Think you "Know Your Enemy"?

Hackers compete in iCTF 2009

UCSB hosts largest security competition ever performed on the Internet



by Alison McElwee

How did the UCSB faculty and staff react when hundreds of hackers staged a coordinated, 'drive-by-download' attack on the school's computer servers?

Actually, they were quite proud.

This year's <u>International Capture the Flag</u> contest was the largest security competition ever performed on the Internet. 56 teams made up of over 800 students from all over the world competed in the one-day event. O rganized by <u>Prof. Giovanni Vigna</u> of the <u>Department of Computer Science</u> at UCSB, the ICTF is a distributed, wide-area security exercise whose goal is to test the security skills of the participants.

"KNOW YOUR ENEMY!" was this year's theme, as participants worked feverishly to compromise other users' web browsers, steal their money and secretly download malicious software onto their computers. At the same time, the teams were charged with protecting their own network systems from the global onslaught.

The winning team was able to keep the most number of their own services available while successfully hacking

through the largest number of security mechanisms in the other teams' services, thereby 'capturing the flag' of their competitors. This year's best hacker honor went to the "CInsect" team from the University of Hamburg, Germany.

The yearly competition exposes many of the devious schemes Internet criminals use to gain access to secured networks and steal a computer user's privacy-or worse. Here's what team CInsect did better than anyone else:

- **Step 1:** Analyzed the code of a number of different browsers, and found vulnerabilities that could be e xploited.
- **Step 2:** Lured the simulated users to a web site under their control by publishing blog entries and u sing search-engine optimization techniques.
- Step 3: Launched effective drive-by-download attacks.
- Step 4: Used this information to keep their own services from being compromised.

Prof. Vigna believes that as the Internet evolves in terms of both the type of services and applications being deployed, the methods of malicious activity changes with it. "Web applications have become tremendously popular, and, nowadays, they are routinely used in security-critical environments, such as medical, financial, and military systems. As the use of web applications for critical services has increased, the number and sophistication of attacks against these applications have grown as well."

The ICTF continues to evolve as well. What started out as a local competition in 2003, it now involves several educational institutions spread across different continents. Loosely based on the original <u>DEFCON Capture the</u> <u>Flag contest</u>, the design of UCSB's competition improves year after year. For 2009, teams could also earn points by completing challenges based on trivia, forensics, and reverse engineering.

Prof. Vigna hopes that by students participating in these sorts of dynamic, live-action security exercises, they will be prepared to participate in the design of a more secure, and ever-changing, Internet.

Related Links

<u>The UCSB iCTF</u> <u>Giovanni Vigna Faculty Profile</u>

Department of Computer Science