The Growth of the Mid-Atlantic CCDC: Public - Private Partnerships at Work

Tim Rosenberg, President and CEO, White Wolf Security, Casey O'Brien, Associate Professor, Community College of Baltimore County

For the past three years, White Wolf Security has partnered with the CyberWATCH Center and the Community College of Baltimore County (CCBC) to design, conduct and score the Mid-Atlantic Regional Collegiate Cyber Defense Competition (CCDC). Over the course of those three engagements, the competition has grown in the number of teams, the size and diversity of infrastructure and the sophistication of the scoring process and visualization.

As the teams finish up the 2008 Mid-Atlantic CCDC Regionals, the principal partners of White Wolf Security and CCBC are already laying the foundations for increasing the scale and complexity of next year's competition. New technologies and more protocol diversity are on the drawing board to include SCADA, RFID, remote, and mobile assets.

This paper will discuss the evolution of the Mid-Atlantic Regional CCDC from a single 3 day event of 5 teams and a handful of servers to two rounds of exercises culminating in a three day exercise involving nearly 20 Class C networks, 1 Class B network, Two Class A networks, 10 Red Cell members, spectators, fiber, VOIP, a real CEO and leadership and team building sessions.

As the exercises continue to mature and expand, easy integration into course lesson plans, labs and quantifiable skill sets becomes not only a possibility, but a necessity.

I. Introduction

In the fall of 2005, White Wolf Security was approached by Casey O'Brien of CCBC to design, host and score the first Mid-Atlantic Regioal CCDC. The spring of 2006 brought 5 teams from Maryland, Pennsylvania, and Virginia. By today's standards, the infrastructure was simple. Each team had a router, a firewall and a small sampling of servers. Scoring was accomplished through a custom Perl script that simply checked network and service availability and integrity. The following year, 8 teams joined the competition and the infrastructure grew to include some additional servers and a choice of firewalls. Finally in 2008, 9 teams participated in two one day regional qualifiers with the top two teams returning later for a three day national qualifier. In 2006, the teams defended a mere 7 assets including router, firewall, servers and an IP surveillance camera. In 2008, teams were responsible for 18 IP assets with more than 10 different operating systems. In 2006 there were only 4 Red Cell members, in 2008, there were more than 8 Red Cell attacking the college teams at any one time. In 2006, the United States Secret Service played an active role as actual law enforcement; requiring teams to conduct a live investigation with actual federal law enforcement. The Service's presence continues to be a key element in the exercise and now requires students to fill in actual Secret Service Network Incident Reports; just as they would in real life. In 2006, the infrastructure was limited to only those assets defended by the student teams. In 2008, we have replicated entire segments of the real internet; thus simulating assets that are not controlled by the defending teams, but are required to maintain functionality and connectivity to the outside world. The area with the most dramatic improvement is with the scoring. In 2006 the scoring engine was a Perl script that accepted minimal input and generated rough scores. In 2008, the scoring engine now supports mapping visualization, basic Red Cell tracking, and three dimensional modeling of the teams' assets.

The growth and scalability of these exercises are the result of corporate partnership with academia. White Wolf Security's exercise infrastructure not only supports the Mid-Atlantic Regional CCDC, but a diverse group of other clients. The Mid-Atlantic region benefits from the corporation's investment in equipment and time to help support a complex and real world environment. However, White Wolf Security is not alone in its partnership with academia to support the CCDC. Bogdan Computer Services built a complete VoIP infrastructure, Promia donated software, Core Security donated Core Impact and several Red Cell members got leave from their employers to participate and enrich the experience; and yet the list continues. Paul Currie a Principal in Action International (a leading business coaching firm in Lancaster, PA) played the role of CEO. All in all; more than ten companies contributed time, person-power, software and hardware; all to the cause of creating a valuable and powerful educational experience. As we rest from the efforts of the regional competition on March 7-9, 2008, we are already designing 2009 and reaching back out to the business community to once again expand and grow the Mid-Atlantic Experience. This paper will describe the many players and diversity of infrastructure in the hopes of providing resources and knowledge for other regional exercises, educational programs and growth.

