Si algún día te preguntas en que ando, esta es la lista de tareas tecnológicas que tengo por hacer:

ADMINISTRACIÓN DE SISTEMAS

- Volver a implementar GoAccess:
  – https://goaccess.io/download
  – https://github.com/nipegun/d-scripts/blob/master/SoftInst/ParaCLI/Servidor-GoAccess-InstalarYConfigurar.sh
- Investigar e implementar análisis de eventos de Windows mediante inteligencia artificial:
  – https://github.com/voytas75/AIEventAnalyzer
- Investigar e implementar Swagger UI:
  – https://swagger.io/tools/swagger-ui/

CIBERSEGURIDAD

- Investigar e implementar pymetasploit3:
  – https://coalfire.com/the-coalfire-blog/pymetasploit3-metasploit-automation-library
  – https://github.com/DanMcInerney/pymetasploit3
- Investigar e implementar metasploit auto-exploitation:
  – https://docs.rapid7.com/metasploit/auto-exploitation/
- Agregar al script de instalación de dockers vulnerables, todos los dockers de Dockerlabs:
  – https://dockerlabs.es/
- Investigar e implementar API fuzzing:
  – https://node-security.com/posts/api-fuzzing/
- Crear un CTF con OWASP Juice Shop y traefik:
  – https://backtrackacademy.com/articulo/como-crear-un-ctf-con-owasp-juice-shop-y-traefik
- Investigar y desplegar instancias individuales de CTFd + docker:
  – https://blog.toadsec.io/2023/07/24/ctfd-whale.html
- Investigar e implementar como dumpear la RAM de una VM de virtualbox con volatility 3
  – https://cylab.be/blog/99/dump-the-memory-of-a-virtualbox-vm-for-volatility3
- Investigar e implementar escáneres de vulnerabilidades para dockers:
  – https://github.com/docker/docker-bench-security
  – https://www.prplbx.com/resources/blog/docker-part2/
- Investigar e implementar un CTF de ataque/defensa:
  – https://github.com/ER-DEF-CTF-Erronkak-sortzen
  – https://github.com/fausecteam/ctf-gameserver
  – https://ctf-gameserver.org/installation/#package-build
  – https://2017.faustctf.net/information/setup/
  – https://2017.faustctf.net/information/basic-vulnbox-hosting/
- Investigar e implementar herramientas de ControlThings.io
  – https://www.controlthings.io/tools
- Hacer una lista de todo el software opensource y no opensource que hay para controlar modbus y hacer una wiki empresarial por cada uno de ellos. Por ejemplo:
  – https://github.com/serhmarch/ModbusTools
  o
  – https://www.modbusdriver.com/modpoll.html

INTELIGENCIA ARTIFICIAL

- Terminar los scripts de instalación de modelos LLM auto-gestionados:
  – https://github.com/nipegun/ia-scripts/blob/main/SoftInst/ParaCli/Modelos/Ollama-Coder-DeepSeek.sh
  – https://github.com/nipegun/ia-scripts/blob/main/SoftInst/ParaCli/Modelos/Ollama-Mistral.sh
  – https://github.com/nipegun/ia-scripts/blob/main/SoftInst/ParaCli/Modelos/Ollama-Gemma.sh
  – https://github.com/nipegun/ia-scripts/blob/main/SoftInst/ParaCli/Modelos/Ollama-DeepSeek.sh
  – https://github.com/nipegun/ia-scripts/blob/main/SoftInst/ParaCli/Modelos/Ollama-Dolphin-Uncensored.sh

PERSONAL

- Terminar el artículo de «sobre como juanqueé mi propio proxmox«
- Terminar páginas a Edu.
- Instalar QTSCloud en Proxmox.
- Instalar el último macOS en Proxmox.
- Comprar las antenas para ambos servidores.
- Terminar artículo de como crear VLAnes en Windows.
- Re-conectar todo el IoT del local.
- Poner en todas las entradas de hacks4geeks, h3 para todos los títulos que vengan posteriores al título de la entrada (que es h2)
- Hacer maleta de widgets
- Lograr instalar Oracle Database Enterprise en Debian.
- Lograr instalar Centreon en Debian
- Crear el tutorial para instalar la última versión de macOS en Proxmox.
- Implementar huella digital en debian.
- Hacer el tutorial de bluetooth en debian.
- Implementar cifrado de carpetas en debian.
- Instalar ICINGA
- Instalar Pandora
- Configurar la app de RetroArch en todos los dispositivos.