Proceedings of the 12th Colloquium for Information Systems Security Education
University of Texas, Dallas
Dallas, TX June 2 - 4, 2008

CANVAS: a Regional Assessment Exercise for Teaching Security Concepts

Michael Collins, Dino Schweitzer, *United States Air Force Academy*, and Dan Massey, *Colorado State University*

Abstract – Competitive exercises are one means to motivate and teach information security concepts to students. Along the Colorado front range, schools have joined together to teach students security concepts using a regional security assessment exercise, known as the Computer and Network Vulnerability Assessment Simulation, or CANVAS. CANVAS shares some elements with a typical "Capture the Flag" exercise, but differs from other security competitions in the overall approach to the exercise, in the exercise objectives, in team makeup, and in the evaluation criteria. Teams are formed at the exercise and combine students from different backgrounds. Points are awarded based on successful strategy and written reports as well as typical "flags". We have successfully run the exercise for two years, and are currently planning the third iteration. This paper will describe the exercise, examine the differences from other competitions, and share our experiences from the first two exercise instantiations.

Index terms – Security education, cyber competitions, cyber defense.

I. Introduction

Competition can be a strong motivator to students and is often used at all levels of education. Individuals compete for top grades, awards, and teacher recognition. Science fairs, spelling bees, and essay contests encourage individuals to outperform their peers. Teachers often show off "best of" projects in front of the class. Team competition is similarly used to entice students to achieve with the added elements of peer pressure and social dynamics. School pride, perhaps as well as fear of failure, play a role in knowledge bowl competitions.

Computer science is no stranger to competitions. The ACM Programming Contest has competed school teams at the regional, national, and international level since 1977. Robotics, gaming, system design, and artificial intelligence have all become arenas for students to pit their knowledge and abilities against opponents. It was inevitable with the rise of computer security as an important educational topic within computer science, that cybersecurity competitions at the individual and team level would soon follow.

This paper first describes common types of security competitions along with details of well-known examples at the national and international level. It will then present a different type of competitive approach developed and used by colleges and universities along Colorado's front range. Our approach uses many elements from the existing competitions and challenges students' technical abilities and knowledge. But our approach adds new features in team development, strategy, and conveying technical details in concise documents. Section III describes our approach in detail followed by a sample scenario, our experience in its effectiveness, and plans for future exercises.

II. Cybersecurity Competitions

By its very nature, information security deals with understanding system vulnerabilities, exploits, and defenses. Students are often taught the tools and techniques of attackers as a means to understand the nature of attacks and appropriate defenses [1]. The term "ethical hacking" was coined to describe the process of attacking a system using the tools of a malevolent intruder for the express purpose of discovering security vulnerabilities [2]. Not surprisingly, the ethical and professional ramifications of teaching students such knowledge has been debated in the literature. Also, not surprising, the very idea of attacking and defending a system immediately gives rise to the notion of a competition.

Different types of cybersecurity competitions have been developed and described in the literature. Perhaps the best known of these are "capture the flag" (CTF) type competitions. These competitions involve both offensive and defensive components. Competitors are assigned a machine or network to defend against attack while simultaneously attempting to hack into their competition. Points are awarded for successively breaking into a machine as well as successful defense. The most highly publicized CTF competitions are hosted at the annual DEFCON hacker's conference with thousands of participants.

The University of California at Santa Barbara (UCSB) hosts the largest academic-based CTF competition each year. In 2007, 35 universities from around the world competed, with the winning team coming from Milano, Italy. Each team is provided an Internet server that provides a number of services. The services have a

number of undisclosed vulnerabilities. Teams are connected via VPN to a main system that acts as a central hub. Each team's goal is to maintain the set of services throughout the contest phase by finding and fixing vulnerabilities. They also attempt to compromise other team's servers based on the discovered vulnerabilities. An automatic scoring system keeps track of available services and services that have been compromised.

A defense-only competition began between the service academies in 2000 as a capstone experience for students in network defense [3]. The competition, known as the Cyber Defense Exercise (CDX), includes the five US service academies along with the Naval Post Graduate School and the Air Force Institute of Technology (advanced degree institutions). The National Security Agency provides support both with White Cell members acting as exercise controllers and score keepers, and Red Cell members as aggressors and network attackers. Students are primarily in their undergraduate senior year and have had some number of courses in information security and computer networking. Similar to CTF competitions, teams are provided a series of network services they must maintain while under attack. Each team designs their network up front and defines network operational roles to each of the participants. Scoring for the competition is based on service maintenance as well as overall network operations, timely reporting, and forensics when compromises occur. Participants are strictly forbidden from taking any aggressive action against competitors. Part of the goal of the exercise is to expose students to an operational environment that they will experience as professional military officers.

