Generative AI Classroom Exercise: Incident Response

Joel D. Offenberg (CISSP PMP)

Howard Community College

The Setup

- Thanksgiving Break looms
- Prof. Joel is inspired to try an AI-focused exercise in class.
- Will an AI-focused exercise help students learn?
- Will an AI-oriented exercise convince students to turn up, rather than skip out on the last class before break?

How to AI in Cyber

- Prof. Joel asks ChatGPT for inspiration: How is AI being used in the practice of cybersecurity?
- *Answer: Instutions are using Generative AI to run incident response simulations*
- After a little research, Prof. Joel finds several examples of real-world organizations using Generative AI for IR table-top exercises (mWISE Conference, 2024; Mardock, A., 2024)
- Good news! Incident Response is the topic leading up to break in the Security+ course!
- Prof. Joel replicates this exercise in a classroom setting.

The Prompt (based on Mardock's work)

Let's play an incident response simulation game. You will be the story-teller and tell us what the incident response team sees. I will be the incident response team and tell you our responses and what we find.

Observations & Recommendations

- Because the prompt was open-ended, ChatGPT would come up with a different scenario each time. If you want a repeatable scenario, you need to specify it in the prompt.
- Having students break into teams of 4-6 and each work on their own scenario would allow more individuals to participate in the discussions.
- It would be interesting to try other GenAI platforms and slightly different prompts.
- Thoughts for grading: have students write up a report or incident response template based on

How Did It Go?

- For a one-off test, this seemed pretty successful.
  - Students, based on informal discussion, felt this was a valuable exercise.
  - The students applied the principles they learned in the CompTIA Security+ curriculum to the exercise.
  - There was discussion about how to interpret what ChatGPT told them and what actions to take or what research to conduct.
  - ChatGPT kept the narrative going and the students really had to think; the responses were not obvious.
  - We (students and instructor!) learned a bit about how GenAI responds in these situations. Examples:
    - It wasn't clear that ChatGPT would allow us to resolve the incident, or if it would just keep adding "more" at each step.
    - ChatGPT would provide a great deal of details in response to each response.
- 16 out of 22 students turned up for class!
  - This was not a graded assignment (points for participation).

References

- Mardock, A. (2024, January). *Prompting for Cyber Incident Response Practice- a generative AI example.* Linkedin: https://www.linkedin.com/pulse/prompting-cyber-incident-response-practice-ai-april-mardock-cissp-kb7uc/

- mWISE Conference (from Mandiant). (2024, October). *Generative AI Cyber Incident Response Tabletop Exercise.* [Video]. YouTube. https://www.youtube.com/watch?v=w5mpUs29JSI