CyberPatriot Tips

Mandy Galante, coach / mentor for Team Mantrap, Red Bank Regional HS

Most important tip: DOCUMENT EVERYTHING you do in both practices and competitions

Competing :

- Be a team - members should contribute, listen and then come up with a plan that everyone can support. Time is important, but keeping everyone in the loop and on the same page will save lots of time in the end.
- Be prepared – make sure all your equipment has been tested, with backups if possible. Have several extra computers with Internet and printing access to use for research and to print out info.
- Have a plan – use the first practice to identify what it means to *secure a system.* Use this information to create a "Do This First" plan of basic configuration steps that you will apply in future competitions.
- Divide up responsibilities – each team member will need to become the "expert" at several things – some of the categories can be OS, services like SQL or DHCP, by types of vulnerabilities. Each member should research and collect resources for their topic which should include software, websites, articles and books.
- When a practice or competition is over, use that experience to figure out what you don't know. Always save the VMs to use for practice and to review with your documentation of what steps you tried.
- There will be a LOT of downtime for restarts, updates and when things don't work – don't waste that time! Use it to collaborate, to do some research or to let out some energy. Downtime and frustration are real-life hurdles in cybersecurity so figure out how to make lemonade out of lemons.

Skills for competing:

(Not necessary for everyone to know ALL of this, but it helps if some level of these skills are already represented in at least a few of your team members)

- Experience with many Windows and Linux Operating Systems, including Server versions. Understand how to install an OS, partitioning, hidden files, services, network settings, file sharing, user creation.
- Experience with Command Line interface for Windows and Linux. Be able to bypass the GUI to perform many basic tasks and also to use tools that are CLI only such as arp, netstat, ping, ipconfig, or tracert.
- Knowledge in basic networking and services – physical and logical addressing, how packets travel, TCP/IP protocols and ports, how to use a packet analyzer, DHCP, DNS, Web Services, SQL, FTP, Telnet.
- Knowledge in basic systems hardening – OS updates, group policies, OS patching, password strengthening, OS service packs, malware detection, common vulnerabilities . . . Oh, wait . . . did I say OS updating?
- Proficient in research to find solutions on the Internet and in reference books

Final Note: Cyberpatriot is NOT a capture the flag or a scripting contest – those types of skills will be marginally useful in performing hardening tasks. However it is helpful to have a basic grasp of computer programming.

Adult help requirements - the Coach and Mentor can be the same person.

Coach - one person who is willing to do all the paperwork, planning, scheduling and nagging. They will serve as the authority for the group in all areas, including team selection and enforcement of behavior.

Mentor - one person with expertise in computers, networking and cybersecurity to provide lessons and guidance. They will instruct on these topics, help develop skills in practice, and help with strategies / assessments in post-competition.