

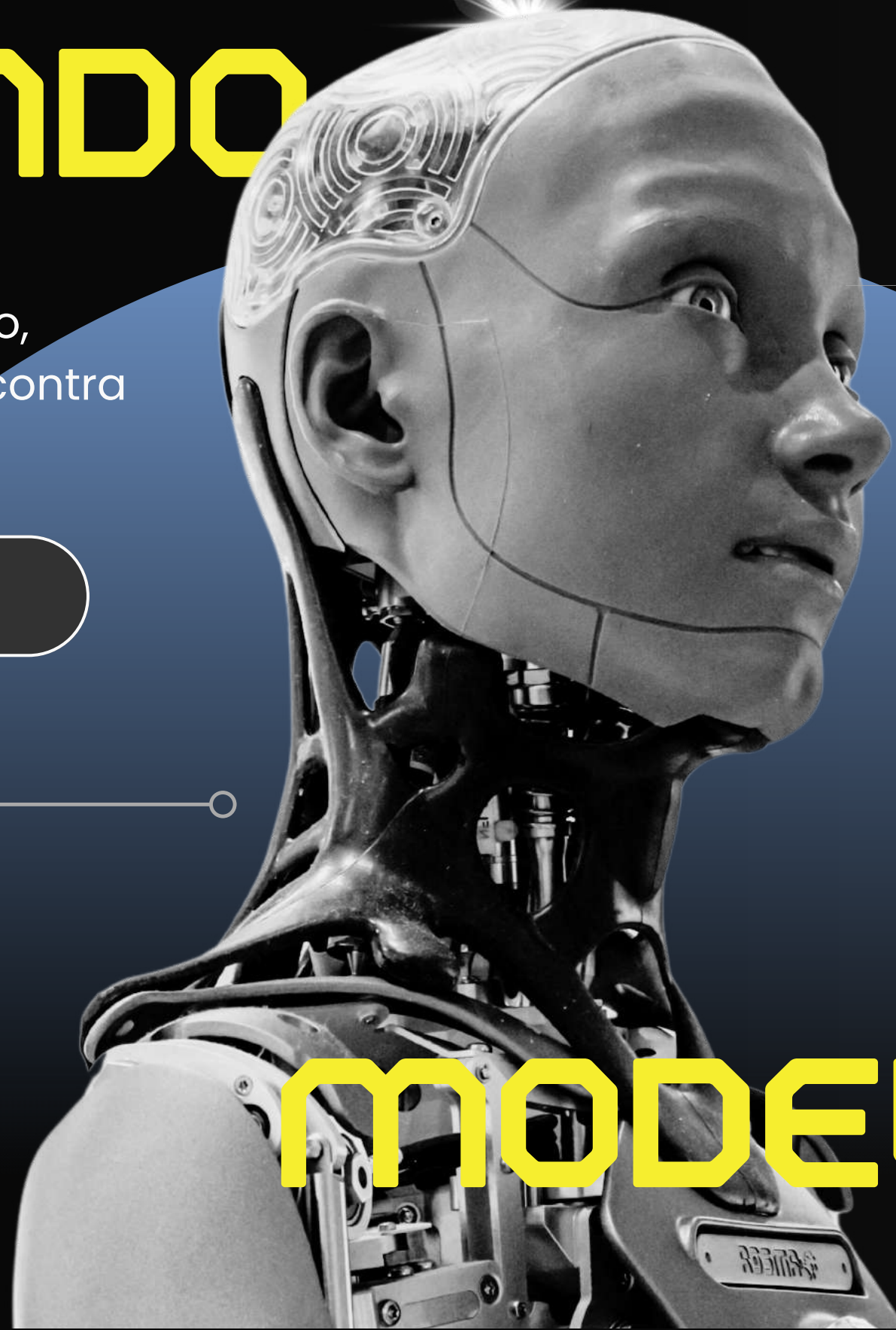
HACKEANDO

Interfaz de inteligencia artificial para auditorías ofensivas y reconocimiento, operada desde una TUI en Kali Linux contra un backend HexStrike en Proxmox.

