http://www.sei.cmu.edu/newsitems/CERT-Team-Uses-XNET.cfm

CERT Uses XNET to Deliver Forensics Challenge

May 31, 2011—An international aid organization website suffers a cyber attack. The host nation's information assurance team quickly determines the attackers stole critical information from a database on the server. They also planted malware to enable them easy access in future attacks. Later, the team learns a taskforce in the field has captured a computer believed to have been part of the attack. From the suite of analysis tools available in the **CERT® Forensic Appliance**, the team employs **LiveView** to create a bootable image of the captured computer and begins forensic analysis. But the team soon encounters a roadblock: All the computer's files are rendered in a foreign language. How can the team deconstruct the attack?

This scenario—the CERT Forensics Challenge—was designed by CERT for the 2011 National Security Agency (NSA) Cyber Defense Exercise (CDX). CERT has played a key role in this competition since its inception in 2001. The CDX pits teams of information assurance students from the nation's service academies against cyber security experts from the NSA. Each student team designs and implements a test network on its campus and, during the four-day exercise, works to defend it against cyber attacks from the NSA. Judges score the teams on their ability to successfully defend their networks and information.

To make the CERT Forensics Challenge both difficult and authentic, CERT tapped its expertise in the field of computer forensics and its long experience supporting DoD activities. It also employed its sophisticated Exercise Network (XNET) environment. CERT created **XNET** to provide real-world readiness testing through synchronous, team-based, scenario-driven cyber exercises. In other words, it's a platform ideally suited for the CDX.

Brian Wisniewski knows the CDX well. As Mission Support Team chief for the Army Reserve Information Operations Command, he led detachments supporting the NSA in several previous CDX events. Wisniewski, who in civilian life is also a member of the CERT Cyber Exercise team, found himself perfectly placed to introduce the CERT Forensics Challenge to CDX 2011. "This was a great opportunity to work with NSA to build a scenario that fits their CDX directive and scoring model," noted Wisniewski. "Overall, the Forensics Challenge was very well received. More than one institution mentioned that it was positioned at just the right level."

Wisniewski credits the success of the Forensics Challenge to the dedication and creativity of his fellow team members. For instance, Brent Kennedy developed a multiple-enclave technology map for the challenge. This tool allowed CDX observers to drill down through a graphical representation during the exercise, providing them a view into the activities of the attacking and defending teams. According to Wisniewski, the CDX observers found this tool useful because it showed them in real time how team members were applying classroom knowledge to problem solving.

Other CERT contributors included Matt Kaar, who created the foreign-language sleight of hand intended to distract the teams from their standard analytical and problem-solving processes. Jeff Mattson and Leena Arora helped Wisniewski create the challenge scenario and provided on-site support. “The challenge gave us an excellent opportunity to highlight the capabilities of the entire CERT Workforce Development team,” said Wisniewski. It also provided the service academy teams with experience with CERT-developed tools, such as those available in the **CERT Forensics Tools Repository** and **LiveView**.

Major T.J. O’Connor, director of the U.S. Military Academy’s (West Point’s) Digital Forensic and Computer Exploitation Courses, sees great value in the CERT Forensics Challenge. “The CDX challenge created by Brian’s team was outstanding and helped reinforce what the cadets had learned in the classroom,” said O’Connor. “What impressed me the most was the realism of the challenge. Having previously served overseas, I can honestly state Brian’s team replicated the environment rather well.” O’Connor specifically cited the way in which the CERT XNET environment incorporated real-world places, databases, unit identifiers, and other details the cadets will likely encounter in their future roles.

“To master the challenge,” noted O’Conner, “the cadets had to have a full understanding of network forensics, file system forensics, analysis of metadata, and information-hiding techniques. The breadth of the skills necessary to master the challenge was impressive. Having participated in three previous Cyber Defense Exercises, I can say without a doubt that this was the most realistic challenge the cadets have experienced to date.”

To the winner go the bragging rights, and this year O’Connor’s team took the title. The CDX, however, is more than a competition—it’s an exercise designed to prepare future leaders in cyber defense in a realistic, live-fire environment. The CERT Cyber Exercise Team developed the Forensics Challenge with this in mind, and learned much in the process. It will use the lessons it learned from CDX 2011 to enhance XNET with new, authentic training scenarios.

To learn more about XNET, visit **http://xnet.cert.org/**.

To learn more about computer forensics at CERT, visit **http://www.cert.org/forensics/**.