# OWASP LATAM Tour 2019 Mexico

# AGENDA



## Conferencias

### Pagos Digitales y NFCitza

Salvador Mendoza (@netxing) es un investigador de seguridad enfocado en procesos de tokenización, información de bandas magnéticas, sistemas de pagos y prototipos especializados. Salvador ha presentado sus investigaciones relacionadas con fallas de seguridad en sistemas de pagos y procesos de tokenización en conferencias internacionales como lo son Black Hat USA, DEF CON 24/25, DerbyCon, Ekoparty, BugCON, 8.8 y Troopers 17/18. Agregando que Salvador

ha diseñado diferentes herramientas para buscar fallas en sistemas de pagos físicos y digitales, en los cuales se incluyen MagSpoofPI, JamSpay, TokenGet, SamyKam y últimamente BlueSpoof.

Durante los últimos años se han introducido diferentes tipos de pagos digitales usando tecnología NFC por diferentes compañías. Algunos dispositivos implementan seguridad en hardware para proteger sus transacciones, como son los elementos seguros de Apple Pay, por ejemplo. Otros usan prevalidación en nube para activar las transacciones usando tokenización, como es Google Pay or Samsung Pay. El mayor problema con este tipo de pagos o con las transacciones NFC es que no implementan ningún tipo de cifrado en la comunicación. Lo que llega a ser vital para que usuarios malintencionados puedan robar datos de clientes o lo más grave, puedan robar transacciones.

En esta charla discutiremos lo fácil que es crear un ataque maestro para poder realizar diferentes tipos de relays en contra de cualquier sistema de pagos que implemente la tecnología NFC. Con simple hardware, como Arduinos o ESP32 y un poco de código, lograremos crear un ataque que nos ayudará a entender y crear sniffers sobre las transacciones NFC. Esto sin necesidad de saber que tipo de protección en cifrado o en hardware está implementando el sistema digital de pagos.

## Network Exploitation of IoT ecosystems

Fotios Chantzis (@ithilgore) es líder de un grupo de ingeniería en Mayo Clinic, donde maneja un equipo a cargo de conducir análisis y evaluación de vulnerabilidades en equipos médicos y de soporte clínico. Foti tiene más de 10 años de experiencia en la industria de la seguridad informática donde ha contribuido a proyectos como Nmap y Ncrack e investigando vulnerabilidades de red que lo han llevado a explotación de TCP y XMPP. Fotis tiene una maestría en ingeniería en computación y es certificado OSCP y OSCE. Actualmente trabaja sobre su doctorado relacionado a seguridad en dispositivos médicos.

Internet of Things (IoT) ecosystems are comprised of a large variety of connected devices that are rife with “smart” features and textbook vulnerabilities. With the advent of ever growing interconnection and interoperability of all these devices, protocols that focus on automation have been developed throughout the years. These often assume an environment with cooperating participants - something that rarely happens in the real world. The fast market pace also leads manufacturers to marginalize security as having low return on investment. IoT devices are usually embedded with low-energy and low processing capabilities, deprioritizing security robustness as a result. All of the above combined make for ecosystems with lots of inherent weaknesses. In this talk we are going to present techniques and attacks on network protocols and insecure implementations commonly found in IoT ecosystems. We are going to explore how penetration testers can abuse zeroconf networking protocols like UPnP, mDNS, WS-Discovery and others to conduct a variety of attacks and how to combine a chain of seemingly lower risk findings into an impactful attack. Other IoT security angles will be explored as well: from the default insecurity of video streaming protocols like RTP, heavily used by networked cameras, to the growing usage of IPv6 and what that entails in terms of the security posture of the IoT world.

## Let's get Social: Historias de un social engineering Pentester

Luis Antonio Aceves (@HumanHardener) es socio cofundador de la empresa Purple Security. Empresa dedicada a la seguridad digital; especializada en pruebas de penetración, análisis de aplicaciones web, móviles, e investigaciones digitales. Actualmente Oficial de Operaciones y Riesgos Cibernéticos; especialista responsable de la evaluación de usuarios de Organizaciones mediante pruebas de ingeniería social, concientización de la seguridad digital y pruebas de penetración física a instalaciones. Con más de 60 assessments de ingeniería social realizados a más de 3 docenas de empresas, se presenta la conferencia “Let´s get social: historias de un social engineer pentester”.

Presentación de los resultados obtenidos en más de 60 social engineering assessments: ejemplos de phishing, vishing, baiting y videos en los que se muestran los pretextos más significativos con los cuales se ha logrado comprometer a usuarios de diferentes empresas mexicanas.

