Defensive and offensive steganography

Hands on keyboard

Madrid 3 de Marzo de 2025

DOSSIER DE FORMACIÓN

/Rooted

Del 3 al 5 de Marzo

Tres días de trainings y Workshops

HOTEL Eurostars iHotel
C. de Virgilio, 4, 28223, Madrid
Pozuelo de Alarcón

Del 6 al 8 de Marzo

Ponencias presentadas por speakers internacionales y expertos técnicos.

KINEPOLIS Ciudad de la Imagen
C. Edgar Neville, s/n
Pozuelo de Alarcón

Presentación

- **Misión**: Queremos compartir conocimientos, atraer diferentes culturas, exponer el talento local y marcar la diferencia.
- **Visión**: Ser responsables haciendo algo diferente, compartiendo cultura y construyendo una red de conocimiento. Ser un evento honesto, confiable, beneficioso y establecer alianzas y colaboraciones con socios, clientes y competidores.
- **Nuestra cultura ganadora y nuestros valores en vivo:** Colaboración, diversidad, talento por todas partes, pasión, calidad y enfoque en los clientes (cada persona que asiste a nuestros eventos).

Profesor: Dr. Alfonso Muñoz

Leading Cybersecurity and AI | Principal Offensive Security and Cryptography/Steganography “expert” – Founder Criptored

PhD. in Telecommunications Engineering from the Polytechnic University of Madrid (UPM, 2010) and postdoctoral researcher in computer network security at the University Carlos III of Madrid (UC3M). A well known professional and hacker had been a cybersecurity Tech Lead for more than 20 years and has published more than 60 academic publications, books (6), patents (2) and computer security tools. He has also worked in advanced projects with US/ASIA/European Organisms, public bodies and multinational companies (global 500). For over almost two decades, he has been involved in security architecture design, penetration tests, forensic analysis, mobile and wireless environments, and information security research (leading technical and scientific teams). Alfonso frequently takes part as a speaker in hacking and cybersecurity conferences [STIC CCN-CERT (5), DeepSec, HackInTheBox (3), Virus Bulletin, Ekoparty, BlackHat USA, BlackHat Europe, BlackHat Asia, BSIDES Panama, RootedCon (12), 8.8, UAD360, Summer Bootcamp INCIBE, No cON Name (3), GSICKMinds, C1b3rwall academy, Cybercamp, Secadmin, JNIC, Ciberseg,X1RedMasSegura, Navaja Negra (4), T3chfest (3), Shellcon, H-c0n...] and commercial and academic security conferences (+100 talks).

He is certified as CISA, CISSP, CEHv8, CHFIv8, CES, CriptoCert Certified Crypto Analyst, OSWP and CCSK. His work as a cybersecurity professional has been recognized by numerous academic and professional awards, including in 2018 as one of the 25 most influential people in Spain in the field of cybersecurity and in 2019 as one of the 50 most relevant people in the protection of digital assets. Recently, SIC magazine award 2024.

He has been interviewed by the main Spanish media and is often consulted on issues of social impact arising from cyber security and privacy. He is a professor in different cybersecurity masters in public and private universities, as well as co-editor of the thematic network CRIPTORED, the oldest and most impacting network in Spain and Latin America on these issues (cybersecurity awareness). This network has received recognition and awards from the most significant actors in the cybersecurity community in Spain (Red-Seguridad Magazine, SIC Magazine, Antonio Ropero-RootedCon Awards, etc.).

Objetivos

El objetivo de este taller es entender y practicar las técnicas y herramientas esteganográficas desde un punto de vista defensivo y de ataque. Taller eminentemente práctico se pondrá foco en tres aspectos: uso de la esteganografía como ciencia anti-forense dificultando la detección de información en sistemas de ficheros y sistemas operativos, esteganografía práctica en contenido multimedia y esteganografía aplicada a malware.

