Diplomado

CiberSeguridad defensa y ataque de un ecosistema tecnológico.

TPX MX SA DE CV.
Diplomado Presencial.
Edición 1, Año 2017.

https://tpx.mx/diplomados/
hola@tpx.mx

tpx.mx @tpx_mx tpx.mx

La seguridad de la información es uno de los pilares más importantes en una empresa, si esta no esta asegurada puede traer serias consecuencias a la empresa o institución o usuario final.

Los ciber ataques han evolucionado y con ello las técnicas y metodologías las cuales son capaces de accesar a sistemas informáticos en cuestión de minutos con el fin de obtener información confidencial, bloquear sistemas, dañar sistemas o modificarlos. Adquirir un nuevo software o hardware de seguridad por más costosos que este sea no resolverá de todo este tipo de problemas, tampoco impedirá que los hackers entren al sistema, es necesario un entrenamiento de inteligencia militar para saber cómo resguardar la información y proteger de estos ataques.

Este diplomado tiene cómo objetivo formar profesionales en el área de la ciber seguridad, con conocimientos del funcionamiento y metodología de los ataques informáticos que han salido a luz el los últimos 03 años y así cómo ataques que han estado en funcionamiento en todas la áreas de en un entorno tecnológico adquirir experiencia en seguridad informática y hacking.

Diplomado Presencial.

Las áreas de ciberseguridad qué el diplomado integrará [más de 120 horas]:

- ✓ Windows
- ✓ Servidores (Linux & BSD)
- ✓ Redes Sociales ingeniería Social
- ✓ Radio Frecuencia. (SDR)
- ✓ Inalámbrica
- ✓ Gobierno Digital.
- ✓ Dispositivos Locales.
- ✓ Sistemas Industriales.
- ✓ Sistemas industriales conectados a internet.
- ✓ Dispositivos conectados a internet
- ✓ Ciber Espionaje y contra inteligencia.

- Presentación.
- La importancia de la Ciber Seguridad y los riesgos.
- Conceptos.
- Ataques y peligros actuales.
- Pilares de la seguridad de la información.
- Gobierno de Seguridad de la Información
- Seguridad de la información e integridad de la información.
- Análisis de riesgos
  - Recabar Información
  - Ecosistema Tecnológico.
    - Arquitectura.
    - Vulnerabilidades.
    - Recurso Humano
    - Amenazas.
- Eventos
  - Ataques
  - Incidentes
    - Respuesta a incidentes.
- Conociendo al atacante.
  - Anatomía de los ataques.
  - Psicología del atacante.
  - Ecosistema de comunicación.
  - Ciber crimen
  - Ciber crimen organizado.
- Seguridad e integridad de la información.
  - Ambientes seguros para la información.
  - Sistema de respaldos y almacenamiento de la información
  - Monitoreo

[+] Introducción

- Presentación
- Definiciones y Software a usar.
- Discusión de diferentes tipos de vulnerabilidades
- Instalación de ambiente de pruebas.
- Métodos de reconocimiento.
- Tipos de Ataques.

[+] Escaneo

- Uso de diferentes herramientas de escaneo.
- Métodos de escaneo.
- Descubriendo vulnerabilidades.

[+] Explotación

- Herramientas de explotación.
  - Armitage
  - Metasploit / meterpreter
  - Empire
- Herramientas de Evasión
  - Shellter
  - Veil-evasion
  - Setoolkit
- Vectores de ataques
  - Malas configuraciones
  - Puertos abiertos
  - Exploits
  - Puertos USB

[+] EXPLOTACIÓN AVANZADA

- Evasión de antivirus.
- Hacking con macros / office.
- Escalación de Privilegios
- BypassUAC
- Lazagne
- Creando malware en powershell y C#
- Ataque fuera de la red con VPN
- Ataque fuera de la red con DNS y VPN

[+] Introducción

- Presentación
- Definiciones y Software a usar.
- Discusión de diferentes tipos de vulnerabilidades
- Instalación de ambiente de pruebas.
- Métodos de reconocimiento.
- Tipos de Ataques.
- ¿Cómo funciona un Servidor en Linux?
- El arte del footprinting
- Introducción al Shell Scripting

Este modulo se complementa con:
Curso Web Penetration Tester Online.

[+] Escaneo

- Uso de diferentes herramientas de escaneo.
- Métodos de escaneo.
- Descubriendo vulnerabilidades.

