USF's SECCDC Final Report

By Alex Taylor (Team Captain)

Preface

SECCDC is the Southeastern Collegiate Cyber-Defense Competition, hosted each year by Kennesaw State University (KSU). The competition has an 8 year history, with this year's (2011) competition being the 8th. Teams from USF (specifically the Whitehatters Computer Security Club [WCSC] at the university) have competed before in 2005 and 2006. However, no members from those past teams are left at the university.

This year, WCSC decided to get a team together and compete for the first time in 5 years. The decision to compete again was largely due to the fact that SECCDC is a defense competition, unlike the typical assault or puzzle-related competitions the club typically enters. SECCDC also has a unique business aspect to it (timed business injections), which the team looked forward to (the team was entirely IT and CS/CSE majors - save for the one Statistician).

Preparation

The team really didn't spend much time preparing for the competition. They had one large meeting at Broadway Pizza where we divided up tasks and assigned each individual a job. They also had some email communication back and forth to build a whitelist request and assemble potential study material for each task. After that, preparation was really left up to each individual person.

Most of the preparation involved getting funding for the group to actually make the 10 hour drive up to Kennesaw. They obtained funding from the USF Student Government to rent a 12-person van for the trip, and also obtained funding through REU work that two of the students were doing to pay for 2 of the 3 hotel rooms and gasoline for the van. The other hotel room was picked up by the USF College of Engineering. That, plus individual contributions for food and a sponsorship by CACI for shirts, resulted in the trip being largely paid for (albeit by a large array of different entities).

Day 1

On the first day, the team was led to their room at noon. Upon entering the team immediately inventoried the hardware that was given to them, and attempted to log into all systems. Unfortunately, it took the team 7 hours to figure out that the passwords to all the systems were "kennesaw", resulting in several servers and a workstation being unusable for most of the first day.

The systems that could be logged into were patched as fully as possible (all Windows XP machines were updated to SP3), and security software was installed where possible (Microsoft Security Essentials). The team also set up the printer on the Windows 7 box, resulting in our team being able to turn in all forms on HAL letterhead.

Significant problems on the first day for the team included not being able to get into the Stonegate firewall at all (the password that was given to us, as well as "kennesaw", did not work) and not being able to

update anything. The Microsoft update servers were blocked completely, as were the update servers for Ubuntu, CentOS, and OpenSuSE. Only having one hour to reconfigure and lock down the Linux servers (due to not having guessed the passwords for them) also posed a problem for the team.

The team did, however, do a number of things right. The team largely kept on top of business injections on the first day, resulting in a number of points having been gained from those early on. The team also did a great job of reconfiguring Windows group policy to lock down the Windows servers and workstations. Installing Microsoft Security Essentials was key in our being able to keep services up the next day. Best of all, the Stonegate firewall was rebooted into safe mode, which saved us from being hit by the red team the following morning through the open SSH port on the firewall itself.

Day 2

The second day of the competition brought attacks from the red team to the network. We were initially spared because of the change to the Stonegate router, but soon the team had to contend with trojans from Metasploit being planted on the Windows XP workstations and the mail server (running Windows Server 2003). Microsoft Security Essentials suspended and removed all these trojans, however the team had forgotten to install it on the mail server initially, resulting in the red team having control of that server during the time that it was installing.

The team also struggled with the new Checkpoint firewall that replaced the old Stonegate firewall. Once it was properly configured and in place, however, it stopped all red team attacks from that point on. Having the IDS feature of the Checkpoint on was responsible for this.

Most of the time on day two was spent attempting to finish business injections while the red team attacked and various other distractions were given to the team. The team finished every injection, but some were late (and still others were very late). This is likely where most of the team's points were lost, and was the most challenging part of day two.

Red team attacks were largely absent or were simply automatically taken care of by software/hardware the team had set up and configured. In fact, by the end of the day the team was one of the only ones left standing (despite massive DoS attacks being launched around 7pm).

Day 3

The third day of the competition was simply a wrap up of how each team did, followed by an award ceremony. The team ended up in third place (behind the University of Northern Kentucky [2nd] and Louisville University [1st]), just barely edging out the host team (Kennesaw State University) by about 50 points. Red team members were present and gave a small talk about things they had encountered during the competition, which was interesting.

Two of the team members, Alex Taylor and Clayton Whitelaw, also presented their research outside the auditorium before and after the awards ceremony. The research – using social media (Twitter) to study social phenomena – wasn't entirely security-related, but was definitely relevant to students in the competition. The

students discussed the wealth of up-to-date and relevant information that could be pulled out of Twitter and aggregated by the Java applet. They also explained the myriad ways this information could be used in tracking information about current events and how it would be useful to news media, researchers, and more.

Attendees thought the Java applet and corresponding Firefox addon were interesting and the information they gathered useful. Unfortunately, not many had much to say in the way of feedback (which is what the students were hoping for). Those who stopped by to hear what the students were saying about the research were supportive, though, which at least showed the students that the research was heading in the right direction.

Assessment

From a technical point of view, the team was very successful. Nearly all red team attacks were stopped (and the ones that did not get stopped were taken care of quickly), and the team ended the competition with a large amount of service points (likely second or third in SLA). The team also was the only one to have submitted a properly formatted incident report (for a SQL injection vulnerability the team found in their eCommerce website). However, the team was not awarded any points for this, due to no points having been deducted for the vulnerability.

Overall, what lost the team the most points was misunderstanding the way business injections were scored. Although the team was aware that turning in an injection late would result in lost points, the team was unaware that this amount would reach zero. The team was also never notified when a particular injection had expired. As a result, the team completed every injection – but many of them were late (sometimes by up to 4 hours late). Had the team known about injection expiration, they could have focused their efforts more on only those injections that could be scored in a reasonable amount of time.

The only real complaint the team had during the competition was the complete lack of feedback from the organizers in regard to score. Although the team understands that the scoreboard provided to the organizers had technical issues, it made it extremely difficult to gauge our progress without a proper scoreboard. The Nagios service was fine as a fallback to track services, but there was still no tracking of injection score available during the competition. This prevented the team from being able to see how they were doing and make changes accordingly.

Conclusion

In general, the competition was a positive experience for the team. They had fun competing in SECCDC, and will likely be back for the competition next year (providing adequate funding is given). The overall format of the competition was interesting and engaging, and the team looks forward to it being refined over the next year.