ANGEL A. PECH

www.upy.edu.mx

CON MODELOS DE IA



ARQUITECTURA



CLIENTE

HexStrike TUI
Kali Linux



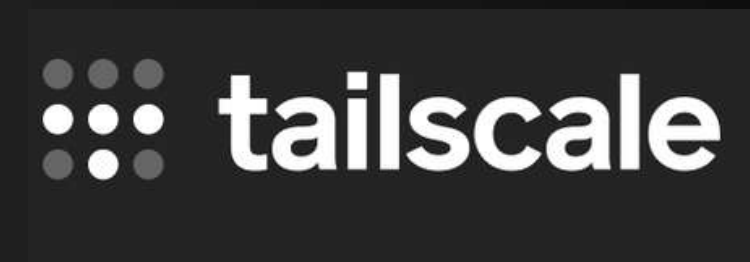
BACKEND

HexStrike Server LXC /
Proxmox VE



CANAL

Tailscale mesh



HERRAMIENTAS Y COMPONENTES

OBJETIVO

Construir Interfaz de IA para reconocimiento ofensivo. Un operador en Kali Linux (`demo_ia.py`) que mande órdenes en lenguaje natural a un backend HexStrike AI en un LXC de Proxmox (`hexstrike_server.py`), que ejecuta nmap y en órdenes libres, consulta un modelo local de Ollama.



LXC IA-UPY

IIA-UPY

Ubuntu 24.04 LTS /
Debian sobre LXC en
Proxmox VE/Ollama
local ejecutando el
modelo Llama 3.5 7B.