In 2004, a proposal was made to create a defense-oriented cybersecurity competition, similar to CDX, as a national collegiate competition [4]. In 2005, the first regional competition was held, and national competitions have been held the past two years. The Department of Homeland Security provides support for the competition. Teams compete in a central location with a preconfigured network simulating a business environment in which they must maintain services while under attack from a Red Team. According to the official website (nationalccdc.org/rules.html), scoring is composed of:

> *Scoring will be based on keeping required services up, controlling/preventing un-authorized access, and completing business tasks that will be provided throughout the competition. Teams accumulate points by successfully completing injects and maintaining services. Teams lose points by violating service level agreements, usage of recovery services, and successful penetrations by the Red Team.*

Penalties can be reduced by up to 50% for completing incident reports as needed when intrusions occur. Similar to CDX, teams are not allowed to conduct offensive operations against other teams.

These competitions are not the only ones being conducted at educational institutions. Several programs conduct individual class competitions to crack passwords, find hidden flags, and assess vulnerabilities. The rules, goals, and level of participation vary greatly. The common element is the concept of using competition as a motivational means to teach students about security.

III. CANVAS

Since 2004, schools along Colorado's front range have investigated various ways of collaborating in information assurance education. An annual workshop provides a forum for sharing experiences in security research and teaching techniques. Joint security–based research projects with participants from different institutions have met with some success. In 2006, Colorado State University (ColoState) and the United States Air Force Academy (USAFA) agreed to hold a joint security competition for students from the two schools to participate in. Based on its success, the competition was expanded in 2007 to include students from five different local universities. The competition is called the Computer and Network Vulnerability Assessment Simulation, or CANVAS.

CANVAS shares many features with the well known "Capture the Flag" events discussed in Section II. Students use existing security toolkits to assess a scenario and gain points by obtaining flags. These flags require varying degrees of skill and test student's knowledge. But unlike other events, we strive for a very diverse set of participants, have a strong focus on team work, and emphasize an ability to convey results as well as achieve specific technical objectives. These are not simply additional benefits of the competition, but rather this is the fundamental philosophy behind the event.

A. Incorporating Different Levels of Expertise

Our event is designed to cover an extremely wide range of students. In other events such as DEFCON, someone with no security experience is not viewed as a possible participant. Our objective is to include and challenge anyone. The only requirement to entry is the motivation to participate.

Clearly many students participating in the event have a strong interest in network security and have acquired some expertise. USAFA cadets may have participated in the service academies CDX and some ColoState students have worked on security research projects. These

students bring a high level of expertise and challenge the event designers to provide difficult scenarios to test expert level skills. To date, no participant has reported finding the exercise too easy and no teams have finished early.

But at the same time, our event is open to novices and students with little or no experience are strongly encouraged to participate. The event designers must also provide enough easily accessible flags so that novice players do not leave frustrated. Our teams include students from a number of universities with dramatically differing course preparation. For example, some ColoState participants excelled in the overall undergraduate program but had essentially no course focusing on security. Other participants had a single security course with little hands-on experience. To date, no team has failed to make any progress and all teams left with some degree of success.

B. *Team Building and Strategy*

A second key aspect of CANVAS is the team structure and resulting requirements for teamwork. In other events, teams are often formed weeks or months ahead of time. For example, the Internet Capture the Flag requires close interaction with a local team that typically practices for a substantial period before the event. In CANVAS, teams are formed on the fly and mix students from different schools who have never met prior to the event. As discussed above, team members range from experts to novices. One of the very first challenges a team must face is identifying skill sets and working with their teammates.

There are aspects to the event that we feel are essential to its success. We clearly benefit from the fact that this is an optional event and no student is there because they are required to participate. Universities cannot mandate participation as part of a course. As a result, we have motivated students with some inherent enthusiasm for the event.

To ensure novices and experts all participate, rules require each team member to have a roughly equal amount of time at the keyboard. Thus an expert who has thorough understanding of the exploitation tools cannot simply work while other team members observe. At a minimum, the "expert" must convey what the novice should type.

