The 2013 NECCDC –Lessons Learned

Conference Paper · July 2013

CITATION
1

READS
140

5 authors, including:

George Markowsky
Missouri University of Science and Technology
126 PUBLICATIONS **2,727** CITATIONS
SEE PROFILE

Daryl Johnson
Rochester Institute of Technology
21 PUBLICATIONS **66** CITATIONS
SEE PROFILE

The 2013 NECCDC - Lessons Learned

G. Markowsky[1], D. Johnson[2], A. Moody[3], R. Soucy[4], and W. Stackpole[2]
[1]School of Computing & Information Science, University of Maine, Orono, ME, USA
[2]Department of Computing Security, Rochester Institute of Technology, Rochester, NY, USA
[3]Information Technologies, University of Maine, Orono, ME, USA
[4]Information Technology Service, University of Maine System, Orono, ME, USA

Abstract—*After having run the 2010 NECCDC at the University of Maine, we had an opportunity to run the 2013 NECCDC at the University of Maine. In the process, we rediscovered some lessons we had learned the first time along with a number of new lessons. We feel that the NECCDC and similar cyber defense competitions are very important for motivating students and for bringing the academic cyber defense community together. We are committed to making sure that the competitions are well supported and continue to improve. We also realized that our past system of basically having each hosting institution essentially build the competition from scratch does not contribute to keeping the competition of high quality and improving. This article serves as a how-to for staging the NECCDC or a similar competition.*

Keywords: A maximum of 6 keywords

1. The CCDC & The Regional Competitions

The Collegiate Cyber Defense Competition (CCDC) system was started in 2004 as a series of competitions designed to provide institutions with an information assurance or a computer security curriculum a competitive environment to assess their students' depth of understanding and operational competency in managing the challenges inherent in protecting computer networks and information systems. Today there are 9 regional competitions throughout the US which serve as qualifiers for the national CCDC competition held each year. The northeast region (NECCDC) was started by RIT in 2008 and represents the states of Connecticut, Maine, Massachusetts, New Hampshire, New York, Rhode Island, and Vermont. We have also had New Jersey schools that are part of the New York metropolitan area compete in the NECCDC. For more details see [1].

2. Some Basic Terminology

The participants at the NECCDC are grouped into teams. The following glossary describes the function of each team.

- Blue The competing teams are referred to as the blue teams. Each blue team functions as if it were a company IT department and carries out a number of tasks.
- Red The Red Team consists of individuals highly skilled in cyber attack. Their task is to stress test the technical skills and group dynamics of the blue teams by creating as much havoc as possible.
- White The White Team consists of individuals with a strong background in information technology. Each blue team is assigned two members of the White Team who monitor that blue team, and act as their managers. They also ensure that the rules of the competition are being followed.
- Black The Black Team consists of individuals highly skilled in networking and infrastructure. Their task is to build and monitor the competition network.
- Inject A task blue teams are asked to perform during the NECCDC.

For an interesting perspective from someone who has served on the various teams, see [3].

3. The 2010 NECCDC

The Northeast Collegiate Cyber Defense Competition (NECCDC) was established in 2008 by the Rochester Institute of Technology (RIT), which also ran the 2009 NECCDC. The University of Maine first competed in the NECCDC in 2009. At that time, RIT indicated a strong preference for another institution to host the 2010 NECCDC. After some discussion, the University of Maine volunteered to host the 2010 NECCDC with support from RIT.

We modeled the 2010 NECCDC on the 2009 NECCDC. We kept the schedule used in 2009, which was based on the schedule used at the National CCDC. The competition begins on a Friday and runs from about noon to 7 PM. The next day the competition runs from about 9 AM to 7PM. The competition concludes on Sunday as it runs from 9AM to Noon. There is a keynote speaker and an awards luncheon starting at 1 PM.

For the 2010 NECCDC we used two buildings. There were no serious problems, but the few teams in the second building felt a bit out of the action. We resolved to hold future competitions in a single building.

In 2009, there were a number of teams that had agreed to come, but who did not show up for the competition. This

was unfortunate, because RIT had turned some teams away thinking that they had a full slate of teams. We decided that for 2010 each team would have to pay a $750 entrance fee. To make this more palatable, we stipulated that all teams that showed up would receive a $750 travel grant. This scheme worked well and all nine teams who had indicated that they would participate showed up.