II. The Defender's network

Figure 1 shows the network diagram from this year's regional qualifier. Figure 2 shows the diagram from the first Mid-Atlantic in 2006 (make sure the Figures and pictures correspond to the correct competiton). Not only has the size of the network vastly increased, so too has the number of operating systems, required services and hardware. The 2006 diagram was designed as a basic, limited use infrastructure. The evolution to 2008 has been based on feedback from the regional participants and those returning from nationals. The growth can be summarized into a few topics; network infrastructure, consoles, real world applications and VoIP.

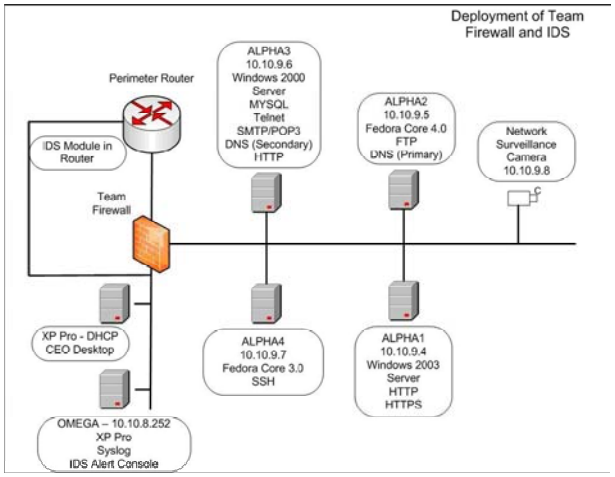

Figure 1 2006 Regional Team Diagram

A. Network Infrastructure (Routers)

One primary change over the years has been the removal of network infrastructure from the team's control. Few universities in the Mid-Atlantic region actively teach Cisco hardware. In 2006, the Red Cell compromised the teams' routers almost immediately. The disparity of Cisco IOS knowledge between the attackers and the defenders was significant. With the head end routers compromised, it was possible for the Red Cell to stop traffic to all the systems, thus preventing the scoring engine from making contact. While a single point of failure like this is a real world risk, the teams lacked the knowledge and experience to adequately mitigate and manage the situation. The result was early frustration on the side of the defenders and an over-focus on the router by the attackers. The teams simply lacked the skill base to manage the equipment. Therefore, the routers were removed from the 2007 Regionals and continue to remain out of play until such time as the participating universities feel comfortable in dealing with them again. Equipment donations by Cisco to several participating teams is making this re-entry a very near term reality.

B. Network Infrastructure (Firewalls)

As in the case of the routers in 2006, firewalls took a similar hit in 2007. In 2007, the decision was made to provide the teams with the choice of Linux versus Cisco PIX firewalls. Six of the competing eight teams chose a Linux build with ipchains, shorewall and webmin. In response to the Cisco difficulties of 2006, it was decided to allow the teams to rebuild their firewalls with the software of their choice. Unfortunately, lack of experience, coupled with the pressures of the engagement resulted in seven of the eight teams successfully locking their firewalls out. All eight teams were sent home early on the first night while the exercise coordinators rebuilt firewalls to allow the resumption of operations the next morning.