More fundamentally, the flags are selected so teams require both tool level expertise and general understanding. For example, a user name and password may be embedded in a web page and teams that view the page source will obtain the flag thus not requiring any tool expertise. Other flags require deeper understanding of how to use the tools effectively. This range of difficulty is an intended feature of the exercise. Although the students may not fully recognize this going into the event, learning to work with a team is as important, if not more so, then having a detailed understanding of the underlying security tools.

C. Conveying Technical Results

A third key aspect of CANVAS is the focus on conveying the overall results. The winning team is not necessarily the team that has captured the most flags. Flags are typically worth tens of points while a final write-up is worth over one hundred points. A team not only needs to succeed in finding exploits, they must convey how this was done and what could be done to mitigate the issue.

In producing this final document, the students must address both a very technical audience such as the head of security or CTO of the company and a general audience such as the CEO of the company. The students must convey sufficient technical points in a concise and convincing way. A highly technical audience, in this case the faculty reviewing the write-up, evaluates the document for technical clarity and correctness. It is equally important that students capture the broader picture and can place the technical results in context.

In our experience, this is an essential learning experience. Reports that lack technical depth are dismissed and viewed as not useful or relevant to the engineers ultimately responsible for the system. But at the same time, too much unnecessary jargon and lack of a broader view make the document of little value to general management that must act on the recommendations and allocate resources to correct the problems.

Overall, these three aspects separate CANVAS from other events. We strongly encourage our students to participate in events such as iCTF, DEFCON, and CDX. But CANVAS is accessible to students who lack the time or experience required for these events. In addition, we hope our exercise conveys lessons on teamwork and communicating technical ideas. These are not simply side effects of the event, but we view them as equally important if not more important than the underlying technical skills.

IV. Exercise Mechanics and Sample Scenario

In 2007, a business scenario was chosen to guide the CANVAS competition. As described above, teams were formed with students of different backgrounds and experiences. In 2007, with five schools participating, no team had two members from the same school. Isolated identical virtual networks were used for each team and a

prepackaged live CD of Backtrack2 was chosen as the sole source of tools teams were allowed to use [5].

Teams had four hours to perform as complete an assessment as possible including a written team report that documented the vulnerabilities and recommended solutions. They could use any of the tools at their disposal to discover vulnerabilities or to study the system in question. About half of the points were allocated to flags that they may found in their active pursuits. The remaining points were awarded based on team final reports. Faculty members from participating schools formed the judging panel to read and rank the team final report submissions for point allocation.

Each school provided an assortment of inexpensive prizes and school memorabilia. After the awarding of prizes, a faculty member provided a "hot-wash" of the network and means to exploit the known vulnerabilities. With additional interaction from students and other faculty a discussion of recommended solutions followed.

Figure 1 gives the network diagram for the CANVAS 2007 exercise. The basic idea was to create a reasonable but simplified scenario for senior undergraduate students and ask them to assess the strength of the system. In this case, the scenario was a company which produced and managed on-line voting systems hired the team to assess the security strength of their system.

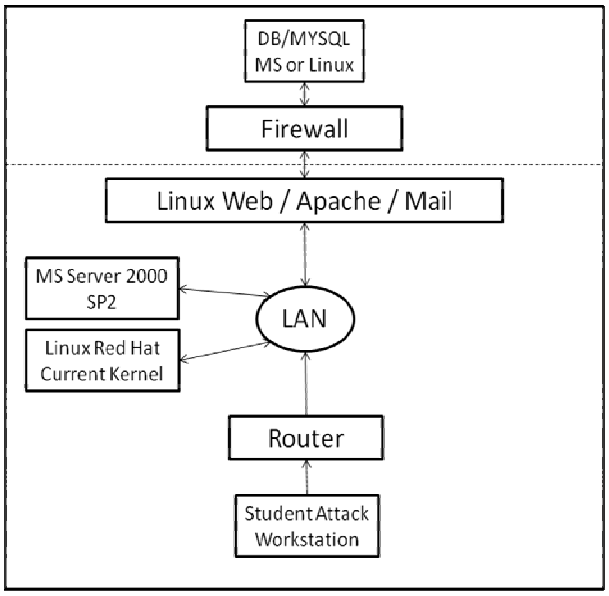

Figure 1. Voting system network diagram

It took extra verbal instructions to underscore that the assessment was about the voting system and security holes that impacted that application. Some additional network features were added to the design completely independent of the voting system. A discovered vulnerability in those features only counted if the team could show its relation to the voting system. The full scenario as provided to students can be found in APPENDIX A with the full guidance for faculty provided in APPENDIX B.

