Student Tech Security Training

ITS Security Office

ITS Security Office

- "Total Security is an illusion – security will always be slightly broken."
- Find strategies for living with it.
- Monitor our Network with IDS
- Incident Response
- Work with Network Security Contacts
- Education
- System Security Assessment
- Policy Compliance
  - Copyright Violations

Network Citizenship Policy

- Intended to protect campus network.
- At UI persons owning or overseeing network connected systems are responsible for securing them.
- Servers, laptops, handhelds, lab equipment, etc.
- Systems posing a threat to campus network will be removed.

Who are the Customers

- Faculty viewpoint
  - Loss of Control
  - Loss of Privacy
  - Transparency
- Unforgettable experiences
- Be a resource
  - Share experiences
  - Lend advice

Baseline Security Standards

- Software Updates
  - Automatic updates
- Anti-virus
  - UI site license
  - Update virus signatures
- Strong Administrator Passwords
- Support Contacts
- Best Practices
  - http://cio.uiowa.edu/ITsecurity/bestprac/

Legal Responsibilities

- **Confidential Data**
  - **HR Data**
  - **University records**
- **Legally Protected Data**
  - **HIPAA - Health Insurance Portability and Accountability Act**
  - **FERPA – Family Educational Rights and Privacy Act**
  - **Graham Leach Bliley**

What's an Incident

- Incidents
  - System Intrusion
    - Web defacement
  - Intrusion Attempts
  - Malicious Scanning
  - Viruses – Malware
  - Others?
- When to Report?
- How to Report?

Incident Response

Where do threats come from?

- Unmanaged machines
- Automated programs or scripts
  - Script kiddies

Types of Threats

- **Malware**
  - **Viruses**
  - **Worms**
  - **Bot Networks**
  - **Trojans**
  - **Key-stroke loggers**
  - **RootKits - Hacker Defender**
- **Software Vulnerabilities**
  - **Privilege Elevation**
  - **Bugs / Glitches / Fuzzing**
  - **Full Disclosure vs. Obscurity**

Types of Threats

- **Social Engineering**
  - **Phishing**
    - **Tricking people to run applications, open e-mail attachments or navigate to websites**
    - **Cross Site Scripting – Trojan website**
- **Identity Theft**
  - **Credential Theft / Impersonation**
  - **Financial Theft**

Report & Prevent

- **Report Phishing**
  - http://www.antiphishing.org/phishing_archive.html
- **Information about Identity Theft**
  - http://www.consumer.gov/idtheft/index.html

Spyware

- Spyware
  - How do you get Spyware
    - By downloading “Attractive” applications, utilities and games
    - Utilities like Weatherbug
    - P2P file sharing
  - Obscure EULAs
  - Captures data from your computer
  - Monitors your actions on the Internet
  - Installs programs without your consent
  - Places “Intelligent” Ads

You might have spyware if:

- You notice new toolbars, links, or favorites that you did not want or place in your Web browser.
- Your default home page, mouse pointer, or search program changes.
- You type the address for a specific Web site, but are taken to another Web site without notice.
- You see a lot of pop-up ads, even if you're not on the Internet.
- Your computer suddenly performs slowly or seems unstable.

Hacking Google

- Use search engines to find vulnerabilities
- http://johnny.ihackstuff.com
- usernames
  - filetype:log username putty
- Management Consoles
  - inurl:rpSys.html
- And Many more

What's our exposure

- Fast Internet connection
- Thousands of fast computers
- University Values
  - Unrestricted Internet access
  - Individual / Academic Freedom
  - Distributed management
  - Unmanaged computers
  - Broad Acceptable Use Policy
- Can we block threats?
- Do we block threats?

Countermeasures & Best Practices

- **Educated Computer Users**
  - **Understand relevant technology**
  - **Understand the threats**
  - **Timely response to problems**

Countermeasures & Best Practices

- Careful Computer Management
  - Automate OS + Application Patching
  - Update Anti-virus signatures
  - Regular reliable backups
  - Strong Passwords
  - Principle of Least Privilege
    - UAC – User Account Control
    - Access Control Lists
  - Security Auditing
    - MBSA – MS Baseline Analyzer
  - Securely Store and Erase Confidential Data

Countermeasures & Best Practices

- Careful Computer Management
  - Physical Security
- MS Threats and Countermeasures guide
  - http://www.microsoft.com/windowsxp/using/helpandsupport/getstarted/ballew_03may19.mspx
    - System services
    - Software restrictions
- XP Security Guide
  - http://www.microsoft.com/technet/security/prodtech/windowsxp/secwinxp/default.mspx

Countermeasures & Best Practices

- Security Tools
  - Host Based Firewall
    - Windows Firewall
    - Symantec Client Security
    - IPSEC Rules
  - Anti-virus
    - Symantec Corporate Edition
  - Anti-spyware
    - Windows Defender
    - Symantec Anti-virus
  - Security Configuration
    - MS Security Templates

Log Monitoring

- How do you know when your being attacked?
- How do you know you've been attacked
  - Security Event Log
  - http://www.ultimatewindowssecurity.com/encyclopedia.html

Windows Defender

- http://www.microsoft.com/athome/security/spyware/software/default.mspx
- Real-time defense
- Few false positives
- Automatic updates

MS 10 ways to work more securely

- http://www.microsoft.com/AtWork/getstarted/worksecure.mspx

Protect Your Computer!

- **http://helpdesk.its.uiowa.edu/security**

Security Vs. Convenience

MBSA Hands - on

- **Identifies Common Vulnerabilities**
  - **Weak or unmannaged policies and configurations**
  - **Missing OS security updates**
  - **User accounts …**

Disaster Recovery

- “Backups, Like care insurance, you don’t need it until you need it.”
- “But if you need it, you’d better have it!”
- Types of Backup
  - Network Drives
  - External Media
    - Tape Drive
    - CD / DVD
    - USB

NT Backup

- **System State**

System Restore

- Restore points
- System Checkpoints

What should I backup?

Does the restore work?

- “Yes, I’m in charge of backups”
- “I said backups, I don’t know who’s in charge of restores”
- Test your restore methods
- Does your backup contain everything needed?

Keeping up to date

- Secunia
- Securityfocus
- CVE
- Slashdot
- RSS
  - Feedreader
  - OMPL

Windows Live One Care

- http://www.windowsonecare.com/
- OneCare
  - Antivirus
  - Antispyware
  - Firewall
  - Performance Tune-ups
  - Data Backup
    - And Restore
- Norton 360

Windows Live Safety Center – Beta

- Safety Center
  - Web Scanner
  - http://safety.live.com/site/en-US/center/howsafe.htm