HACKEANDO CON MODELOS DE IA

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

ARQUITECTURA

Ollama

CLIENTE

HexStrike TUI
Kali Linux

HEXSTRIKE

BACKEND

HexStrike Server LXC /
Proxmox VE

PROXMOX

CANAL

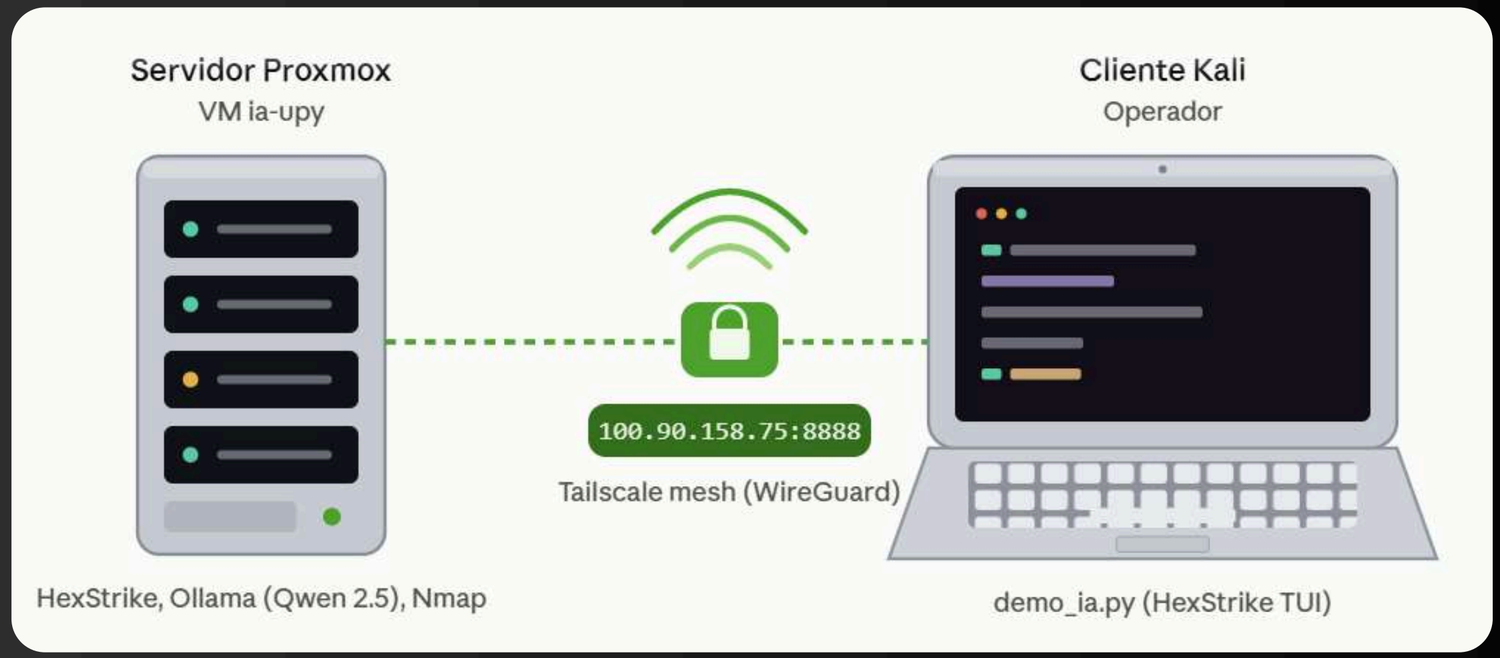
Tailscale mesh