## It’s not magic, it’s DevSecOps

Ronen Riesenfeld cuenta más de 24 años de experiencia en el área de TI, 10 años de experiencia desarrollando aplicaciones utilizando herramientas de automatización en ambientes de DevOps y más de 5 años en desarrollo seguro. Ha participado en proyectos de asesoramiento y asistencia en revisiones de código. Ronen posee una maestría en sistemas de Información y un amplio conocimiento en la incorporación de la Seguridad dentro de ciclos de desarrollo y ambientes de DevOps. Actualmente es *Sales Engineer* en Checkmarx.

La seguridad perimetral, el análisis dinámico y otras soluciones de seguridad no estática dan una incorrecta percepción de que las aplicaciones están seguras, percepción que reduce el sentido de urgencia por la implementación holística de la seguridad. En esta plática, se mostrará cómo complementar con otro tipo de tecnologías de seguridad ayudará a fortalecer los cimientos de las aplicaciones sin entorpecer los procesos e integrándose de manera orgánica como por arte de magia, facilitando así el desarrollo seguro a alta velocidad.

# Talleres

## Assessing Io(M)T Systems

Fotios Chantzis (@ithilgore) es líder de un grupo de ingeniería en Mayo Clinic, donde maneja un equipo a cargo de conducir análisis y evaluación de vulnerabilidades en equipos médicos y de soporte clínico. Foti tiene más de 10 años de experiencia en la industria de la seguridad informática donde ha contribuido a proyectos como Nmap y Ncrack e investigando vulnerabilidades de red que lo han llevado a explotación de TCP y XMPP. Fotis tiene una maestría en ingeniería en computación y es certificado OSCP y OSCE. Actualmente trabaja sobre su doctorado relacionado a seguridad en dispositivos médicos.

### SHORT Course Abstract/Session Description

This workshop will teach participants how to assess Io(M)T devices from a software & network security perspective. We will leverage tools of the trade including Nmap, Ncrack, Wireshark and libraries such as pynetdicom and show how to extend them. By the end of the workshop, you will have knowledge of a robust methodology for conducting vulnerability assessments on IoT & IoMT systems.

### FULL Course Abstract

This workshop will teach participants how to assess medical and IoT devices from a software & network security perspective. We will leverage tools of the trade including Nmap, Ncrack, Wireshark, and Python libraries such as pynetdicom and show how to extend them. By the end of the workshop, you will have knowledge of a robust methodology for conducting vulnerability assessments on IoT & IoMT systems. Participants will be provided with a virtual machine that they can use during the training.

We will start by exploring the threat landscape of the medical / IoT device field by going over the most common vulnerabilities and various attack scenarios that chain security issues together to gain access to high-impact clinical assets.

We will cover vulnerabilities on the insecure DICOM protocol. We are going to showcase how to leverage pynetdicom to write python scripts for attacking DICOM and exploit insecurely configured PACS servers

leading to the extraction of sensitive PHI (Protected Health Information). DICOM, being a highly complex protocol, is also poorly implemented in libraries which allows for memory corruption vulnerabilities to be found by simple fuzzing.

Another aspect of the training will cover vulnerabilities found in IoT infrastructure with a focus on IP cameras and video management servers. These often run insecure protocols like zeroconf and have web portals that are easily authentication brute-forceable and poorly configured. We are specifically going to examine the WS-Discovery protocol which provides some interesting attack vectors by putting too much trust on the local network.

Hands-on exercises will be conducted by the students throughout the training for each section under the guidance of the instructors. The final part of the workshop will have a CTF challenge for participants to practice their skills on an emulated medical ecosystem.

### Course Syllabus/Outline

1. Overview of the Io(M)T threat landscape
    - Common vulnerabilities in Io(M)T devices
    - Threat & Attack Chain Scenarios
2. Attacking PACS servers (DICOM)
    - Decoding DICOM commands
    - Finding AET combinations
    - Attacking DICOM with pynetdicom
    - Exploiting insecure PACS servers
3. Breaking Surveillance Cameras
    - WS-Discovery Primer
    - Rogue cameras
    - Attacking IP camera software

4. Capture-the-Flag

### Approximately what percentage of your course is lecture vs hands on?

**35% lecture, 65% hands-on**

### What are the keywords you would use to describe the topic areas covered by your course?

Medical device security, IoT, healthcare security, clinical security, DICOM, PACS, network security, Nmap, Wireshark, Ncrack, pynetdicom, Orthanc, router, cameras

### Who Should Take This Course:

Information security professionals interested in learning about medical device & IoT security. IT admins working in these environments.

