Scenarios

The scenarios are an important part of the CCDC events. The scenarios provide context for the competition. Scenarios have included inheriting and protecting a Smart Grid system, recovering from confidential data loss and the firing of an IT team, and responding as field operations units deployed to specific areas designated as local disaster aid distribution centers. The NCCDC 2012 team packet is provided in Appendix C as an example of a presentation of a scenario and related materials provided to competitors.

In the 2013 NECCDC competition, Blue Teams were told that they were hired to take over IT operations for EnV research. At the request of major stakeholders, including the Department of Energy, the previous IT team was let go after confidential and proprietary EnV research documents surfaced online. As the new IT department, Blue Teams were tasked with securing the EnV network, while maintaining business operations.[22]

Competition Scenario

Your team, along with a new CIO, has been hired to take over IT operations for EnV research, Inc. At the request of major stake holders, including the Department of Energy, the previous IT team was let go after confidential and proprietary EnV research documents surfaced online.

As the new IT department, you will be tasked with securing the EnV network, while maintaining business operations.

Corporate Profile

EnV Research, Inc.

www.env.com

"Powering a greener world though sustainable energy solutions."

"EnV Research is a high-tech green energy startup focused on enabling renewable biofuels. Using the V372 chemical agent developed by EnV, a complex compound biofuel can be stabilized and suitable as a drop-in replacement for traditional petroleum-based fuel sources.

Each biofuel is different. For the V372 agent to work, the biofuel must first be tested using the EnV biofuel test kit to determine the proper levels of V372 needed. Test kits and V372 agent are purchased directly from EnV Research though its online store.

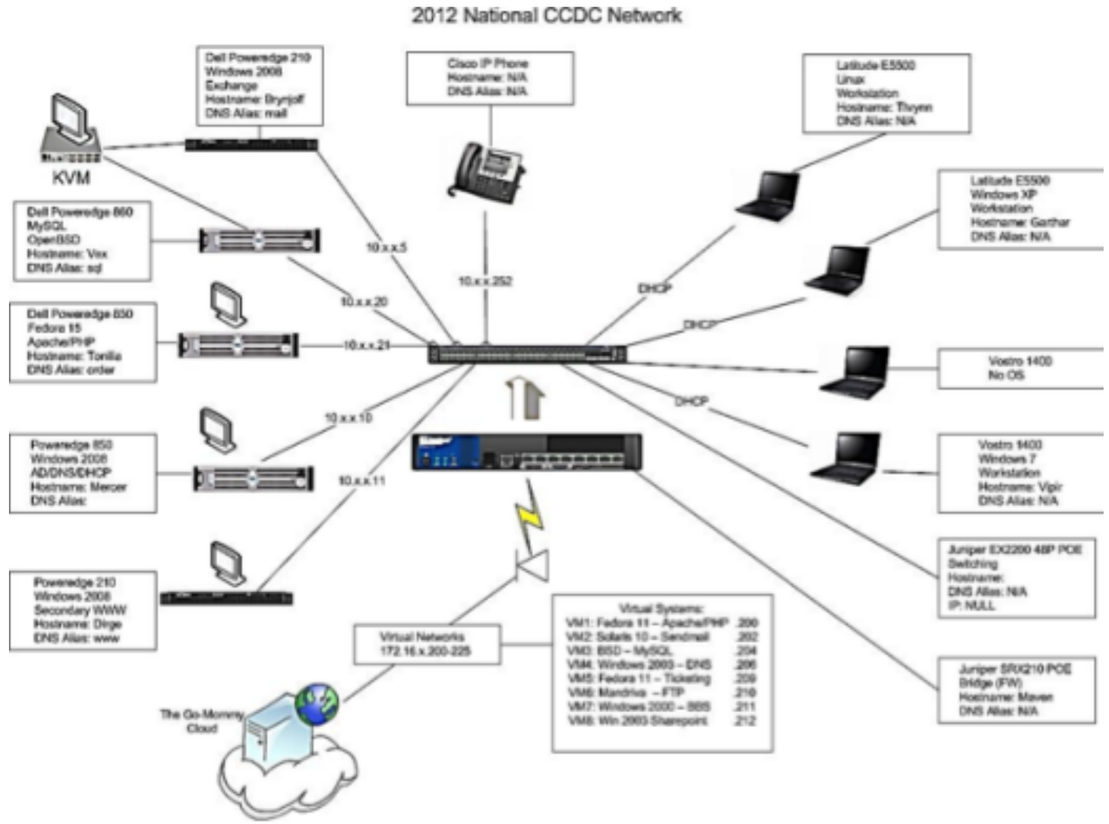
After the success of V371 which had limited availability, EnV Research commercialized V372, a next-generation agent, which quickly became used by thousands of energy companies world-wide. Today EnV is rapidly becoming one of the leading biofuel research companies in the world."