During the 2010 NECCDC there was little for the coaches to do. One vendor gave a talk about opportunities with his company, and the coaches met to decide on the venue for the 2011 NECCDC. One of the highlights of the 2010 NECCDC was that our winner, Northeastern University, went on to win the National CCDC the same year.

The 2010 NECCDC was the first cyber defense competition supported by the Department of Homeland Security. We were able to get a $10,000 grant from the Department of Homeland Security to help support the competition. Because of their experience with the NECCDC, the Department of Homeland Security now grants $15,000 to each of the regional competitions in addition to their support of the national competition.

In the 2010 NECCDC, the Red Team was captained by Daryl Johnson who captained the NECCDC Red Team from its inception and does so to this day. The Black Team was captained by Andy Moody and the White Team was captained by Tom Vachon and Ray Soucy.

4. The 2013 NECCDC

The 2011 and 2012 NECCDC competitions were hosted by Northeastern University. The physical location of the competition was the EMC training facility in Franklin Massachusetts. There were 19 schools interested in participating in the 2012 NECCDC, but there were only 12 openings. During the coaches' discussions it became clear that we would need to institute a qualifying round to select the schools that would be invited to the NECCDC. It was also decided that the next host would be required to organize the qualifying round of the competition. After some discussion the University of Maine received the opportunity to host the 2013 NECCDC. Based on our experience with the 2010 NECCDC, we came up with the following guiding principles for the 2013 NECCDC.

1) We would use a virtual competition for the qualifying round.
2) The competition would be held in a single building.
3) We would have a NECCDC Symposium for the coaches and others.
4) We would stress close cooperation between the Black, White and *RED* Teams in designing and running the competition.
5) We would select our keynote speaker from among our distinguished Red Team.
6) We would stress to the students that the NECCDC is not designed to be fair as a competition between the Blue Teams and the Red Team – the job of the Red Team is to provide challenges that the Blue Teams can use to distinguish themselves. In this sense, the more unfair the competition, the easier it will be to separate the truly great teams from the field.
7) We would provide a better scoring system along the lines discussed in [4].
8) We would provide more feedback to the Blue Teams.

We were able to accomplish all of the above goals for the 2013 NECCDC. We were extremely pleased as well by the fact that the winner of the 2013 NECCDC, RIT, went on to win the National CCDC.

5. Support for the Competition

Napoleon Bonaparte is famously to have said "an army marches on its stomach." This maxim applies to the NECCDC, and providing food for the competition is one of the major expenses. With 10 blue teams each having 8-10 people (counting coaches and alternates), the White Team with 25-40 people, the Red Team of 15-20 people and the Black Team of 4-8 people, plus visiting administrators, media and a scattering of other people, most meals have 150-200 people participating.

[2] shows the schedule for the NECCDC. On Friday, there are refreshments in the morning and lunch for all participants. We also had a dinner for the Red, White and Black teams, and snacks and beverages throughout the day for everybody. On Saturday we provided three meals for everyone, and on Sunday two meals. In addition, we provided constant snacks and beverages on all three days. The snacks and beverages cost about $1,000 for the event.

The competition received significant support from both Cisco and Dell. Cisco supplied all the networking gear, while Dell supplied 36 PCs (24 desktops and 12 laptops). Altogether we used 80 PCs of all types for the blue teams since each blue team received 8 computers. The computers for each blue team need to be identical. We wanted to have two spares of each computer so we needed 96 computers for the blue teams. Besides the 36 computers contributed by Dell, 48 computers came from the School of Computing and Information Science, and 12 came from the Mathematics and Statistics Department. There were, of course, additional computers used by the Black and White Teams. The Red Team members primarily used their own computers. We also needed to find identical printers for each of the teams. This complicated matters some since most of the clusters have heterogeneous collections of printers. Fortunately, we still had the printers we had purchased for the 2010 NECCDC.

There were several lessons that we learned this time around.

1) It is not a surprise, but collecting donations is harder than getting them.

- Bureaucracies have become more difficult to work with. This includes both university and company bureaucracies.
- Corporate donors like to use American Express cards so make sure you have some way to accept them.
- Do not get university development people involved in fundraising for the NECCDC because they will treat the donors as the property of the university and not the competition.

2) Start on the fundraising as early as possible.

The direct cost of the competition is somewhere between $20,000 and $25,000, so some fundraising is definitely required. To help with fundraising was one of the reasons that we created the NECCDC Foundation.

