NECCDC 2024 | FAQ

Info Session #2 | Q&A - Thursday Jan 4, 2024, 6pm ET

Q: What's the URL for Authorized Repo's?
A: Authorized Repos | NECCDC 2024

Q: What's the PDF for RT Advice?
A: Advice_from_NECCDC_RT.pdf

Q: Do you have advice for how teams should discuss root cause when RT malware/tools were built into the systems prior to the competition?
A: The reason why RT puts things on systems ahead of the competition is to be fair. Those that don't pre-deploy is a problem in that only 9/10 teams are affected due to the timing so that team gets a free pass with no implants. Most malware tools have a persistence system (if you can find and get rid of it / or reboot and have it go away … then do that). This happens at Nationals more, and we bring this to Regional (one or more systems vulnerable to end-day. Need to be able to identify systems and fix vulnerabilities, or block attackers.

Q: Will https://neccdl.org/neccdl/members/ be updated by the 20th?
A: Yes, the website will be updated as soon as possible. We do have a lag receiving information from Nationals.

Q: Do teams need to compete together in the same room and/or on-campus for the beta?
A: For the beta, the teams don't need to be on campus or in the same room, but yes, it is highly recommended as it helps with practice. However, we realize that it's not always possible for some teams based on break times.

Q: Do you want any cameras on during the qualifier?
A: For authentication purposes, team members bring a valid school ID which on-site moderators validate.

Q: Will there be another window for Github submissions before Regionals?
A: Unfortunately, there is not another window for Github submissions before Regionals due to Nationals rules.

Q: Are we still using ScoreStack, another open source project, or Nationals scoring engine?
A: We are using ScoreStack.

Q: If we are a first time team (i.e. still trying to finalize a faculty sponsor) and end up registering/submitting roster on Jan. 19, do we still need to submit a moderator on that day?
A: We can generally help with new teams. Also, you just need someone affiliated with your institution to be the coach, e.g., IT staff, prof, etc.

Q: Is there a suggested hotel, or a hotel that Pace is working with for the regional?
A: Waiting for a response, but for now, https://www.pace.edu/nearby-hotels
Millennium Downtown Hotel World Trade Center 55 Church Street New York, NY. 10007 (212) 693-2001 Exclusive discount offer for Pace University affiliates: 20% off the best available rates. Also Holiday Inn Financial District 51 Nassau Street New York, NY 10038 Exclusive discount offer for Pace University affiliates: 15% off the best available rates (Financial District location only). Use Corporate ID # 100203474 when booking. Book online or call (855) 914-1383 for reservations.

Q: Are there any scholarships or grants for participation in Regionals?
A: We will see what the numbers look like. If you are aware of any potential sponsors, please do connect us to sponsor@neccdl.org

Q: Are there updates on parking?
A: Waiting on response - will get sometime next week

Q: 3 windows servers, only AD shown in service list? Is CA no longer a service? Or file stuff?
A: AD consists of a lot of moving parts. You will see the typical parts in play domain services, DNS, and will probably see a CA somewhere since you need an element of trust in the environment. Need to trust yourself, teammates, and ensure your machines can trust each other.

Q: Wireguard is not in new topo, will blue teams use a different access method?
Is CA handled by Vault?
A: Wireguard will be the main entry point for blue teams. Can’t currently answer Vault question.

Q: It was stated that there won't be much of the "competition theme" during Qual, but the diagram we were shown during the session features a PLC. Does this mean we should expect to see some level of OT during quals?
A: What we mean is not a lot of injects related to OT stuff. This is a cyber defense competition, and not PLC management competition. Wanted to add an element of ticking services you need to keep running like your other ones, that we can relate to the OT side of things. In no way will you be asked to be OT operators. However, you are the Blue Team who has governance over the complete IT + OT infrastructure. Having responsibility for what happens on that OT network will be yours. Having an awareness of asset inventory on OT and the boundary of IT/OT will be

yours. In Qual, PLC will exist and may be a component of scoring, but won't have any functionality besides being there. Won't have functional dependencies or dynamic things going on in that space. For Regional, this will change.

Info Session #1 | Q&A - Friday Oct 20, 2023, 6pm ET

General Black Team Advice: Emphasis on RHEL IDM/FreeIPA, look into automation. For Qualifiers no AWS console access. Will be new technology that you have to learn that will be foreign to you. Credential management and Kubernetes. Some subject to change. Some would be taken out, not put in.

Q: Will the presentation be made available to share?
A: Presentation and Q&A documents will be shared after review for accuracy

Q: Do you have an anticipated time frame for knowing about hotels?
A: Have an idea of what hotels will give a discount rate. Can probably get out within a few days.Will keep trying to get better rates, but have a short list.

Q: What are the discounted hotel rates looking like?
A: https://www.pace.edu/nearby-hotels - discounts up to 20%

Q: Travel?
A: Consider travel - parking is not readily available.

Q: For firewalls - there was Palo Alto, training, is there more insight?
A: With host-based firewall rules, lots of iptables, Windows firewall, and other OS that show up. Can provide documentation that will give insight. Want to make sure you're comfortable with services. Talked about virtualized appliances in quals, but believed may be pushing too much. Host-based firewall rules would give a good foundation for a mindset for more centralized management.

Q: Qualifier / Regional Remote
A: Will be remote in that not all teams will be in the same location physically. However, all teams are expected to be physically present together on their campus in the same location. If there is a need for an exception, it needs to be discussed between the Coach/Edu Rep, the Director, and NECCDL.

Q: Is there a time when we should have moderator contact information?

A: Will be near the registration deadline. Please recruit people who have some experience, e.g., alumni, industry, or local professional organizations. Let us know if you are a new team and/or you need help with moderators.

Q: Will AWS resources be provided for blue team prep?
A: Learning materials can have links provided. The free tier for AWS - focus on VPC and Security groups.

Q: What should you advise for AWS setup?
A: AWS offers free training through AWS Academy. Can use the free tier for configurations for security groups, how to backup an instance, take a snapshot and if you can run things on your local hypervisor, go for that. Learn services on own infra and then learn AWS via AWS: https://aws.amazon.com/education/awseducate/

Q: The line between Qualifier and Regional?
A: In Qual, will not have AWS console access. Emphasis on host-based firewalls there. Andrew can recommend some labs that AWS Educate provides.

Q: MacOS?
A: AWS does provide MacOS AMI's for virtualization for EC2 instances. Up in the air right now with Black Team in discussing implementing that concept. Not a critical role, but in a typical world, you will see Windows and Mac. Definitely train for it. 99% will see in Quals or Regionals. Difference between AWS and hypervisor, if you were to allocate money to AWS, spin up some MacOS EC2 and play for an hour or two. Wouldn't spend too much time on it, but should know how to do the basics with it.

Q: WIll the Regionals be held in Manhattan or Westchester?
A: Manhattan

Q: What about safety concerns?
A: Can get a meeting with the emergency response / security department. The campus location is a pretty safe area and students frequently take a train down there. Can get a more outlined approach for security. Don't have the information at hand now.

Q: RHEL 8 or RHEL 9?
A: Hint: Version listed in AWS AMIs