RESEARCH PAPERS REFERRED

S. No	Paper Title	Author(s)	Year	Summary	Dataset Used	Preventive Methods	Results	Strengths	Limitations
1	Automated Penetration Testing: Formalization and Realization	C. Skandylas, M. Asplund	2024	Discusses formalization of automated penetration testing, evaluating AI-based approaches for security assessment	-	AI-driven automated pentesting	Highlights improvements in AI-based security analysis	Framework for automated penetration testing	Ethical concerns, reliance on AI
2	CIPHER: Cybersecurity Intelligent Penetration-testing Helper for Ethical Researcher	Derry Pratama, Naufal Suryanto, Andro Aprila Adiputra, et al.	2024	Proposes an AI-driven assistant for penetration testers, utilizing NLP models to automate security assessments	Pentesting QnA Dataset, OpenHermes Dataset	AI-assisted penetration testing guidance	AI models improve efficiency in security testing	AI-driven penetration testing frameworks	Model hallucinations, reliance on pre-trained knowledge
3	Maximizing Penetration Testing Success with Effective Reconnaissance Techniques using ChatGPT	Sheetal Temara	2024	Explores ChatGPT's role in reconnaissance for penetration testing	Case study using ChatGPT queries	AI-assisted reconnaissance	Improves penetration testing planning	Efficiency gains	Potential biases, incorrect responses
4	Offensive AI: Enhancing Directory Brute-forcing Attack with the Use of Language Models	Alberto Castagnaro, Mauro Conti, Luca Pajola	2024	Investigates AI-enhanced directory brute-forcing attacks	1M URLs (universities, hospitals, etc.)	Language Model-based brute-forcing	Increases efficiency by 969%	AI significantly improves attack rates	Ethical concerns, misuse
5	PentestGPT: An LLM-empowered Automatic Penetration Testing Tool	Gelei Deng, Yi Liu, Víctor Mayoral-Vilches, et al.	2024	Evaluates LLMs for penetration testing, introduces PentestGPT framework	HackTheBox, VulnHub (182 sub-tasks)	LLM-guided pentesting	Outperforms GPT-3.5 by 228.6%	Interactive penetration testing	LLMs struggle with context retention
6	Getting pwn'd by AI: Penetration Testing with Large Language Models	Andreas Happe, Jürgen Cito	2024	Examines LLMs as AI sparring partners for penetration testers	MITRE ATT&CK tactics, vulnerable VM	AI-guided security testing	Shows AI-assisted penetration testing potential	AI assists human testers	LLMs struggle with full context retention
7	An AI-Based Approach for Automating Penetration Testing	-	2024	Discusses AI-assisted pentesting, explores automation challenges in ethical hacking	-	Automated AI-based penetration testing	Improves efficiency in vulnerability identification	AI reduces manual effort	Ethical concerns, reliance on training data

8	Towards Automated Penetration Testing: Introducing LLM Benchmark, Analysis, and Improvements	Isamu Isozaki, Manil Shrestha, Rick Console, Edward Kim	2024	Proposes an LLM-based benchmark for penetration testing, evaluates GPT-4o & Llama 3.1	PentestGPT benchmark (HackTheBox, VulnHub)	AI-driven pentesting automation	GPT-4o, Llama 3.1 show progress, but not fully automated	Structured benchmarking for AI in pentesting	LLMs require human oversight
9	AUTOATTACKER: A Large Language Model Guided System to Implement Automatic Cyber-attacks	Jiacen Xu, Jack W. Stokes, Geoff McDonald, et al.	2024	Introduces AUTOATTACKER, an LLM-guided system for automating post-breach attacks	Simulated network, Metasploit	AI-driven cyber-attacks	GPT-4 achieves full attack automation	Enhances security testing	Risk of AI-powered cyber-attacks
10	Knowledge-Informed Auto-Penetration Testing Based on Reinforcement Learning	Yuanliang Li, Hanzheng Dai, Jun Yan	2024	Uses reinforcement learning with reward machines for automated penetration testing	MITRE ATT&CK datasets	AI-powered lateral movement automation	RL improves efficiency in pentesting	Knowledge-guided AI decisions	Complexity in RL implementation
11	Hacking, The Lazy Way: LLM Augmented Pentesting	Dhruva Goyal, Sitaraman Subramanian, Aditya Peela	2024	Introduces 'Pentest Copilot,' an LLM-assisted pentesting tool	Testbenching framework (Boot2Root box)	LLM-augmented penetration testing	GPT-4-turbo improves efficiency	AI-driven pentesting assistance	Requires ethical safeguards
12	PenTest++: Elevating Ethical Hacking with AI	Haitham S. Al-Sinani, Chris J. Mitchell	2024	AI-augmented penetration testing system, PenTest++, integrates automation	Simulated pentest environment	AI-enhanced pentesting workflows	AI streamlines pentesting, reduces effort	Scalable automation	AI hallucinations, ethical concerns
13	A Unified Modeling Framework for Automated Penetration Testing	Yunfei Wang, Shixuan Liu, Wenhao Wang, et al.	2024	Introduces AutoPT-Sim, a modeling framework for penetration testing automation	Publicly available network dataset	Policy automation for pentesting	AutoPT-Sim improves AI-assisted security testing	Unified approach for pentesting modeling	AI limitations in real-world applications