Herding Cats: How to Launch a Cyber Security Club in an Academic Setting

Matt Piazza, Aspen Olmsted
Department of Computer Science
College of Charleston
Charleston, USA

Abstract

On an enterprise network there are innumerable concerns on a large enterprise network. These concerned are enhanced by the masses of uncontrollable students and non-technical professors engaging in uncontrollable, unsafe internet activity. It is infeasible to implement a widespread bring-your-own-device policy in this setting. Certain groups can be considered 'at risk' for unsafe behavior. In this paper, we will examine how we can use network design to mitigate the risks associated with the formation of an on-campus, student-run cyber security club. In our case, we had to find a way to segregate unwanted, possibly malicious traffic and activity from the sensitive main campus network. We propose the use of an entirely separate private network for the club's use only. The club must manage the private network to provide ample learning opportunities for the members. Appropriate safeguards should be in place between the private network and the Internet. However, those safeguards should be entirely selected, deployed, and maintained by the club. Approval from and consultations with the university's Information and security divisions is crucial for members' learning.

1. Introduction

The College of Charleston was one of the few schools invited to the inaugural Palmetto Cyber Defense Competition in 2013. A ragtag group of students with little or no knowledge specific to cyber defense or computer security showed up and took home third. The next year, with a bit more notice, team captain (Chad Hobbs, '14) sent out an all-inclusive call for participants. I went to that meeting with next to nothing in my head about security. It was an introduction to security through hacking. Not anything like what we would be doing in competition a few months later. Some of the attendees of that initial meeting reconvened the next week for another training session during which we participated in more "Red" team activities. Only once the weaklings fell off the training schedule, and we felt the looming competition date did we begin to examine essential network-based services like Active Directory and MySQL that we were confident would be used in the actual competition.

Over the following summer, I tried to learn as much about security as possible. I read "Blue" team books, played wargames, and chatted with hackers. I knew that we needed a running start before any cyber defense competitions, so I tried to find other security-minded students as soon as the fall semester started. As early as the first week of school a group of interested students met on Thursday evenings to talk about security and to hack. We began a very simple wargame, named Bandit [1], and I quickly realized the disparate state of the group's Linux command line skills. We set up an instant messaging service and chat room hosted by slack.com, so we could plan future meetings and stay in touch through the rest of the week. We agreed to meet one week later and adjourned.

Through my summer war gaming, I had heard of a few capture the flag events that we could participate in, so I quickly registered a team for NYU's Cyber Security Awareness Week Capture the Flag. We competed remotely over a weekend in September after only a handful of meetings. In total, four students from the College of Charleston competed in that competition.

That was all before we could call ourselves a club at all. After talking to Dr. Olmsted about security during class, he told me that my old teammate (Leo Pate) from the Palmetto Cyber Defense Competition was attempting to start up a cyber-security club on campus. I talked to Leo about it, and we agreed to form a legitimate club as soon as possible. I let Leo handle the paperwork, school government association side of things – I much prefer security. I lead workshops on Thursday nights three weeks a month, and on the fourth Thursday we would drive fifteen minutes to a local Information Systems Security Association meeting where we could learn a lot from industry professionals.

Finally, at the beginning of the spring semester, we were granted club status (but no funding). Through our steady attendance to the local ISSA meetings, we did receive one generous private donation that allowed us to travel out of state for the South Eastern Collegiate Cyber Defense Competition. For the remote SECCDC qualifier, we also tapped back on Chad from the previous year to supervise us and to enforce the rules of the competition. And when we qualified for the on-site

competition, we scurried to assemble a final team as our competitors were dropping like flies. We made it through the SECCDC and faced the PCDC (which is South Carolina only) the following weekend and took home third after going in overconfident and under prepared.

Approaching the next year of the club's life, we became determined to set up a lab in which we could hone our skills and simulate security competitions. Within our academic network there are, of course, restrictions on what can go through the network perimeter. More importantly, peer-to-peer connections between machines on the 802.1x network. These restrictions severely limit the amount of security topics we can learn about within this network. Our solution was to separate ourselves off the main network into a private network for use only by the security club in the pursuit of security knowledge. Since the College of Charleston owns a class B network, we assume that they will have at least one IP address for our network. The remainder of this paper is an outline of our proposal to the college's IT department.

2. Related Work

Over the past few decades, there has been a push to incorporate cyber security education into the curriculum of higher education at all levels. Campbell et al. [1] study programs at the junior college and community college level. McGettricet al. [2] suggests ways to incorporate cyber security education to all levels of higher education including associate degrees, bachelor's degrees, master's degrees and Ph.D. degrees.

