/Rooted

Pentesting a SmartContracts & Web3

MADRID

6 de Marzo de 2024

DOSIER DE FORMACIÓN

/Rooted

Días 4-6 de Marzo

Tres días de trainings y workshops

HOTEL Eurostars iHotel
Pozuelo de Alarcón

Días 7-9 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).

Profesor: Pablo González

Máster Universitario en Seguridad Informática por la Universidad Internacional de La Rioja. Ingeniero en Informática por la Universidad Rey Juan Carlos. Ingeniero Técnico en Informática de Sistemas en la Universidad Rey Juan Carlos. Premio al mejor expediente de su promoción en la Universidad Rey Juan Carlos y Premio Extraordinario Fin de Carrera en Ingeniería Técnica en Informática de Sistemas. MVP Microsoft Security desde 2017.

Trabaja en Telefónica como Responsable del Departamento de Ideas Locas del área CDO. Es docente y Director en el Máster de Seguridad de Tecnologías de la Información y de las Comunicaciones en la Universidad Europea de Madrid. Además, es docente en otros másteres de seguridad de la información. Trabajó en Informática64 durante 4 años en Formación, Consultoría y Auditoría.

Tiene diversas publicaciones en el ámbito de la Seguridad de la Información en la editorial 0xword

Pablo ha impartido formación en Rooted CON 2013-2019. También ha sido docente en los Labs de No cON Name 2013 y 2014 con Metasploit para Pentesters. Ha sido ponente en Rooted CON 2013, 2014, 2016, 2018 y 2019, No cON Name, Navaja Negra y otros congresos como Hackron, Sh3llCon, Cybercamp o Rooted Valencia, entre otros. Ponente en congresos internacionales como la Black Hat Europe Arsenal 2017, 2018 y 2019, BlackHat USA 2020, BlackHat Europe 2022, 8dot8 en 2014,2018 y 2019, EkoParty 2018, LeHack 2019, Bsides Colombia en 2016 o el IEEE SBS Gold en 2012. Fundador de hackersClub Academy

Objetivos

Entender el contexto de la web3 y de los SmartContracts

Conocer metodología para realizar pruebas de intrusión y análisis de seguridad en un proyecto web3

Conocer vulnerabilidades que pueden afectar a un proyecto Web3 (en sus distintos ámbitos)

Practicar sobre entornos de SmartContracts y detectar vulnerabilidades

Aprender cómo llevar a cabo proyectos con SmartContracts mejorando su seguridad

A quién va dirigido

- Profesionales del sector de la Seguridad de la Información
- Estudiantes
- Administradores de sistemas y redes
- Desarrolladores que quieran mejorar su perfil
- Cuerpos y Fuerzas de Seguridad
- Docentes

Requisitos: Conocimientos

Conocimientos básicos de:

- ✔ Aplicaciones web
- ✔ Ciberseguridad y vulnerabilidades (básico)

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:

- ✔ Mínimo 8 GB RAM de memoria. Recomendable 8-12 GB RAM.
- ✔ Software de virtualización Virtual Box o Hyper-V (VMWare también es viable)
- ✔ Se facilitará información sobre software a instalar (se instala rápido, no hace falta traerlo)
- ✔ Docker instalado y funcionando (Opcional)

Contenido

En este taller se mostrará cómo llevar a cabo un pentesting a SmartContracts (y web3) y cómo detectar vulnerabilidades realizando pruebas de tipo SAST y de tipo DAST. Se mostrarán propuestas de estándares y metodología para llevar a cabo estas auditorías. Además, se mostrarán algunas de las principales herramientas OpenSource para aplicar metodología en el mundo web3.

Se parte de una introducción al ecosistema web3 dotando al alumno de los recursos y explicaciones necesarias para poder entender cómo funciona la web3. Se mostrará de forma práctica un entorno local dónde desplegar una blockchain, utilizar un Wallet y disponer de la posibilidad de desplegar de manera sencilla contratos. La idea es que el alumno se familiarice rápidamente con el laboratorio y con todas las herramientas (opensource) necesarias para crear el laboratorio.

La base y la comprensión entre el cambio del mundo web2 al mundo web3 es importante, por eso se dota al taller de esta transición (mostrando paralelismos). La mayoría de los proyectos (en el mundo real) serán web2.5, dónde se juntan tecnologías web2 con tecnologías web3. El pentester deberá conocer ambos mundos para poder aplicar sus conocimientos sin las barreras de entrada de estos mundos.

Contenido

Se expone una parte de metodología con el objetivo de facilitar las bases de auditoría y conocer las principales vulnerabilidades que existen en estos proyectos de web3 (focalizando energía en los SmartContract). Se explicarán técnicas de detección de vulnerabilidades basadas en SAST y DAST.

Además, se utilizará una plataforma (parecido a un CTF) para llevar a cabo algunas pruebas y ejercicios en el taller. Todas las pruebas son desarrolladas por el docente.

Agenda (i)

1- Introducción a web3 (blockchain, wallet/EOA, smart contract, transacciones, dapps, etc)

1.1- Relación web2 y web3

2- Montaje entorno de pruebas y laboratorio (Montaremos un laboratorio de 0 en pocos minutos para ir realizando el taller sobre dicho laboratorio)

3 - Clasificación de vulnerabilidades (éstas se explicarán de forma esquemática y se explicarán a través de contratos de ejemplo. Además, en algunos casos se ejecutarán dichos contratos en blockchain local para que el alumno pueda ver la vulnerabilidad paso a paso).

Ejemplos de vulnerabilidades: Re-Entrancy, Denegación de servicio, Gas DOS, Tx.Origin, Ice-Phishing, Signature Replay, etc.

Agenda (ii)

4 - Pruebas que verificar con análisis estático (aquí se estudian las pruebas mediante el uso de herramientas OpenSource como, por ejemplo, mythrhil o slither y se muestran ejemplos. También se estudiará el bytecode, los Opcodes y el ABI). Todo con enfoque práctico.

5 - Pruebas que verificar con análisis dinámico (aquí se despliegan contratos sobre blockchain local o testnet y se lleva a cabo el uso de metodología para detectar vulnerabilidades a través de técnicas de interacción con las funciones, fuzzing, etc)

Agenda (iii)

6 - Plataforma CTF para ir poniendo en práctica todo lo visto en el taller. Retos originales y preparados por el docente.

7 - Parte final. Se propone un ejercicio (modo CTF) para que los alumnos lo hagan en casa (se explica el entorno)

8 - Conclusiones

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 **SEIS (6)** asistentes para que el curso pueda celebrarse.

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