

Descripción:

Este taller está orientado a profesionales y entusiastas de la ciberseguridad que deseen explorar técnicas de seguridad ofensiva aplicadas a dispositivos de comunicación. Durante el desarrollo del taller, se revisarán los conceptos clave de las redes de comunicación y los principios generales de la seguridad ofensiva. Posteriormente, los participantes identificarán y explotarán vulnerabilidades y debilidades en los sistemas.

Contenido del Taller:

- Conceptos generales de la seguridad ofensiva en redes
- Ataque al plano de administración
- Ataque a funciones de capa 2 y 3

Requerimientos Técnicos:

- Máquina virtual con instalación mínima de Ubuntu 24.04 LTS (4 GB recomendados)
- Máquina virtual con Mikrotik (RAM 768 MB recomendados)
- Conexión a internet

Este taller combina teoría con ejercicios prácticos en un entorno controlado, permitiendo a los participantes aplicar los conocimientos adquiridos en situaciones reales de manera ética y responsable.

Software Utilizado en el Taller:

El desarrollo del taller consiste en la instalación de herramientas y uso de versiones específicas de software, el día del taller se proporcionarán algunos scripts para agilizar el desarrollo de este por lo que se sugiere que por lo menos la versión de Linux sea la indicada. La configuración de herramientas usadas por quien dicta el taller es la siguiente:

VMware Workstation 17.6.0

- Licenciado para uso personal (requiere registro en Broadcom.com para la descarga).
- Versión utilizada: VMware-workstation-full-17.6.0-24238078.exe.
- Descarga: <https://blogs.vmware.com/workstation/2024/05/vmware-workstation-pro-now-available-free-for-personal-use.html>

Ubuntu Desktop 24.04.1 LTS

- Instalación Mínima
- <https://ubuntu.com/download/desktop>

MikroTik CHR (Cloud Hosted Router)

- Se usará la versión 4.60.6 que posee algunas vulnerabilidades
- Descarga para VMware: <https://download.mikrotik.com/routeros/6.40.6/chr-6.40.6.vmdk>
- Descarga para otros hipervisores: <https://download.mikrotik.com/routeros/6.40.6/chr-6.40.6.img.zip>

Consultas

Daniel Pacheco

- daniel.pacheco@usach.cl
- <https://chat.whatsapp.com/L7GSN6Xuq26ATXc3dumlj3>
- <https://www.linkedin.com/in/dpacheco/>