

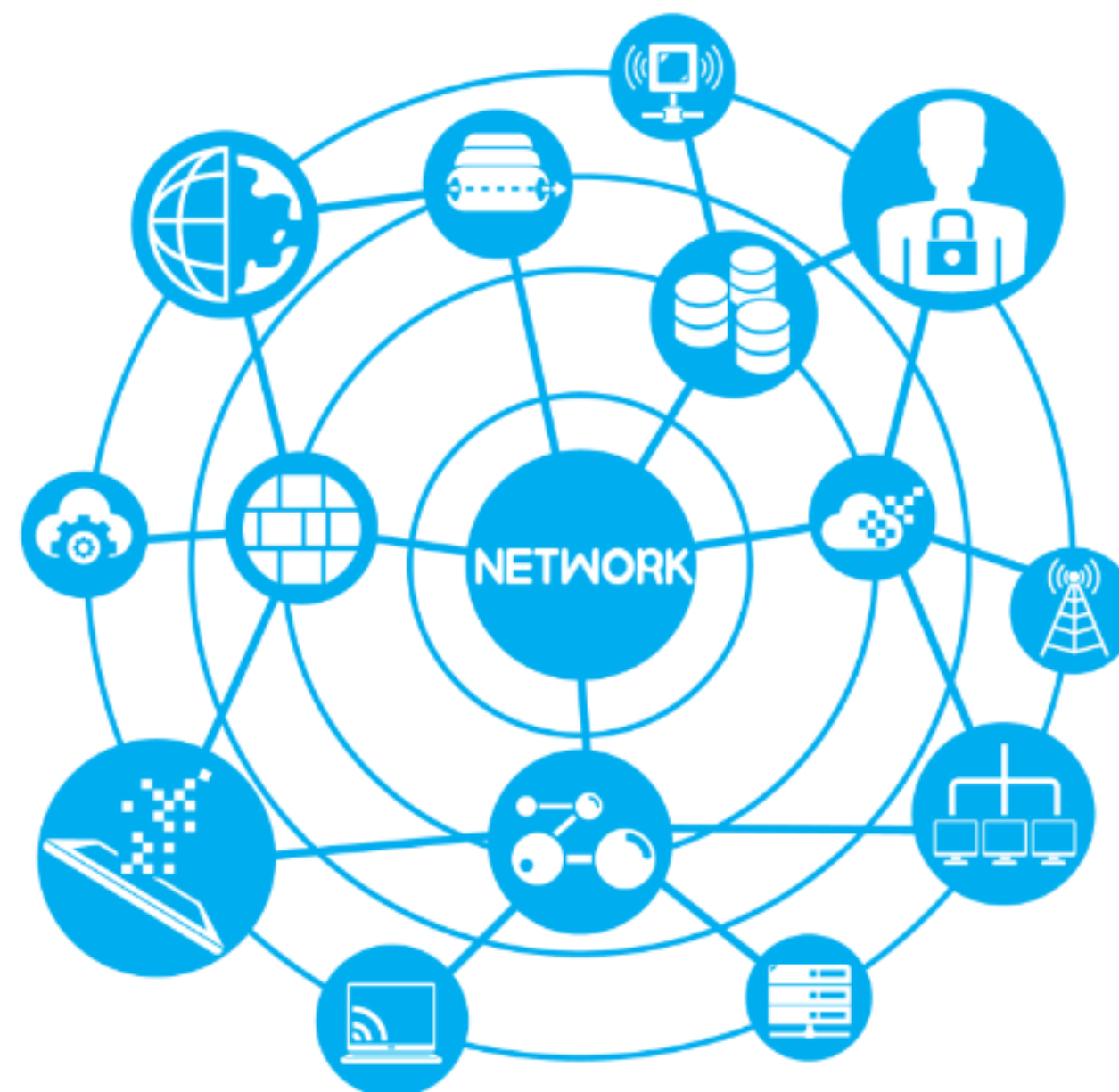


# Energiza!

Metodología del Hacking  
Ético

## Fases del Hacking Ético

1. Reconocimiento
2. Enumeración
3. Explotación
4. Post-explotación
5. Elaboración del informe



## Fase 1 - Reconocimiento

- **Objetivo:** Recolectar información del sistema objetivo.
- ♦ *Pasivo:* Google Dorks, Whois, Shodan.
- ♦ *Activo:* Nmap, OpenVAS, Maltego.
- Clave para mapear el entorno sin ser detectado.



## Fase 2 - Enumeración

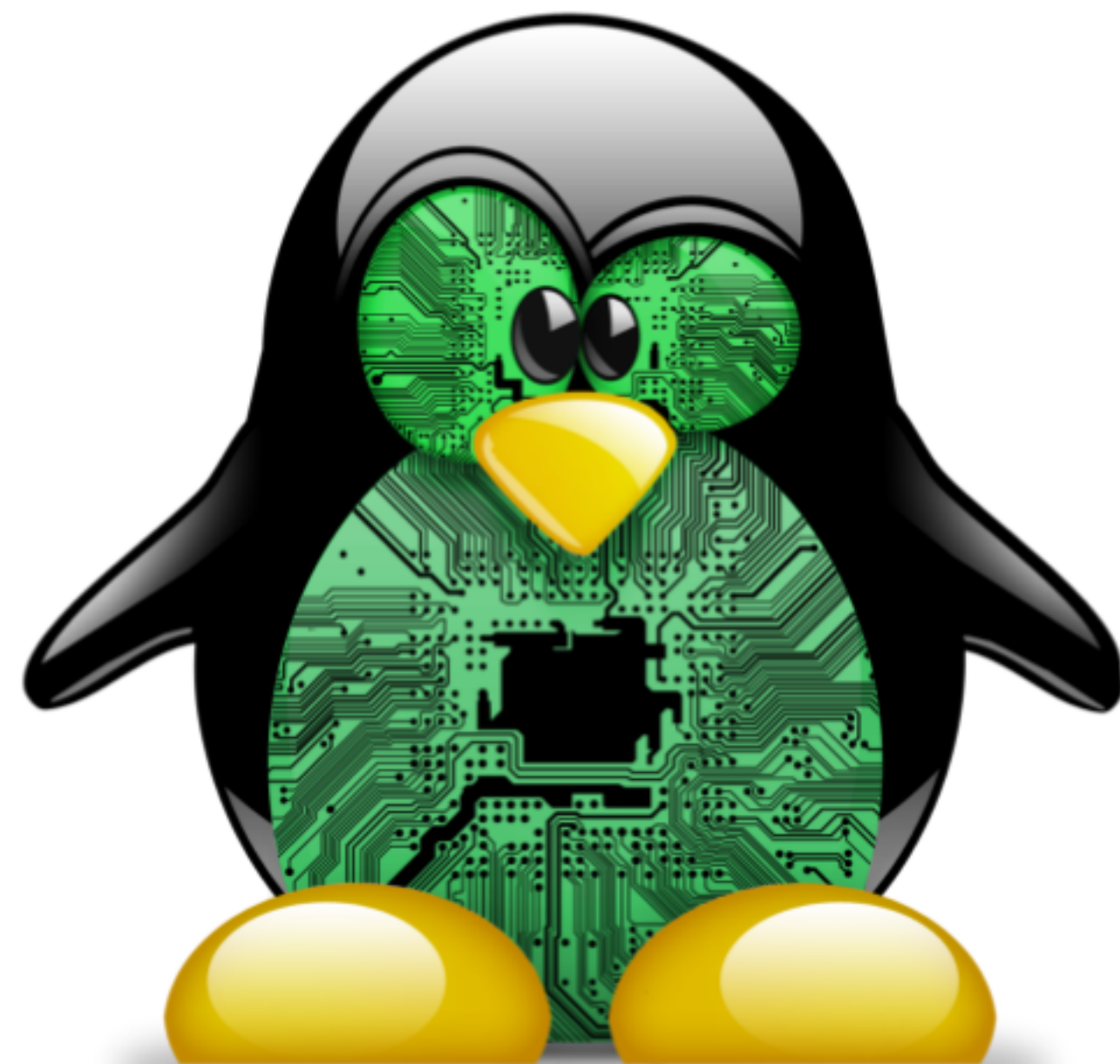
- Detección de servicios, rutas ocultas y credenciales.
- Herramientas:
  - Enum4linux (SMB)
  - Dirbuster / Gobuster (directorios)
  - Nmap NSE Scripts (servicios/vulnerabilidades)





## 💥 Fase 3 - Explotación

- Acceso no autorizado mediante vulnerabilidades encontradas.
- Herramientas:
  - Metasploit Framework
  - SQLMap
  - Burp Suite (manual + automatizada)
- Riesgo elevado: requiere autorización formal.