6. The Qualifying Round

At the 2012 NECCDC it was decided to create a qualifying round. After discussions with the Red Team Captain it became clear that the effectiveness of the Red Team decreased once the number of blue teams grew above 10. The Red Team was hampered by having to try all its exploits against every blue team. It was also clear that the qualifying round would have to be virtual since it would be too difficult and expensive to try to replicate the NECCDC for the qualifying round.

After some discussions with Dwayne Williams of the National CCDC and some searching, we were led to David Durkee and the Center for Systems Security and Information Assurance (www.cssia.org). With CCSIA's help we held the qualifying round and selected 10 teams to participate in the NECCDC from the 14 teams that signed up for the qualifying round. We are very grateful to David Durkee and CSSIA for their help with the qualifying round. We are also grateful to the NSF which supports CSSIA.

We learned a lot from running the qualifying round. First, we need to hold the qualifying round earlier in the year so as not to interfere with preparation time for the NECCDC. Second, you cannot just reuse NECCDC injects in a virtual qualifying round. Third, you need to plan better and allow more time if you want substantial red team activity.

One goal of the qualifying round is to determine which teams have the necessary base knowledge to be competitive in the NECCDC. To do this, there must be more injects per hour than in the NECCDC, but they need to be simpler because of the short time span of the qualifier. Examples of appropriate injects are demonstrating the ability to filter a packet capture and identify specific traffic or being able to write a description of a given technology from a security perspective.

7. Scoring

The national CCDC provides two scoring systems. The Scoring Engine (SE) is a system that simulates remote end-user traffic and awards points for successful service checks. The Inject Scoring Engine (ISE) is a web-based portal that provides on-line delivery of injects and allows each team to see the status of services externally. These two systems are indispensable tools and are distributed as virtual machines. For the 2013 NECCDC a new scoring system was tested to address concerns raised over the 2012 competition [4].

In previous competitions an effort was made to balance the various components of the final score. In practice, however, the aggressive and unpredictable SLA violation component of the Scoring Engine caused the service check points to completely dominate the final score rendering the inject score and the Red Team score largely irrelevant. For 2013 a weighted system was used: 40% service checks, 40% inject scores, and a 20% ranked score for Red Team activity. The scores were scaled in each category so that the top team in each category received 100%.

The specific weighting used is not as important as the idea that the knowledge and skills elements of the event are equally weighted in terms of assessment, and that the activity of the Red Team is a significant component of the final result.

A major concern with scoring for 2013 that should be addressed for future competitions is the need for a dedicated scoring manager, separate from the main judge. In the 2013 NECCDC having the main judge also be responsible for scoring resulted in a copy-and-paste error in a spreadsheet that swapped 3rd and 4th places.

There are a few areas for improvement in the scoring infrastructure. At present each team's ability to receive and submit injects is dependent on its network being functional. Consequently, injects might not be completed simply because of Red Team, or even the team's own activity. We recommend that each team receive a dedicated terminal to access the inject portal on a separate network.

We need a better system for collecting Red Team activity scores for Red Team activity to speed up scoring. We propose that a Red Team component be included in the Inject Scoring Engine that would provide the Red Team captain with direct portal access to submit incidents for approval.

The NECCDC needs to do a better job of providing teams with access to the details of their results along with explanations from the White Team on why points were awarded or deducted. As part of this goal for more feedback, we asked the White Team to take notes on their observations of each team. Some members of the White Team provided very good information, while others provided none. We recommend that future white teams receive an on-line training session to better explain their role and responsibilities.

A goal that was not realized due to time and man-power limitations, was the generation of a team-specific result packet which would include all injects, their scores, and feedback that could be used to prepare for future competitions. Other ideas for improvement include having the

Scoring Engine actually test connectivity and function of the services. This would include such things as login capability with password for services like SSH, or purchasing items at an appropriate price through the e-commerce system.

8. The Red Team

The 2013 NECCDC embraced the mantra *THE RED TEAM IS NOT THE ENEMY*. Since the purpose of the NECCDC is help to pick the strongest cyber defense team to represent the Northeast in the National CCDC, we want to ensure that the NECCDC stresses teams enough to differentiate clearly between the best team, the next best, etc. In short, the competition should be challenging enough and the scoring opportunities great enough to produce a clear scoring separation among the teams.

This year we included the Red Team in all phases of preparing and running the NECCDC. There was extensive consultation before the event and the Red Team Captain was included in all discussions and made significant contributions to the design of the NECCDC. The results of this year's competition were quite good with the NECCDC Champion winning the national title as well.

