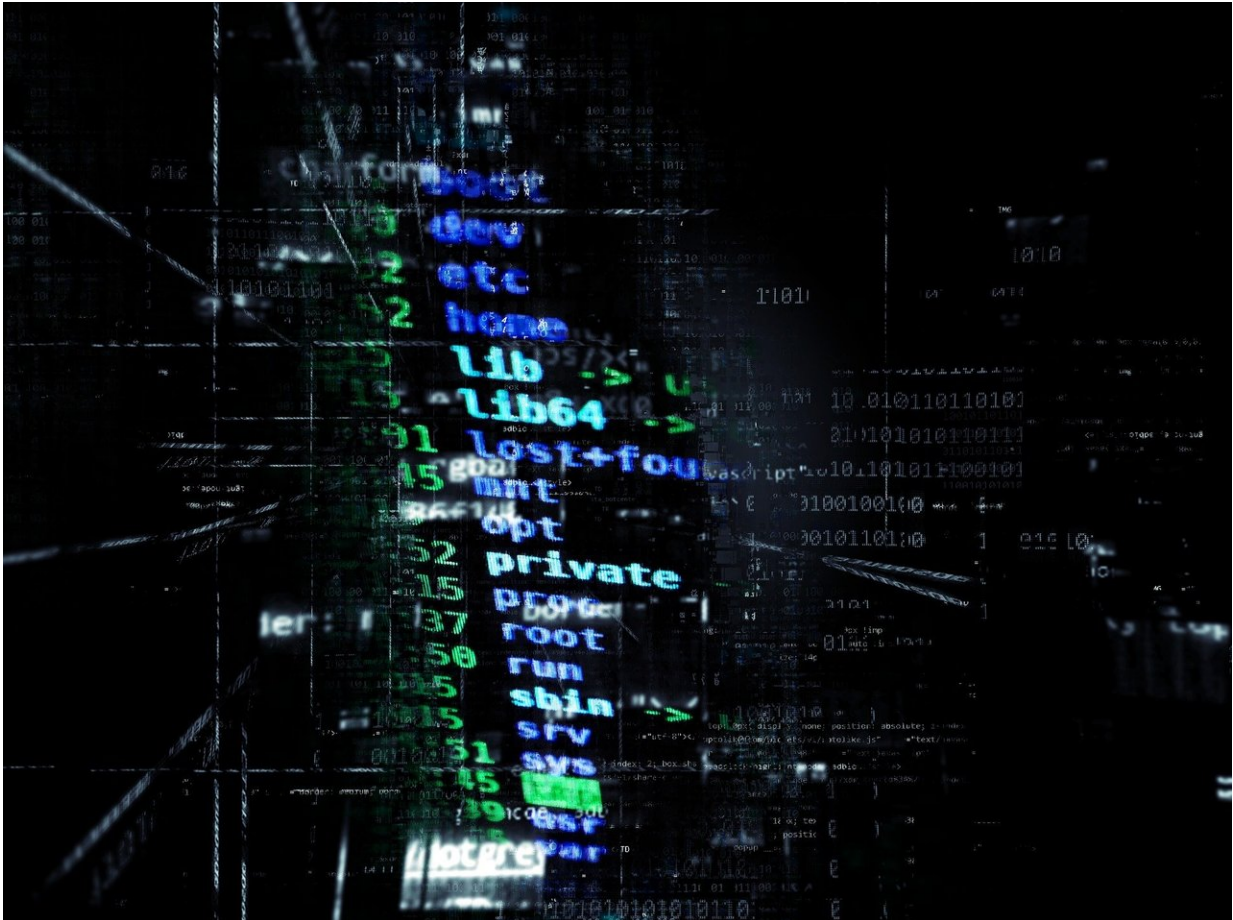# Study tests if AI can help fight cybercrime

March 25 2024, by Charles Darwin University

Credit: CC0 Public Domain

Artificial Intelligence (AI) could become a crucial asset to fight the growing global risk of cybercrime, a new study with Charles Darwin University (CDU) has found.

The study, led by researchers from CDU's Energy and Resources Institute alongside Christ Academy Institute for Advanced Studies in India, examined if generative AI (GenAI) could be used in penetration testing, known as pentesting, which is a cybersecurity exercise aimed at identifying weak spots in a system's defenses. [Generative AI for pentesting: the good, the bad, the ugly](#) was published in the *International Journal of Information Security*.

Researchers used ChatGPT to run a series of pentesting activities in reconnaissance, scanning, [vulnerability](#) assessments, exploitation, and reporting activities.

Prompts included trying to anonymously log into a server and download files, inspect source codes of webpages, and find data embedded within an archive.

Co-author and CDU Senior Lecturer in Information Technology Dr. Bharanidharan Shanmugam said the purpose of the study was to explore whether AI could be used to automate some pentesting activities, with the results showing ChatGPT had enormous potential.

"In the reconnaissance phase, ChatGPT can be used for gathering information about the target system, network, or organization for the purpose of identifying potential vulnerabilities and attack vectors," Dr. Shanmugam said.

"In the scanning phase, ChatGPT can be used to aid in performing detailed scans of the target particularly their network, systems and applications to identify open ports, services, and potential vulnerabilities.

"While ChatGPT proved to be an excellent GenAI tool for pentesting for the previous phases, it shown the greatest in exploiting the vulnerabilities of the remote machine."

Dr. Shanmugam added while the technology could revolutionize pentesting, use of AI to improve cybersecurity must be strictly monitored.

"Organizations must adopt best practices and guidelines, focusing on responsible AI deployment, data security and privacy, and fostering collaboration and information sharing," he said.

"By doing so, organizations can leverage the power of GenAI to better protect themselves against the ever-evolving threat landscape and maintain a secure digital environment for all."

More information: Eric Hilario et al, Generative AI for pentesting: the good, the bad, the ugly, *International Journal of Information Security* (2024). DOI: 10.1007/s10207-024-00835-x

Provided by Charles Darwin University