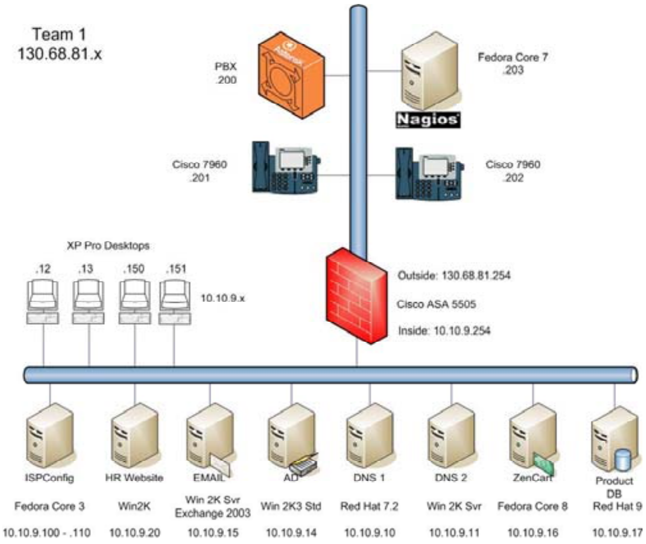

Figure 2 2008 Regional Team Diagram

In the 2008 competition, we settled on using the Cisco 5505 firewalls for the student teams. Their size and low cost makes the 5505 easy to acquire and deploy. Furthermore, their built in 8 port switch with power over ethernet (POE) capabilities reduces power requirements and saves on desktop space. Lastly, the Cisco Adaptive Security Device Manager (ASDM) provides an intuitive graphical user interface making configuration easy. Console access is still available for those teams who wish the greater flexibility of the Cisco IOS, but it is no longer required. An additional benefit of the 5505 ASDM is that it is the same on the larger rack mounted ASA devices, thus providing additional training and eduction to those who will continue to maintain and monitor Cisco equipment during their professional career.

C. *Consoles*

One of the challenges in growing the size of the defenders' networks is providing adequate console access. Most of us in this line of work use VMware to maximize hardware utilization in an effort to keep costs under control. The down side to virtualization is that it reduces the number of keyboard, video and mice that a team can use. In 2006 and 2007, there were far too few consoles. This left many team members shoulder surfing or simply not engaged at optimal levels. In 2008 we approached a larger scale by significantly increasing the amount of hardware and installing web admin tools where necessary. Each team had 6 laptops with two to three virtual machines running on 5 of the laptops. The Asterisk PBX server was run in headless mode on dedicated PC hardware. This design, combined with the embedded operating systems of the VOIP phones and PDA allowed for enough diversity of targets with plenty of consoles to go around.

Teams are allowed between four and eight students. In the 2008 regional, there was one team with four participants. They were clearly overwhelmed in trying to manage and control the volumes of assets, business injects and attacks. On a team of eight, the structure eventually evolved into:

1. One team captain who managed and spent some time at a keyboard.
2. One person managing the VOIP phones and business inject emails
3. Five people at keyboards with one floating between the internet, or dealing with the Secret Service.

With a maximum team of 8, it appears that six sets of keyboards, mice and screens makes a good exercise. However, as we continue to grow the scope of the competition, it is likely that we will need to add additional hardware. In 2009 we are already looking at adding one extra set of hardware for forensic processing and one for remote control. The remote control terminal will be used to manage those assets that are deployed away from a team's physical infrastructure. As most enterprises have grown beyond the traditional network DMZ, teams will need to address the issues of managing and securing remote and mobile assets. This environment also provides more target opportunity for the Red Cell and allows more complex business injects such as virtual private networks and remote networks.

D. *Real World Applications and Laws*

Building and deploying enterprise applications of any kind is a time consuming event. Through the use of open source applications, database generators and good scripting we've been able to create a diverse and functional corporation.

Open source enterprise applications such as Orange HRM (http://www.orangehrm.com) and Open EMR (http://www.openemr.org) allow for rapid creation of real world applications. These framework applications are just two examples of the many that are out there. However, just having a functional human resources website up does not make for an interesting target. Several states have notification requirements in the event of a data breach. If there is no data in the databases, then there is not much to report on from the defending side. Also, without a populated database, the Red Cell is left merely obtaining root access and then what? The solution is one of many low cost database data generators. We use the DTM data generator available for under $200. This allows for rapid population of customer, patient and human resource databases. (http://www.sqledit.com/dg). For those interested in large scale e-commerce product population, there is Etilize (http://www.etilize.com) which will provide over seven hundred and fifty thousand produces via a comma separated file for less than $5,000.

As part of the continuing public/private partnership, White Wolf Security has partnered with Millersville University to create several fully functional web applications. Three applications are under development at this time; 1) an e-commerce site, 2) an inventory/order fulfillment site and 3) an e-bank for consumers and business. The final result will be a complete, integrated solution that lets spectator/participants open a bank account, buy things online and have them 'delivered'. All the while the applications will be exchanging inventory and shipping information while the bank moves money from consumer to e-commerce to inventory site.

Current and pending legislation requires notification of a data breach. Some of those statutes have a stated minimum number of records (i.e. 10,000) that must be compromised before notification is required. The use of real applications with fully populated databases provide the teams' with real experience in incident analysis, forensic techniques and working with law enforcement.

