

# IT Auditing From the Hackers Perspective



Closing

Secure360

May 10, 2010

LarsonAllen<sup>®</sup>  
LLP

CPAs, Consultants & Advisors

# Review

## Internal Threats

- Identifying vulnerable internal systems
  - Host discovery
  - Vulnerability identification
  - Privilege escalation
  - Administrative completeness



# Review (cont.)

## External Threats

- Vulnerabilities in website applications
  - Code execution, SQL Injection, XSS
  - “Sanity Checking”
- Email “Spear” Phishing
  - Technical controls
  - User awareness

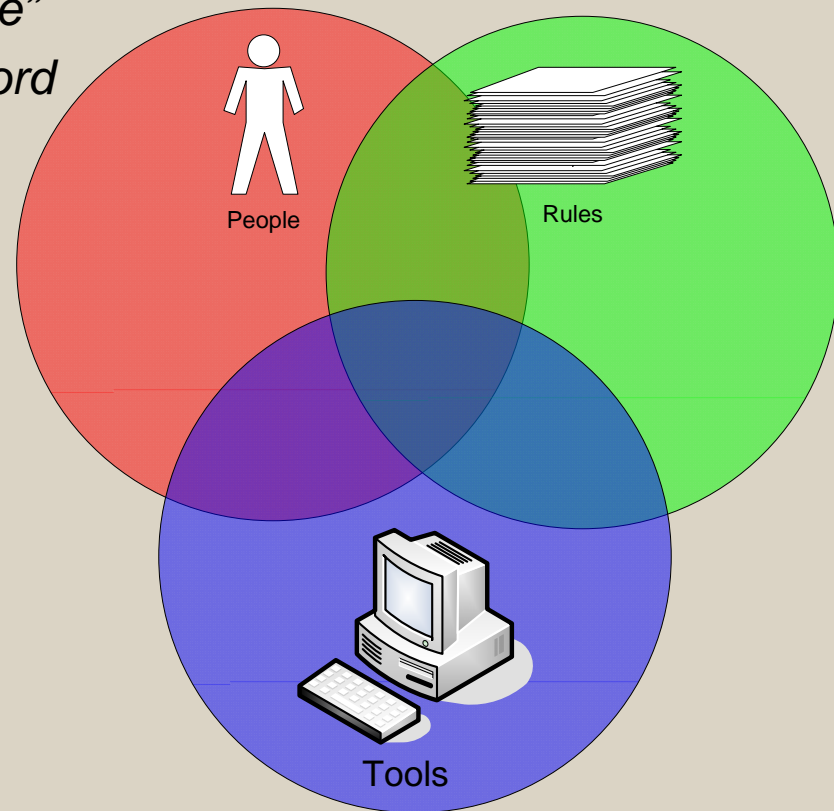


# Definition

“A secure system is one we can depend on to behave as we expect.”

Source: “*Web Security and Commerce*”  
by Simson Garfinkel with Gene Spafford

- Confidentiality
- Integrity
- Availability



# *Security = Culture!!*

Security is a **BUSINESS** issue, NOT a technical issue!!

- *Administrative Policies / Procedures*
- *Physical Access Controls*
- *Technical Security Controls*



# Thank You

**The presentations will be available here:**

<http://www.larsonallen.com/presentations.aspx?TaxId=160&sort=descending>

**Randy Romes, CISSP, MCP**

Principal, Information Security Services

612-397-3114

[rromes@larsonallen.com](mailto:rromes@larsonallen.com)



# Security Tools

- **Nmap**  
<http://nmap.org>
- **Nessus**  
<http://www.nessus.org/>
- **Metasploit**  
<http://www.metasploit.com/>
- **Cain & Abel**  
<http://www.oxid.it>
- **John the Ripper**  
<http://www.openwall.com/john/>
- **Fgdump**  
<http://www.foofus.net/fizzgig/fgdump/>



# Security Tools (cont.)

- **Wireshark**  
<http://www.wireshark.org>
- **dsniff**  
<http://www.monkey.org/~dongsong/dsniff>
- **Microsoft Baseline Security Analyzer (MBSA)**  
<http://technet.microsoft.com/en-us/security/cc184923.aspx>
- **Superscan**  
<http://www.foundstone.com/us/resources/proddesc/superscan.htm>
- **Scanline**  
<http://www.foundstone.com/us/resources/proddesc/scanline.htm>
- **Unicornscan**  
<http://www.unicornscan.org/>



# Security Tools (cont.)

- **Amap**  
<http://www.thc.org/thc-amap/>
- **Paketto**  
<http://www.doxpara.com/paketto>
- **Netcat**  
<http://netcat.sourceforge.net/>
- **NetBIOS Enumerator**  
<http://nbtenum.sourceforge.net>
- **Nikto**  
<http://www.cirt.net/nikto2>
- **Wikto**  
<http://www.sensepost.com/research/wikto/>



# Security Tools (cont.)

- **WinLHF & SqlLHF**  
<http://snap.lhftools.com/>
- **THC-Hydra**  
<http://www.thc.org/thc-hydra/>
- **Medusa**  
<http://www.foofus.net/jmk/medusa/medusa.html>
- **L0phtCrack**  
<http://www.l0phtcrack.com>
- **DumpSec**  
<http://www.somarsoft.com>
- **LanSpy**  
<http://lantricks.com/lanspy>



# References and Links

- **Port list**  
<http://www.iana.org>
- **List of publicly disclosed compromises**  
<http://www.privacyrights.org/ar/ChronDataBreaches.htm>
- **Good security news site**  
<http://www.securityfocus.com>
- **Default Password Lists**  
<http://www.phenoelit-us.org/dpl/dpl.html>



# References and Links (contd.)

- **Email Phishing Resources**

<http://www.antiphishing.org>

<http://www.millersmiles.co.uk/>

- **Center for Internet Security**

<http://www.cisecurity.com>

- **ISACA**

<http://www.isaca.org/mn>

- **CANAUDIT**

<http://www.canaudit.com>

