

Investigación de sistemas operativos y herramientas: QEMU y Nmap

Yossed Mauricio Riaño Páez
Miguel Montaña
Jeferson Hernández

21 de octubre de 2025

Resumen

Este documento presenta una revisión teórica detallada sobre diversas distribuciones Linux, sus enfoques principales y las herramientas QEMU y Nmap. Se explica el papel de la virtualización en la computación moderna, así como la importancia del análisis y la seguridad de red. También se discuten los fundamentos del software libre, la estructura de los sistemas operativos y los principios básicos de auditoría de red. Este trabajo busca consolidar los conocimientos teóricos adquiridos en clase, enfatizando el aprendizaje autónomo y la investigación aplicada.

Índice

1. Introducción	3
2. Sistemas operativos Linux	3
2.1. Debian	3
2.2. Ubuntu	3
2.3. Fedora	3
2.4. Kali Linux	3
2.5. Arch y Manjaro Linux	3
2.6. Otras distribuciones	4
3. Virtualización con QEMU y VirtManager	4
3.1. Conceptos básicos	4
3.2. Ventajas de la virtualización	4
3.3. Proceso general de instalación	4
4. Inspección y auditoría de red con Nmap	4
4.1. Principales modos de escaneo	4
4.2. Importancia en la seguridad	5
5. Conclusiones	5
6. Referencias	5

1. Introducción

Los sistemas operativos basados en Linux representan una de las mayores comunidades de software libre en el mundo. Su versatilidad, seguridad y estabilidad los convierten en la base de servidores, infraestructuras en la nube, sistemas embebidos y equipos personales. Comprender la estructura y funcionamiento de estas distribuciones permite entender mejor la interacción entre hardware, kernel y usuario.

Además, las herramientas de virtualización como QEMU y VirtManager facilitan la creación de entornos de prueba seguros y replicables, ideales para investigación y enseñanza. A su vez, utilidades como Nmap contribuyen a la evaluación de la seguridad de red, detección de vulnerabilidades y análisis de tráfico.

2. Sistemas operativos Linux

Linux no es un único sistema operativo, sino un conjunto de distribuciones que comparten el mismo núcleo (kernel) y difieren en gestión de paquetes, entornos gráficos y objetivos. Entre las más relevantes se encuentran:

2.1. Debian

Debian, creado en 1993, es conocido por su estabilidad, seguridad y amplia comunidad. Se utiliza principalmente en servidores, proyectos científicos y bases de sistemas derivados. Su gestión de paquetes mediante APT ha servido de modelo para otras distribuciones.

2.2. Ubuntu

Ubuntu, basado en Debian, es la distribución más difundida entre usuarios nuevos gracias a su facilidad de uso y soporte comercial. Cuenta con versiones de largo soporte (LTS) y está presente tanto en escritorios como en servidores y nubes empresariales.

2.3. Fedora

Desarrollada con el apoyo de Red Hat, Fedora funciona como plataforma de innovación, incorporando tecnologías recientes antes de que lleguen a Red Hat Enterprise Linux. Su ciclo rápido de actualizaciones fomenta la experimentación.

2.4. Kali Linux

Kali Linux se centra en la ciberseguridad. Incluye herramientas para análisis forense, pruebas de penetración y auditoría de sistemas. Es empleada por profesionales en seguridad informática y en formación académica.

2.5. Arch y Manjaro Linux

Arch Linux prioriza la personalización completa del sistema, mientras que Manjaro facilita su instalación y uso sin sacrificar potencia. Ambas distribuciones promueven el principio “hazlo tú mismo”, fomentando la comprensión técnica del sistema.

2.6. Otras distribuciones

Distribuciones como CentOS, Rocky Linux, Garuda o Alpine complementan el ecosistema, enfocándose en estabilidad, rendimiento o minimalismo según las necesidades del usuario.

3. Virtualización con QEMU y VirtManager

3.1. Conceptos básicos

La virtualización permite ejecutar varios sistemas operativos de manera simultánea sobre una misma máquina física. QEMU (Quick Emulator) es un software de código abierto capaz de emular hardware completo, mientras que KVM (Kernel-based Virtual Machine) permite la virtualización asistida por hardware en procesadores modernos. VirtManager ofrece una interfaz gráfica para gestionar entornos QEMU/KVM.

3.2. Ventajas de la virtualización

- Aislamiento de entornos de prueba.
- Uso eficiente de recursos mediante virtualización de hardware.
- Creación de entornos seguros para formación o auditoría.
- Reducción de costos en infraestructura física.

3.3. Proceso general de instalación

Para implementar máquinas virtuales con QEMU/KVM en Linux:

1. Instalar dependencias: `qemu-kvm`, `libvirt-daemon-system`, `virt-manager`.
2. Habilitar el servicio `libvirt` y agregar el usuario al grupo correspondiente.
3. Crear discos virtuales con el formato `qcow2` y asignar recursos (CPU, RAM, almacenamiento).
4. Configurar interfaces de red (modo puente o NAT) para permitir la comunicación de las VMs.
5. Supervisar las máquinas virtuales mediante VirtManager o la línea de comandos con `virsh`.

4. Inspección y auditoría de red con Nmap

Nmap (Network Mapper) es una herramienta de código abierto utilizada para explorar redes y servicios. Permite conocer los equipos activos, los puertos abiertos, los servicios que se ejecutan y los sistemas operativos involucrados.

4.1. Principales modos de escaneo

- **Descubrimiento de hosts (-sn):** detecta dispositivos conectados a una red sin escanear puertos.

- **Detección de servicios y versiones (-sV):** identifica los programas que atienden en los puertos abiertos y sus versiones.
- **Detección avanzada (-A):** combina múltiples pruebas para determinar sistema operativo, servicios y scripts de seguridad.

4.2. Importancia en la seguridad

El uso de Nmap es fundamental para la gestión de redes empresariales, detección de vulnerabilidades y control de acceso. Permite verificar políticas de firewall y detectar configuraciones erróneas.

5. Conclusiones

El análisis de sistemas operativos Linux demuestra la riqueza y diversidad del ecosistema del software libre. La virtualización con QEMU y VirtManager proporciona una plataforma ideal para el aprendizaje práctico, la experimentación y la simulación de entornos complejos. Finalmente, Nmap representa una herramienta indispensable para comprender la topología y seguridad de una red, integrando los conocimientos de administración, redes y seguridad informática.

6. Referencias

- QEMU Project. *QEMU Documentation*. Disponible en: <https://www.qemu.org/documentation/>
- Virt-Manager Project. *Virt-Manager User Guide*. Disponible en: <https://virt-manager.org/>
- Lyon, G. (2009). *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Insecure.Com LLC.
- Cisco Systems. *Cisco Catalyst 2960 Series Switches Documentation*. Disponible en: <https://www.cisco.com/>
- Stallman, R. (2002). *Free Software, Free Society: Selected Essays of Richard M. Stallman*. GNU Press.
- Tanenbaum, A. (2014). *Modern Operating Systems*. Pearson Education.