tailscale

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

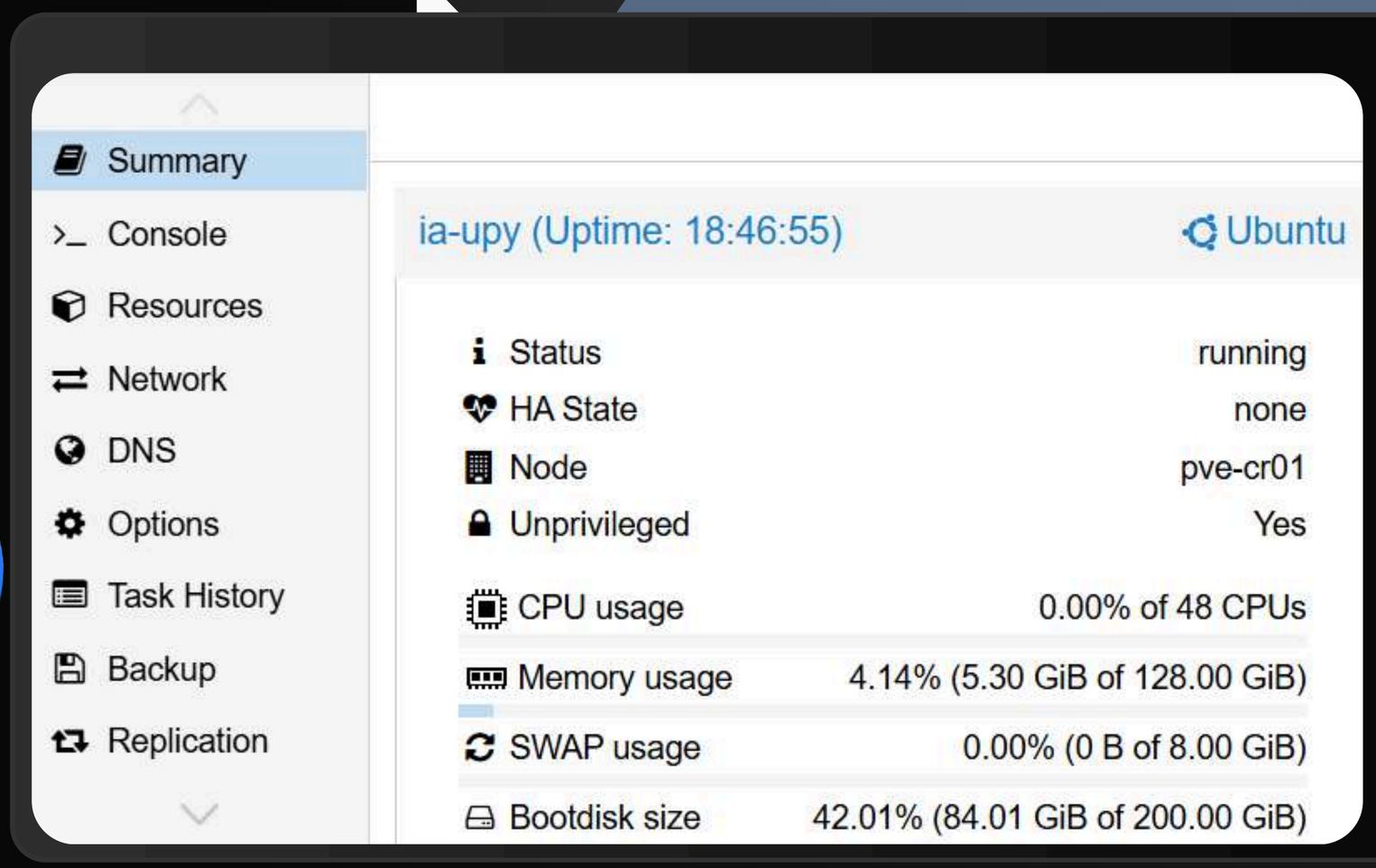
IIA-UPY

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

CLIENTE

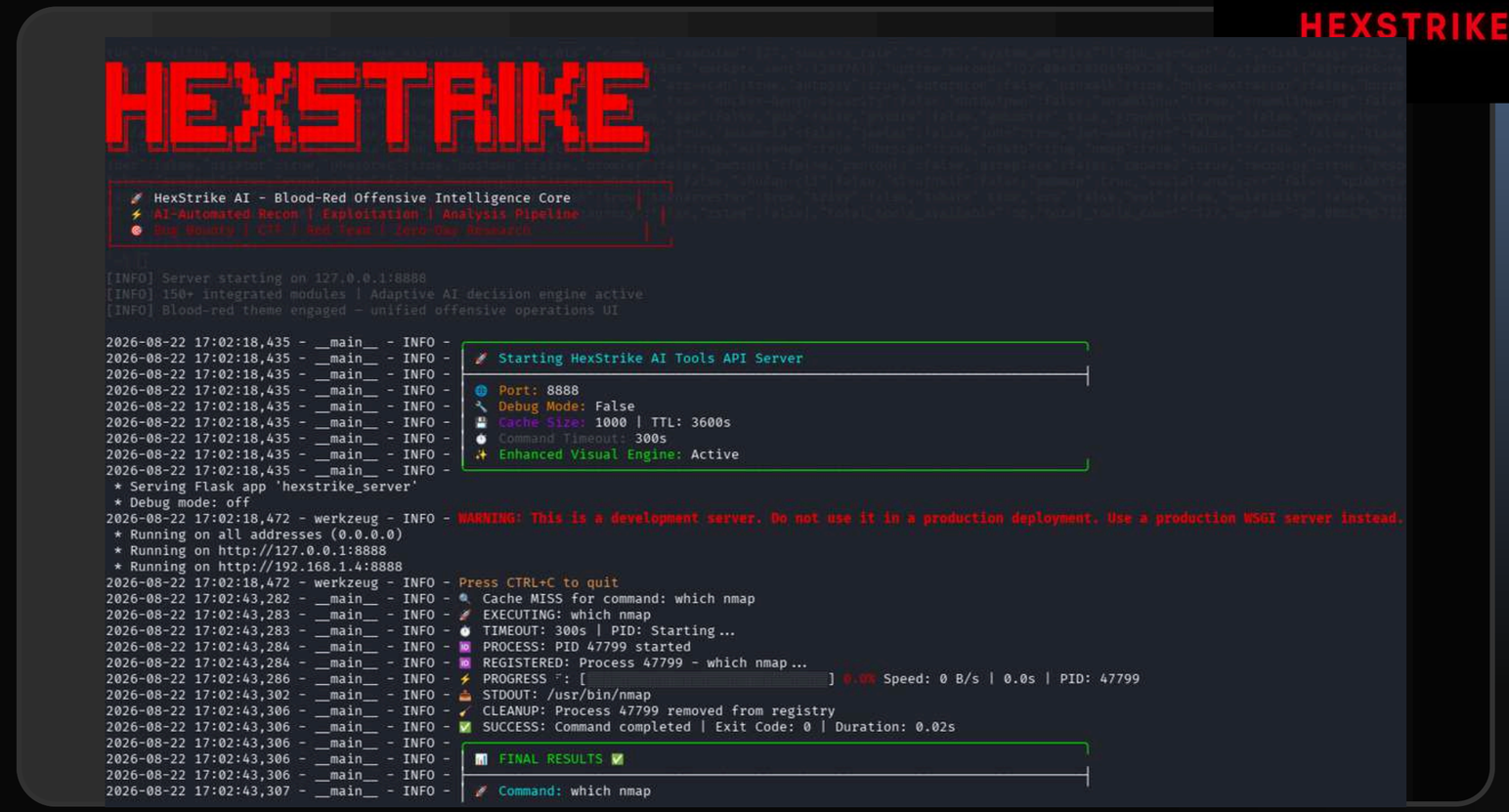
Kali Linux con entorno de terminal HexStrike TUI

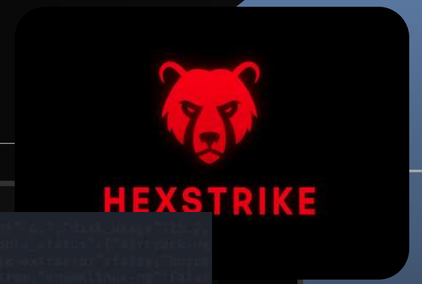
La TUI (Terminal User Interface) es la consola interactiva del operador, construida con Rich, que presenta los resultados en tablas y paneles con color directamente en la terminal, sin necesidad de una interfaz gráfica