The 2014 MACCDC scenario was built around disaster management. The eight Blue Teams responded as field operation units deployed to specific areas designated as local disaster aid distribution centers. The field operation teams were responsible for deploying the data systems necessary to support the disaster response activities and delivery of aid to the local site. This part of the mission involved physical layer components and establishment of connections to a higher-level management center. Once deployed, the units maintained their systems to ensure that the necessary data arrived at the Maryland Emergency Management Agency (MEMA), which was charged with distributing aid. The units were also responsible for defending their systems from a rouge disaster site. This site was actually operated by the Red Team who attempted to have aid shipments rerouted and disrupt the flow of aid. Spectators played the role of displaced persons and provided data that specified the type and quantity of aid needed.[23]

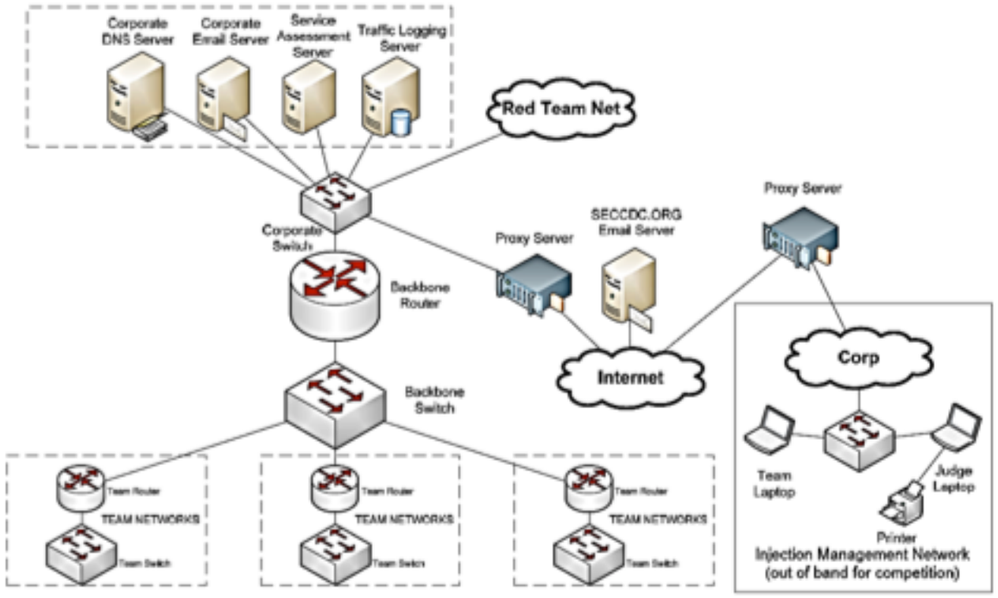
22. Northeast Collegiate Cyber-Defense Competition Team Packet (March 8-10, 2013) On0ro at the University of Maine. http://neccdc.net/wordpress/wp-content/uploads/2013/02/2013_NECCDC_Team_Packet.pdf

23 .http://maccdc.org/about/#sthash.YcpiuJzO.dpuf

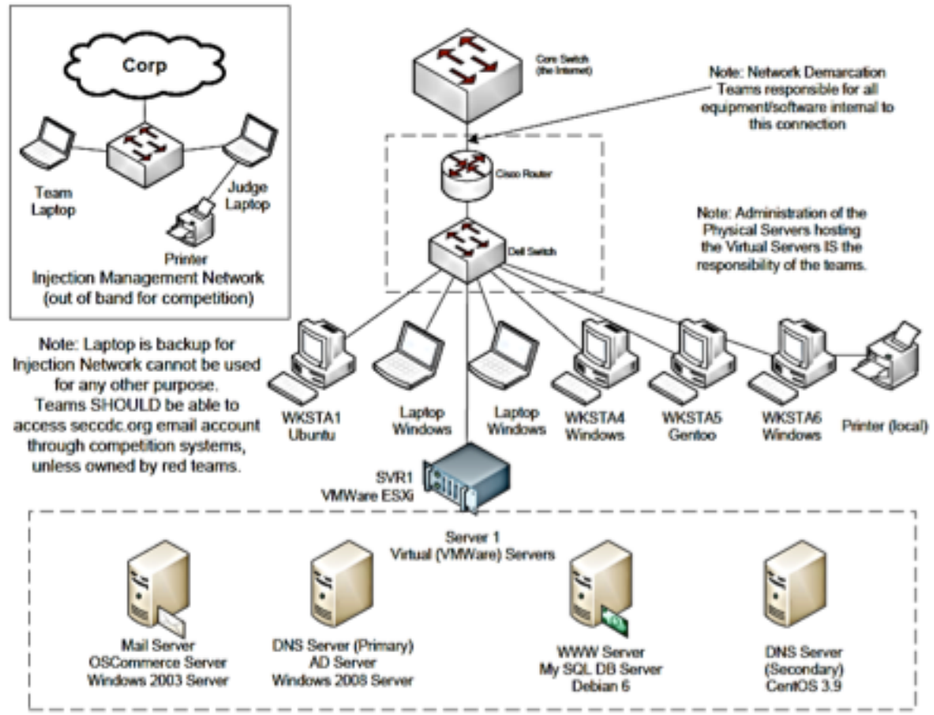
Competition Configurations



In general, CCDC events have similar network layouts. Normally, the competition networks are mostly standalone, with Internet access used primarily for obtaining patches and research. The Internet connection is either by limited external connectivity through the competition network or as a separate "outside network." The Red Team network, the White Team network, and each team network connects to a central networking device (e.g., router, firewall) that is maintained by the Operations Team.[24]



Individual team networks are connected to the competition network through networking equipment (e.g., switch, router). The rules specify that no other equipment may be connected to the competition network at any time (unless specifically given to the Blue Teams as part of the competition by the event organizers). Furthermore, each team is provided with an email account to send files to be worked on after hours. This email address is monitored to prevent teams from deleting it or using it for personal use.

