LATEST NEWS » Thursday, 21:37 EDT

- Facebook rolls out mobile privacy
- Firefox 4.0 beta download scam on Twitter
- Fighting illegal content on the Internet
- How can I know if my computer is infected? 10 signs of infection
- ZeuS variants hide behind snatched certificates
- Remote monitoring tool for social networking activity
- Top 5 undiscovered vulnerabilities found on enterprise networks
- Phishers target mobile phone users
- Win a copy of "Nmap Network Scanning" or "Hacking Exposed: Windows Forensics"
- IP-based control over enterprise networks
- ISSE 2010
- iPhone jailbreaking technique paves way for attacks

Big firms fail the test as social engineers demonstrate their abilities at Defcon

Posted on 02 August 2010.

The social engineering capture-the-flag-style contest planned for the second and third day of this year's edition of Defcon was executed without a hitch. No financial information, personal data, passwords or other sensitive information was asked for or received, no government or any other agency's feathers were ruffled, and the set goal of showing just how much information can be collected using social engineering tactics has been reached.

All ten targeted companies (Google, Microsoft, Apple, Cisco, BP, Shell, Ford, PG&E, Coke, and Pepsi) "failed" the test. "Not one company shut us down, although certain employees within the company did. But we (participants) were able to call right back and get another employee that was more willing to comply," says Christopher Hadnagy, developer and community member of Social-Engineer.org (the organization that made the contest happen) and operations manager with Offensive Security, a penetration testing company that also offers training in that department.

ZDNet reports that Social-Engineer.org plans to release a report in a couple of weeks, in which results and details of the specific attacks will be revealed. But, in the meantime, they refuse to reveal which companies fared worse than others in the contest.

They do say that out of some 50 employees approached via phone by the contestants, only 3 became suspicious and terminated the call without divulging any information, and - interestingly enough - all three were women.

"One woman said 'this question sounds fishy to me' and hung up within the first 20 seconds," recounts Hadnagy. "We all clapped."

Among those who failed to recognize the calls for what they are, there were those who even shared software version numbers with the attackers when prompted - a fact that would allow criminals to tailor further attacks in such a way as to exploit known and unknown vulnerabilities in the software.

The final report is eagerly awaited not only by the security community and forward-thinking businesses that recognize the danger that such attacks present to their functioning, but by law enforcement and U.S. federal agencies as well.

Author: Zeljka Zorz, HNS News Editor.

More recent news

- Facebook rolls out mobile privacy
- Fighting illegal content on the Internet
- Remote monitoring tool for social networking activity
- Top 5 undiscovered vulnerabilities found on enterprise networks
- Phishers target mobile phone users