[+] Web Hacking

- Vulnerabilidades, Exploits y días cero
- Escaneo - httpd
- Escaneo de vulnerabilidades.
- Vectores de ataques:
  - Factor Humano.
  - Remote File Inclusion
  - Local File Inclusion
  - Code Injection
  - SQL injection.
  - Herramientas de SQLi para pentest
  - Web Shell
  - XSS
  - Dos y DDoS.

[+] Seguridad

- Instalación y configuración de Apache
- Instalación y configuración de MySQL
- Políticas de Seguridad en Servidores Web.
- Detección de archivos y código malicioso.
  - Primeros Pasos.
  - Automatización.
- Herramientas de monitoreo Servidores.
  - Primeros Pasos.
  - Automatización.
- Web Forense.
  - Reportes .
- Pentest
  - Reportes.

[+] Introducción

- Qué es la ingeniería social.
- La psicología cómo vector de ataque.
- Ejemplos de Ataques recientes.
- Introducción al Phishing
- Introducción al Spoofing
- Riesgos en una empresa
  - Robo de datos
  - Fuga de datos
  - Ataques dirigidos

[+] Vectores de ataque.

- Acceso físico
  - Baiting: ruber ducky
  - Baiting: bash bunny
- Social-Engineer Toolkit
  - Phising: email o SMS, QR-images
  - Web: DNS Spoofing.
  - Payloads: creación de archivos maliciosos.
  - Phishing
- Puntos de acceso falsos.

[+] Laboratorio

Se realizará un laboratorio con el conocimiento adquirido en el modulo 02 y modulo 03, en el cual se realizarán estos vectores de ataque, emulando a los ataques que pueden dañar a las organizaciones o empresas.

[+] Radio Frecuencia.

- Radio definida por software.
- Procesador digital de señales, DSP (Digital Signal Processor)
- GNU Radio.
  - Entendiendo espectro electromagnético
    - Radiofrecuencia

- Instalando GNU Radio
  - Herramientas y programas de utilidad
  - Desarrollo del procesamiento gráfico de señal

- Análisis y retransmisión de sistema de video vigilancia (cámaras RF)
- Análisis de RF Bells
- Análisis de RF Drones
- Análisis de RF Vehículos

[+] Laboratorio

Se realizará un laboratorio con el conocimiento adquirido, en el cual se realizarán estos vectores de ataque, emulando a los ataques que pueden dañar a las organizaciones o empresas.

[+] Inalámbrico

- Tipos de Ataques
- Técnicas de Sniffing
- Técnicas MITM
- Cookie stealing
- WireShark
- Análisis de patrones
- Técnicas de Scanning
- WPS, WPA,
- Hardware
  - Piña Wifi

[+] Dispositivos conectados a Internet.

- ¿Qué son los dispositivos conectados a internet?
  - Ataques y robo de información.
- Detectando dispositivos conectados a Internet
  - Herramientas Publicas
  - Herramientas Privadas.
- Vectores de ataque.
  - Puertos
  - Protocolos de comunicación
- Detectando sistemas Industriales conectados a internet
  - Vectores de ataque.
    - Puertos
    - Protocolos.
- Metodología de pruebas de seguridad dispositivos y maquinas conectados a internet.
- IoT
  - API security
  - security analytics
  - encryption
  - authentication
  - Network Security

- Espionaje cibernético..
  - Contraespionaje
- Vectores de ataques.
  - Robo de información
  - Backdoors
  - Malware
  - Evasión de antivirus.
  - Análisis de Redes Sociales.
  - Análisis De datos
- Recolección de información
  - Internet
  - Redes Inalámbricas
  - Garbage collector.
- Servicios en internet
  - Sistemas Informáticos.
    - Detección de intrusos.
    - Detección de ataques.
    - Análisis de un sistema comprometido.
- Dispositivos inalámbricos
  - Detección de intrusos
  - Detección de ataques.
  - Análisis de una red comprometida.
- Telefonía.
  - Detección de intrusos
  - Detección de ataques.
  - Análisis de una red comprometida

El temario se encuentra en constante actualización, conforme a las nuevas metodologías de hacking y ciber seguridad, por lo que tiene cambios sin previo aviso con el fin de mejorar la calidad del diplomado.

Ultima actualización: Septiembre 2017

TPX MX SA DE CV
Aguascalientes México.
Una empresa dedicada a la ciberseguridad e investigación científica.