/Rooted

Defensive and offensive steganography

Hands on keyboard

MADRID

7 al 9 de Marzo de 2022

DOSIER DE FORMACIÓN

/Rooted

Días 7-9 de Marzo

Tres días de trainings y workshops

HOTEL Eurostars iHotel
Pozuelo de Alarcón

Días 10-12 de Marzo

Ponencias presentadas por speakers internacionales y expertos técnicos.

KINEPOLIS
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 congresos).

Objetivos

En este training, orientado a la práctica del hacking y la protección de comunicaciones, podrás introducirte y sentar bases en la disciplina de la esteganografía desde un punto de vista práctico. Esta disciplina es necesaria para perfiles centrados en la protección de comunicaciones, seguridad ofensiva y hacking ético, respuesta ante incidentes o expertos forenses, etc. Se cubrirá la ocultación en contenido multimedia, protocolos de comunicaciones (covert channels), sistemas de ficheros y formatos, esteganografía lingüística, estegomalware, etc.

Aunque es necesario cubrir teoría, el taller se diseña para ser eminentemente práctico para practicar ataque y defensa utilizando conceptos y herramientas esteganográficas.

El conocimiento de este taller le permitirá adicionalmente diseñar sus propios mecanismos de protección a medida y entender los de terceros.

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
- …

/Rooted

Profesor: Dr. Alfonso Muñoz

Head of Cybersecurity Unit & cybersecurity research | Principal Offensive Security and Cryptography/Steganography Expert @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 with more than 19 years of experience, he has worked in advanced projects with European organizations, law enforcement agencies and multinationals (global 500 and IBEX-35). For more than a decade he has been involved in the design of secure architectures, technical security assessment (hacking), forensic analysis and security in mobile environments and wireless networks, leading technical and scientific research and innovation teams.

Alfonso is a regular speaker at the main cybersecurity conferences (STIC CCN-CERT, DeepSec, HackInTheBox, Blackhat, Ekoparty, Virus Bulletin, RootedCon, 8.8, No cON Name, GSICKMinds, Cybercamp, Secadmin, JNIC, Ciberseg, X1RedMasSegura, Navaja Negra, T3chfest, etc.), has published more than 60 publications of impact in the area (IEEE, ACM, JCR, ...), patents (2), books (5) and opensource cybersecurity tools. 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.

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.).

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

Agenda (i)

El taller tendrá una duración estimada de 8 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 (1h)
    a. Limitaciones de la criptografía, criptoanálisis y retos futuros
2. Historia de la esteganografía. Conexión con técnicas modernas (30 min)
3. Definición de conceptos de esteganografía y estegoanálisis. Técnicas y variantes (30 min)
4. Ocultación y detección de esteganografía en contenido multimedia (2h)
    a. Técnicas y uso de herramientas esteganográficas. Demos
    b. Técnicas y herramientas de estegoanálisis (visual, estadístico, EoF, fuerza bruta, …). Demos y reversing
    c. Técnicas y herramientas de esteganografía avanzada. Reducción de impacto

Agenda (ii)

5. Esteganografía en sistemas operativos, sistemas de ficheros y formato de ficheros (1h)
    a. Esteganografía en sistemas ficheros (fragmentación, borrado, sectores, volúmenes ocultos, ads, …)
    b. Esteganografía en código ejecutable y evasión de AV con esteganografía y compresión.
    c. Esteganografía en lenguajes de marcado
    d. …
6. Network steganography y covert channels (1h)
    a. Herramientas y conceptos para covert channels en multitud de protocolos de la torre TCP/IP
    b. Demos y evasión de DLPs: Mística/Wireshark, Cloakify, …
7. Esteganografía en malware y polyglots (1h)
    a.…
    b. Reversing de estegomalware en APP Android
    c. Creación de polyglots con Powerglot
8. Esteganografía en Internet y redes sociales. Evasión de filtrado y eliminación de esteganografía (30 min)
9. Esteganografía lingüística y textual (30 min – 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.

/Rooted

FAQ

- Dónde se celebra la formación?
  - A diferencia del Congreso RootedCON, las formaciones se celebran en el Hotel Eurostarts i-Hotel
  - Aquí puedes encontrar el mapa de la zona: Google Maps
- Qué diferencia hay entre BootCamp y RootedLab?
  - Diferenciamos los training por horas de formación. Un RootedLab tiene 8 horas de formación, mientras que un BootCamp tiene unas 24h.
- 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.
- Como puedo registrarme?
  - Para el registro, ve directamente al RootedManager: 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.
- Puedo pagar con transferencia bancaria?
  - Si, desde el propio RootedManager podrás gestionar el pago mediante transferencia bancaria.
- El training incluye comida?
  - Los training no incluyen comida. Pero hay varias opciones en la zona, y el profesor os dará más información.

/Rooted

Contacto:

info@rootedcon.com