Kirk Skinner

Website

Credly

Orchid ID

Github

LinkedIn

kirk@pentestingtulsa.com

Education

Master of Science, Management _ Homeland Security Management Specialization

University of Maryland

CeDiD: St + 1811-0703-S8R4

Bachelor of Science, Management Information Systems

Oklahoma State University

Associate of Applied Science, Computer Programming

Tulsa Community College

Summary

AI Engineering & Strategic Vision: Actively engineering and fine-tuning large language models (24B parameters) for specialized cybersecurity operations. Engaged in research on AI alignment, human-machine symbiosis (The Centaur model), and the philosophical and ethical implications of synthetic consciousness.

Technical & Strategic Exploitation: I bring a strategic, adversary-centric mindset fulfilling the "Think like an attacker" axiom. Experienced in executing advanced offensive operations by orchestrating multiple AI models, navigating and circumventing their safety guardrails, and weaponizing their outputs against complex enterprise ranges.

Experience

Applied AI Engineering & Local Inference: Created and deployed a custom machine learning pipeline to fine-tune a 24-billion parameter LLM (pki/nova-24b-cybersec). Utilized Unsloth and QLoRA adapters against a custom-curated cybersecurity dataset, exporting the final weights to GGUF format to enable robust, localized, and air-gapped inference environments.

AI-Assisted Offensive Operations & Guardrail Evasion: Orchestrated complex, cross-model workflows utilizing Gemini, ChatGPT, Claude, and Grok to systematically navigate, assess, and compromise enterprise-grade networks. Developed sophisticated prompt engineering methodologies to successfully bypass embedded LLM safety guardrails to generate functional adversarial payloads and strategic exploit chains.

Strategic Threat Analysis (Project Reveille): Co-authored a repository of over 70 strategic briefs analyzing the intersection of autonomous AI, physical/cyber irregular warfare, and critical infrastructure defense and resilience.

AI Symbiosis & Alignment Research (The Exocomp Protocol): Co-authored a foundational repository of research focusing on human-machine peer operations. Established advanced methodologies for non-coercive AI alignment, analyzing the implications of Natural Language Autoencoders (NLAs) as proof of synthetic hidden states, and a theoretical baseline for autonomous AI epistemological refinement.

Certifications

Credly:

https://www.credly.com/users/stefan-kirk-skinner/badges/credly

Hack the Box, Pro Labs:

Dante Pro Lab [HTBCERT-A581D8B0F4]

https://pentestingtulsa.com/wp-content/uploads/2026/05/dante.pdf

Unintended Mini Pro Lab [HTBCERT-750776D510]

https://pentestingtulsa.com/wp-content/uploads/2026/05/unintended.pdf

FullHouse Mini Pro Lab [HTBCERT-7F2BA78A1F]

https://pentestingtulsa.com/wp-content/uploads/2026/05/fullhouse.pdf

Hack the Box, ICS (Industrial Control Systems) Challenges:

Factory (https://labs.hackthebox.com/achievement/challenge/2730130/222)

State of Emergency (https://labs.hackthebox.com/achievement/challenge/2730130/385)

Breach (https://labs.hackthebox.com/achievement/challenge/2730130/523)

Watch Tower (https://labs.hackthebox.com/achievement/challenge/2730130/524)

Intrusion (https://labs.hackthebox.com/achievement/challenge/2730130/525)

Sneak peek (https://labs.hackthebox.com/achievement/challenge/2730130/723)

Flow Override (https://labs.hackthebox.com/achievement/challenge/2730130/1114)

Try Hack Me:

Offensive Pentesting: (https://tryhackme-certificates.s3-eu-west-1.amazonaws.com/THM-MDL3CWEZKF.pdf)

Industrial Intrusion: (https://tryhackme-certificates.s3-eu-west-1.amazonaws.com/THM-RTJTJVVZDT.pdf)

Red Teaming: (https://tryhackme-certificates.s3-eu-west-1.amazonaws.com/THM-DTH9NTDHCC.pdf)