The emphasis in the design was to ensure a wide range of possible issues ranging from beginning to advance assessment capabilities. Specific attacks ranged from SQL injection to full exploitation to root with METASPLOIT. The design team tracked known exploits with attack trees which also allowed a check on the sophistication required to implement each attack.

V. Our Experience

Both years we have offered CANVAS were a big success from the instructors' viewpoints. The biggest surprise from the first offering was the benefits gained from how teams were formed.

While no formal study was made, all students and faculty recognized the challenge and trepidation of many students being faced to work this problem with complete strangers. Leadership, teamwork, and communication skills which are essential to the student's success were truly tested. In fact, both years of CANVAS have subjectively demonstrated that the design of the teams and the social interaction required by this competition are core elements in the success of the exercise.

We found that a single day event of four hours worked very well to keep the competition reasonable for the best to find most if not all of the holes and keeping the weaker teams motivated for the entire exercise. The faculty also enjoyed working together to judge the "hot washes" and assisting teams with hints when they were stuck.

The structure of scoring and providing hints needs improvement. The original concept was that receiving hints "cost" the team some points in the final tally. However, some faculty recorded the hint giving, while others did not. Some faculty gave more information in the same hint than others and provided additional assistance.

One obstacle to growing the exercise is that it is designed for the traditional undergraduate experience making involvement by night students more difficult. While we encourage schools with different demographics to experiment with forming teams and running this type of exercise remotely, our experience at USAFA and ColoState indicate our students are better served by meeting their teammates face to face.

VI. Future Plans

Building on the success of the 2007 event, the third CANVAS event will be held in April 2008. Again, a business scenario is chosen to guide the competition. Subprime Online, a fictitious online mortgage company, is being acquired by a larger bank. The student teams must assess the security of Subprime Online. Particular concerns to our fictitious bank include general web presence and network security, the security of customer data whose exposure could lead to identity theft, and the protection of financial data.

As in previous events, the prepackaged live CD Backtrack2 is the sole source of tools teams are allowed to use. Each team works on an isolated network that includes typical services such as web and database servers. Each team also has a laptop on a public network that can be used to research vulnerabilities and potential exploits.

In the 2008 event, each team's network also includes a Cisco router with a range of simple and more complex vulnerabilities. For example, the username and password are the Cisco factory defaults and a simple Google search reveals this information and will be provided as a hint. Other more complex vulnerabilities allow the teams to find and exploit a final hidden machine that contains sensitive financial data for SubPrime Online.

Teams gain points by capturing "flags" and writing a report to CTO and CEO of the bank acquiring SubPrime Online. The underlying exploits share many of the successes of the previous events and include weak passwords, imperfect operational practices, and exploitable software. Some flags are easily obtainable using tools on the Backtrack2 CD. Other flags do not require any use of tools, but do require analysis and understanding of how different components interact.

At the start of the event, students from the participating universities will be grouped into fourteen teams of 3 to 4 people with varying degrees of expertise. Simple flags and a series of hints help ensure every team makes some progress and we again hope no team will be able to exploit all flags.

As a result of this event, we hope some students are inspired to gain deeper insights in computer security and pursue careers in this critical area. But equally important, we hope all students gain experience working in diverse teams and conveying technical results in a clear and concise manner.

VII. References

[1] P. Logan and A. Clarkson, "Teaching students to hack: curriculum issues in information security," in *Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education* (SIGCSE '05), February 2005.

[2] Saleem, S. "Ethical hacking as a risk management technique", in *Proceedings of the 3rd Annual Conference on information Security Curriculum Development,* InfoSecCD '06, September 2006.

[3] T. Augustine and R. Dodge, "Cyber Defense Exercise: Meeting Learning Objectives thru Competition," in *Proceedings from the Tenth Colloquium for Information Systems Security Education*, Adelphi, MD, 2006.

[4] G. White and R. Dodge, "The National Collegiate Cyber Defense Competition," in *Proceedings of the Tenth Colloquium for Information Systems Security Education*, Adelphi, MD, 2006.

[5] http://www.remote-exploit.org/backtrack.html accessed April 2008.

Appendix A

CAVEAT

Front Range Voting Machines (FRVM) is a fictitious company located in Denver, Colorado. It was created for the "Front Range Capture the Flag" contest sponsored by the USAFA on 25 April 2007.