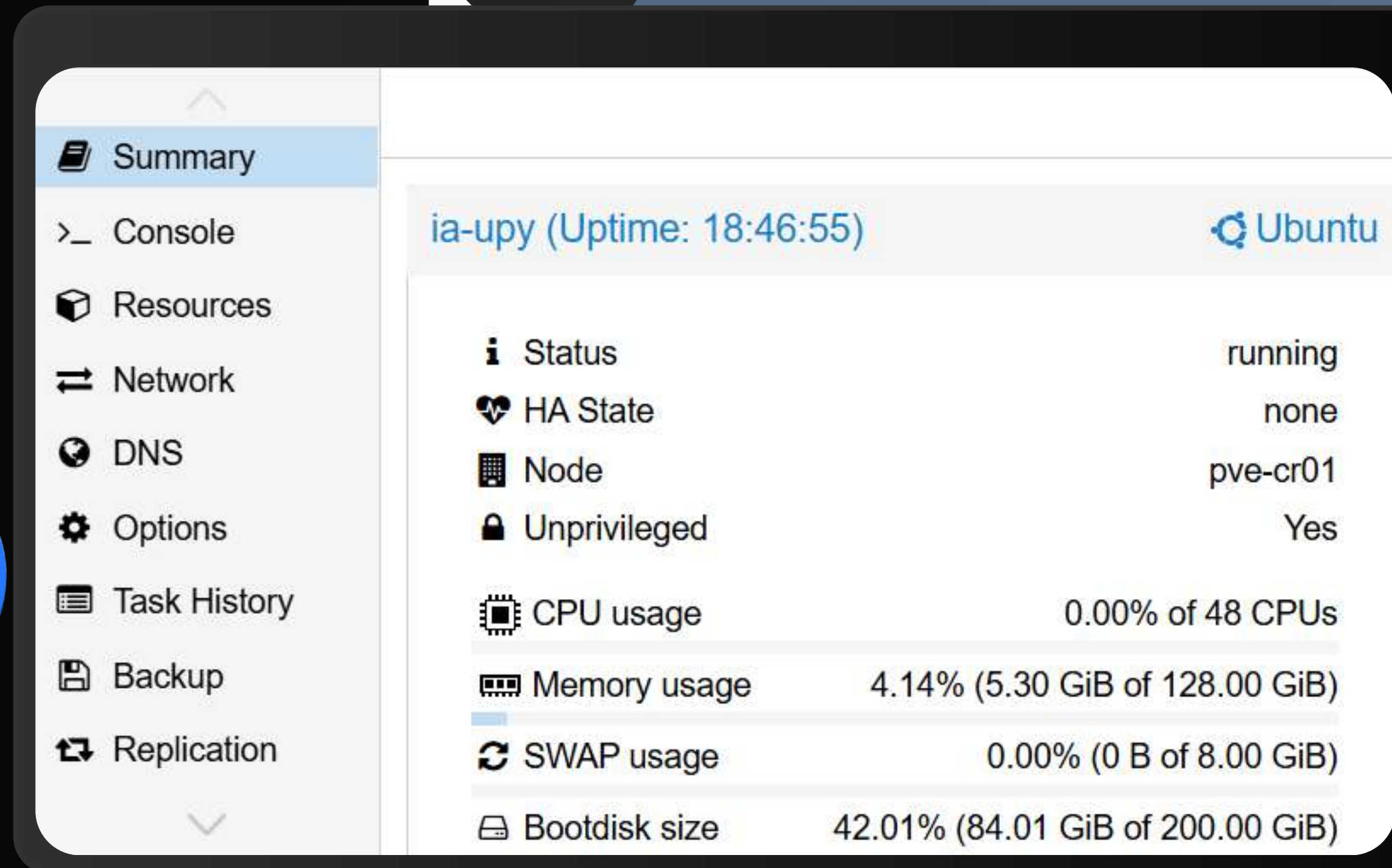


CLIENTE

Kali Linux con entorno de
terminal HexStrike TUI



La TUI (Terminal User Interface) es la
consola interactiva del operador,
construida con Rich, que presenta los
resultados en tablas y paneles con color
directamente en la terminal, sin
necesidad de una interfaz gráfica



The image shows a screenshot of the Proxmox VE web interface. On the left is a sidebar menu with options: Summary, Console, Resources, Network, DNS, Options, Task History, Backup, and Replication. The 'Summary' tab is selected. The main panel displays details for an LXC container named 'ia-upy' (Uptime: 18:46:55) on the 'Ubuntu' node. The container is running and unprivileged. Resource usage is shown for CPU (0.00% of 48 CPUs), Memory (4.14% of 128.00 GiB), SWAP (0.00% of 8.00 GiB), and Bootdisk (42.01% of 200.00 GiB).

Property	Value
Status	running
HA State	none
Node	pve-cr01
Unprivileged	Yes
CPU usage	0.00% of 48 CPUs
Memory usage	4.14% (5.30 GiB of 128.00 GiB)
SWAP usage	0.00% (0 B of 8.00 GiB)
Bootdisk size	42.01% (84.01 GiB of 200.00 GiB)

HEXSTRIKE

HexStrike AI orquesta herramientas de pentesting mediante IA, traduciendo lenguaje natural en auditorías de seguridad automatizadas.



HEXSTRIKE

HEXSTRIKE

HexStrike AI - Blood-Red Offensive Intelligence Core
AI-Automated Recon | Exploitation | Analysis Pipeline
Big Bounty | CTF | Red Team | Zero-Day Research

[INFO] Server starting on 127.0.0.1:8888
[INFO] 150+ integrated modules | Adaptive AI decision engine active
[INFO] Blood-red theme engaged - unified offensive operations UI

```
2026-08-22 17:02:18,435 - _main_ - INFO - Starting HexStrike AI Tools API Server
2026-08-22 17:02:18,435 - _main_ - INFO - Port: 8888
2026-08-22 17:02:18,435 - _main_ - INFO - Debug Mode: False
2026-08-22 17:02:18,435 - _main_ - INFO - Cache Size: 1000 | TTL: 3600s
2026-08-22 17:02:18,435 - _main_ - INFO - Command Timeout: 300s
2026-08-22 17:02:18,435 - _main_ - INFO - Enhanced Visual Engine: Active
* Serving Flask app 'hexstrike_server'
* Debug mode: off
2026-08-22 17:02:18,472 - werkzeug - INFO - WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:8888
* Running on http://192.168.1.4:8888
2026-08-22 17:02:18,472 - werkzeug - INFO - Press CTRL+C to quit
2026-08-22 17:02:43,282 - _main_ - INFO - Cache MISS for command: which nmap
2026-08-22 17:02:43,283 - _main_ - INFO - EXECUTING: which nmap
2026-08-22 17:02:43,283 - _main_ - INFO - TIMEOUT: 300s | PID: Starting...
2026-08-22 17:02:43,284 - _main_ - INFO - PROCESS: PID 47799 started
2026-08-22 17:02:43,284 - _main_ - INFO - REGISTERED: Process 47799 - which nmap...
2026-08-22 17:02:43,286 - _main_ - INFO - PROGRESS: [ ] 0.0% Speed: 0 B/s | 0.0s | PID: 47799
2026-08-22 17:02:43,302 - _main_ - INFO - STDOUT: /usr/bin/nmap
2026-08-22 17:02:43,306 - _main_ - INFO - CLEANUP: Process 47799 removed from registry
2026-08-22 17:02:43,306 - _main_ - INFO - SUCCESS: Command completed | Exit Code: 0 | Duration: 0.02s
2026-08-22 17:02:43,306 - _main_ - INFO - FINAL RESULTS
2026-08-22 17:02:43,306 - _main_ - INFO - Command: which nmap
```

