Penetration testing seminar held at CETES

By James Meeks
A&E Editor

The vast world of the Internet grows every day and, as technology progresses, the danger of personal information being stolen increases. Businesses find ways to keep not only their information but also client information safe from hackers to exploit.

To keep information safe, businesses must employ the help of IT auditors to test the security of their systems. These tests, known as "Penetration Testing," help businesses find new ways to keep information safer.

Gregory Steen, a Cameron University graduate and current student at the University of Tulsa, gave a presentation over the Business of Penetration Testing, explaining the basics of conducting a test and legal issues an auditor faces while performing these tests.

According to Steen, penetration testing is a type of audit that a business can strike an agreement on with their client. The test simulates a malicious attack and provides insight into a system's security flaws.

"It provides feedback to businesses as to what their security posture is like and it enumerates weaknesses and gives countermeasures," Steen said. "You can give them countermeasures and suggestions once you are through with your audit."

Steen explained how to start a negotiation with potential clients, as well as looking into what needs to be covered before starting the test itself. "Penetration testing is an agreed form of an audit between two parties," Steen said. "You want to get this in writing and be legal for what you're doing — you don't want to get in trouble with the law or any type of legal issue because you decided to do something you weren't supposed to do."

According to Steen, he uses multiple programs in the course of his job that help crack passwords thus making systems recognize him as an authorized user. Medusa and Hydra are two of the password cracking systems Steen uses as an auditor.

According to Steen, IT auditors must test the systems to find all of the holes in the network security because if the IT technicians test their own work, they may overlook holes that are exposed.

During his work as an IT auditor in Tulsa, Steen said, he was given a "get out of jail free card." This card allowed Steen to go around the City of Tulsa, testing out different computer systems without getting in trouble with the law.

Steen explained that after a test, a post-audit report must be written and delivered to the client.

"The client is going to want you to give them feedback, you can't go into a penetration test and step at the end without giving them feedback," he said. "They have to know what you looked at and what they can do to fix it."

Steen suggested the use of encryption files for users that use storage from cloud technology. "I use an encryption file on the cloud-based storage that only I know the password to, so if it were to get attacked and they get the information out of there, they're going to have an encrypted file that's going to be useless," he said.

According to Steen, there are encryption tools out there that normal users can download for free to protect their files.

"Anything that may have a Social Security Number on it that could represent them electronically, they need to keep that in an electronic vault encrypted and stored; even in their own computers and laptops, because those are the type of things thieves want to get at physically and digitally," Steen said.