FORMACIONES TÉCNICAS / ROOTEDLABS

Panamá 2024

/Rooted®

/Rooted®

Introducción

Introducción

- El objetivo principal de esta formación es la utilidad. Todos los temas se enfocarán desde un punto de vista pragmático y aplicable.
- Naturalmente, se introducirán conceptos teóricos y elementos de apoyo que se consideren relevantes, pero en todo momento se busca el valor directo e inmediato para el alumno.
- Aunque las temáticas son muy técnicas, también existen objetivos académicos en gestión.

Sobre los formadores

Pablo San Emeterio

@psaneme | mailto:pablo@vapasec.com

- Premio 2019 Revista SIC Mejor proyecto de comunicación y 2016 Jorndas JNIC Mejor herramienta de innovación
- Jefe de Servicios Ofensivos y Threat Intelligence en Telefonica durante 8 años
- Fundador y Director Ejecutivo de VAPASEC
- Más de 20 años de experiencia en el sector de la ciberseguridad en empresas como Optenet y Telefónica.
- Codirector del programa de radio CiberAfterWork de Capital Radio en el que se acerca la seguridad a empresas y ciudadanos todos los lunes

Sobre los formadores

Román Ramírez Giménez
@patowc | mailto:rramirez@rootedcon.com

- Premio a la trayectoria profesional otorgado por el Ministerio de Defensa/ CCN-CERT.
- Cruz blanco de la Guardia Civil (medalla orden del mérito).
- Responsable de arquitectura de seguridad en Ferrovial durante 10 años.
- Cofundador de RootedCON.
- Cofundador y CEO de BE Real Talent, propaganda · is.
- Más de 30 años en el sector de la ciberseguridad y la tecnología, habiendo desarrollado funciones en empresas tales como TB-Solutions (Intercomputer/encomIX), PSINet, eEye Digital Security, PricewaterhouseCoopers o Ferrovial.

Esquema de las formaciones

- RT-LAB-01: Introducción al **exploiting**. En noventa minutos se hará una introducción a la creación de exploits para desbordamientos de pila y algunos otros enfoques.
- RT-LAB-02: Introducción al **reversing**. Aunque algunos conceptos se habrán observado en el laboratorio anterior, en esta sección se aprenderá a manejar herramientas y técnicas de ingeniería inversa con Ghidra, radare2 e IDA.
- RT-LAB-03: Introducción a Frida y el reversing/explotación de aplicaciones móviles y otras.

RT-LAB-01
Introducción al exploiting

/Rooted®

RT-LAB-01: Introducción al exploiting

- REQUISITOS DE CONOCIMIENTO:
  - Necesario conocimientos básicos de computadoras.
  - Deseable conocimientos básicos de servicios de Internet y redes
  - Deseable conocimientos básicos de programación
- REQUISITOS DE EQUIPO:
  - Ordenador portátil con capacidad de virtualización
  - Al menos 4GB de RAM disponibles para una máquina virtual
  - VirtualBox, VMWARE u otras herramientas de virtualización

RT-LAB-01: Introducción al exploiting

- Esquema formativo:
  - Introducción a la arquitectura de computadoras
  - Diferencias importantes entre 32 y 64 bits
  - La pila (stack)
  - Ataques de desbordamiento de pila
  - Protecciones contra estos ataques
  - Ejercicios: ataques a ejecutables en Windows 32 bits
  - Ejercicios: ataque a un ejecutable en Linux 32 bits
  - Ejercicios: explotación de navegadores

Temas que se van a ver dentro del contenido

- Temáticas de referencia:
  - Stack Buffer Overflow
  - Detección de bad characters
  - Medidas de mitigación 1 (stack cookies)
  - Bypass stack coockies
  - SEH, medidas de mitigación 2 (DEP, ASLR)
  - Bypass DEP
  - Bypass ASLR
  - Explotación de navegadores

RT-LAB-02
Introducción al reversing

/Rooted®

RT-LAB-01: Introducción al reversing

- REQUISITOS DE CONOCIMIENTO:
  - Necesario conocimientos básicos de computadoras.
  - Deseable conocimientos básicos de servicios de Internet y redes
  - Deseable conocimientos básicos de programación
- REQUISITOS DE EQUIPO:
  - Ordenador portátil con capacidad de virtualización
  - Al menos 4GB de RAM disponibles para una máquina virtual
  - VirtualBox, VMWARE u otras herramientas de virtualización

RT-LAB-02: Introducción al reversing

- Esquema formativo:
  - Introducción a la ingeniería inversa
  - Cómo leer ensamblador de forma eficaz
  - Cómo analizar la estructura de un programa
  - Seguir y controlar la ejecución de un programa
  - Introducción a Ghidra
  - Introducción a radare2
  - Introducción a IDA Pro
  - Cómo continuar

Temas que se van a ver dentro del contenido

- Temáticas de referencia:
  - Examen preliminar de ejecutables
  - Imports y exports
  - Entender los distintos recursos de información de las herramientas
  - Seguimiento de la lógica de ejecución
  - Breakpoints
  - Buscar cadenas, funciones y otros elementos

RT-LAB-03
Introducción a Frida (+aplicaciones móviles)

/Rooted®

RT-LAB-01: Introducción al reversing

- REQUISITOS DE CONOCIMIENTO:
  - Necesario conocimientos básicos de computadoras.
  - Deseable conocimientos básicos de servicios de Internet y redes
  - Deseable conocimientos básicos de programación
- REQUISITOS DE EQUIPO:
  - Ordenador portátil con capacidad de virtualización
  - Al menos 4GB de RAM disponibles para una máquina virtual
  - Android Studio y el emulador de dispositivos de Android

RT-LAB-03: Introducción a Frida

- Esquema formativo:
  - Breve introducción a la instrumentación binaria dinámica (DBI).
  - Instalación de Frida y objection.
  - Usos típicos de Frida en entorno móvil.
  - Configuración de Burp, autoridades de certificación e intercepción de tráfico ssl de aplicaciones.
  - Engañando al GPS, a los sensores, al antiroot y al pinning.
  - Uso avanzado de Frida en Windows 64 bits.

Temas que se van a ver dentro del contenido

- Temáticas de referencia:
  - Creación de un terminal Android virtualizado
  - Examen de aplicaciones Android
  - Hookear aplicaciones en Android
  - Hookear y jugar con aplicaciones en Windows 11
  - Evadir los mecanismos antiroot
  - Evadir el certificate pinning
  - Engañar a los sensores del terminal: GPS

REGALO

- Los asistentes a este laboratorio recibirán una copia gratuita del libro “Beginning Frida” escrito por Román Ramírez en colaboración de Pablo San Emeterio.

/Rooted®

PRECIOS

Precios de los laboratorios

#	Laboratorio	Detalle	Total ($)
1	**RT-LAB-01** **Introducción al exploiting**	Técnicas de exploiting en Win32, algunos ejemplos en Win64 y Linux.	$144,80
2	**RT-LAB-02** **Introducción al reversing**	Introducción al reversing con Ghidra, IDA Pro y radare2 (y otras herramientas interesantes).	$164,80
3	**RT-LAB-03** **Introducción a Frida**	Introducción a Frida y a la ingeniería inversa de aplicaciones móviles. Otros usos en Windows 11.	$136,90

Muchas gracias.

/Rooted

CCN-CERT centro criptológico nacional

20 ANIVERSARIO Centro Criptológico Nacional