### Student Requirements

Participants will need a computer with VMware Player, VMware Fusion, or VirtualBox. Ideally they should have Kali Linux already installed.

### Is this course for beginners, intermediate or advanced students?

This is an intermediate course.

### How many years of practical experience would the ideal student have to get the most out of this course?

Participants should be familiar with the command line, basic TCP/IP networking, general security concepts. Previous programming experience would be helpful but isn't required. 2 or 3 years of practical experience would be ideal.

### What Students Should Bring

Participants will need a computer with VMware Player, VMware Fusion, or VirtualBox.

## ARM e IoT hacking

Luis Raul Valencia (@security_raul) is an advisor and enthusiast in Cybersecurity with experience in reverse engineering, cyber-operations, penetration tests, forensic analysis, among others. Interested in mobile security, IoT, drones, SCADA, NFC and exploit development.

En el workshop se dará una introducción a ARM, el cual es la tecnología base de la gran mayoría de IoT. Demostrando principalmente la estructura a nivel ensamblador de ARM y como generar payloads. Complementando con demostraciones de ataques comunes a Zigbee, MQTT, CoAP, BLE y Wifi; los cuales son los protocolos más usados de IoT.

Liga de registro: TBD

## Introducción al análisis de paquetes con Wireshark

Arturo Torres (@artur_t0rres) es Consultor de Seguridad en Fortinet para la región norte del país, siendo además, parte del equipo de investigación y desarrollo de FortiGuard contra amenazas cibernéticas globales. Arturo cuenta con conocimientos de Seguridad Perimetral, Pruebas de penetración, threat hunting, consultoría y diseño de soluciones de seguridad. Ha publicado en foros de tecnología e impartido conferencias para el sector educativo y el sector empresarial y eventos como de seguridad como OWASP LATAM. Arturo se unió a Fortinet en el 2016, y ha ocupado diferentes posiciones en otras compañías de tecnología como Especialista de seguridad en Alestra, además de que actualmente se desempeña como docente en una carrera de Seguridad Informática en la Universidad Autónoma de Nuevo León. Arturo es Ingeniero en Electrónica y Comunicaciones por la Universidad Autónoma de Nuevo León y cuenta con una maestría en Administración, Negocios y Relaciones Industriales, por la misma universidad..

Wireshark es el analizador de redes más popular del mundo con más de 500,000 descargas por mes. Y sí, sigue siendo gratis. Este taller se formó para desarrollar habilidades en la captura y análisis de paquetes con el objetivo de poder identificar anomalías basadas en las capturas de tráfico y detectar infecciones o comportamientos maliciosos para generar un reporte con evidencias e indicadores de compromiso (IOC). El taller cubrirá los siguientes temas:

- Introducción al análisis de paquetes
- Interfaces de Wireshark
- Captura de paquetes
- Manipulación de columnas en los paneles de paquetes
- Disectores (Dissectors) de Wireshark
- Analizando tráfico en puertos no estándar
- Visualización de tráfico y aplicaciones
- Detección de problemas de latencia

- Detección y análisis de endpoints de comunicación
- Listado de tráfico de aplicaciones
- Construcción e interpretación de tablas y gráficos
- Threat Hunting con Wireshark

Liga de registro: TBD

## Técnicas OSINT para pentesters

Murena Lavín Martínez (@murenalm) actualmente tiene el rol de Coordinadora de Gestión de Incidentes de Seguridad y Procesos en SCITUM, desde donde coordina equipos especializados en seguridad informática, buscando establece estrategias para encontrar de manera proactiva los huecos de seguridad y riesgos asociados a la infraestructura de operación y aplicaciones de negocio de diferentes organizaciones. Cuenta con las certificaciones de SANS Institute, GIAC Penetration Tester (GPEN), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE), GIAC Continuous Monitoring Certification (GMON), de CompTIA, Security+; de ISC2, Certified Information Systems Security Professional (CISSP); además de las certificación ITIL v3 y SCRUM-SDC.

Karla Stephany Perez Rodriguez En la actualidad desempeña el rol de Consultor Tiger Team en SCITUM, en donde realiza “hackeos éticos”, análisis de vulnerabilidades , ingeniería social, campañas de phishing/vishing, por mencionar algunos. Posee las certificaciones de EC-Council, Certified Ethical Hacker (CEH), además de la certificación  Tenable Certifies Nessus Engineer (TCNE) por Tenable.