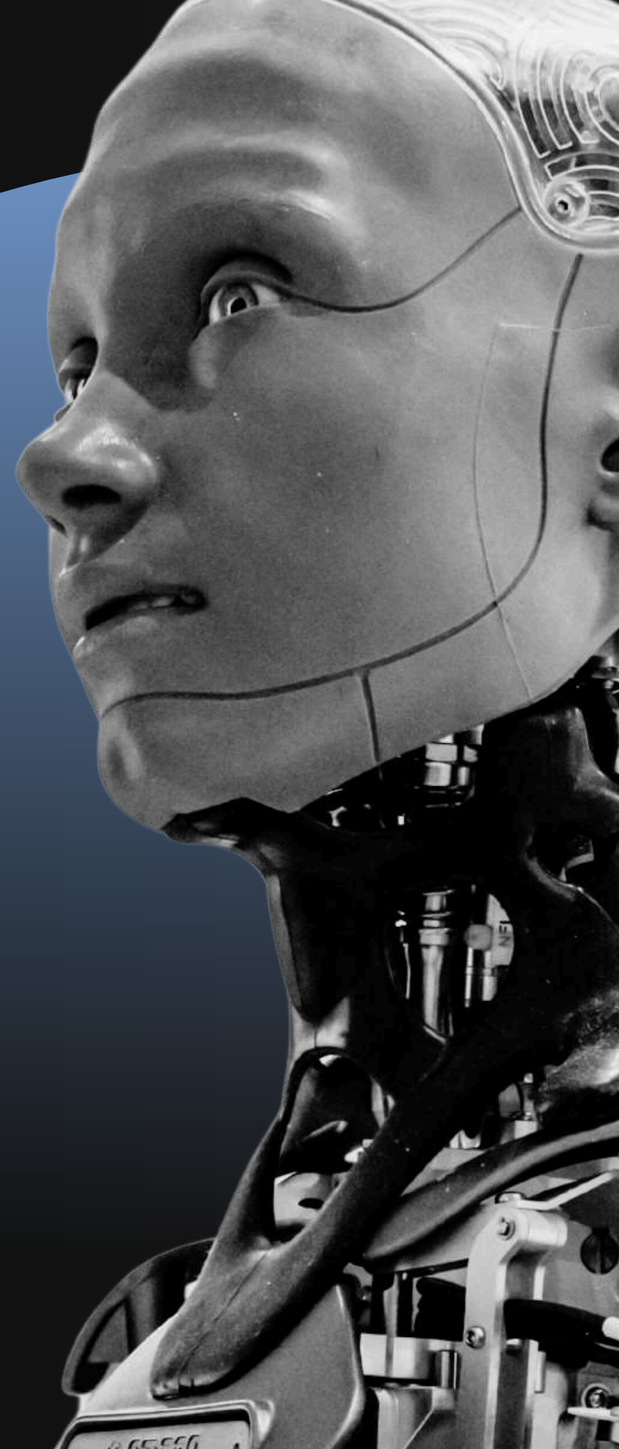


HEXTRIKE

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







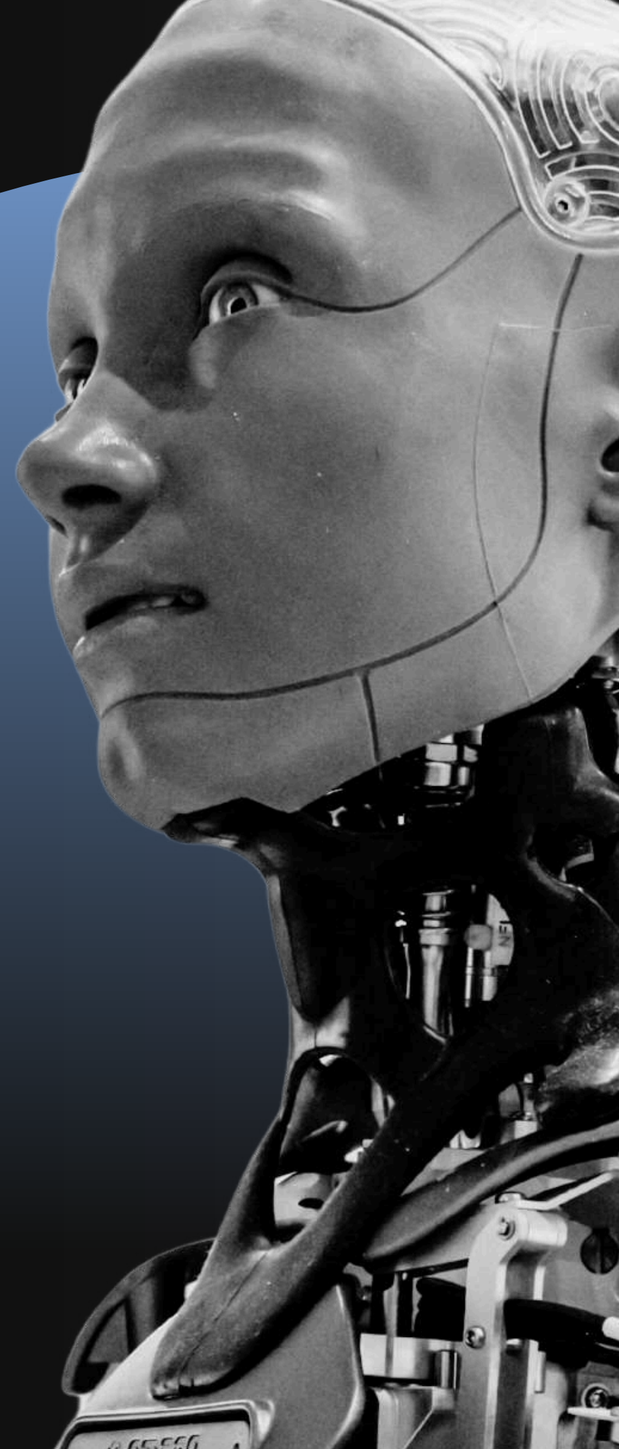
OLLAMA

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

01

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

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 -tuln | 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:*
```

CLIENTE (KALI LINUX)

03