More implementation has occurred at the junior college and community college level because it is easy to add a two or four-semester program of some subset of the following ten components:

- Access Control and Identity Management - In this component students learn concepts about controlling access to system resources. They learn the access control models, terminology, best practices, tools, and remote and network considerations to controlling access.
- Cryptography – In this component students learn about cryptographic attacks and the tools to ensure data integrity. They will learn about hashing, symmetric and asymmetric encryption, and certificates. Methods of implementing cryptography are also often presented.
- Policies, Procedures, and Awareness – In this component students discuss security policies, procedures and security awareness. Students learn security classification levels, documents, business continuity plans, risk management considerations, incident response, trusted computing, software development concerns, and management of employees.
- Physical Security – In this component students examine the fundamentals of physically securing access to facilities and computer systems, protecting a computer system with proper environmental conditions and fire-suppression systems, and securing mobile devices and telephony transmissions.
- Perimeter Defenses – In this component, students learn concepts about perimeter defenses to increase network security. Topics often include types of perimeter attacks, security zones and devices, configuring a DMZ, firewalls, NAT router, VPNs, protections against web threats, Network Access Protection (NAP) and security for wireless networks.
- Network Defenses - In this component students discuss network device vulnerabilities and defenses, providing security for a router and switch, and implementing intrusion monitoring and prevention.
- Host Defenses - In this component students learn about the types of malware and how to protect against them, protecting against password attacks, managing file system security, and procedures to increase network security of a operating systems.
- Application Defenses - In this component students discuss basic concepts of securing web applications from attacks, fortifying the internet browser, securing e-mail from e-mail attacks, concerns about networking software, and security considerations when using a virtual machine.
- Data Defenses - In this component students discuss the elements of securing data, such as implementing redundancy through RAID, proper management of backups and restores, file encryption, implementing secure protocols, and cloud computing.
- Assessments and Audits - In this component students examine tools that can be used to test and monitor the vulnerability of systems and logs that provide a system manager the ability to track and audit a variety of events on a system.

Cyber Security at the Bachelors and Master's degree levels should include the study of components outlined above plus secure software development and information and application security architectures. Components at this level require computer science and software engineering course backgrounds that allow the students to:

- Develop and administer distributed systems that guarantee high concurrency and uptime. These systems can withstand network partitions and denial of service attacks.
- Develop and manage software and data architectures that can withstand malicious or erroneous data input and not expose sensitive information to the application user.

The junior college and community college level curriculum was easy to add because it allows learning without in a controlled environment. This includes a simple example or simple laboratory experiments. The curriculum at the bachelors or masters curriculum level is more difficult to add because it requires operating systems in a hostile environment.

One tool universities have used to expose the students to distributed, and hostile environments are Collegiate Cyber Defense Competitions. Conklin [3] studies the use of these competitions in computer science curriculums. Unfortunately, the students only acquire experience in administering and managing systems and software developed by others.

3. South Carolina Data Breech

Our college is part of the South Carolina state government. Over the last few years, the state has been trying to tighten up its defenses against malicious users. The tightened regulations affect the kind of activities cyber-security students can perform on the public network. This tightening is a direct result of a major data breach by the South Carolina Department in 2012 [5].

On August 13th, 2012, a malicious email was sent to multiple South Carolina departments of revenue employees. Some of the users clicked on an embedded link, unwittingly executing a malware and compromising their local workstations. The malware captured the user's security credentials and passed them back to the attackers. A few weeks later, the attacker logged into the machines using a Citrix remote client using the user's credentials.

The attacker was able over the following month to load more password grabbing software onto more machines. These new stolen credentials ultimately allowed the attacker access to database software. On September 12th, the attacker was able to locate a 74GB backup of the department of revenue database. It took the attacker two days to copy the backup from the department of revenue's servers to their own. After the data had been transferred, the attacker did not log in again.

4. Club Security Scenarios

To convince the Information Technology department of the need of a private network, we outlined the following specific scenarios that could happen on the private network:

1. Port scanning within the private network

a. Anna has just joined the cyber security club, and we are going over the concept of ports during the workshop that day. Anna has not heard of ports. John quickly and easily shows Anna how ports look by running an nmap scan of Justin's laptop as seen in Figure 2 below. Apparently, Justin is listening for PostgreSQL connections on port 5432 as a result of some software he has recently installed. In addition to port 5432, Justin is listening for SSH connections on port 22 since he just booted up Kali Linux for the first time and Kali has SSH enabled by default.

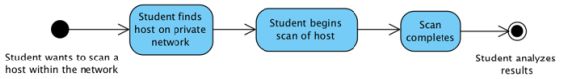

Figure 1. UML Activity Diagram

2. Sniffing traffic inside the private network

a. Zach wants to see if anyone is transmitting passwords in plaintext so that he can alert them to their foible. He launches Wireshark and filters out everything but plaintext hypertext transfer protocol packets. He does not see any passwords after twenty minutes, so he gives up and meets David at their favorite lunch spot (Leon's).

