Penetration Testing: What, Why and How

Presented by: Aaron Oh

Date: July, 2007

Electrosoft

What is Penetration Testing? (Definition)

- **Widipedia Definition:** A penetration test is a method of evaluating the security of a computer system or network by simulating an attack by a malicious user, commonly known as a hacker.
- **NIST-SP 800-42 (Guideline on Network Security Testing) Definition:** Penetration testing is security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation.
- **My definition (simpler):** simulating malicious activities by a hacker to assess security posture of an organization

Why perform Penetration Testing? (Primary Objectives)

- The assessment of real security threats to business systems
- Relating the impact of technical vulnerabilities to business risks
- Ensuring timely and sufficient security solutions through risk-based security assessment

Why perform Penetration Testing? (Sales Points)

- Regulatory Risk (Sarbanes and Oxley, Independent Financial Audit, GLBA, HIPAA, etc.)
- Loss of Reputation
- Third-Party Reliability

How do you perform Penetration Testing? (General Methodologies)

- Comprehensive Pen-test Includes Two Scenarios:
  - External Penetration Testing
    - Internet Network Testing
    - Dial-up Testing
    - Social Engineering
    - Wireless Testing
  - Internal Penetration Testing
    - Network Testing
    - Social Engineering

How do you perform Penetration Testing? (General Methodologies)

General Technical Methodology

- Footprinting
  - Arin.net, Google
- Scanning
  - Nmap, Netbios Scanners (NTIS, NBTEnum), Nikto, Wikto
- Exploitation
  - Manual Testing, Non-impact Tools, Risk Management
- Comprehensive Vulnerability Scanning
  - Nessus, Axent NetRecon, eEye Retina, ISS Scanner, CyberCop)
- Risk and Impact Evaluation