Our Culture

FRVM is about providing software and technology solutions that fundamentally change the ways our clients achieve success.

Whether we are teaming with a book publisher or an internet mapping company, to deliver new ways for students to learn geography, or help the State of Colorado evaluate and protect its new electronic voting system, or tackling the most important problems facing the Intelligence community, we consistently transform our core competencies in advanced research, interactive media, software development, systems engineering and integration into innovative solutions that excite, stimulate, and empower our customers. We hire the best and challenge them.

Our People

FRVM's commitment to its employees is paramount. We invest in our people throughout their careers with an aggressive program of business incentives, training, education, and growth opportunities. Our family-friendly culture is backed with an

extremely flexible leave program, full benefits, and a dynamic environment where people are encouraged to express their potential and grow their interests. Our employees have access to season tickets for the Broncos and Rockies. They are reimbursed for travel on mass transportation.

Our Vision

FRVM is a start up company with big ideas. We seek out the most creative challenges imaginable and focus our innovative energies in solving them. We are committed to expanding our national presence, attracting the best and brightest to our team, and remaining true to our family-friendly culture.

Penetration Test

FRVM built a voting system using a web interface. It can be used to tally votes for political elections, or television shows such as "American Idol". There is a web front end and a MYSQL database back end. You have been hired to perform a penetration test. You are to evaluate all computers you find. Are they secure? If not, then what is the problem and how does FRVM fix it?

Although the system is in constant use and is in final testing, you are expected to test the web interface and may vote. You may not change any code. You cannot create accounts, backdoors or root the boxes. Our company is continuing to use the computers for final testing while you are doing pen test. If you have a question about what is legal, please ask.

Contest Information

You are being hired by "Front Range Voting Machines" to perform a penetration test on a network, its computers and the voting application. The machines include Linux and Microsoft workstations/servers, a Web Server, and a back end database machine using MYSQL. The system administrator is Diana Gates. Her logon ID is "DianaGates". There are root or admin accounts on each machine. Your job is to perform a professional penetration test on this system and see if it is secure. Are there any security holes? How would you fix them? Is there anything else going on the customer should be aware of?

Start by enumerating the workstations outside the firewall before going after the web server and back end database. Start out with NMAP. Map the network and services.

There are five flags to capture. The flags are JPEG pictures of people. You are to determine who the people are and why they are important. Don't go looking in obscure places. They are out in the open. If you find a hole in a machine, the flag is close by. Take notes as you go. You will need them for the final report.

The penetration test will last four hours. The write up or "Hot Wash" will take one hour. You will NOT be graded on how quickly you finish. It is more important that you be complete. The Hot Wash should be one or two pages and include:

Hot Wash
- Flags Found
  - Who are they?
  - What are their contributions? One sentence is fine.
- Security holes
- How to repair the holes.
- Recommendations.
- Did you find evidence of other hacking?
- Anything else?

You must read, sign and agree to the ground rules. Finally, a big hint is to make sure you read all documents in their entirety. You may use the Internet, if you have access.

Since there are other teams going after a similar goal, I would NOT recommend that you stand up and announce that you found out how to penetrate a particular machine using a specific technique. Other teams could be listening.

Finally, you do not have to write buffer overflows and the like to be successful.

APPENDIX B

For contest judges

We worked hard to lead the students into learning about penetration testing instead of just amateur hacking. If they pay attention, they will find there is something amiss along with the configuration and OS problems. We also focused on the skill set and the different vulnerabilities in the system. There are UNIX password problems that have to be guessed, there are old Windows OS problems that can be solved using Metasploit, there are DB problems and there are application problems. There is no one technique that will cause any one team to win.

Part of this contest at the virtual company, FRVM, is to capture flags. The "flags" will be pictures of famous computer scientists. Other than Bill Gates, the other computer scientists will probably not be recognizable. It would also be nice for the students to understand what these people's contributions were. One sentence is fine. Steganography will be used and the JPEGS and contain the actual names of the scientists. Steganography will be hinted at in some emails left on the mail server. They will have to download the program from the Internet to decode. I will have the program on a disk if necessary.

The other behind the scene thing going on is some rigging of an election. The system administrator has been compromised and has been paid off by someone from the outside. She is going to make sure one candidate wins. The students should not only perform the penetration test, but also keep their eyes open for mischief.

We are always concerned that one group will finish in record time. We have added some complications or layers that can be used if necessary.

There should be fifteen minutes before the contest for the students to read the documentation.