Collaboration between the Red Team and the White Team provides a "juicy" environment for the blue teams to experience, and for the Red Team to exploit. In a "real-life" environment, the defenders of such an infrastructure would likely not be aware of a zero-day vulnerability already in place in their infrastructure. The necessity for the blue teams to both discover and mitigate in-place exploits is an exercise that adds a real life element of stress to the competition.

The NECCDC is not a test of the Red Team's abilities. The Red Team is a partner in testing the blue teams' abilities. They are a component in the White Team's arsenal of tools to assess the blue teams. The back story used in the NECCDC is that each blue team is taking over for a removed, failed system administration team. Attackers could have been ingrained in the systems for months or years. This will *not* be reflected in any sitebook or documentation. That is one of the challenges for the blue teams. Such embedded advanced persistent threats (APTs) would have a good knowledge of the architecture of a system after weeks, months or even years of surveillance.

8.1 Blue Team Debriefing

The NECCDC is a wonderful testing exercise but it is also a great learning opportunity for the students. In the past the Red Team gave a single hour long debriefing to all teams at once from a very general perspective. Two years ago in response to a request by some struggling new teams, the Red Team meet with them before the collective debriefing and gave them some very specific feedback for their team. The response was overwhelming. The next year we eliminated the large debriefing and utilized the time to give individualized feedback to each team. The Red Team was split up into teams of two and each meet with two blue teams for about 20-30 minutes giving them some general and specific feedback and offered them a chance to ask questions. This has turned out to be an extremely valuable addition to the competition and was repeated at the 2013 NECCDC. The challenges of giving valuable feedback to the blue teams is another factor in limiting the number of teams competing at the NECCDC to 10.

8.2 Red Team Composition and Assignments

From its inception the NECCDC has been fortunate to have both a great collection of Red Team members and relative stability in the composition of the team. Several of the regulars on the Red Team are regular speakers at Black Hat and DefCon, have well-regarded books, and are the authors of widely used cybersecurity packages. Not all interested members are able to make every NECCDC so it is good to have a pool of high-quality professionals to draw from.

Each of the Red Team members needs to possess a strong knowledge and ability to exploit some portion of the infrastructure. Not everyone on the team must have an incredibly wide variety of penetration testing skills, even though having individuals with such breadth is certainly desirable. As long as the Red Team is well-balanced, and its members possess among themselves a reasonable set of skills to exploit and infrastructure, they should be effective.

A Red Team should have somewhere between 10 and 15 members to make sure that enough exploits are being deployed against the blue teams, but at the same time avoiding the chaos and confusion that would result from having too large a Red Team.

The skill sets necessary for a successful Red Team cross all fields: operating systems, Web services, network services, cryptography, database, etc. But not surprisingly, the most important trait is team work and camaraderie. No individual can "know it all" and during the time-crunched pressure of the NECCDC Red Team members must recognize their limits and know when to seek co-operation.

8.3 Attacking the Blue Teams

There are two philosophies of how to organize a Red Team for attacks on the blue teams. One can either assign individual to specific blue teams or one can assign individuals to handle particular types of attacks and to launch them against all blue teams. Assigning Red Team members to particular blue teams is simple, but leads to unbalanced results because the skills of the Red Team members are not uniform. The NECCDC exclusively uses the second approach and Red Team members select particular attacks that they must run against all blue teams. We feel that this is the best way to get results that can be compared.

This approach of aligning Red Team members by skills allows us to adhere to the Golden Rule that a successful

exploit can be recorded only after it is attempted against all the blue teams. This ensures that all blue teams get the same Red Team attention and that no blue team gets "picked on." This also allows the Red Team to form sub-teams along the lines of reconnaissance, exploitation, persistence, and post-exploitation. The Red Team is also sub-divided by platform expertise. Each sub-team's success is passed to the next sub-team to take advantage. For the Red Team having access to the boardroom in the Red Team hotel for use over night has been invaluable.

The NECCDC Red Team has developed a reporting system that records and submits successful attacks. Exploits must be validated by the Red Team Captain before they are released to the White Team. The validation must confirm that the exploit has been tried against all blue teams, that the exploit can be scored, and that all necessary information has been recorded clearly. More information about creating and running a Red Team is available in [5]. Some thoughts about how to maximize the educational effectiveness of a red team can be found in [6].