E. *Voice Over IP*

A new feature of the 2008 regional competition was the introduction to Voice Over IP. Using Freepbx (http:/www.freepbx.org), twenty Cisco 7960 phones and the gracious donation of time from Bogdan Computer Services, the teams were all given a VoIP PBX server and two VoIP phones. The phones and servers not only added to the size of the defending infrastructure, but were also used to send business injects, field support calls from spectators and facilitate communication from the CEO to the teams.

II. The Red Cell and Public Assets

In 2006 and 2007, the Red Cell attacked from a single Class C network. While a functional requirement at the time, it made the defender's task of identifying attacks relatively straight forward. In addition, there were no spectators or traffic generators. As a result, all traffic was malicious and from the same block of 254 addresses.

In 2008, with the addition of signifiant equipment at the routing core, we were able to expand the range of Red Cell addresses to six class C networks. This allowed the Red Cell to break up attack patterns, set up rogue IRC servers and to pass reverse shells back to different networks and hosts.

This diversity of address space was made possible through a layer three route aggregator at the core, VLANs and VLAN trunks and fiber uplinks.

This expansion at the core also allowed us to add a new feature in 2008 - public assets. Public assets are those systems that are not owned by either the Red Cell or student teams, but are required to support a certain degree of functionality. Examples of these in the real world are the root DNS servers, upstream PBX servers, software update and download sites. Through the use of VMware, website mirroring software and additonal layer two switches, we were able to put the following assets into 'play' for use by either team:

1. time.nist.gov - a central NTP server was setup and resolved to the actual time.nist.gov IP address of 192.43.244.18
2. www.sysinternals.com - A mock up of the old Sysinternals website was placed in game for teams to download resources and tools.
3. www.2008ccdc.com - an internal website hosting old (and vulnerable) copies of client side software; thus expanding the target space to include client side attacks
4. Two root DNS servers - two master root DNS servers were placed at their actual IP addresses of 198.41.0.4 and 192.228.79.201. This allowed for rapid deployment of team DNS and mail servers. Since all copies of DNS servers know to look for those roots, we easily added domains, MX records and begun forwarding email.
5. www.arin.net - Another in-game asset was a re-creation of www.arin.net to facilitate ownership lookups of attacking IP address.
6. Windows Update Server - a WSUS server was deployed to facilitate the updating of the various Windows operating systems.

There is a practical purpose to the deployment of these assets: they fundamentally reduce the load on the internet connections. Other reasons for deploying these servers 'in game' is to better monitor performance of the defending teams, provide more creative business injects and a more dynamic, realistic and scalable exercise.

I. Scoring and Visualization

The scoring engine for the 2008 regional competition is the most visible improvement. In 2006, the score was tallied through a Perl script that simply checked network service availability and integrity. Today, the score engine supports geo-location of IP assets, three dimensional visualization, an interactive news ticker, sponsorship information, Red Cell tracking and a message ticker for the Red Cell to leave messages for the spectators.

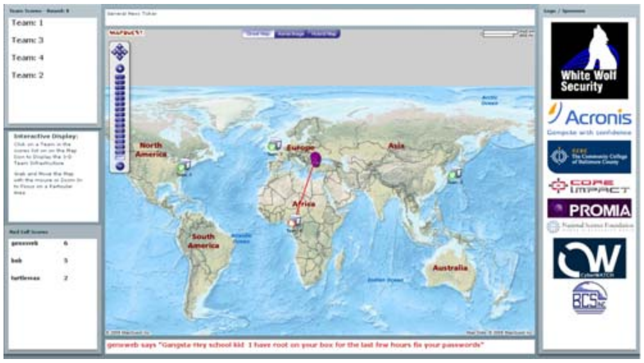

Figure 3 Map view of scoring engine

Figure 3 is the scoring engine map view. Each round, the map is drawn with attackers (the skull icon and the teams). The engine supports geo-IP lookups allowing you to build geographically meaningful scenarios (assets in a certain city/country with attackers in specific locations.) In this sample image, you can see a Red Cell member engaging in attacks with Team 4 in Africa. This information is generated via a 'phone home' script. Each Red Cell member is given a phone home script that they are to execute on each system they compromise. If the engine picks up a phone home, it connects the appropriate attacker IP to the taget/victim. The system even supports island hopping and will allow a Red Cell to attack from another system than where they started. The map also supports full zoom, mapping and drawing features as well since it is the complete Mapquest engine.

