

Cyber War!

It started out like any other class with lecture and questions and the Set-Up.

However, this class was special! This was the final day of Kevin McLaughlin's Information Security and Privacy course at the CEAS - Applied Science and time to put all the lessons into practice. Following a presentation on company and organization security, ways to disrupt that security, and questions, Quinn Shamblin, UCit Information Security Officer, described the companies that had been established and their network.



Quinn Shamblin(far right), prepares his defending team

He then declared the companies open for business and half the class was challenged to "break in" and take all three of the preset targets. Each target represented critical data that if stolen would harm the organization loss of all three would be catastrophic.

12:00 PM But first, it was time for lunch and strategy planning by both the attackers and the company defenders.



Brian Rappach Attacking to find every possible way to break in..

Bill Weed, Applied Science Information Technology Analyst, had spent much of the prior day transforming a computer classroom into a cyber battlefield. The room was partitioned into two areas screened from each other with computer systems divided yet all connected into a common network like the Internet. Two companies were established one the main company and the second a smaller subsidiary.

In point-of-fact, the subsidiary was a "honey pot" - an industry term for a computer designed to lure hackers so that their activities may be recorded and their identity unmasked. The main organization sat behind sophisticated firewalls on its own sub-network which had additional network protections.

Attackers would be challenged here!

Did all of the defenders leave for lunch? Was there an opportunity to use a USB "switchblade" on them and ensure victory before the defenders finished eating?

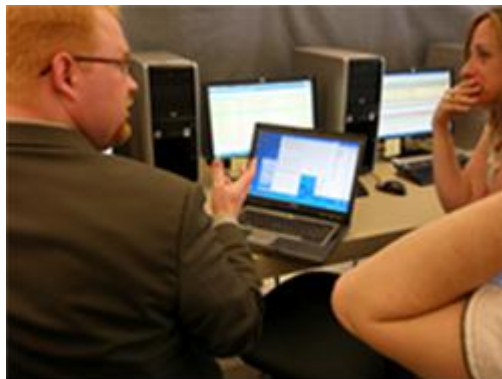
One very effective way to gain data from a system without anyone knowing is to break into a facility, plug in a flash drive with special software called Switchblade, copy what you want, and then leave. "You must have physical security before system and network security have value," stated Quinn Shamblin. "If I have physical access to your computer, I own your computer."

1:00 PM The defenders left one of their team with the room to provide security - the targets are secure.

The defenders were armed with monitoring software, their firewalls, and ghost files (files placed in the storage systems to mimic real files) and these students needed all of their tools as the attackers began their assault. It was stealthy at first as the company was identified and the defenses probed.



Bill Weed into Action...



All set for the Cyber War

Then a way in was discovered and the attackers under the guidance of "White Hat" hackers, Tim Wright, lltimwright@woh.rr.com, and Brian Rappach, US Dept. of Veterans Affairs, turned loose "Wire Shark", network monitoring software, and moved to acquire the three targets. Overwhelming the defenders was done quickly.

1:25PM "We own your company. We have the targets. Are you ready to quit?" rang out across the room. "Wait. We'll verify the signatures on targets to be sure you have the right ones!" came back...

Remember the "honey pot" and the ghost files? The attackers got the one valid target left in the subsidiary and two ghost files. The cost, however, was severe. The attackers were identified. Their IP addresses were captured and in an actual company defense these would be on the way to the FBI.

"The attackers got the "easy prey" and our students were able to go to school on their moves. These folks really know their business and our students are fortunate to be able to work with professionals like Tim and Brian," stated Shamblin. "A real attack would take place over a much longer time frame. The probes would be near impossible to detect and the initial moves into our system might not have shown but these situations familiarize the students with the tools and the thinking behind a hacking effort."



They have the IPs

1:30 PM "Here's the location of the main system. Can you get the other two targets?"

The attack resumed on the main company.

2:00 PM Attack over... Today the firewalls held and the main systems remained secure.

Exercises like the Cyber War of 2009 are standard training exercises for agents of the FBI, NSA, law enforcement around the country as well as private security firms. Computer systems come under attack several thousand times a day and exercises like this help agents react more quickly and effectively to threats.

This day's winners came from both sides of the partition. One student commented that he now really understood what it takes to protect a system - and he was one of the attackers!

Related Links

[IT opportunities at Applied Science](#)

[Security Updates from UCIT](#)

[Bit by Byte - Cyber War 2008](#)