Penetrate Testing

C. Edward Chow

Outline of The Talk

- Definition, Concepts on Penetration Testing/Hacking
- Anatomy of a Hack
- Framework for penetration studies
- Skills and Requirements of a Penetration Tester
- SAN list of Security Holes
- Internet Penetration
- Dial up Penetration
- Internal Penetration
- References:
  - CORE IMPACT - Penetration Testing: Assessing Your Overall Security Before Attackers Do
  - Pages 165,277 Security in Computing.
  - Hack I.T, Security Through Penetration Testing, by T.J. Klevinksy, Scott Laliberte, Ajay Gupta.
  - http://www.hackingexposed.com/win2k/links.html

Definition

- Vulnerability (Security Flaw): specific failure of the system to guard against unauthorized access or actions. It can be procedures, technology (SW or HW), or management.
- Using the failure of the system to violate the site security policy is called *exploiting the vulnerability*
- Penetration Study is a test for evaluating the strengths of all security controls on the computer system. It intends to find all possible security holes and provides suggestions for fixing them.
- Penetration Testing is an authorized attempt to violate specific constraints stated in the form of a security or integrity policy.
- Penetration Testing is a testing technique for discovering, understanding, and documenting all the security holes that can be found in a system.
- It is not a proof techniques. It can never prove the absence of security flaws. It can only prove their presence.
- Example goals of penetration studies are gaining of read or write access to specific objects, files, or accounts; gaining of specific privileges; and disruption or denial of the availability of objects.
- What is the difference between penetration testing and hacking/intrusion?