El objetivo de este taller es aplicar algunas técnicas y herramientas de OSINT en un ejercicio tipo CTF (Capture the flag) para buscar información en la web relacionada con personas desaparecidas (de fichas reales de personas desaparecidas de la fiscalía del estado de Quintana Roo). Al finalizar el taller, toda la información recopilada por los participantes se hará llegar al gobierno de Quintana Roo como una contribución de la comunidad de entusiastas de la seguridad informática, en la búsqueda de información que pueda ayudar a las autoridades en sus investigaciones.

El taller permitirá a los participantes practicar y mejorar sus habilidades de OSINT así como contribuir con la comunidad local dentro de un marco de respeto en todo momento a las personas desaparecidas y sus familias.

Liga de registro: TBD

## Introducción a la tecnología RFID y NFC

Salvador Mendoza (@netxing) es un investigador de seguridad enfocado en procesos de tokenización, información de bandas magnéticas, sistemas de pagos y prototipos especializados.

Salvador ha presentado sus investigaciones relacionadas con fallas de seguridad en sistemas de pagos y procesos de tokenización en conferencias internacionales como lo son Black Hat USA, DEF CON 24/25, DerbyCon, Ekoparty, BugCON, 8.8 y Troopers 17/18. Agregando que Salvador ha diseñado diferentes herramientas para buscar fallas en sistemas de pagos físicos y digitales, en los cuales se incluyen MagSpoofPI, JamSpay, TokenGet, SamyKam y últimamente BlueSpoof.

Andrés Sabas (@Sabasacustico) es un apasionado del hardware, ingeniero en electrónica por el Instituto Tecnológico de Aguascalientes, co-fundador de The Inventor's House hackerspace en Aguascalientes, CEO de Electronic Cats hardware libre hecho en México, ha participado como director del makerspace campus party México, miembro activo de maker México, ha participado en eventos de tecnología como ponente y tallerista en áreas como educación espacial, IoT, redes LPWAN y todo tipo de sistemas embebidos. Le gusta jugar juegos de mesa y ver series.

Las tecnologías inalámbricas como tarjetas de acceso RFID o sistemas de pagos por medio de NFC están adaptando rápidamente en nuestras vidas. Últimamente vemos estas tecnologías en los hoteles, renta de carros e incluso sistema de pagos que se están transformando en un nuevo ecosistema sin contacto. ¿Pero qué tan seguras son estas tecnologías?

En este curso, se educara para determinar qué tipo de sistema físicos de proximidad se están implementado en los sistemas de control. Los tipos más genéricos de tarjetas y el los diferentes tipos de ataques. Más que un curso teórico, es un curso práctico. Donde se utilizaran herramientas como ACR122, Chameleon Mini, Proxmark3 en sus diferentes versiones. Incluso se implementaran herramientas específicas para explotación de sistema de pagos como MagSpoof, BlueSpoof.

En el primer día se dará una introducción al tipo de modulación en las tecnologías de baja frecuencia. Se practicará implementando un ambiente virtualizado con herramientas precargadas. A los estudiantes se les otorgará un USB con la imagen que usaremos durante el taller, donde se incluirán todas las herramientas a nivel de software. Practicaremos desde cómo reconocer una tecnología donde no se conoce un tag previamente, de cómo identificarlo y cuales son los pasos para clonarlos o realizar ataques de repetición con otro tipo de hardware.

En el segundo día hablaremos de la tecnología de alta frecuencia y sus modulaciones. Se explicarán los riesgos de los sistemas de pagos y se practicará con ataques de repetición(replay) y ataques de retransmisión(relay) usando herramientas automatizadas. Se practicará con sistemas de pagos reales como lo son Apple Pay, Samsung Pay y Google Pay. Incluso usaremos un reloj inteligente como lo es Fitbit Ionic para analizar su sistema de seguridad de elemento seguro.

Liga de registro: TBD

## Técnicas actuales de hacking

Jaime Andrés Restrepo (@DragonJAR) es Ingeniero en Sistemas y Telecomunicaciones de la Universidad de Manizales. Information Security Researcher con más de 10 años de experiencias en Ethical Hacking, Pen Testing y Análisis Forense. Docente Universitario en Pre y Post-Grado, Speaker y Organizador de diferentes eventos Internacionales de Seguridad Informática, Fundador del DragonJAR Security Conference de DragonJAR SAS y de La Comunidad DragonJAR, una de las comunidades de seguridad informática mas grandes de habla hispana y referente en el sector.

