The Great Computer Challenge, 2025
Cybersecurity Challenge, Level 4

Background

Teams will solve a selection of cyber security problems using their choice of tools. Contestants will be given a Virtual Machine (VM) for the competition. Contestants should install any tools they might need on their computer before the event.

Guidelines & Requirements

VMWare Workstation Player is needed. Each team member may have a computer for the cyber security challenge.

Internet Access: Yes. The computer should have a compatible wireless adapter. *If possible, avoid the use of Tablets and Chrome Books.*

Helpful tools and skills: Kali Linux, firewall basics, Microsoft Baseline Security Analyzer, Sysinternals tools, bash scripting, HTTP, FTP, nmap, sqlmap, netcat, Wireshark, Nikto, ZAP, burp suite, hex editor, and desktop.

Cyber Security teams can use the tools listed (or others) on Kali Linux, but to solve the problems, teams will need to know some Windows firewall basics, using MSBA, sysinternals tools, and bash scripting. It is also expected that contestants have a basic understanding of http and ftp.

Challenge

Jeopardy-style CTF: web-based competition environment, letting students demonstrate cybersecurity knowledge in a competitive game.

Challenge List

Crypto, Cyber Concepts, Exploitation, Forensics, Networking, Reconnaissance, Software Tools, Reverse Engineering (Intro and advanced), Web Concepts

Judging Criteria

Judges will evaluate the answers to problems without considering the tools used. Solutions will be delivered digitally, and an auto point tracker will be available during the competition, but it does not denote official final scores. Solutions will be evaluated based on answers to cybersecurity questions and evidence provided. Final point tallies will be available and announced at the closing ceremony. Individual feedback can be requested following the close of the competition.

Have fun and thanks for participating in the Great Computer Challenge, 2025!