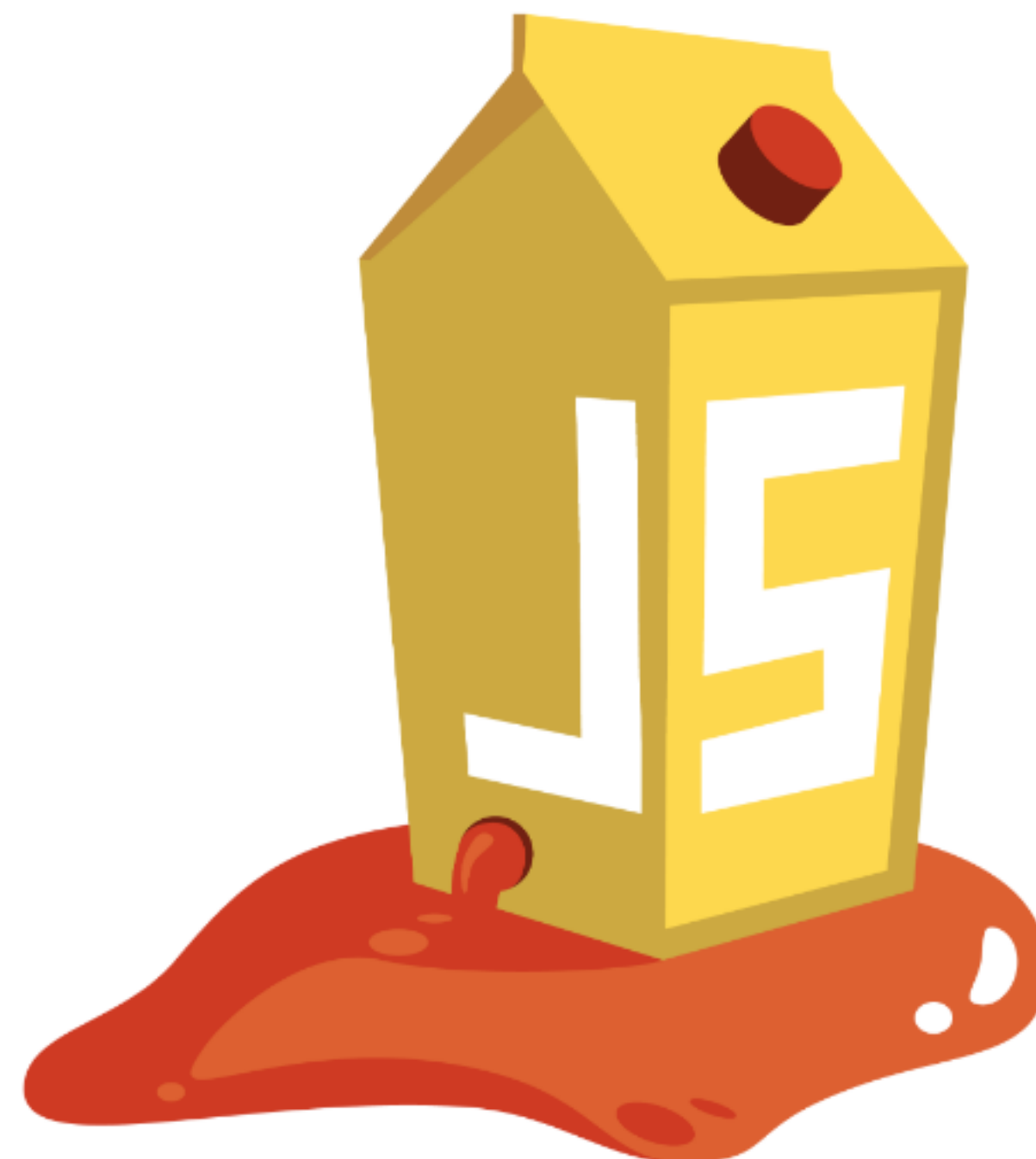
## Fase 4 - Post-Explotación

- Persistencia, escalado de privilegios, movimiento lateral.
- Técnicas y herramientas:
  - Meterpreter
  - Proxychains + SSH pivoting
  - Privesc scripts (Windows/Linux)



## Fase 5 - Elaboración del Informe

- Entregable esencial con impacto organizacional.
- Buenas prácticas:
  - Evidencias (logs, capturas)
  - Clasificación OWASP / CVSS
  - Recomendaciones con cronograma técnico





