19 May 2022

Volatility (1:00 – 1:50 pm EST)

Ransomware and the Zero Trust Framework (2:00 – 2:50 pm EST)

Mark your calendars and come join your friends in the CAE community for a Tech Talk. CAE Tech Talks are free and conducted live in real-time over the Internet so no travel is required. Capitol Technology University (CTU) hosts the presentations using Zoom which employs slides, VOIP, and chat for live interaction. Just log in as Guest and enjoy the presentation(s).

Below is a description of the presentations and logistics of attendance:

PRESENTATION #1

Topic: Volatility

Time: 1:00pm – 1:50 pm EST

Location: https://captechu.zoom.us/j/664120328

Just log in as Guest and enter your name. No password required.

Presenter(s): George Meghabghab, Roane State Community College

Description: Volatility is an open-source memory forensics framework for incident response and malware analysis. The presentation is of practical nature and will involve a hands-on analysis of a memory image. The presentation will extract network information, process information, event logs and hive registers. We will recover event logs and show how they would like at the time of the actual acquisition. Ban accounts will be recovered. We will also include hybrid malware analysis of our processes and determine which process caused the malware infection.

PRESENTATION #2

Topic: Ransomware and the Zero Trust Framework

Time: