Study tests if AI can help fight cybercrime

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


Dr Bharanidharan Shanmugam

DARWIN, NORTHERN TERRITORY, AUSTRALIA, March 25, 2024 /EINPresswire.com/ -- Artificial Intelligence (AI) could become a crucial asset to fight the growing global risk of cybercrime, a new study collaboration with Charles Darwin University (CDU) in Australia and Christ Academy Institute for Advanced Studies in India, 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 defences.

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 organisation 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 revolutionise pentesting, use of AI to improve cybersecurity must be strictly monitored.

“Organisations 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, organisations can leverage the power of GenAI to better protect themselves against the ever-evolving threat landscape and maintain a secure digital environment for all.”

Generative AI for pentesting: the good, the bad, the ugly was published in the International Journal of Information Security.

Emily Bostock
Charles Darwin University
media@cdu.edu.au
Visit us on social media:
Facebook
Twitter
LinkedIn
Instagram
YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/698475936

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2024 Newsmatics Inc. All Right Reserved.