3. Download and inspect potentially harmful software

a. Callum is competing in NYU's CSAW CTF again this year. He embarks on a challenge entitled 'Fluffy.' The only offered challenge is an unidentified .exe. He connects to a Windows 7 virtual machine on the local ESXi box and downloads the fluffy executable. Upon running it, he determines that it is not harmful to run, and it simply gives him the flag when he asks nicely. He retrieves the flag and terminates the program.

4. SSH to a host within the network

a. Aspen's Linux-based laptop listens for SSH connections by default. John logs in with an account that Aspen created for him and accessed a text file that contains a list of members in the club. He copies it to his machine using scp and logs off.

5. Club Security Use Cases

To convince the Information Technology department of the need of a private network, we outlined the following generalized use cases that could happen on the private network. The ways that students in an academic club can use a piece of infrastructure vary and are inherently unpredictable. But by offering the IT department an white-list of activities we can mitigate the opportunities miscreants and vandals have to take advantage of our design. Granted, the activities that should be whitelisted on cyber security club's network are already going to be more dangerous than an average user's network usage. By combining this basic whitelist with the ethics agreement in section VI, we all-but-guarantee the safety of our network. It will

see limited use by a known group of people, so that responsibility may fall swiftly on any malefactors.

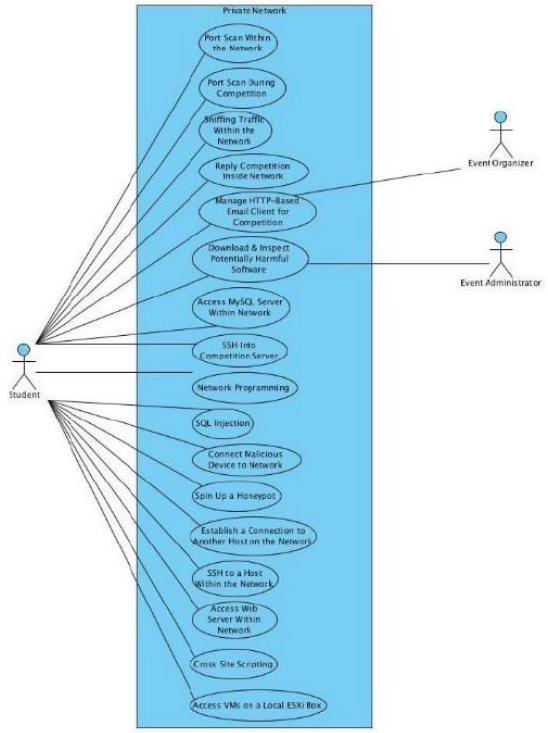

Figure 2. UML Use Case Diagram

Name: Port Scanning Within the Private Network
Roles: Students
Entry Condition: Student wants to scan another machine on the network
Flow: Student begins a scan of the open ports (using tools like nmap) of another machine on the private network
Exit Condition: The scan completes
Name: Sniffing traffic inside network
Roles: Student

Entry Condition: Student wants to see if any interesting traffic is flowing through the network
Flow: Student launches software application (Wireshark) that will sniffs network packets, Student observes network behavior, and Student terminates packet-sniffing software
Exit Condition: Student terminates packet-sniffing software

Name: Download and inspect potentially harmful software
Roles: Student, Event Administrator
Entry Condition: Event Administrator offers Student some software that may be harmful
Flow: Event Administrator offers Student software to inspect for a competition, Student downloads binary executable or other possibly malicious file to the sandbox, Student reads its contents, Student determines if it's safe enough to run, Student runs or deletes software to determine is malware is present and, if so, what it's doing, Student terminates running software
Exit Condition: Student terminates running software or removes associated files from the virtual machine / sandbox File Size: 1Kb–1GB

Name: ARP cache poisoning
Roles: Student Attacker, Student Victim
Entry Condition: Student is on the private network and wants to execute an ARP cache poisoning attack
Flow: Attacker poisons Victim's ARP table by insisting that Attacker is the default gateway for the network, Attacker becomes the default gateway in Victim's ARP table, all of Victim's traffic is routed through Attacker, Attacker watches all traffic flow from Victim, taking anything of interest like unencrypted passwords
Exit Condition: Attacker ends the attack

Name: Replay competition inside of network
Roles: Student
Entry Condition: Students want to practice for future competitions by replaying old competitions within the private network
Flow: Student downloads image of a challenge server, student deploys virtual machine inside the network, and other Students access the server and capture its flags
Exit Condition: Students capture flags and turn off the VM
File Size: 1.5–3 GB