9. The White Team

The White Team is responsible for judging the event. White Team members are assigned based on their experience and background to tasks such as proctoring a team room or assisting with scoring written deliverables from teams. Each White Team member should have a strong background in at least information technology.

The White Team Captain is in charge of the injects and making sure that tasks are delivered to the blue teams in a timely manner. Ostensibly, the Director of the competition is a member of the White Team, but there are so many things that must be tracked during the competition that the Director is focused on other things. One duty at the 2013 NECCDC that fell to the Director, was running the NECCDC Symposium.

There should be 2 White Team members per blue team. In addition there need to be an extra 2 to 4 White Team members available for other tasks. Add to that the White Team Captain and a separate, dedicated scoring manager and it is clear that a white team needs at least 26 people. Given that it is often the case that white team volunteers are not able to assist for the full three days of the competition, one should plan on having 30 or so people on the White Team.

So far we have not used blue team coaches for the White Team to avoid any questions about a team coach influencing the results. Cyber defense competitions differ from other competitions in that the coaches plan a minimal role during the competition. In particular, unlike sports, the coaches of cyber defense teams are actually capable of competing and influencing the outcome of the event. We are interested in getting the coaches more involved and having the NECCDC be more of an educational event. In the 2013 NECCDC we ran a symposium which addressed this concern to some extent. More remains to be done in this area.

A pool of laptops and desktop computers should be available for White Team members since there are often issues with them using their corporate laptops to run some of the White Team software such as IRC or Google Apps. The White Team must be prepared to handle complaints or concerns about individual or team misconduct. Over the course of the NECCDC we have had both individual disqualifications and team disqualifications. Fortunately, neither occurred in the 2013 NECCDC.

It is good to have some people play the part of "foolish" users on blue team systems. They would click on web links, try to log in to the systems and in general do things that may cause problems. We are considering fielding a separate team to do this or perhaps using some members of the White Team to carry out these tests.

10. The Black Team

The Black Team is responsible for setting up and maintaining the competition network. It must work closely with the White and Red Teams, and provide network monitoring sufficient to detect any transgressions of the rules. It must also provide maintenance support to the blue teams. This can include reimaging computers or dealing with hardware failures.

For both 2010 and 2013, the White Team and Black Team have been referred to as the Grey Team. The Black Team requires strong technical skill and experience in configuring and preparing the event infrastructure, but is also instrumental in introducing common security problems into the infrastructure for teams to locate and correct. Ideally, the Black Team has specialists in Windows, Linux, and networking, each with a security focus.

A black team should have a minimum of 4 people for the NECCDC. Since setting up the competition involves a lot of work, it is good if the Black Team can draw on some temporary help for moving equipment around and imaging computers. All members of the Black Team need to be team players and able to work in a dynamic and, at times, chaotic environment.

The Black Team should have a solid core group. Each member of the Black Team must be aware of the time commitment involved. Core members should be available to create images, direct setup and takedown as well as be available for all (or majority of) the competition weekend. There will be late nights and long days as well as some early mornings to get ready.

Effective and timely communication between the Red, Black and White Teams is essential to the smooth running of the event. In 2013 we used several IRC channels to facilitate that communication which worked quite well. In particular this cut down on the need for White Team members in the

rooms to physically run up to the White Team room to ask questions or bring results back to the scorers.

11. Infrastructure

There are some non-trivial infrastructure requirements for hosting the NECCDC. First, there must be 10 good sized rooms for the blue teams. There should be a secluded room for the Red Team convenient to the competition, but not obviously visible to the blue teams. There needs to at least one operations room and a White Team Headquarters. It is helpful for there to be a separate Director's area for handling the media and visitors. This area can also provide room for scoring and other judging activities. There should also be a room that can be used for repairing hardware or working on competition infrastructure.

Blue team room size is important. There needs to be adequate room for the blue team, equipment and up to 2 White team members. Collaboration space should be provided within the blue team room as well. While White and Black team rooms can be different rooms it is best to have one room adequate for the combined White and Black teams.

As mentioned earlier, all blue teams must be supplied with the same exact computer systems, networking gear, peripherals, and supplies. This is to ensure fairness and to simplify staging the competition. We believe that having at least two spares of all systems used is sufficient for the NECCDC.

