# ESCUELA POLITÉCNICA NACIONAL

**FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA**
**DEPARTAMENTO DE ELECTRÓNICA, TELECOMUNICACIONES Y REDES DE INFORMACIÓN (DETRI)**
**CARRERA DE INGENIERÍA EN TELECOMUNICACIONES**
**FUNDAMENTOS DE SEGURIDAD (TELD852)**
**PERÍODO: 2025-B**

---

# LABORATORIO N.º 1

## FAMILIARIZACIÓN CON LAS HERRAMIENTAS DE LABORATORIO: KALI LINUX Y MATLAB

---

## 1. INTRODUCCIÓN

El presente laboratorio tiene como objetivo principal introducir al estudiante en el uso de las herramientas que conforman el entorno de trabajo para la asignatura *Fundamentos de Seguridad*. Este entorno está conformado por **Kali Linux**, una distribución especializada en ciberseguridad y pruebas de penetración, y **MATLAB**, una plataforma de simulación y programación de alto nivel orientada al análisis numérico y al desarrollo de algoritmos criptográficos.

El propósito académico de este laboratorio es promover la **familiarización con herramientas profesionales** utilizadas en entornos reales de seguridad informática, tanto ofensiva como defensiva, y al mismo tiempo reforzar el **componente ético** del ejercicio de la ingeniería. Las actividades deben realizarse exclusivamente en un entorno controlado, evitando toda acción que implique vulnerar sistemas ajenos.

---

## 2. OBJETIVOS

**Objetivo general:**
Familiarizar al estudiante con las herramientas de laboratorio orientadas al análisis de seguridad informática y a la implementación de algoritmos criptográficos.

**Objetivos específicos:**

- Identificar las principales herramientas de Kali Linux destinadas a la recolección de información, explotación de vulnerabilidades y análisis forense.
- Explorar MATLAB como entorno para la simulación e implementación de algoritmos de cifrado clásico, moderno, simétrico y asimétrico.
- Comprender el funcionamiento básico de las funciones hash y los certificados digitales.
- Analizar los resultados obtenidos y reflexionar sobre la aplicación ética de estas herramientas.

---

## 3. FUNDAMENTOS TEÓRICOS

### 3.1. Kali Linux

Kali Linux es una distribución de código abierto basada en Debian, diseñada para pruebas de penetración y auditorías de seguridad. Incluye un conjunto amplio de herramientas clasificadas en diferentes categorías, entre las cuales destacan:

| Categoría | Herramientas principales | Descripción |
|---|---|---|
| **Information Gathering** | `nmap`, `whois`, `dnsenum`, `theHarvester` | Permiten recolectar información sobre hosts, dominios, servicios y direcciones IP. |
| **Vulnerability Analysis** | `OpenVAS`, `Nikto`, `Nessus` | Identifican vulnerabilidades presentes en servicios o configuraciones inseguras. |
| **Exploitation Tools** | `Metasploit Framework`, `Social Engineer Toolkit (SET)`, `BeEF` | Permiten explotar vulnerabilidades con fines educativos o de prueba controlada. |
| **Wireless Attacks** | `airmon-ng`, `airodump-ng`, `aircrack-ng` | Análisis y pruebas de seguridad en redes inalámbricas. |
| **Forensics / Reverse Engineering** | `Autopsy`, `binwalk`, `radare2` | Herramientas de análisis forense y de ingeniería inversa. |

Kali Linux se configura generalmente en entornos virtualizados (VMware o VirtualBox), aislados de la red de producción, garantizando así un entorno seguro para pruebas.

### 3.2. MATLAB

MATLAB (Matrix Laboratory) es un entorno de programación numérica ampliamente utilizado en ingeniería para la resolución de problemas científicos y el desarrollo de algoritmos. En el contexto de la seguridad informática, MATLAB permite implementar algoritmos criptográficos y analizar su comportamiento.

#### Aplicaciones criptográficas:

- **Cifrado clásico:**
  - *César*, *Vigenère*, *Hill*.
  - Operan sobre texto alfabético y se basan en desplazamientos o transformaciones lineales.
- **Cifrado moderno simétrico:**
  - *DES*, *AES*.
  - Utilizan una clave compartida entre emisor y receptor.
- **Cifrado asimétrico:**
  - *RSA*, *ElGamal*.
  - Basados en pares de claves pública/privada.
- **Funciones hash:**
  - *MD5*, *SHA-1*, *SHA-256*.
  - Generan una huella digital única de un mensaje.
- **Certificados digitales:**
  - Estructuras que permiten validar la identidad de un emisor mediante una autoridad certificadora (CA).

# 4. PROCEDIMIENTO

## 4.1. Preparación del entorno

1. Instalar **Kali Linux** en VirtualBox o VMware.
2. Instalar **MATLAB** (versión académica o de prueba).
3. Configurar el adaptador de red en modo "Bridge" o "NAT".
4. Comprobar conectividad entre el sistema anfitrión y la máquina virtual.

## 4.2. Actividades en Kali Linux

1. Ejecutar un escaneo básico con `nmap`:

   ```
   nmap -sS 192.168.0.0/24
   ```

2. Identificar un servicio vulnerable con `Nikto`:
   nikto -h http://192.168.0.10

3. Explorar el entorno de **Metasploit Framework**:
   msfconsole
   help

## 4.3. Actividades en MATLAB

1. Crear un script para ingresar una matriz de nxn.
2. Determinar si la matriz tiene inverso.
3. Encontrar el inverso de la matriz.
4. Implementar el método de gauss-jordan para calcular el inverso de la matriz.

# 5. INFORME

El informe deberá incluir:

- Evidencias gráficas (capturas de pantalla, resultados de comandos).
- Explicación detallada de cada paso ejecutado.
- Fragmentos de código MATLAB comentados.
- Reflexión sobre los resultados obtenidos.

# 6. CONCLUSIONES Y RECOMENDACIONES

- La combinación de Kali Linux y MATLAB ofrece una visión integral del ciclo de ciberseguridad: detección, explotación y mitigación.
- Es esencial mantener la práctica en entornos aislados y respetar los principios éticos del uso de herramientas ofensivas.
- El análisis criptográfico complementa las competencias técnicas del ingeniero en telecomunicaciones.

## 7. PREGUNTAS DE REFLEXIÓN POST-LABORATORIO

1. ¿Qué diferencias existen entre el reconocimiento pasivo y el activo en Kali Linux?
2. ¿Qué ventajas y desventajas presentan los cifrados simétricos frente a los asimétricos?
3. ¿Cuál es el propósito de una función hash y cómo se utiliza para verificar la integridad de los datos?
4. ¿Qué elementos garantizan la autenticidad de un certificado digital?
5. ¿Por qué es fundamental la ética profesional en el uso de herramientas de explotación?