FULL HACKING WITH AI COURSE

✅ HACK WITH AI — Tools, Links & Practical Uses (Complete List)

(For Ethical Hacking, Pentesting & Bug Bounty)

🔵 MODULE 1 — AI Models & Platforms

1. Large Language Models (LLMs)

Tool	Link	Uses
ChatGPT	https://chat.openai.com	Payload generation, code analysis, recon automation, report writing
Claude AI	https://claude.ai	Large file analysis, log reading, source code review
Google Gemini	https://gemini.google.com	Android/security analysis, image-based URL inspection
Meta Llama Models	https://ai.meta.com/resources/models-and-libraries/	Local/offline pentesting automation
Qwen 2.5	https://huggingface.co/Qwen	Self-hosted AI for private recon/analysis

---

🔵 MODULE 2 — Recon Automation Tools + AI Workflows

1. Subdomain Enumeration

Tool	Link	Uses
Subfinder	https://github.com/projectdiscovery/subfinder	Fast passive subdomain discovery
Amass	https://github.com/owasp-amass/amass	Deep recon, DNS mapping
Chaos Dataset	https://chaos.projectdiscovery.io	Public bug bounty subdomains
Crt.sh	https://crt.sh	View SSL certificates & hidden subdomains
SecurityTrails	https://securitytrails.com	IP/Domain data, historical DNS

AI Use:

- Filter false positives
- Identify dev/staging domains
- Find vulnerable services based on tech stack

2. Directory Bruteforcing

Tool	Link	Uses
FFUF	https://github.com/ffuf/ffuf	Fast directory/file discovery
Dirsearch	https://github.com/maurosoria/dirsearch	Wordlist-based scanning
Gobuster	https://github.com/OJ/gobuster	Subdomains/dirs on big servers
Wordlists (SecLists)	https://github.com/danielmiessler/SecLists	All wordlists needed for recon

AI Use:

- Generate targeted wordlists
- Summarize 10k+ scan results
- Identify patterns from discovered endpoints

3. Tech Stack Fingerprinting

Tool	Link	Uses
WhatWeb	https://github.com/urbanadventurer/WhatWeb	Detect CMS, plugins, versions
Wappalyzer	https://www.wappalyzer.com	Tech stack profiling
BuiltWith	https://builtwith.com	Web frameworks, JS libraries

AI Use:

- Suggest version-specific CVEs
- Generate exploit checklists
- Analyze JS files for hidden endpoints

🔵 MODULE 3 — AI for Vulnerability Identification

1. Source Code Review Tools

Tool	Link	Uses
Semgrep	https://semgrep.dev	Static code analysis
Bandit (Python)	https://github.com/PyCQA/bandit	Python security scanning
ESLint Security Plugin	https://www.npmjs.com/package/eslint-plugin-security	JavaScript security checks

AI Use:

- Explain vulnerability
- Suggest fixes
- Generate PoC payloads

2. Log Analysis

Tool	Link	Uses
ELK Stack	https://www.elastic.co/elastic-stack	Large log analysis
Wazuh	https://wazuh.com	Threat detection

Tool	Link	Uses
Splunk Free	https://www.splunk.com	Basic SIEM for training

AI Use:

- Detect suspicious activity
- Spot SQLi/XSS attempts
- Identify brute force patterns

🔵 MODULE 4 — AI + Burp Suite

Tool	Link	Uses
Burp Suite Community/Pro	https://portswigger.net/burp	Full interception, scanning, exploitation
BurpGPT Plugin	https://github.com/aress31/burpgpt	AI analysis inside Burp
Logger++	https://github.com/nccgroup/LoggerPlusPlus	Request/response logging
Autorize	https://github.com/Quitten/Autorize	Access control testing

AI Use:

- Analyze requests/responses
- Create payload variations
- Generate exploit chains
- Detect hidden parameters

🔵 MODULE 5 — AI Tools for Exploitation

1. SQL Injection

Tool	Link	Uses
SQLMap	https://github.com/sqlmapproject/sqlmap	Automated SQLi exploitation

Tool	Link	Uses
NoSQLMap	https://github.com/codingo/NoSQLMap	MongoDB/NoSQL injection

AI Use:

- Analyze SQL errors
- Generate payloads
- Write custom scripts

2. XSS Tools

Tool	Link	Uses
XSStrike	https://github.com/s0md3v/XSStrike	XSS fuzzing
DalFox	https://github.com/hahwul/dalfox	XSS scanning automation

AI Use:

- Build payload polyglots
- Obfuscate scripts
- Analyze DOM source code

3. SSRF Tools

Tool	Link	Uses
Interactsh	https://app.interactsh.com	Out-of-band testing
SSRFire	https://github.com/bcoles/ssrf	SSRF exploitation

AI Use:

- Generate cloud metadata payloads
- Map internal endpoints

4. RCE / Deserialization Tools

Tool	Link	Uses
ysoserial	https://github.com/frohoff/ysoserial	Java deserialization payloads
PHPGGC	https://github.com/ambionics/phpggc	PHP gadget chains

AI Use:

- Modify gadget payloads
- Identify vulnerable classes

🔵 MODULE 6 — AI for Bug Bounty Automation

Platforms

Platform	Link	Uses
HackerOne	https://hackerone.com	Official bug bounty programs
Bugcrowd	https://bugcrowd.com	Managed programs
PentesterLab	https://pentesterlab.com	Practical labs
TryHackMe	https://tryhackme.com	Beginner-friendly labs
HackTheBox	https://hackthebox.com	Advanced pentest labs
Intigriti	https://intigriti.com	EU-based bug bounties
YesWeHack	https://yeswehack.com	Global bug bounty programs

