El proceso de enumeración, identificación de vulnerabilidades y explotación es fundamental para cualquier profesional de la ciberseguridad y constituye la base en la preparación para la certificación eLearnSecurity Junior Penetration Tester (eJPTv2). Este proceso permite identificar, evaluar y explotar las debilidades de los sistemas, formando las habilidades prácticas necesarias para la certificación.

1. Enumeración: La enumeración es el primer paso y se enfoca en obtener información detallada sobre los sistemas objetivo en una red. En esta fase, se utilizan herramientas como WhatWeb, que permite identificar tecnologías y versiones de aplicaciones web; arp-scan, para detectar dispositivos conectados a la misma red mediante análisis ARP (Address Resolution Protocol); y Nmap, una herramienta esencial para el escaneo de puertos y servicios. Estas herramientas ayudan a perfilar los sistemas, determinando los servicios y configuraciones de red que podrían ser vulnerables.
2. Identificación de Vulnerabilidades: Una vez enumerados los servicios y versiones de software, se procede a identificar vulnerabilidades específicas asociadas a ellos. Aquí se puede optar por una combinación de investigación manual y herramientas automatizadas. En este caso, Metasploit, una plataforma poderosa integrada en Kali Linux, facilita la identificación y explotación de vulnerabilidades conocidas. Metasploit permite buscar exploits específicos para cada sistema o servicio identificado y verificar su aplicabilidad en entornos controlados.
3. Explotación: La última fase, la explotación, se centra en intentar aprovechar las vulnerabilidades detectadas en la fase anterior. Utilizando Metasploit desde Kali Linux, el pentester puede lanzar exploits específicos y ejecutar payloads que permiten acceder o comprometer los sistemas de destino. Esta etapa es crucial para evaluar el impacto de las vulnerabilidades en un sistema real, y también es una competencia clave evaluada en la eJPTv2.

Practicar estas fases utilizando herramientas como WhatWeb, arp-scan, Nmap y Metasploit en entornos de prueba es esencial para la preparación de la eJPTv2. La certificación pone a prueba la capacidad de realizar pruebas de penetración básicas en redes y aplicaciones web, lo que exige una comprensión detallada de la enumeración, la identificación de vulnerabilidades y la explotación de sistemas.

https://youtu.be/TRyugTw-bgg