SkillsUSA Maryland State Championship
Cyber Security State Competition Update (3/3/26)

Cyber Security

Thank you for participating in the SkillsUSA Maryland Cyber Security competition on **Saturday, April 18, 2026**. This year, there will be seven distinct sections of the competition:

Sections:

1. CompTIA Security+ Technical Exam (Multiple Choice Questions)
2. Cisco Packet Tracer Challenge
3. Network (Wireshark)/Digital Forensics Challenge
4. Log Analysis Challenge
5. Scripting for Cybersecurity Challenge
6. Vulnerability Assessment Pentesting Challenge
7. Technical Interview Challenge
   - *Professional Activities Interview Topic:*
     Cyber Security Considerations of Agentic Artificial Intelligence (AI)

Schedule (Subject to Change):

08:00 – 08:10 am	Orientation
08:10 – 08:40 am	Technical Exam
08:40 – 12:00 pm	Competition Performance
12:00 – 12:30 pm	Lunch
12:30 – 1:00 pm	Competition Performance
1:00 – 1:30 pm	End of Contest/Contest Debrief

Equipment and Materials:

Supplied by each contestant (each team member should have):

- Resume
- Writing instrument
- Laptop or desktop computer capable of running Cisco Packet Tracer and Wireshark
  - Minimal software needed/website access on laptop or desktop for contest:
    - Cisco Packet Tracer version 9.0.0 (as of this writing)
    - Wireshark version 4.6.3 (as of this writing)
    - Ability to access Google Suite including Google Forms
    - Ability to access metadata2go.com, bellard.org/jslinux, trinket.io/python, cyberchef.org, and tenable.com/plugins

Competition Details:

The technical exam portion of the state competition (section 1) will be completed via Google Forms. ***Both*** team members will ***separately*** be completing the technical exam and then added together to comprise the team score. This testing will be separate from any of the testing students completed in the SkillsUSA online testing system prior to the start of the competition.

Students can have one or both team-members log on to access and download the Packet Tracer material from their contestant Google Drive folder (section 2) ***using their own laptop*** on the CCCTC public Wi-Fi. Please check to ensure your equipment is functional prior to the competitive event. Students will also need at least one member to ***create a free Cisco NetAcad*** username and password. Please visit www.netacad.com for a free account. It is also **recommended** that you sign-up and practice on the Intro to Packet Tracer free course to become familiar with the software prior to the event. ***End devices, switches, routers, firewalls, and servers*** may be configured during this challenge.

Students can have one or both team-members log on to access and download the Wireshark PCAP material from their contestant Google Drive folder (section 3) ***using their own laptop*** on the CCCTC public Wi-Fi. Please check to ensure your equipment is functional prior to the competitive event. Wireshark will only be used for analyzing pre-captured PCAP data and students ***will not*** have to capture live traffic on their laptops. Students will also complete a digital Portable Document Format (PDF) metadata forensics challenge using a free web browser-based tool (metadata2go.com).

Students can have one or both team-members log on to access and download the log analysis (text file) material from their contestant Google Drive folder (section 4) ***using their own laptop*** on the CCCTC public Wi-Fi. Students will complete a log analysis challenge using a free web browser-based command line tool (bellard.org/jslinux).

Students can have one or both team-members log on to access and download Python script files (.py) from their contestant Google Drive folder (section 5) ***using their own laptop*** on the CCCTC public Wi-Fi. Students will assess password validation script logic using a free web browser-based Python interpreter (trinket.io/python) and analysis/decoding tool (cyberchef.org).

Students can have one or both team members log on to access and download an identified vulnerabilities PDF report from their contestant Google Drive folder (section 6) ***using their own laptop*** on the CCCTC public Wi-Fi. Students will analyze collected information to identify, prioritize, and provide justification for vulnerabilities that pose the possibility of exploitation.

During the morning competition performance time, students will have a scheduled technical interview (section 7) with a panel to mimic a real-life scenario meeting in which students will provide legally sound advice and recommendations to management centered around the topic of ***agentic artificial intelligence*** (students are encouraged to research this topic prior to competition day to gain familiarity). Students will be given 10 minutes to provide a verbal response to technical questions.

FAQs:

Q: "The update stated that the students will need to bring their own laptops to the event. What specs are required for the competition? Will they be required to download anything? Will they need to be able to install software?"

A: The laptops must be able to run Packet Tracer and Wireshark software and be able to navigate the internet. These are the only needed special applications to compete. ***Packet Tracer AND Wireshark MUST be installed PRIOR to the competition.*** Please verify ***prior*** to arriving the day of the competition these applications have been successfully installed, can be opened with student permissions, and in the case of Cisco Packet Tracer, logged in.

Q: "Will student laptops need to have admin rights?"

A: Admin rights are **not** required AFTER installing Packet Tracer and Wireshark. No additional software will be required as the only other accesses needed will be Google Suite tools such as Google Forms as well as other free and openly available web-browser-based tools (see *Equipment and Materials*).

Q: "For Section 1 (CompTIA Security+ Technical Exam), would contestants be awarded the industry certification if we pass the test per CompTIA Security+ requirements? Or is this exclusively for competition points?"

A: For the SkillsUSA Maryland state Cyber Security contest, competitors will be completing a CompTIA Security+ technical exam representative of the SYO-701 certification competencies to be taken via Google Forms. At the SkillsUSA Maryland state level, this station is exclusively for competition points.

Q: "Will competitors be expected to perform any live data capture? (Wireshark PCAP, Log .txt, Nessus .nessus Scans, etc.)"

A: Students will NOT be performing ANY live data capture at the SkillsUSA Maryland state Cyber Security contest. Students will be analyzing pre-captured artifacts and can use free, online tools day-of the competition for analysis (see *Equipment and Materials* section).

Q: "For the *Log Analysis* section, is there any additional software required bring up the logs itself?"

A: Competitors can use the free web browser-based Linux command line terminals at bellard.org/jslinux to leverage Linux command line text tools in the browser to extract details of interest from a text log file. While competitors are welcome to bring a computer with the Linux operating system installed to use command line tools for this challenge, it is not required, nor is using command line tools to analyze the pre-captured text log file. Any text editor of choice may also be used, should that be the competitor's preference for this challenge.

Note:

Specific written test or challenge questions, including the specific assessment items in the Packet Tracer, Wireshark PCAP, digital forensics, log analysis, script, vulnerability assessment, or technical interview will not be addressed by the Chair prior to the competitive event. Please reference the Cyber Security SkillsUSA National Technical Standards for further guidance of what subject matter students should be expected to perform within.

Additional Questions?:

Please email arthurbridder@gmail.com and carbon copy (CC) SkillsUSA Maryland State Director Chuck Wallace at charles.wallace@maryland.gov with any queries regarding the competitive event. Responses will be compiled and shared with competing students and instructors via the State Conference webpage.

Brad Ridder

SkillsUSA Maryland Cyber Security Contest Chair