🔵 MODULE 7 — AI Agents & Automation Frameworks

Tool	Link	Uses
LangChain	https://python.langchain.com	Build AI pentest agents
LlamaIndex	https://www.llamaindex.ai	Document-based automation
FastAPI	https://fastapi.tiangolo.com	Host your AI tools
AutoGPT	https://github.com/Significant-Gravitas/AutoGPT	Automated tasks
OpenAI API	https://platform.openai.com	Build AI hacking tools

🔵 MODULE 8 — AI + Malware Analysis Tools

Tool	Link	Uses
Ghidra	https://ghidra-sre.org	Malware reverse engineering
Detect It Easy	https://github.com/horsicq/Detect-It-Easy	Identify file types
VirusTotal	https://virustotal.com	Static + behavioral analysis

AI Use:

- Decode obfuscated strings
- Explain malicious functions
- Generate IOCs

🔵 MODULE 9 — Social Engineering + AI Tools

Tool	Link	Uses
GPT Email Analyzer	—	Identifies phishing content
HaveIBeenPwned	https://haveibeenpwned.com	Breach data lookup
OSINT Framework	https://osintframework.com	Recon sources

🔵 MODULE 10 — AI Tools for Defensive Security

Tool	Link	Uses
CrowdSec	https://crowdsec.net	Modern IDS
Wazuh	https://wazuh.com	Endpoint monitoring
ELK Stack	https://www.elastic.co	Threat detection

Conclusion — AI Tools

- AI tools automate **recon**, reducing hours of scanning into minutes.

- AI models generate **precise payloads** for SQLi, XSS, SSRF, LFI/RFI, and deserialization testing.
- AI-assisted Burp Suite plugins help identify **patterns, missing parameters, auth flaws, and logic issues**.
- AI code analyzers detect **vulnerabilities from source code** instantly.
- AI generates **custom wordlists**, endpoint predictions, and tech-stack–specific attack paths.
- AI agents execute **continuous, autonomous bug bounty recon** without manual work.
- AI improves **false-positive filtering**, reducing noise from subdomain scans and fuzzing tools.
- AI enhances **log analysis**, spotting anomalies and attempted attacks instantly.
- AI transforms raw outputs (Nmap, FFUF, Burp logs) into **human-readable summaries**.
- AI tools help create **professional reports**, CVSS scoring, PoCs, and mitigation guidance.
- AI greatly speeds up **threat detection**, responding to suspicious events in real time.
- AI boosts **learning speed**, helping beginners master concepts much faster.
- The combination of AI + traditional tools creates a **supercharged ethical hacker workflow**.

🤖 AI Tools Used in This Course (Complete List)

🔵 1. Large Language Models (Core AI Engines)

- **ChatGPT**
- **Claude AI**
- **Google Gemini**
- **Meta LLaMA (local models)**

- **Qwen (local/open-source models)**
- **Mistral AI**
- **DeepSeek**

🔵 2. AI Automation Frameworks

- **LangChain** — build custom hacking agents
- **LlamaIndex** — create document-based AI systems
- **AutoGPT** — automates long tasks
- **OpenAI API / Claude API / Gemini API** — integrate AI into tools
- **FlowiseAI** — no-code AI pipeline builder
- **FastAPI (with AI)** — host custom security agents

🔵 3. AI-Enhanced Recon Tools

- **BurpGPT (Burp Suite plugin)**
- **ChatGPT Recon Prompt Packs**
- **AI Wordlist Generators**
- **AI Fingerprinting Assistants**
- **AI Screenshot Analyzer Tools**
- **AI DNS/Endpoint Pattern Detectors**

🔵 4. AI for Payload Creation

- **AI Payload Builder** (In ChatGPT / Claude)
- **AI XSS Polyglot Generator**
- **AI SQLi Payload Designer**
- **AI SSRF Payload Mapper**
- **AI LFI/RFI Bypass Generator**
- **AI Encoding/Decoding Tools**

🔵 5. AI Code Review & Static Analysis Tools

- **AI Code Explainer (ChatGPT / Claude)**
- **SecureGPT**
- **ASTRA AI Code Review**
- **AI SAST Assistants**
- **AI Dependency Vulnerability Checkers**

🔵 6. AI for Log Analysis & SIEM

- **AI Log Analyzer**
- **AI SIEM Assistant**
- **AI Threat Intelligence Tools**
- **AI-Based Nmap Output Analyst**
- **AI Burp Traffic Analyzer**

🔵 7. AI for Bug Bounty Automation

- **AI Recon Agent**
- **AI Endpoint Discovery Agent**
- **AI Subdomain Classifier**
- **AI Screenshot Classifier (Staging vs Prod)**
- **AI Vulnerability Prioritizer**
- **AI Bug Report Writer**

🔵 8. AI Tools for Malware & Binary Analysis

- **AI Malware Code Explainer**
- **AI Reverse Engineering Assistant**
- **AI IOC Generator**
- **AI Pattern Recognition for Malware Behavior**

🔵 9. AI OSINT & Social Engineering

- **AI OSINT Data Summarizer**
- **AI Person/Company Recon Assistant**
- **AI Phishing Simulation Generator**
- **AI Threat Modeling Tools**

🔵 10. AI for Reporting & Documentation

- **AI CVSS Scoring Tool**
- **AI Report Generator**
- **AI PoC Writer**
- **AI Executive Summary Writer**
- **AI Remediation Suggestion Tool**

Summary: Why These AI Tools Matter

- Speed up recon
- Generate payloads
- Analyze code
- Read logs
- Find vulnerabilities
- Write reports
- Automate full pipelines
- Build custom hacking agents