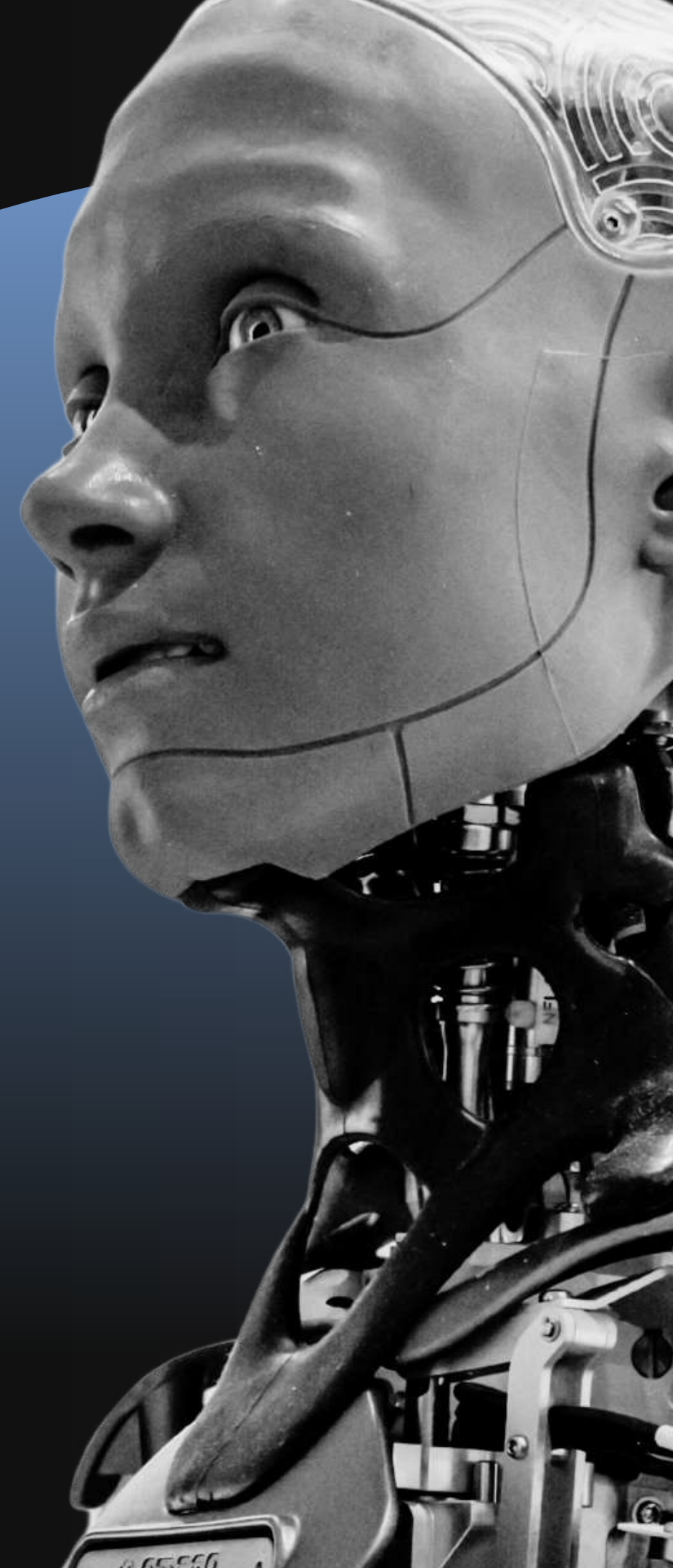
OLLAMA

Es una herramienta que permite descargar y ejecutar modelos de lenguaje de forma local en tu propia máquina, sin depender de la nube ni de APIs externas, garantizando privacidad total sobre los datos de la auditoría.