Name: Manage HTTP-based Email client for competition
Ports: 80, 443, 8080, 8443
Roles: Student, Event Organizer
Entry Condition: Event Organizer gives Student email credentials
Flow: Event Organizer gives Student credentials to an email account for competition; Student configures mail client, and student checks emails, competition ends
Exit Condition: Competition ends

Name: Access MySQL database within the network
Ports: 3306
Roles: Student
Entry Condition: Student runs a MySQL server on the private network, and another Student wants to connect to it
Flow: Student runs a MySQL Server on a machine in the network, another Student connects to that machine via the MySQL protocol, Student queries database, and Student terminates connection
Exit Condition: Student terminates connection to the other Student's MySQL server

Name: SSH to a host within the network
Ports: 22
Roles: Student
Entry Condition: Student is running an SSH server on the private network, and another Student wants to access it
Flow: Student runs an SSH server on the network, another Student access that server via SSH or Putty, Student uses the command line until they accomplish their task or become fatigued; Student ends the connection
Exit Condition: Student terminates the connection

6. White Hat Agreement

Each member of the club was asked to sign a white hat agreement. This process was used to ensure that each member understood their ethical responsibilities while participating in the club. The agreement follows:

- As a member of this club, you may be exposed to systems, tools and, techniques related to Information Security. With proper use, these components allow a security or network administrator to understand better the vulnerabilities and security precautions in effect. Misused, intentionally or accidentally, these components can result in breaches of security, damage to data or other undesirable results.

Since these club experiments will be carried out in part in a public college network that is used by people for real work, you must agree to the following before you can participate. If you are unwilling to sign this form, then you cannot participate in the club activities.

Student agreement form

I agree to:

- Examine only the special course accounts for privacy vulnerabilities (if applicable).
- Report any security vulnerabilities discovered to the course instructors immediately, and not disclose them to anyone else.
- Maintain the confidentiality of any private information I learn through the course exercise.
- Actively use my course account with the understanding that its contents and actions may be discovered by others.
- Hold harmless the course instructors and my University for any consequences of this course.
- Abide by the computing policies of my University and by all laws governing the use of computer resources on campus.

I agree to NOT:

- Attempt to gain root access or any other increase in my privilege on any University workstation.
- Disclose any private information that I may discover as a direct or indirect result of this course exercise.
- Take actions that will modify or deny access to any data or service not owned by me.
- Attempt to perform any actions or use utilities presented in the laboratory outside the confines and structure of the labs.
- Utilize any security vulnerabilities beyond the target accounts in the course or beyond the duration of course or exercise.
- Pursue any legal action against the course instructors or the University for the Consequences related to the course.

Moreover, I consent for my course accounts and systems to be examined for security and privacy vulnerabilities by other students in the course, with the understanding that this may result in information about me being disclosed (if applicable). This agreement has been explained to me to my satisfaction. I agree to abide by the conditions of the Code of Ethics and White Hat Agreement.

6. Conclusion

In this paper, we relate the experience of establishing a cyber-security student club in a state-funded liberal arts college. We present specific scenarios and generic use cases of the student presented to the college's information technology division. We also present a student "White Hat Agreement" that each club member must sign to participate in the club. We have received positive feedback from the IT department and we fully expect to have a private network in place for the opening of the Spring 2016 semester. There are two, exclusive sets of desires at play here:

- those of the university - to maintain network safety,
- and those of the club - to experiment with scenarios that are as close to real-world and as hostile as possible.

Since having both on the same network is not practical, we suggest totally separating the two networks. One safe network for general use by the student body and one dirty network for use by the club during security exercises.

7. References

[1]"Bandit Wargame," OvertheWire, [Online]. Available: http://overthewire.org/wargames/bandit. [Accessed 30 06 2015].

[2] R. D. Campbell, E. K. Hawthorne and K. J. Klee, "The role of two-year colleges in educating the cyber-security workforce.," ACM SIGCSE Bulletin, vol. 35.3, pp. 235-235, 2003.

[3] A. McGettrick, L. N. Cassel, M. Dark, E. K. Hawthorne and J. Impagliazzo, "Toward curricular guidelines for cybersecurity," in In Proceedings of the 45th ACM technical symposium on Computer science education, 2014.

[4] A. Conklin, "Cyber defense competitions and information security education: An active learning solution for a capstone course," in In System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on, 2006.

[5] "The South Carolina Data Breach: A Lesson in Deaf and Blind Cybersecurity," Security Week, 28 11 2012. [Online]. Available: https://www.securityweek.com/south-carolina-data-breach-lesson-deaf-and-blind-cybersecurity. [Accessed 30 06 2015].