvío de paquetes

3. Rutas estáticas

Tipos de rutas estáticas

Ejemplo de configuración en Packet Tracer

4. RIP

Funcionamiento de RIP

Ejemplo de configuración en Packet Tracer

Fallo de seguridad de RIP

Configuración segura de RIP

5. OSPF

Conceptos clave de OSPF

Estados de funcionamiento de OSPF

Funcionamiento de OSPF (área única)

Ejemplo de configuración en Packet Tracer

Fallo de seguridad de OSPF

Configuración segura de OSPF

6. HSRP

Protocolos de redundancia de primer salto

Funcionamiento de HSRP

Ejemplo de configuración en Packet Tracer

Fallo de seguridad de HSRP

Configuración segura de HSRP

7. Introducción a la Capa 7

Capa 7 (Modelo OSI)

8. DHCP

Funcionamiento de DNS

Funcionamiento de DHCP

Ejemplo de configuración en Packet Tracer

Fallo de seguridad de DHCP

Configuración segura de DHCP

9. SNMP

Funcionamiento de SNMP

Ejemplo de configuración en Packet Tracer

Fallo de seguridad de SNMP

Configuración segura de SNMP

7. Curso de Triage informático

1. Introducción

Presentación

Tipos de malware y características

Procesos, conexiones, puertos y protocolos

Diferencias entre un Hacker y un Cracker

C&C (Comand & Control) y direccionamiento

Test repaso Introducción

2. Búsqueda de malware

Mito y realidad sobre el malware

Metadatos, firma y descripción

Análisis heurístico y Herramientas

Test repaso Búsqueda de malware

3. Análisis de archivos ejecutables

Paquetes, ruta de instalación y ruta de ejecución

Uso de recursos

Establecimiento de conexiones

Test repaso Análisis de archivos ejecutables

4. Emails y phishing

Emails sospechosos y archivos infectados

Laboratorio: Creación de máquinas virtuales con VMware

Test repaso Emails y phishing

8. Curso de desarrollo seguro

1. Ciclo de desarrollo seguro de software

Introducción al curso y presentación del profesor

Ciclo de desarrollo de software

Requisitos

Arquitectura y diseño

Implementación

Testeo

Despliegue

Mantenimiento

2. Seguridad en el desarrollo

Validación de entradas

Práctica de validación de entradas

Codificación de salidas

Práctica de codificación de salidas

Criptografía

Práctica de criptografía

Buffer overflow

Práctica de buffer overflow

3. Seguridad en los procesos y procedimientos

Autenticación y manejo de contraseñas

Práctica de Autenticación y manejo de contraseñas

Manejo de sesiones

Práctica de manejo de sesiones

Manejo de errores y log

Práctica de manejo de errores y log

4. Seguridad en la configuración del entorno

Control de acceso

Práctica de control de acceso

Protección de datos

Prácticas de protección de datos

Seguridad de comunicaciones

Práctica de seguridad de comunicaciones

Configuración del sistema

Práctica de configuración del sistema

Seguridad en Bases de datos

Práctica de seguridad en Bases de datos

Manejo de ficheros

Práctica de manejo de ficheros

Manejo de memoria

9. Curso de Introducción al Esquema Nacional de Seguridad (ENS)

1. Introducción

Presentación

2. Esquema Nacional de Seguridad

Enfoque, objetivos, alcance y aplicabilidad

Activos

Concepto de madurez

3. Marco organizativo

Política de seguridad

Comité de seguridad

Roles y responsabilidades

4. Marco operacional

Planificación de la seguridad

Acceso a la información

Explotación de servicios internos y externos

Continuidad de servicio y monitorización

5. Medidas de protección

Protección de instalaciones

Gestión del personal

Protección de equipos

Protección de las comunicaciones

Protección de soportes

Desarrollo seguro

Protección de la información

Protección de los servicios

6. Análisis de riesgos

Activos y amenazas

Cálculo del riesgo

Herramienta PILAR: Características e instalación

Herramienta PILAR: Primeros pasos y creación de un proyecto

Herramienta PILAR: Amenazas y riesgos

7. Adecuación y mantenimiento

Implantación de medidas técnicas

Redacción de procedimientos operativos

Herramienta INES