Introducción al Pentesting con Python y Kali Linux

Jaime A. Parada D.[a]

[a]*Centro de Computación Paralela y Distribuida (CCPD)*
Escuela de Computación – Universidad Central de Venezuela (UCV)
jaime.parada@ciens.ucv.ve

Resumen: Este tutorial de pentesting proporciona una introducción a Kali Linux mostrando a los participantes cómo usar las técnicas de hacking ético y cómo realizar un flujo de trabajo de pentesting profesional utilizando dicha distribución especializada en ciberseguridad. Comienza presentando conceptos de hacking ético y actores de amenazas, para después pasar a enfoques y metodologías de pentesting. Se describen las etapas del pentesting, utilizando un marco teórico así como labortatorios prácticos que utilizan una de las plataformas de pentesting más utilizadas como lo es Kali Linux. Los participantes aprenderán cómo construir su propio entorno de laboratorio de pentesting, realizar reconocimiento pasivo y activo usando OSINT en las organizaciones objetivo, realizar escaneo de vulnerabilidades usando múltiples herramientas como Nessus, y realizar pentesting a nivel de red, sitios web y aplicaciones web.

Palabras Clave: pentesting, pentest, pruebas de penetración, kali linux, ciberseguridad.

1 Introducción

Actualmente vivimos en un mundo cada vez más interconectado. Cada persona, hogar, organización empresa, etc., depende hoy día mucho más que antes de activos tecnológicos, los cuales se encuentran en equipos computadores de hogar, teléfonos inteligentes, equipos computadores de oficina, servidores, entre otros. Además, tendencias tecnológicas han determinado un desplazamiento hacia la computación en la nube, junto a otras tecnologías como lo son la conectivad 5g y el Internet de las Cosas. En este panorama, no es un secreto el aumento significativo de riesgos para la sociedad digital. Diversos estudios señalan el aumento de ataques realizados por ciberdelincuentes. Aunado a esto, los principales marcadores del mercado tecnológico han ya advertido del déficit de profesionales en el área de la ciberseguridad. En este panorama, es conveniente educar a estudiantes de las carreras relacionada con la computación acerca del pentesting. El pentesting es una actividad realizada por hackers éticos, con la finalidad de evaluar algunos de los aspectos más importantes de la postura de ciberseguridad de las organizaciones. En este tutorial, veremos una rápida introducción a este fascinante, y cada vez más importante, campo de la

computación utilizando como herramienta de trabajo el lenguaje de programación python y la distribución de seguridad Kali Linux.

2 Objetivos

General

Proporcionar a los participantes del tutorial una visión teórico práctica del pentesting profesional, empleando como herramienta de trabajo la distribución Kali Linux.

Específicos

- Presentar a los estudiantes la terminología empleada en el mundo del pentesting, así como las metodologías que se utilizan
- Proporcionar una introducción a las tecnologías de virtualización y al sistema operativo Linux (instalación, línea de comandos, bash, scripting y herramientas básicas)
- Presentar escenarios de pentesting empleando el lenguaje de programación python y la distribución Kali Linux, durante las diferentes etapas del pentesting

3 Contenidos del Tutorial

1. Introducción al mundo del Hacking
2. Instalando y configurando Kali Linux
3. Línea de Comandos de Linux, bash scripting y herramientas prácticas
4. Reconocimiento
    1. Recolección de información pasiva
    2. Recolección de información activa
5. Escaneo de Vulnerabilidades
6. Pentesting a nivel de Red
7. Ataques a Aplicaciones Web

4 Metodología

4.1 Duración

El presente tutorial tendrá una duración de 8 horas.

4.2 Público Objetivo

Estudiantes de carreras de informática, computación y sistemas.

4.3 Requerimientos técnicos y operativos

Conocimientos básicos de redes de computadores (protocolos de aplicación y red, dispositivos de red, conceptos de enrutamiento y conmutación).

Conocimientos de programación en python. Si no conoce el lenguaje python, debe al menos saber programar en algún lenguaje de scripting.

Un equipo por partipante que posea la capacidad para ejecutar Oracle VM VirtualBox o Vmware Workstation 15 Pro. La configuración recomendada es la siguiente: Procesador i5 o superior, 300 GB de espacio en almacenamiento secundario, Mínimo de 4GB de RAM (preferiblemente 8GB), conexión a Internet.

4.4 Idioma

El tutorial será dictado en español.

4.5 Resumen curricular del presentador

Jaime Parada es profesor de la Escuela de Computación de la UCV, y adscrito al Centro de Computación Paralela y Distribuida, desde hace 18 años. Egresado de la Licenciatura de Computación de la Universidad de Carabobo, obtuvo su título de Magister en Ciencias de la Computación en la Universidad Central de Venezuela. Su trabajo académico ha estado orientado entre otros al área del High Performance Computing (HPC) y Sistemas Distribuidos. Dentro de estas actividades trabajó en diversos proyectos de investigación nacionales e internacionales (EELA2, etc). Ha participado en grupos de investigación en propagación de ondas sísmicas y sismología computacional en colaboración con organizaciones venezolanas y universidades extranjeras (Fundación Venezolana de Investigaciones Sismológicas - Funvisis, San Diego State University - SDSU). Fue Director de Tecnología en el Ministerio Público de Venezuela y miembro del Consejo Directivo de la Fundación Infocentro. Ha trabajado con organizaciones (PNUD) y empresas privadas (startups tecnológicas) internacionales. En particular, se desempeñó como Director del VenCERT (Sistema Nacional de Gestión de Incidentes Telemáticos de Venezuela), principal ente de

Ciberseguridad de Venezuela. Actualmente se dedica a las áreas de la Ciberseguridad y la Computación en la Nube (Cloud Computing).

Referencias

Kali Linux (https://www.kali.org/)

Penetration Testing Methodologies and Standards – PTES (https://resources.infosecinstitute.com/penetration-testing-methodologies-and-standards/)

OWASP Testing Guide (https://owasp.org/www-project-web-security-testing-guide/v41/)