Escalada de privilegios y persistencia en Linux

Valencia

15 Octubre 2024

DOSSIER DE FORMACIÓN

/Rooted

Día 15 de Octubre

Formaciones

ADEIT Fundación Universidad-Empresa de la Universidad de Valencia.

Día 16 de Octubre

Ponencias presentadas por speakers internacionales y expertos técnicos.

Ciudad de las Artes y las Ciencias Valencia

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: Manuel González Regal

- Catedrático de Informática en ciclos de Formación Profesional (FP) en Xunta de Galicia
- Docente de los módulos de *Hacking ético* en el curso de especialización de FP en Ciberseguridad en entornos IT y de *Seguridad y alta disponibilidad* en el ciclo superior de Administración de sistemas informáticos en red
- Ponente y formador en talleres en MorterueloCON (2022, 2023 y 2024), ViCON (2023 y 2024), Encuentro Gallego de Ciberseguridad - CiberGAL (2023 y 2024), Jornadas de Ciberseguridad en la FP de Galicia (2024), …
- Más de 16 años de experiencia impartiendo formación sobre ciberseguridad y ganador de varios premios de innovación educativa de FP en materia de ciberseguridad
- Certificaciones: OSCP, OSWP, BTL1

Objetivos

Al hablar de GNU/Linux nos referimos a un sistema operativo presente en el 100% de los supercomputadores, en más del 80% de los servidores y en una amplia gama de dispositivos como móviles, routers, televisores, …

Conocer y aplicar las técnicas de elevación de privilegios y persistencia en estos sistemas es de gran importancia, tanto para aquellos que se dedican a la seguridad ofensiva como a la seguridad defensiva, por lo que en las prácticas del taller:

- se explicarán los conceptos de escalada de privilegios y persistencia
- se realizará una enumeración exhaustiva de los sistemas vulnerables para encontrar vías de escalada de privilegios
- se aplicarán diversas técnicas de escalada de privilegios y persistencia, entendiendo los principios en que se basan y su posible impacto en los sistemas
- se explicarán los rastros que dejan las acciones realizadas durante la escalada de privilegios y persistencia, y que permitirán su detección

A quién va dirigido

- Profesionales del sector de la Seguridad de la Información, tanto del ámbito ofensivo como defensivo
- Administradores de sistemas y/o redes
- Estudiantes
- Docentes
- Cuerpos y Fuerzas de Seguridad
- Cualquiera que esté interesado en aprender y profundizar en las técnicas de escalada de privilegios y persistencia en sistemas GNU/Linux

Requisitos: Conocimientos

- Conocimientos básicos generales de SO GNU/Linux
  - uso básico de la línea de comandos
  - sistema de ficheros
- Conocimientos básicos en redes TCP/IP
- Conocimientos básicos de virtualización

IMPORTANTE: no se necesita disponer de conocimientos avanzados, ya que en el taller se explicará todo lo necesario

Requisitos: Técnicos

Para el correcto funcionamiento del taller será necesario que los alumnos dispongan de equipos con:

- sistema de virtualización Virtualbox (se proporcionarán máquinas vulnerables en .ova)
- capacidad para ejecutar al menos dos máquinas virtuales simultáneamente
- al menos 8GB de memoria RAM

Guía de Contenidos I

1. Escalada de privilegios y persistencia en la Cyber Kill Chain y en MITRE ATT&CK
2. Escalada de privilegios
    1. Tipos
        - horizontal
        - vertical
    2. Enumeración
        - manual vs automatizada
        - sistema operativo, software, usuarios/grupos, credenciales, red, recursos compartidos, …
    3. Exploits
        - Kernel
        - servicios locales
        - binarios

Guía de Contenidos II

2.4 Credenciales de acceso

- archivos de configuración
- historial
- reutilización de contraseñas
- SSH keys
- ataque de fuerza bruta
- sudo
  - escape a shell
  - abuso de funcionalidad
  - variables de entorno
- grupos especiales (sudo, admin, lxd, docker, …)
- memoria RAM

Guía de Contenidos III

2.5 Configuraciones erróneas

- tareas programadas
  - PATH
  - permisos
  - wildcards
- SUID/SGID
  - abuso de funcionalidad
  - Shared Object Injection
  - variables de entorno
- Capabilities
- NFS
- permisos inadecuados en ficheros sensibles
  - /etc/passwd, /etc/shadow
  - authorized keys
  - …

Guía de Contenidos IV

3. De la escalada a la persistencia
    - creación de cuentas
    - manipulación de cuentas
    - tareas programadas
    - Event Triggered Execution
    - Boot/Logon Initialization Scripts
    - Server software component - web shell
4. Detección
    - historial
    - integridad
    - logs
    - monitorización

Costes

- El precio final de este **RootedLAB** es **175 €**

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

IMPORTANTE:

Se requiere un mínimo de **CINCO (5)** asistentes para que el curso pueda celebrarse.

FAQ

1. ¿Dónde se celebra la formación?
   - Las formaciones se celebran en en el edificio del ADEIT Fundación Universidad – Empresa de la Universidad de Valencia.
   - Plaza Virgen de la Paz, 3 46001 Valencia
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 9:00h de la mañana, pero procura estar un poco antes para poder acreditarte y tener tu portátil preparado. El primer día recomendamos estar a las 8:30h.
   - Las formaciones suelen acabar entre las 18:00h y 19:00h.
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