MODELO QWEN 2.5:7B

active			
NAME	ID	SIZE	MODIFIED
qwen2.5:7b	845dbda0ea48	4.7 GB	7 hours ago

Qwen 2.5 7B es un modelo de lenguaje de código abierto desarrollado por Alibaba, capaz de razonar, seguir instrucciones y generar código, lo bastante ligero para correr localmente en CPU dentro del contenedor.



GUIÓN DE LA DEMOSTRACIÓN



VERIFICAR EL SERVICIO ACTIVO

```
root@ia-upy:~# # ✓ Verificar:
systemctl is-active ollama
ollama list
active
NAME
FIED
qwen2.5:7b
```

01

CLIENTE (KALI LINUX)

```
(kali@kali)-[~]
$ # ✓ Verificar: Kali debe VER al backend por la malla
tailscale status # el nodo ia-upy debe aparecer activo
ping -c 3 100.90.158.75 # debe responder con tiempos, no "unreachable"
100.108.177.52 kali lab.soc26@ linux -
100.78.108.91 dell lab.soc26@ windows -
100.81.199.38 guacamole lab.soc26@ linux -
100.90.158.75 ia-upy lab.soc26@ linux -
100.80.249.64 pc-a lab.soc26@ windows offline, last seen 9d ago
100.71.246.87 pve-cr01 lab.soc26@ linux -
100.72.84.6 pve lab.soc26@ linux offline, last seen 6d ago
100.67.144.12 servidor-zd83 lab.soc26@ windows offline, last seen 19d ago
100.92.71.119 wazuh-server lab.soc26@ linux offline, last seen 13d ago

# Health check:
# - Some peers are advertising routes but --accept-routes is false
PING 100.90.158.75 (100.90.158.75) 56(84) bytes of data.
64 bytes from 100.90.158.75: icmp_seq=1 ttl=64 time=481 ms
64 bytes from 100.90.158.75: icmp_seq=2 ttl=64 time=109 ms
64 bytes from 100.90.158.75: icmp_seq=3 ttl=64 time=103 ms

— 100.90.158.75 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 102.669/230.900/480.775/176.708 ms
```

03

LEVANTAR EL SERVIDOR HEXSTRIKE

02

```
root@ia-upy:~# # ✓ Verificar: proceso vivo, puerto escuchando y la API responde
pgrep -af hexstrike_server.py # debe listar el proceso con su PID
ss -tln | grep 8888 # debe mostrar el puerto en LISTEN
curl http://localhost:8888/health # Flask debe devolver un JSON de estado
341898 python3 hexstrike_server.py
tcp LISTEN 0 128 0.0.0.0:8888 0.0.0.0:*
```

CONFIRMAR EL ENDPOINT Y EJECUTAR

04

⚡ HEXSTRIKE AI - INTERACTIVE OFFENSIVE CHAT ⚡
Escribe tus órdenes en lenguaje natural | Escribe 'salir' para finalizar

● OpSec-Operator: escanea 100.90.158.75
● Agente IA procesando instrucción en Proxmox...

● SERVICIOS DETECTADOS

Puerto	Estado	Servicio / Versión
22/tcp	OPEN	ssh OpenSSH 8.9p1 Ubuntu
80/tcp	OPEN	http nginx 1.18.0
8888/tcp	OPEN	http HexStrike API Daemon v1.0

Resultado del agente:

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 8.9p1 Ubuntu
80/tcp	open	http	nginx 1.18.0
8888/tcp	open	http	HexStrike API Daemon v1.0

● Estado: COMPLETED
● Acción Sugerida: Analizar vectores de ataque sobre los servicios detectados.

TUI (TERMINAL USER INTERFACE)

GRACIAS

angel.pech@upy.edu.mx



UNIVERSIDAD
POLITÉCNICA
DE YUCATÁN