In the top left hand corner of the screen are the team standings. By mousing over, you can see the points for each team. Otherwise, it simply lists the team in their rank order.

The middle left text block has some general user instructions while the lower left block reports Red Cell activity. For every phone home script that a Red Cell member executes, their count increases by one. Shown here are the handles or nicknames of the attackers with ‘genexweb’ in the lead with six compromised systems.

The bottom text string in red is the Red Cell message board. With each phone home script, the attacker is able to insert a text string for display on the board. In this case, it is a taunt to the defending team to change their passwords. In other arenas, you could require them to report back how they got in or some other message.

The full right hand column is place holder to thank sponsors, donors and others involved. In this case, we have inserted the logos of all those who worked to make the 2008 Mid-Atlantic Regional CCDC a success.

Finally, in the top message box is a news ticker that is used by the White Cell (or operations team) to distribute messages to the spectators/participants. This could be used to facilitate news, e.g., ‘Team 1 suffered a data breach, 1000 records compromised’, business inject status or any other message you would like to convey to the group at large.

Left clicking on any team starts off a three dimensional animation that rotates the team’s assets around a central axis, showing status, Red Cell entry and integrity checks.

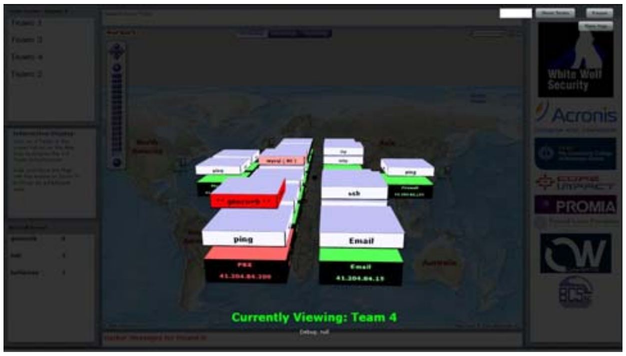

Figure 4 Three Dimensional score view.

Figure 4 is a still of a three dimensional animation from the 2008 Mid-Atlantic Regional CCDC. The bottom square shows the IP address and name/purpose of the system. In this example, you can see the PBX server and email server. If the bottom is green, the system is reachable and the services have all passed their requisite checks. The PBX server is shown in red with a floating red **genexweb** rectangle. This indicates that a Red Cell member has compromised the system and successfully executed the phone home script. In the back can be seen a lighter red MySQL (80) box. This indicates a failed service check and the corresponding point penalty. If a service is not reachable at all, it is placed on the IP address and grayed out. The animations continue to revolve and cycle through all the teams until such time as the ‘view map’ button is clicked on above.

The important thing to note about this scoring engine is that the display. Configuration and monitoring of the entire system is web driven. The system even manages and sends business injects via email.

II.Future work and partnerships

IP controlled SCADA devices are presently under construction at White Wolf Security’s offices in Lancaster, PA. These devices are manufactured with enterprise PLC’s from Modicon and control power flow to teams through a web server on the PLC. These and other physical/cyber devices will continuously be developed and deployed in future exercise. Also under development is the integration of RFID and, through another corporate partnership, 802.11 enable surveillance robotics. As more companies experience the Mid-Atlantic CCDC, they are seeing it as a test bed for their own products, tools and resources. In the case of the robotics, a Lancaster, PA firm became involved through other means and discovered that their robotic solutions would make for interesting assets in an exercise. More CEO’s will get involved and play the required role and the Secret Service will continue their law enforcement involvement.

III.Conclusions and Future Work

Work continues on the scoring engine, infrastructure roll out and development. As more and more companies get behind this process, the exercise will grow in size and complexity, thus enriching the educational experience for all involved.

The diversity of players in the 2008 Mid-Atlantic CCDC, combined with the hard work of many people, is what makes this process work. Scaling up the core routing infrastructure is a pre-requisite for the CCDC to grow. If some one is willing to take on that responsibility, it makes it easier for other companies to ‘hang’ additional infrastructure off the back-bone and grow the exercise to what ever size best fits the needs of the region.