Ethical Hacking: A Security Supervisor's Perspective

- **Agenda**
  - Welcome and overview of "Ethical Hacking"
    - Wayne Boone
  - Introduction and comments by three Ethical Hacking Practitioners
    - Salim Douba, Cygnos IT Security
    - Eric Jacksch, MTS Allstream
    - Patrick Naubert, Tygerteam
  - Networking Break
  - Introduction and comments by three Security Supervisors
    - Jacques Adams-Robenheimer, PWGSC
    - Paul Beauchamp, Office of the Privacy Commissioner
    - Marie-Helene Langevin, Industry Canada
  - Moderated panel
    - Q&A

Classic Definitions

- **HACKER noun 1. A person who enjoys learning the details of computer systems and how to stretch their capabilities—as opposed to most users of computers, who prefer to learn only the minimum amount necessary. 2. One who programs enthusiastically or who enjoys programming rather than just theorizing about programming.**
- **Hacking**
  - the rapid crafting of a new program or the making of changes to existing, usually complicated software
    - *E. S. Raymond, The New Hacker's Dictionary, MIT Press, Cambridge, MA (1991)*

Evolving Definitions

- **Hacker (AKA Cracker)**
  - Someone who bypasses the system's access controls by taking advantage of security weaknesses left in the system by developers
    - *Hansche et. al., Official (ISC)^2 Guide to the CISSP Exam*
  - Person who is totally immersed in computer technology and programming, and who likes to examine the code of programs to see how they work … then uses his or her computer expertise for illicit purposes such as gaining access to computer systems without permission and tampering with programs and data. At that point, this individual would steal information and install backdoors, virii and Trojans
    - *J. Chirillo, Hack Attacks Revealed*

Some Definitions contd

- **Script Kiddies**
  - Person, normally … not technologically sophisticated, who randomly seeks out a specific weakness over the internet to gain root access to a system without really understanding what he is exploiting because the weakness was discovered by someone else. A script kiddie … uses knowledge of a vulnerability to scan the entire internet for a victim
    - *Webopedia*
  - [Those] with few true skills … who lack the ability to devise their own attacks, download and … run other people's programs, or scripts, to launch an attack.
    - *Tittel et. al., CISSP Study Guide*

Some Definitions contd

- **Phreak**
  - Person who breaks into … telecommunications systems to [commit] theft
    - *J. Chirillo, Hack Attacks Revealed*
- **Cyber punk**
  - Recent mutation of … the hacker, cracker, and phreak
    - *J. Chirillo, Hack Attacks Revealed*

Types of Hackers

- **Communal Hacker**
  - "graffiti artist"
    - Need to control, gain acceptance
- **Technological Hacker**
  - "Forces" advancements
- **Political Hacker (AKA Hacktivist)**
  - Has a message
- **Economical (sic) Hacker**
  - Personal economic gain
- **Governmental Hacker**
  - Common terrorist
    - *J. Chirillo, Hack Attacks Revealed*

The "Ethical Hacker"

- **Someone who is**
  - Skilled
    - Programming and networking skills
    - Installation and maintenance skills
    - System management skills
  - Knowledgeable
    - Hardware and software
  - Completely trustworthy
  - Discrete
  - Patient, persistent and methodical
  - "Certified"
    - Certified Ethical Hacker

ANATOMY OF A HACK

Anatomy of a Hack - Methodology

- Footprinting
- Scanning
- Enumeration
- Gaining Access
- Escalating privilege
- Pilfering
- Covering tracks
- Creating back doors
- Denial of service

Anatomy of a Hack Methodologies - Footprinting

- **Objective**
  - Target Address range, namespace, acquisition and information gathering are essential to a surgical attack.
- **Techniques**
  - Open source search
  - Whois
  - Web interface to whois
  - ARIN whois
  - DNS zone transfer

Anatomy of a Hack Methodologies - Scanning

- **Objective**
  - Bulk target assessment and identification of listing services focuses the attacker's attention on the most promising avenues of entry
- **Techniques**
  - Ping sweep
  - TCP/UDP port scan
  - OS Detection

Anatomy of a Hack Methodologies - Enumeration

- **Objective**
  - More intrusive probing now begins as attackers begin identifying valid user accounts or poorly protected resource shares
- **Techniques**
  - List user accounts
  - List file shares
  - Identify applications