A quién va dirigido

- Profesionales relacionados con la protección de la información
- Profesionales dedicados a la seguridad ofensiva o hacking ético
- Profesionales IT, infraestructuras de red, SOCs, etc.
- Profesionales forenses/DFIR
- Administración pública y FCSE
- Especialistas en ingeniería inversa/malware
- Estudiantes TIC
- …

Requisitos: Conocimientos

Conocimientos básicos de:

- ✓ Informática – Sistemas operativos Windows – Linux
- ✓ Conocimientos básicos de seguridad informática
- ✓ Deseable, aunque no imprescindible, conocimiento de programación. Ej, Python

Requisitos: Técnicos

Para el correcto funcionamiento del training será necesario que los alumnos dispongan de equipos con acceso de administrador para poder añadir, eliminar software o cambiar cualquier configuración del mismo.

Las máquinas deben contar con las siguientes características mínimas:

- ✓ Sistema operativo Windows 7 o superior y distribución Linux. Alguna de las dos o ambas pueden estar virtualizadas
- ✓ 8GB de memoria RAM

Guía de Contenidos:

El taller tendrá una duración estimada de 8 (+1) horas en la que se cubrirá de manera global los principales conceptos y herramientas para utilizar la esteganografía en múltiples escenarios. A continuación, se adjunta una planificación aproximada.

1. Espionaje masivo de las comunicaciones. Privacidad y fuga de información (30 min)

2. Definición de conceptos de esteganografía y estegoanálisis. Técnicas y variantes (30 min)
3. Técnicas esteganográficas “anti-forenses” (1h)
    - Ocultación práctica en sistemas operativos
    - Ocultación en sistemas de ficheros
    - Esteganografía en código ejecutable
    - Esteganografía en lenguajes de marcado y programación
4. Ocultación práctica en contenido multimedia. Técnicas y uso de herramientas esteganográficas (2:30h)

Guía de Contenidos II

5. Estegomalware y polyglots. Fuga de información y covert channels (2:30h)

Arquitectura de Command and Control. Técnicas esteganográficas en malware
Evasión de antivirus con técnicas esteganográficas. DEMOS
Detección de APTS esteganográficos - Estegoanalisis. DEMOS
Estrategias de detección y herramientas de estegoanálisis

Eliminación de APTs con ataques activos. CDR (Content Disarm and Reconstrution). DEMOS
Esteganografía en redes sociales. Evasión de filtrado y eliminación de esteganografía
Reversing de estegomalware en Android

Polyglots. Autoejecución de estegomalware y uso de herramienta Powerglot

Bonus track: Ocultación lingüística. Ocultando información en lenguaje natural y uso de IA (1h)

Costes

El precio final de este **RootedLAB** es **250 €**

Puedes registrarte y formalizar el pago en: https://reg.rootedcon.com

IMPORTANTE:
Se requiere un mínimo de **DIEZ (10)** asistentes para que el curso pueda celebrarse.

FAQ

1. ¿Dónde se celebra la formación?
   - Las formaciones se celebran en **Eurostars I-hotel C/Virgilio,4 28223, Pozuelo de Alarcón (Madrid)**
   - Aquí puedes encontrar el mapa de la zona: Google Maps
2. ¿Qué diferencia hay entre BootCamp y RootedLab?
   - Diferenciamos los trainings por horas de formación. Un **RootedLab tiene 8 horas** de formación, mientras que un **BootCamp tiene unas 24h**.
3. ¿Qué horario tiene la formación?
   - La formación comienza a las 9 de la mañana, pero procura estar un poco antes para poder acreditarte y tener tu portátil preparado. El primer día recomendamos estar a las 8.
   - Las formaciones suelen acabar entre las 19h y 20h.
4. ¿Cómo puedo registrarme?
   - Para el registro, ve directamente al Rooted Manager: https://reg.rootedcon.com. Ahí, una vez registrado podrás seleccionar la formación y pagar directamente. Una vez se imparta la formación podrás solicitar la factura siguiendo los pasos indicados.
5. ¿Puedo pagar con transferencia bancaria?
   - Si, desde el propio Rooted Manager podrás gestionar el pago mediante transferencia bancaria.
6. ¿El training incluye comida?
   - Los trainings **no incluyen comida**. Pero hay varias opciones en la zona, y el profesor os dará más información.

/Rooted

Contacto:
info@rootedcon.com