Seminar

CYBERSECURITY x CYBERSECURITY

Shift the Core, Know the Unknown

CYFENCE

Shift Up Technology - AI Offensive Security

ปัญหาปัจจุบันในวงการ Security

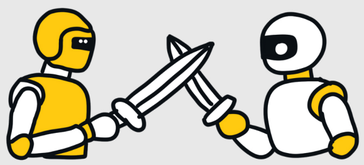
ความซับซ้อนของระบบเพิ่มขึ้น

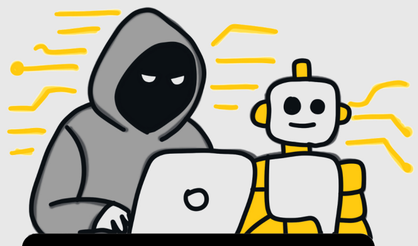
งานซ้ำซากจำนวนมาก

ข้อมูลมหาศาล (Data Overload)

The AI Arms Race

- แฮกเกอร์ใช้ AI ทำ Recon อัตโนมัติ, เก็บข้อมูลเหยื่อ และเจาะระบบ
- ฝั่งป้องกันก็ต้องใช้ AI เช่นกัน (EDR/XDR/SIEM)
- ทีม Offensive ต้อง “ยกระดับ” เพื่อเท่าทันคู่ต่อสู้





AI Co-Pilot Concept

AI ไม่ได้แทนคน แต่ช่วยเพิ่มความสามารถ ทำงานร่วมกับเครื่องมือ Pentest (เช่น Burp Suite, Kali, Hexstrike) ผ่านระบบ MCP (Model Context Protocol)

General-Purpose Gen AI

AI ที่ใช้งานทั่วไป เช่น

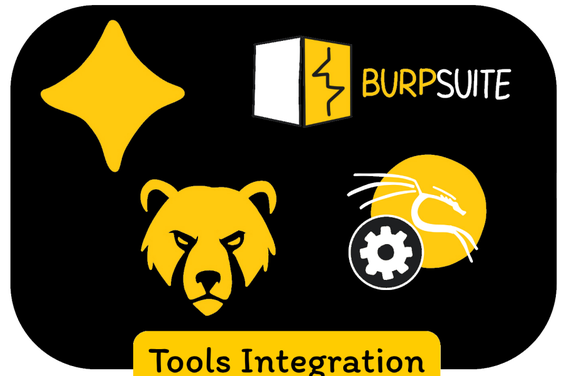
1. Web (Chatbot อย่าง ChatGPT)
2. IDE (VS Code + Extensions)
3. Desktop App (Claude Desktop)
4. CLI

ข้อจำกัดของ AI ทั่วไป

- ข้อมูลล้าสมัย / Hallucination
- ปัญหาความเป็นส่วนตัว
- Workflow ซับซ้อน ต้องคัดลอกผลข้ามเครื่องมือ

MCP Framework

“หัวใจ” ของ AI Offensive Security
เชื่อม AI กับเครื่องมือจริงแบบมีบริบท
MCP = Vehicle ที่ขับเคลื่อน Gen AI
ช่วยทำงานกับ Burp, Kali, Hexstrike



Tools Integration

- Burp Suite MCP → ช่วยค้นหาและรายงานช่องโหว่
- Kali MCP → ทำ Lab CTF อัตโนมัติ
- Hexstrike MCP → Automate Offensive Tasks
- Gemini CLI MCP → ใช้ AI ผ่าน Command Line

AI-Assisted Pentesting Workflow

1. Reconnaissance
   สรุป OSINT อัตโนมัติ
2. Scanning & Enumeration
   วิเคราะห์ผลสแกน
3. Exploitation
   นำเสนอช่องโหว่/payload
4. Post-Exploitation
   ช่วย escalate สิทธิ์
5. Reporting
   เขียนรายงานสรุปผล

คุณพิชญะ โมริโมโตะ
บริษัท สยามฉนัดแฮก จำกัด