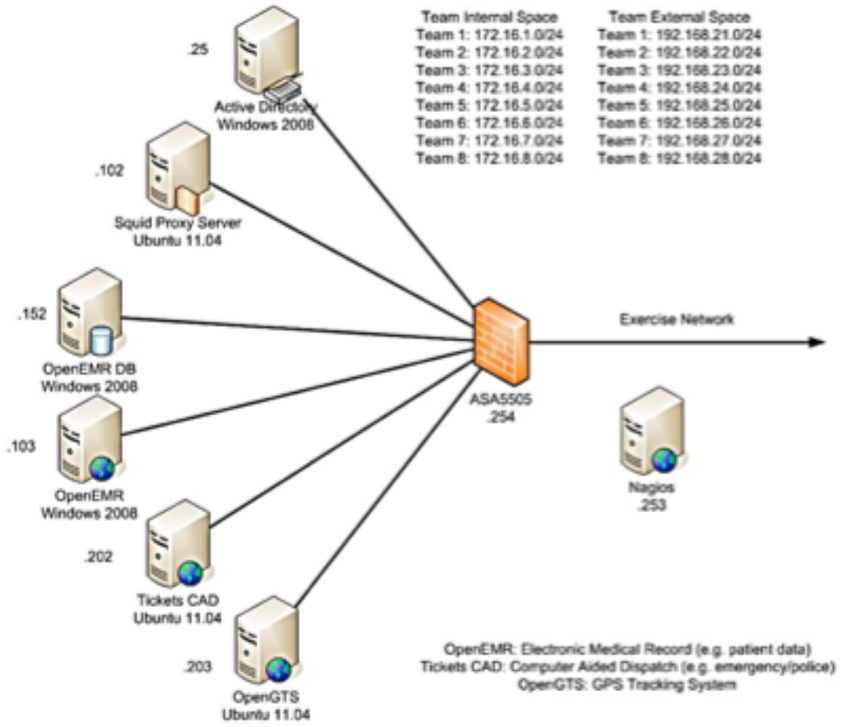


In addition to a description of the network topology, some CCDC competitions provide detailed general system information. In 2012, the MACCDC provided the following information about the systems, the roles they play and their configuration:

- Each team will be provided user-level access to a vSphere server. This server is the primary host of all your defended systems. You will connect to the vSphere server using provided PCs. Connecting information will be provided at the event.
- Team vSphere access will be limited to basic Administrator functionality. You will be able to power on/off the guest operating systems and add media (e.g., CDdrives).
- Teams will NOT be able to revert to snapshot.

24. http://www.seccdc.org/2013_docs/2013_SECCDC_TeamPacket_Final.pdf

- Teams will NOT be able to take a snapshot.
- To revert to a snapshot teams must contact Exercise Control.
- The Operations Team has access to teams' vSphere servers through an Administrator account



Post-Competition Assessment

So the competition has come to an end. The team is either still celebrating a victory or concentrating more on completing course work and perhaps enjoying a little free time. Either way the process of achieving success in the CCDC should still be present in the minds of participants and advisors. Two often understated tasks take place after the competition has concluded; post-competition debriefs and assessments. This final piece can often lead to valuable learning opportunities by giving team members a chance to analyze their individual experiences. It can also provide team advisors with information that can be used to evaluate and make improvements to programs of study. Last and definitely not least this information will lay the ground work for preparing next year's team.

A team's final score in the CCDC doesn't matter. The purpose of preparing for and playing in the competition is for players to experience activities and challenges that they might see in their future jobs. While the CCDC is an artificially generated environment, the attacks and business injects are all based on real world examples and designed by very experienced people. So, soon after the CCDC has ended it is important to schedule a debrief meeting. This will give team members an opportunity for post-competition to synthesize an understanding of their individual experience. There are several questions that can guide a post competition discussion which will provide faculty, team leaders, and future team members with the most valuable information. Some leading question may include:

- What skills were you able to apply that you learned from your course work?
- What are some examples of skills needed but no team member possessed?
- Are there skills that were needed but not presently included in your program of study?
- Describe the communications processes (or lack thereof) that occurred within the team during the competition.
- In terms of team composition in what area was the team lacking?
- Which team strategies worked and didn't work?
- Was the team effectively managed? What could have been done differently?
- Were there any obstacles that prevented the team from working together?
- Were the team member assignments relevant to the skills of those assigned?
- If you had it to do all over again how would you prepare differently for the competition?

Team Network Diagram