TALLER

2018 actividades

INVESTIGACIÓN
OSINT & THREAT
INTELLIGENCE

UNED

GOBIERNO DE ESPAÑA

MINISTERIO DEL INTERIOR

IUISI

Instituto Universitario de Investigación sobre **Seguridad Interior**

Del **9** al **13 abril**

Instituto Universitario
MISSISSIPPI
(1ª Planta)
Calle de la Santísima Trinidad 5
Madrid

TALLER
INVESTIGACIÓN OSINT & THREAT INTELLIGENCE

2018 actividades

Presentación

Las **amenazas en Internet han evolucionado** de manera que ya no se producen apenas ataques desde un punto de vista considerado clásico hoy en día, es decir, atacando directamente la infraestructura expuesta a internet.

Las amenazas **actuales utilizan capas de infraestructura, productos y servicios** capaces de evadir los controles de seguridad tradicionales, como los productos basados en firmas o en heurísticas clásicas.

El **enfoque actual de seguridad** de la información debe evolucionar hacia un modelo más agresivo y dinámico basado en el conocimiento profundo de este tipo de amenazas para defender nuestra infraestructura e información.

El **objetivo principal de este taller** no pretenden ser un manual académico sobre fundamentos de seguridad y amenazas. No busca ceñirse a una estructura rígida, sino ir evolucionando desde una visión básica, hacia un entendimiento más profundo de las amenazas y presentar distintas técnicas que permitan a los asistentes estar un paso por delante sobre las amenazas en Internet.

Para ello, **se han diseñado diversas sesiones fundamentalmente prácticas** en las que esta visión analítica proporciona a los analistas e investigadores la capacidad de detectar y defenderse contra las nuevas amenazas en Internet, mientras que todavía están madurando.

Durante dichas sesiones **se proporcionarán diversas metodologías prácticas y proactivas** que den visibilidad sobre las nuevas amenazas sofisticadas y evasivas.

Inscripción

Es **gratuita y se realizará** a través de un formulario habilitado en la página web del IUISI:
http:\\www.iuisi.es

Link formulario: https://goo.gl/DiBXVG

Objetivos

En este taller **se pretender ofrecer** a los asistentes acceso a una nueva mentalidad a la hora de tratar la inteligencia y hacer frente a las amenazas emergentes.

Esta visión analítica dota a los analistas de la capacidad de detectar y defenderse contra las nuevas amenazas en Internet, mientras que todavía están madurando.

Finalmente, **el objetivo de estos talleres es** el de proporcionar metodologías prácticas y proactivas que den visibilidad sobre las nuevas amenazas sofisticadas y evasivas.

Destinatarios

Miembros de las FCSE y otras AAPP dedicados a la investigación tecnológica y/o a la mitigación de incidentes

Plazo de Inscripción abierto hasta las 23:00 del día 05 de abril.

Programa

Lunes 09 de Abril

9:00 – 9:30 Inauguración.

9:30 – 11:50 **Taller 1: "Obtención De Información En Fuentes Abiertas (OSINT)"**
Ponente: Javier Rodríguez
(Cybersecurity & CyberIntelligence Manager en TARLOGIC)

11:50 – 12:20 DESCANSO

12:20 – 15:30 Continuación Taller 1

15:30 Fin de la Jornada

Martes 10 de Abril

09:00-11:30 **Taller 2: "Minería De Datos y Generación Relaciones"**
Ponente: Javier Rodríguez
(Cybersecurity & CyberIntelligence Manager en TARLOGIC)

11:30-12:00 DESCANSO

12:00-15:00 **Taller 3: "Análisis de Redes Sociales y OSINT dirigido a Personas"**
Ponente: Javier Rodríguez
(Cybersecurity & CyberIntelligence Manager en TARLOGIC)

15:30 Fin de la Jornada

Programa

Miércoles 11 de Abril

10:00-12:00 **Taller 4: "Introducción al Threat Intelligence"**
Ponente: Manuel Quintans (Senior Malware Researcher en S21Sec)

12:00-12:30 DESCANSO

12:30-14:30 Continuación Taller 4

14:30-15:30 DESCANSO COMIDA

15:30-17:30 Continuación Taller 4

17:30 Fin de la Jornada

Jueves 12 de Abril

10:00-12:00 **Taller 5: "Threat Intelligence Research"**
Ponente: Manuel Quintans (Senior Malware Researcher en S21Sec)

12:00-12:30 DESCANSO

12:30-14:30 Continuación Taller 5

14:30-15:30 DESCANSO COMIDA

15:30-17:30 Continuación Taller 5

17:30 Fin de la Jornada

Viernes 13 de Abril

10:00-12:00 **Taller 5: "Threat Intelligence Research"**
Ponente: Manuel Quintans (Senior Malware Researcher en S21Sec)

12:00-12:30 DESCANSO

12:30-14:00 Continuación Taller 5

14:00-14:15 CLAUSURA

Descripción del contenido

Taller 1 - Obtención De Información En Fuentes Abiertas (OSINT)

Duración: 05 horas
Temario:
Introducción al OSINT.

OSINT vs WEBINT.

El Ciclo de inteligencia OSINT.

Enumeración y conocimiento de técnicas de análisis.
(ACH / DAFO / Reformulación / Indicadores / Mindmaps)

Enumeración y conocimiento de herramientas de obtención

Diseño de checklist.

Taller 2 - Minería De Datos y Generación Relaciones

Duración: 02 horas
Temario:
Metodología "Systemic Operational Design".

Introducción/objetivos.

Comprensión de la comunidad virtual.
• SNA
• Grafos.

Taller 3 - Análisis de Redes Sociales y OSINT dirigido a Personas

Duración: 03 horas
Temario:
Obtención de información.
• Buscadores
• Optimización de búsquedas/Dorks.
• Buscadores específicos.

Técnicas de obtención de información:
• Facebook.
• Twitter.
• LinkedIn.

Análisis y Elaboración.

Descripción del contenido

Taller 4 - Threat Intelligence

Duración: 08 horas

Temario:

Conoce a tu enemigo

Teoría de las amenazas

Tipos de amenazas

Evolución de las amenazas

Estado actual de las amenazas

Modelado de amenazas

Ciclo de vida de las amenazas

Malware Research

Intelligence Research

Taller 5 - Intelligence Research

Duración: 08 horas

Temario:

Introducción al mundo Underground

Open Source Intelligence

Intelligence Crawling

Malware Crawling

Monitorización de actores

Análisis con grafos

Monitorización de campañas

Monitorización de Botnets

Evaluación final.

OSINT
OPEN SOURCE INTELLIGENCE

Material necesario

El personal que participe en el curso deberá estar equipado con lo siguiente:

Ordenador portátil:
- Sistema operativo Windows.
- Office 2003 en adelante
- Software para ejecución de máquinas virtuales (VM Player o Virtual Box)

Perfiles creados específicamente para el curso en RRSS:
- Facebook
- LinkedIn
- Twitter.

Direcciones de correo electrónico creados específicamente para el curso en:
- Gmail.
- Yahoo
- Hotmail.

Conocimientos recomendados

- Nociones sobre arquitectura y funcionamiento de Internet (DNS, TCP/IP, …etc.)
- Conocimientos básicos sobre Teoría General de Sistemas Operativos (Estructuras de ficheros, ejecución de procesos, comunicaciones, …etc.)
- Experiencia en la investigación tecnología y el análisis de dispositivos.