## Estándares y Metodologías

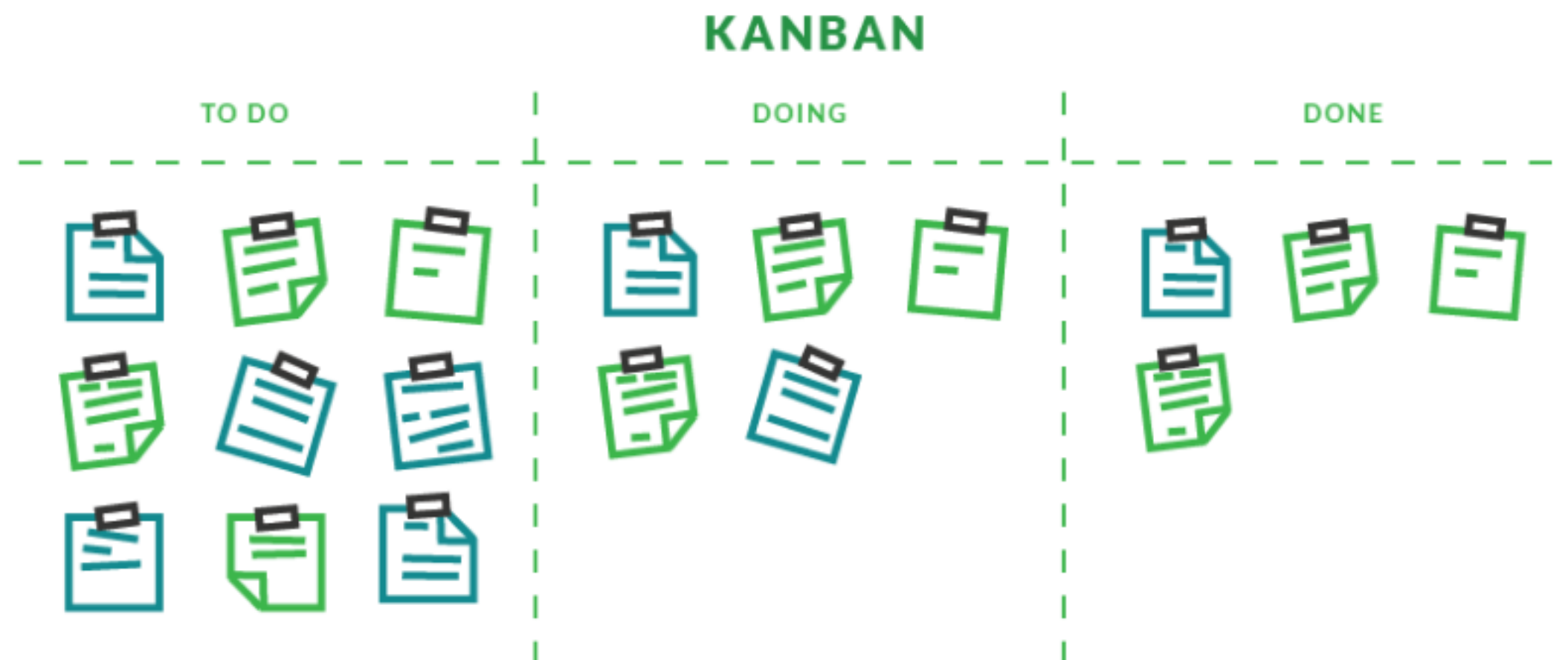
- **OWASP Testing Guide:**
  - Auditoría de apps web.
  - 90+ pruebas clasificadas por riesgo.
- **PTES:**
  - 7 fases desde pre-engagement hasta lecciones aprendidas.
  - Ideal para entornos corporativos.










## Gestión del Tiempo y Planificación

- Cronogramas por fase (ej: Gantt).
- Sprints técnicos con checkpoints.
- Flexibilidad frente a hallazgos críticos.
- Tableros ágiles para control del proceso.



## Caso Práctico

-  Google Dorks → documentos PDF indexados
-  Nmap → Apache + phpMyAdmin expuestos
-  SQLMap → extracción de credenciales
-  DirtyCow → escalado de privilegios
-  Informe → mitigaciones y recomendaciones precisas

```
0111001011100111101011
1000110010101001010101
1010110110101011011011
11101011HACKED11110110
0001010100100001011111
1001010101010101010100
1111100111111011001000
```

## ✓ Conclusiones

- Hacking ético = defensa ofensiva con base normativa.
- Permite:
  - Evaluación real de riesgos
  - Fortalecimiento de seguridad
  - Mejora de cumplimiento normativo
- Herramienta clave para organizaciones resilientes.