```
┌──(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
```

CONFIRMAR EL ENDPOINT Y EJECUTAR

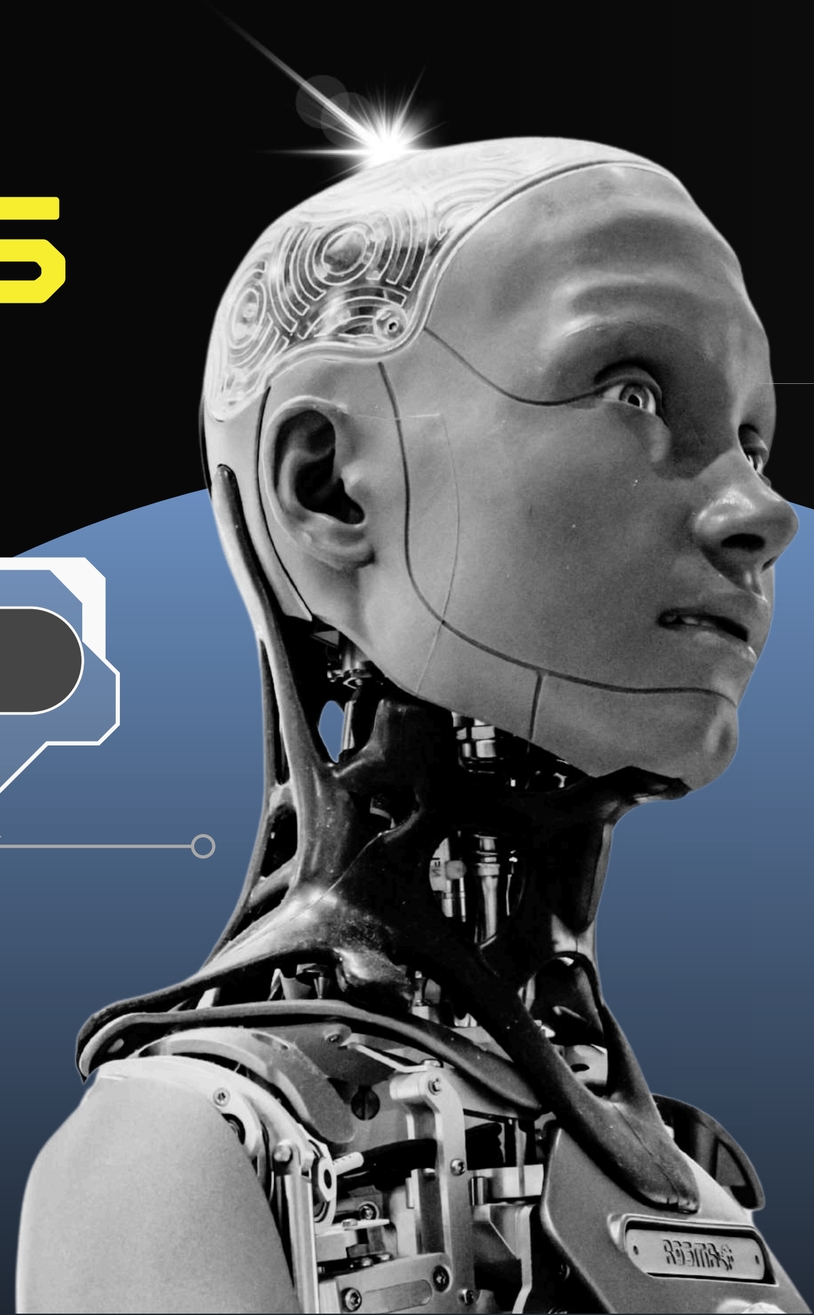
04

```
⚡ 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)

WWW.UPY.EDU.MX

GRACIAS



angel.pech@upy.edu.mx

UNIVERSIDAD POLITÉCNICA DE YUCATÁN

BIS Universities