Anatomy of a Hack Methodologies – Gaining Access

- **Objective**
  - Enough data has been gathered at this point to make an informed attempt to access the target
- **Techniques**
  - Password eavesdropping
  - File share brute forcing
  - Password file grab
  - Buffer overflows

Anatomy of a Hack Methodologies Escalating Privileges

- **Objective**
  - If only user-level access was obtained in the last step, the attacker will now seek to gain complete control of the system
- **Techniques**
  - Password cracking
  - Known exploits

Anatomy of a Hack Methodologies Pilfering

- **Objective**
  - The information gathering process begins again to identify mechanisms to gain access to trusted systems
- **Techniques**
  - Elevate trusts
  - Search for clearnet passwords

Anatomy of a Hack Methodologies Covering Tracks

- **Objective**
  - Once total ownership of the target is secured, hiding this fact from system administrators becomes paramount, lest they quickly end the romp
- **Techniques**
  - Clear logs
  - Hide tools

Anatomy of a Hack Methodologies Creating Back Doors

- **Objective**
  - Trap doors will be laid in various parts of the system to ensure that privileged access is easily regained at the whim of the intruder
- **Techniques**
  - Create rogue user accounts
  - Schedule batch jobs
  - Infect startup files
  - Plant remote control services
  - Install monitoring mechanisms
  - Replace apps with trojans

Anatomy of a Hack Methodologies Denial of Service

- **Objective**
  - If an attacker is unsuccessful in gaining access, they may use readily available exploit code to disable a target as a last resort
- **Techniques**
  - SYN flood
  - ICMP techniques
  - Identical SYN requests
  - Overlapping fragment/offset bugs
  - Out of bounds TCP options (OOB)
  - DDoS

Comments by Ethical Hacking Professionals

- **A bit about you and your company**
- **Other terms for what you do, and how do you distinguish them from "ethical hacking"?**
  - Penetration testing
  - Red team testing
  - Security Posture Assessments
  - Technical Vulnerability Assessments
- **What methodologies or methods do you use, both technical and non-technical (social engineering)?**
- **Which steps of the anatomy of a hack do you use?**
- **What are the typical outputs or deliverables of your work?**
- **What would be typical follow-on actions by the client upon receipt of your deliverables?**
- **What is the "value added" that you bring to the client?**

Comments by Security Practitioners

- A bit about you and your organization
- How relevant is ethical hacking to your overall security program?
- What would be typical follow-on actions that you would take upon receipt of ethical hacking deliverables?
- What are your preferences as to in-house versus third party services?
- How do you address the fear of allowing a third party ethical hacker into your systems, ie., how do you balance value of the skill sets that they bring versus the trust that you must put into them?

Coffee Break

Panel Questions

- Any additional comments on the attributes of an ethical hacker?
- Do ethical hackers require a strong security background? Are they security specialists *per se?*
- What kind of a mindset should be adopted when conducting an ethical hack?
- How important are professional certifications in this specialty?
- It has been suggested that it is preferable to conduct ethical hacking "in-house" since it has the potential to expose critical vulnerabilities. How would you respond?

Panel Questions

- Do you think that ethical hacking is too dangerous to take place on live systems, since you are affecting live data, and potentially affecting the CIA of an accredited system. Why or why not?
- What is the potential and impact of ethical hackers "turning" and attempting extortion after the fact?

Conclusion and Wrap-up

International Council of Electronic Commerce Consultant (EC-Council)

- **Mission Statement**
  - Foster professional standards
  - Provide for communication among all E-commerce professionals, including corporate e-commerce consultants in government, business, and education, independent consultants, and aspiring e-commerce professionals such as students
  - Provide for education through the development of curriculum, publishing of articles and books, professional papers, and the sponsoring of seminars and conferences

International Council of Electronic Commerce Consultant (EC-Council)

- **Mission Statement (contd)**
  - Stimulate the continued growth of the E-commerce by providing a forum for the raising of new ideas and an effective mechanism for dialog on these issues
  - Provide security, legal and marketing white papers in E-commerce as well as an area on the latest trends in the Internet on each of those items
  - Provide accreditation for E-commerce certification and training programs