Some means of moving equipment in bulk is recommended, we used large carts capable of holding 4-6 systems (including monitors, keyboards and mice) for the 2013 NECCDC. Be sure to have a sufficient number of power cables, outlet strips and network cables for the competition. For the 2013 NECCDC we used approximately 150-200 network patch cords of various lengths and between 40 and 50 power strips. We also used about two dozen longer extension cords.

12. The Blue Teams

Experience has shown that the NECCDC is a highlight in the education of prospective cybersecurity professionals. Given the lack of a standard curriculum and detailed training guides for the cyber defense competitions, it is not always easy for prospective coaches and team members to put together an effective blue team. Blue teams must understand what a business inject looks like and also how the Scoring Engine works to successfully compete.

Some schools hold mock competitions that expose students to an environment very similar to the one provided in the NECCDC. Preparation and an understanding of the competition environment is likely to improve the performance of the blue team. Experience has shown that students who have taken a cyber defense techniques class will do better in the NECCDC than students who not had such a class. Such classes should prepare students both technically as well as teaching them the fundamentals of cybersecurity team work (see [16]).

Over the years, the Cybersecurity Education Session of the Security and Management Conference has covered many topics of interest to people interested in starting and running a blue team for cybersecurity defense competitions. Some papers of general interest include [7], [8], [9], [10], [11], [12], [13], [14], [15], and [16]. For a paper that discusses how keyloggers can be used in cybersecurity education see [17]. For a discussion of running cyber defense competitions in high school see [18]. Finally, for a discussion of references that can be used to teach SELinux see [19]. We hope to present more papers related to this in the current and future sessions of this workshop.

We note that so far, the NECCDC has not subsidized the expenses of blue teams at the NECCDC. Anyone planning to take a non-local team to the NECCDC needs to have at least $2,000 to cover the cost of transportation, hotels and meals on the trip.

13. The NECCDC Symposium

As noted earlier, we ran the NECCDC Symposium in parallel with the competition. The schedule for the competition is available at [20]. Space prevents us from going into more detail, but the Symposium was successful and produced some very good dialog among the coaches. We note that we were able to work the Symposium into one of the injects.

14. Publicity and Photo Releases

A goal of the NECCDC is to generate publicity for the purposes of attracting more students to the field. The 2013 NECCDC received coverage on all the local TV stations as well as in the local paper. More details will be available at [2] soon. We have traditionally required all participants to sign a photo release [21], which should actually be called a media release. The reason for this is that when the media comes it is not always clear who will and who will not in any photos or videos. To avoid any possible problems we have required a press release from everyone.

For the 2013 NECCDC we permitted a few students to come who did not sign a press release. Consequently, we found ourselves in a few difficult situations that required students to not be in photos. After some discussion among the coaches, it was decided that everyone participating in the NECCDC and any of its activities will have to sign a media release. If they choose not to, they will not be allowed to compete in any round of the NECCDC.

15. The NECCDC Foundation

At the 2013 NECCDC, it was decided by unanimous vote of the coaches to establish the NECCDC Foundation

which would take ownership of the NECCDC competition. The NECCDC Foundation will ensure that the collective knowledge and experience related to running the NECCDC is passed on in an organized manner to each host school in turn. It will seek to get as many schools as possible involved in the process of preparing and staging the NECCDC, and it will help with some key items. The details are still being worked on, but here are some areas that the NECCDC Foundation will help with.

1) It will provide an orderly method for finding host schools.
2) In conjunction with the host school it will handle fundraising for the NECCDC.
3) It will try to raise funds so that eventually it can help schools support their blue teams.
4) The University of Maine Foundation will act as the initial 501 (c) 3 charitable institution for the NECCDC so that all contributions to support the event will be tax deductible.
5) The NECCDC Foundation will help organize the Qualifying Round.
6) The NECCDC Foundation will help provide the Red Team.
7) The NECCDC Foundation will help the host institution set up and prepare the Black and White Teams.

We created a temporary board of directors who will serve until June 30, 2013 at which time we will elect a more permanent board of directors. We hope to persuade the captains of the various teams to serve as advisors to the captains of the next host's teams if their help is needed. The details still need to be worked out, but this looks like a promising development in the history of the NECCDC.

As a final note, the coaches voted unanimously that any institution hosting the NECCDC will automatically have its Blue Team advance to the NECCDC. This is in compensation for all the extra work and distraction that the host institution needs to deal with.