En este taller se cubrirán los siguientes temas durante dos días:

- ¿Como realizo un pentesting a una aplicación web?
- Recolección de información pasiva/activa.
- Analizando todo antes de meter la primer comilla.
- Conociendo y Explotando los fallos de seguridad web más comunes.
- Ataques a aplicaciones Web - OWASP TOP 10++
- Post-Explotación, ya tengo acceso... ¿ahora qué hago?
- ¿Cómo realizar un pentesting a una infraestructura?
- Fuerza bruta "inteligente" a servicios encontrados.
- Consiguiendo y Conservando el Acceso
- Técnicas actuales de ataques dirigidos a usuarios
- Ataques de Denegación de Servicio
- Post-Explotación - ¿tengo shell y ahora qué hago?
- Identificación del entorno
- Extracción de evidencias
- Escalación de privilegios
- Técnicas actuales para captura de Tráfico
- Técnicas actuales para ataques MITM
- Saltando entre redes - Pivoting
- Saltando contramedidas (Firewall, Antivirus, IDS, etc...)
- Ataques a equipos de Red

Liga de registro: TBD

## Introducción al exploiting en Windows

Luis Velazquez (@0xjar8) es consultor Red Team en Global Cybersec. Cuenta con experiencia profesional realizando pruebas de penetración y análisis de vulnerabilidades. Es egresado de la carrera de Ingeniería en Sistemas Computacionales por el Instituto Tecnológico de Minatitlán. Se considera un aficionado a las CTF's y un apasionado al Hacking. Cuenta con la certificación de OSCP.

Hoy en día existen un gran número de personas dedicadas a las ciberseguridad que utilizan exploits, sin embargo, no todos conocen cómo es que estos se desarrollan. La finalidad del taller es introducir a los asistentes a la explotación de software en sistemas operativos Windows; abarcando los conceptos básicos necesarios para poder descubrir y aprovecharse de vulnerabilidades del tipo Stack Buffer Overflow, así como resolver algunos de los problemas que se podrían presentar durante el desarrollo del exploit y las protecciones que se han ido desarrollando para mitigar este tipo de técnicas.

El taller cubrirá los siguientes temas:

- Conceptos básicos de ensamblador y arquitectura de computadoras.
- Fuzzing y exploiting.
- ¿Stack Buffer Overflow?.
- Técnicas de salto a la Shellcode.
- Structured Exception Handler (SEH).
- Egg Hunters.
- Mecanismos de protección.

Liga de registro: TBD

## Mobile App Security Testing

Edgar Baldemar Ramos (@edgarbaldemarmx) actualmente se encuentra en la empresa Purple Security como encargado de: desarrollo de estrategias y auditorías de seguridad ofensiva (Hacking Ético), investigador y desarrollador de prototipos y análisis de malware, auditor de seguridad de aplicaciones web, experto en OWASP y asesor de técnicas y controles de aseguramiento en procesos de desarrollo de software. Cuenta con las certificaciones de EC-Council, Certified Ethical Hacker (CEH), Certified Security Analyst (ECSA) y Certified Incident Handler (ECIH); además de Certified Information System Auditor (CISA) por ISACA.

La adopción de dispositivos móviles es una tendencia en aumento y con ello los riesgos de seguridad digital en aplicaciones y plataformas móviles. El **Workshop Mobile App Security Testing** se ha diseñado para proporcionar al asistente recursos y técnicas de apoyo para la identificación de riesgos de seguridad

y la ejecución de análisis de seguridad en aplicaciones móviles de las plataformas más posicionadas de la industria (Android & iOS).

En el taller se cubrirán los siguientes temas:

- INTRODUCCIÓN A PLATAFORMAS ANDROID & IOS
- TOP 10 RIESGOS DE SEGURIDAD EN MÓVILES
- METODOLOGÍA Y RECURSOS DE OWASP
- ANÁLISIS ESTÁTICO
- ANÁLISIS DINÁMICO
- QUICKWINS MOBILE PENTEST
- MECANISMOS DE SEGURIDAD EN APPS DE PRUEBA VS APPS EN PRODUCCIÓN

Es indispensable el asistente cuente con un equipo de cómputo portátil con capacidad de virtualización mínima deseable:

- 8GB RAM o superior
- 50GB disponible de almacenamiento o superior
- Vmware Player / Workstation / Fusion instalado

Liga de registro: TBD