EXPLOTACIÓN DE SISTEMAS DE PAGOS NFC

Entrenamiento Presencial

TPX MX SA DE CV.
Curso Presencial.
Edición 1, Año 2018.

http://tpx.mx/cursos/nfc-hacking
cursos@tpx.mx
tpx.mx @tpx_mx tpx.mx

En la actualidad los sistemas de pagos físicos y digitales que utilizan tecnologías como NFC o MST van cambiando constantemente. Agregando nuevas tecnologías que de manera especulativa pueden ayudar a contener ciertos ataques; pero de igual forma abren nuevas brechas que pueden ser utilizadas por los atacantes de manera colateral.

El curso tiene como propósito ayudar a entender y prevenir las amenazas reales que pueden enfrentar todo tipo de instituciones que manejan pagos digitales y físicos. El poder detectar e informar de manera adecuada estos ataques, entender la lógica, que medios se pueden explotar y qué dispositivos son implementados.

Durante el curso, el educando podrá interactuar con tecnología utilizada para ataques RFID, entender de primera mano vulnerabilidades en el diseño NFC, explotación lógica y física. Se presentarán demostraciones con pagos digitales reales y su posible explotación.

De igual manera se dará a conocer un análisis crítico de la mentalidad de un atacante. Así como ataques o extracción de datos nunca antes documentados utilizando tecnologías y explotando el débil diseño en la que recaen los pagos actuales.

El alumno podrá relacionar toda esta información con su experiencia y añadir nuevos conceptos y metodologías para aplicar este conocimiento de manera apropiada.

[+] **Duración:** 10 horas

[+] **Quien debería tomar este curso.**

- Desarrolladores del sector Bancario
- Entusiastas de la seguridad y hacking
- Desarrolladores de sistemas de Pago
- RedTeams encargados de comprometer infraestructura.

[+] **Requisitos del estudiante.**

- Se recomienda experiencia básica en sistemas de pagos pero no necesaria..

[+] **Lo que los estudiantes deben llevar al curso.**

- Laptop con al menos 10GB de espacio libre y más de 4 GB en RAM, con accesos USB.
- Maquina Virtual
- Android con soporte NFC (en caso de no tener notificar)

[+] **Que se proporciona a los estudiantes.**

- Dispositivos NFC (solo durante el entrenamiento, con opción a compra)
- Documentación digital.

Día 01
05 horas

1. Introducción.

- Terminologia
- Diferencia entre pagos físicos y digitales
- Comunicación NFC
- Estructura de comandos APDU
- Explicación de los procesos de tokenización
- Diferencias y similitudes entre Elemento de Seguridad(SE) y Emulación de tarjeta(HCE)

2. Visa PayWave y Mastercard PayPass

- Tipos y formas de transacciones
- Que es Visa MSD
- Analizando una transacción física y una digital(Chip Vs NFC).

3. Pagos físicos, digitales y sus estructuras.

- Tarjeta con Chip EMV
- Tarjeta con tecnología NFC
- Android Pay
- Samsung Pay
- Apple Pay
- Reloj Fitbit Ionic.

4. Ataques de Repetición.

- Cuando la flexibilidad se convierte en un problema
- Descubriendo elementos débiles usando investigaciones del Dr. Roland y Peter Fillmore
- Alterando bytes en comandos APDU
- Ataques de fuerza bruta contra los sistemas de tokenización
- Analizando dispositivos de repetición
- Demostraciones / Lab

Día 02
05 horas

5. Ataques de Retransmision

- Planeación y estructura del ataque
- Por qué es tan letal un ataque de retransmisión?
- Realmente necesito comandos APDU?
- Moviendo APDUs entre protocolos T0 <-> T1
- Moviendo una transacción de Chip a NFC
- Creando un Franquestein(SDR, APDU, NFC)
- Demostraciones / Lab

5. Mitigar ataques

- Bounding distance protocol
- Comandos especializados en el lado de la terminal
-

6. Conclusiones.

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 entrenamiento.

Ultima actualización: Agosto 2018

TPX MX SA DE CV

Aguascalientes México.

Una empresa dedicada a la ciberseguridad e investigación científica.