16. The 2014 & 2015 NECCDC Competitions

In part because of the creation of the NECCDC Foundation and the promise of support in setting up the NECCDC, there was much more interest in hosting the NECCDC than has been true in the past. As a result of various discussions it has been determined that the 2014 NECCDC will be held at the University of New Hampshire in March 2014. We are glad to report that there is serious interest from at least two schools to host the 2015 NECCDC. We hope to have many schools host this event in the future so the burden is shared more widely and cybersecurity gets more support and exposure.

17. Conclusions

The NECCDC is a tremendously positive event in the preparation of the next generation of cybersecurity professionals and deserves widespread support. We have seen the positive impact on the students as a result of trying out, preparing and practicing for, and competing in the NECCDC. They acquire a great appreciation for the knowledge gained and the importance of cybersecurity to both our personal and business world. We hope that this paper has conveyed some of the excitement and promise of this event.

References

[1] The National CCDC website. [Online]. Available: http://www.nationalccdc.org/
[2] The NECCDC website. [Online]. Available: http://neccdc.net/
[3] Jeffrey C. Scaparra, "One Individual's Three Perspectives on the Collegiate Cyber Defense Competition," in *Proc. SAM'10*, 2010, pp. 307-313.
[4] George Markowsky, "Toward a More Perfect Scoring System for the NECCDC," in *Proc. SAM'12*, 2012, pp. 230-235.
[5] Daryl Johnson, "The Assembly and Provisioning of a Red Team," in *Proc. SAM'11*, 2011, pp. 530-534.
[6] Jeffrey C. Scaparra and Jeffrey R. Bullock, "Red Teaming for Education," in *Proc. SAM'11*, 2011, pp. 512-517.
[7] Patrick Engebretson, Joshua Pauli, and Joshua Bosma, "Lessons Learned from an Evolving Information Assurance Lab," in *Proc. SAM'10*, 2010, pp. 261-266.
[8] Jean Gourd, "Cyber Storm: The Culmination of an Undergraduate Course in Cyber Security," in *Proc. SAM'10*, 2010, pp. 300-306.
[9] Joshua Pauli and Patrick Engebretson, "A Cradle-to-Grave Approach to Retaining Students in Information Security Programs," in *Proc. SAM'10*, 2010, pp. 255-260.
[10] Nicholas Capalbo, Theodore Reed, and Michael Arpaia, "RTFn - Enabling Cybersecurity Education through a Mobile Capture the Flag Client," in *Proc. SAM'11*, 2011, pp. 500-506.
[11] Cory Cavanagh and Raymond Albert, "Goals, Models, and Progress towards Establishing a Virtual Information Security Lab in Maine," in *Proc. SAM'11*, 2011, pp. 496-499.
[12] Ronald Cheung, Joseph Cohen, Henry Lo, and Fabio Elia, "Challenge Based Learning in Cybersecurity Education," in *Proc. SAM'11*, 2011, pp. 524-529.
[13] Sonja Glumich and Brian Kropa, "DefEX: Hands-On Cyber Defense Exercises for Undergraduate Students," in *Proc. SAM'11*, 2011, pp. 487-493.
[14] Cory Cavanagh and Raymond Albert, "Implementation Progress, Student Perceptions, and Refinement of a Virtual Information Security Laboratory," in *Proc. SAM'12*, 2012, pp. 197-200.
[15] William D. Casper and Stephen M. Papa, "A Multi-Disciplined Security Engineering Education Approach," in *Proc. SAM'12*, 2012, pp. 243-248.
[16] Brandon Mauer, William Stackpole, and Daryl Johnson, "Developing Small Team-based Cyber Security Exercises," in *Proc. SAM'12*, 2012, pp. 213-217.
[17] Christopher Wood and Rajendra Raj, "Keyloggers in Cybersecurity Education," in *Proc. SAM'10*, 2010, pp. 293-299.
[18] Raymond Albert, George Markowsky, and Joanne Wallingford, "High School Cyber Defense Competitions: Lessons from the Trenches," in *Proc. SAM'10*, 2010, pp. 280-285.
[19] Linda Markowsky, "An SELinux Sourcebook for Cybersecurity Education," in *Proc. SAM'10*, 2010, pp. 248-254.
[20] 2013 NECCD Symposium Schedule. [Online]. Available: http://neccdc.net/wordpress/?page_id=99
[21] 2013 NECCD Media Release. [Online]. Available: http://neccdc.net/wordpress/wp-content/uploads/2013/02/NECCDCPhotoRelease2013.pdf