

Annual hacking game teaches security lessons

Robert Lemos, SecurityFocus 2005-08-04

LAS VEGAS -- The weekend-long Capture the Flag tournament stressed code auditing as a measure of hacking skill this year, a move that emphasized more real-world skills, but not without controversy.

The annual Capture the Flag tournament at DEF CON has always attracted participants from a variety of background, looking to try their hands at online attack and defense. Under a new set of organizers this year, the game pitted teams and individuals against each other to find and exploit vulnerabilities in their opponents' systems to score points. The game, dubbed "WarGamez" this year, put more emphasis on real-world skills compared to previous years, said [Giovanni Vigna](#), associate professor of computer science at the University of California at Santa Barbara and the leader of team Shellphish, which [won the event](#).

"The game required skills that are also required by both security researchers and hackers, such as ability to analyze attack vectors, understanding and automating attacks, finding new, unpredictable ways to exploit things," Vigna said. "It's about analyzing the security posture of a system that is given to you and about which you initially know nothing."

The latest incarnation of the game--run by a group of security professionals who asked to only be identified by their group name, Kenshoto--attracted students, military computer experts, security professionals and hobbyist hackers. For the teams, the controversy surrounding security researcher Michael Lynn's [outing of a high-profile vulnerability](#) in Cisco Systems' routers, mattered little. Finding vulnerabilities in each other's servers became the focus of their world.

In previous years, the game allowed each side to run their own server, and required that certain services be available. This year, the organizers ran a central server on which each team's virtual server ran.

The move was not without controversy, however, as it removed from the contest any teams that concentrated on defending their systems by using a specialized operating system, said Crispin Cowan, director of software engineering for Novell's Linux division, SUSE.

"Prior games involved both attackers and defenders working on the problem, but because Kenshoto took total control of the reference servers to be defended, there is very little defense that can be deployed," Cowan said. "Their scoring system also made defense essentially worthless other than to deny other teams points."

Cowan competed for several years as the leader of a team fielded by secure Linux operating system vendor Immunix, which was bought by Novell in May. Porting services over to its security-enhanced operating system became a signature strategy of the team.

The Capture the Flag game is suppose to measure security researchers and hackers abilities to attack and defend systems, said one of the organizers, not necessarily be a test of products.

"We did intentionally de-emphasize defense, because it is a hacking competition, after

all," said the organizer. By agreement, the group that ran the game adopted the name Kenshoto and would only speak anonymously. "However, defensive skills were tested."

Some teams had success deploying Tripwire, a data-integrity checker that can find changed files, and monitoring traffic with an intrusion detection system, he said. A knowledgeable defender could also lockdown the systems, further hardening them.

In the end, however, the game focused on finding and exploiting vulnerabilities.

"What it takes to be an elite hacker is to find vulnerabilities in custom software," said the Kenshoto member. "It is not code auditing per se. They have to reverse engineer, and we have made it difficult to reverse engineer."

The Kenshoto group ran all the teams' virtual servers on a single machine using a technique known as "jailing," which limits each team or individual to separate directories on the master system. The computer ran the FreeBSD operating system and utilities and services were written in Perl, Java and C. The group also ran an in-game auction site known as eDay.

Each team's authentication token, or totem, was placed on the bottom of a can of Tab, which the team was expected to guard.

While a few individuals and teams used the eDay auction site, most of the deals for items were done behind the scene, according to one member of Kenshoto. One team's can of Tab, which held the team's secret code on the bottom, went for 101 beers, the organizer said.

The teams each sought to score points by keeping services running, stealing or overwriting digital tokens on each server, and producing advisories with working exploit code. Rooting the main Kenshoto mainframe would earn massive points, according to the rules, but a failed attempt would penalize the team "back into the stone age."

Auditing did play a big role in the game's strategy, said the Kenshoto organizers, because finding flaws is a major factor in attack and defense in the real online world.

"The auditing people did as part of the game was similar to the job of anyone trying to find risks in third party software, be it a black hat or someone trying to determine whether third-party software is safe to integrate with an existing system," said one organizer.

Notable differences, however, include the time pressure, the fact that participants not only had to find a vulnerability but exploit the flaw, and that the teams did not have access to any source code.

The winning strategy balanced finding flaws with hardening the systems services, said Vigna of the winning team Shellphish.

"On the defense side, we had people responsible for monitoring--both manually and using automated tools--incoming traffic and running processes to find out how we were attacked," he said. "We also had people that make sure that our services were up and running ... Finally, we had people who would choose a service and try to find exploitable vulnerabilities."

In the end, however, Novell's Cowan remained unconvinced that focusing on finding flaws in arbitrary systems had much to do with real-world network security.

"The Kenshoto game is not invalid, it just focuses specifically on code auditing to the exclusion of all else," Cowan said. "If Kenshoto's game of this year persists, then ... anyone else with any significant interest in defense (will not participate), and the game will be entirely dominated by code analysis players."

[Privacy Statement](#)

Copyright 2005, SecurityFocus