NECCDC 2023 - Information Session #2
Thursday Dec 15, 2022

Q&A Session

Q: What is useful to know?
A: Docker Swarm has mesh networking, which may need to be paid attention to

Q: Do we anticipate training?
A:Will have training provided for moderators.If you have any suggestions for moderator training, let us know.

Q: Would someone affiliated with a different school participate as a moderator for another school?
A: We're going to say no.

Q: Is SOC returning this year? What is happening? Will SOC be a separate set of room and equipment?
A:So far, we will let the teams decide where to dedicate resources. Most things will revolve around SaaS solutions for Qualifier. Regional there will be more focus on the SOC / SIEM component.

Q: ID Management - AD/LDAP anything happening in that realm? Linux or Windows-based.
A:Yes, that can be expected. We will confirm the level later. There will be Windows AD in the mix.Qualifier is just some hours in one day, so will not expect students to build everything from scratch. Teams can expect a reasonable setup for Windows AD.

Q: Do you anticipate Red Team to have much presence as Qualifier?
A:Same as usual. Maybe put stuff on screen, nothing too heavy. Save their "good stuff" for Regional.

Q: Will we be expecting Cisco integration for Qualifier?
A:

Q: Had mentioned earlier the Qualifier will be Linux heavy. What is the balance between Linux and Windows?
A: Docker swarm and SaaS solution itself will be purely Linux. Will be supporting infrastructure that is Windows. For a typical SaaS solution what infrastructure is needed to support it? Majority is Linux.

Q: Hints about the flavor of Linux?
Can expect Alpine Linux which could be one of many common images that is associated with SaaS.

Q: Last year you offered Wazuh training. Will you offer some training for Docker, etc.?
A:Had reached out to Docker and requested offering training / resources. Even if they don't provide anything, go to Docker.com, which has amazing documentation.

Q: What orchestration will need to be familiar with?
A:Docker stack, ansible, terraform using for infrastructure on our side (not necessarily into competition itself)

Q: Any preconfigured pipelines?
A:Idea is a company using Jenkins to carry out services. Won't be just bare bones.

Q: Should we expect to use pfsense or any router software like that?
A:Networking element is still being decided since involvement with Cisco. Potentially Cisco element in Regional.. Expect bulk on networking technical challenges to be in containers themselves. Docker has a nice networking stack, and can set up nice overlay networks within Docker itself. May throw in a surprise?

Q: Network Firewalls?
A: For Qualifier, since heavy focus on containers, and will not just throw in Cisco firewall right away, that the focus will be more on the firewalls within the hosts and Docker containers. When it comes to Docker swarm and mesh networking, implications on firewalls. So understanding host-based firewalls teams would be something teams would benefit from and understanding how firewalls and mesh networking interact with each other would be something that might be tricky.

Q: Do you expect availability zones to be exposed to students?
A: Will be high availability to Docker swarm, but only have availability zones to be exposed in Regional.

Q: Do you see vulnerability management from the start of competition or would we see injects?
A: We have historically had injects related to vulnerability scanning and management. Idea that as a SaaS provider with all Docker containers how will you watch out for the existence of vulnerabilities if you would be notified? How would you handle that?

Q: How many endpoints can we expect?
A: 8-9 endpoints / EC2 instances

Q: How many colleges have submitted rosters / payments so far?
A: We're almost at double digits so far.

Q: Is orientation still available?
A: Yes, contact Dave Murray orientation@neccdl.org