



THE UNIVERSITY OF IOWA

Computer Security Handbook

November, 2001

Published by

CIO Office, Information Technology Services
300 University Services Building
e-mail: it-security@uiowa.edu
URL: <http://www.its.uiowa.edu/cio/itsecurity/>
Phone: (319)-335-6332

Version 1.1, November 26, 2001

Version 1.1
November 26, 2001



Table of Contents

SANS “Top 20” Security Vulnerabilities list	3
Security Guidelines for End Users	4
Security Guidelines for Workstations	5
Microsoft Server Guidelines	6
Unix Server Guidelines	7
Macintosh-Specific Security Issues	8
Security Incident Response – Basic Procedures	9
Keep Informed: Subscribe to Security Mailing Lists	10
Web Resource Links	11

SANS “Top 20” Security Vulnerabilities list

General

- G1 - Default installs of operating systems and applications
- G2 - Accounts with No Passwords or Weak Passwords
- G3 - Non-existent or Incomplete Backups
- G4 - Large number of open communication ports
- G5 – Not filtering packets for correct incoming and outgoing addresses
- G6 - Non-existent or incomplete logging
- G7 - Vulnerable CGI Programs (Web Servers)

Specific to Windows

- W1 - Unicode Vulnerability (Web Server Folder Traversal) (IIS)
- W2 - ISAPI Extension Buffer Overflows (IIS)
- W3 - IIS RDS exploit (Microsoft Remote Data Services)
- W4 - NETBIOS - unprotected Windows networking shares
- W5 - Information leakage via null session (unauthenticated) connections
- W6 - Weak hashing in SAM (LM hash)

Specific to Unix

- U1 - Buffer Overflows in RPC Services
- U2 - Sendmail Vulnerabilities
- U3 - Bind Weaknesses
- U4 - R Commands (rlogin, rsh, rcp)
- U5 - LPD (remote print protocol daemon)
- U6 – sadmind and mountd
- U7 - Default SNMP Strings

For detailed descriptions and remedies, see the SANS Institute webpage at <http://www.sans.org/top20.htm>

Security Guidelines for End Users

Use Strong Passwords. Choose passwords that are difficult or impossible to guess, and use different passwords for your various accounts. Change passwords regularly.

Make Regular Backups of Critical Files. Backups of “My Documents” and other non-system files and databases on your workstation should be taken at least weekly, and stored on a secure file server, or on removable media.

Make use of Virus protection. Install it, and update the virus definitions at least weekly. Update the program monthly. Scan all files on a regular basis, and always scan all incoming files for viruses.

Do not leave computers logged on or unattended when not in use. Employ a password protected screen-saver program. Shut your machine down overnight.

Do not open unexpected e-mail attachments. Never open attachments from strangers, and do not open them from known sources unless you’re expecting to receive them.

Keep software up to date. Regularly download and install security updates and new releases for application programs, and install security patches for your operating system.

Be wary of sharing personal information. Be sure web sites have a security/privacy policy you agree with, and be sure they use a secure site. (Check for the “closed lock” or “key” in the information area of your browser window.) Never tell your password to *anyone*, not even to support or help desk staff.

Adapted from “Seven Simple Computer Security Tips for Small Business and Home Computer Users” - The National Infrastructure Protection Center, <http://www.nipc.gov/warnings/computertips.htm>

For virus information and downloads of anti-virus software, see the campus Virus Resource Center at <http://www.its.uiowa.edu/cs/helpdesk/virus/>

Security Guidelines for Workstations

- Update operating systems and application software frequently
- Require users to login to their workstation and employ screen-saver passwords
- Configure appropriate object, device, and file access controls (ie do not allow ‘everyone’ access to files)
- Use system logging mechanisms to track changes to critical files and to track logins
- Make frequent backups of critical files and databases (user files that are not on a standard system image)
- Install and configure anti-virus software. Configure it to update virus definitions weekly, and update the program monthly. Configure it to always scan incoming email files.
- Do not allow local modem access to workstations – use the University’s Remote Access Service
- Restrict/disable network services (ftp, telnet, and personal web servers) that are not required for operation – don’t start unnecessary services.
- Secure all file shares with passwords, and allow access only as required, to authorized users
- Employ a method for imaging workstations for quick recovery. Only include the necessary programs and services in the image. Always create a new image after software is updated/patched.

Also see

Best Practices for Workstation Protection

<http://www.its.uiowa.edu/cio/itsecurity/bestprac/bpworkst2.htm>

CERT’s Windows 95/98 Computer Security Information

http://www.cert.org/tech_tips/win-95-info.html

For virus information and downloads of anti-virus software, see the campus Virus Resource Center at <http://www.its.uiowa.edu/cs/helpdesk/virus/>

Microsoft Server Guidelines

- Install the latest service packs, and all new security-related hotfixes as they are released. If a service pack is re-applied, you must also reinstall all hotfixes that were applied afterwards.
- Use the Network Security Hotfix Checker program (Hfnetck.exe)
- Use the NTFS file system instead of FAT
- Place the system in a secure location (locked room, air conditioned, UPS, etc)
- Limit the information available through a null (anonymous) connection, which are the resources available to the everyone group
- Replace Everyone group with Authenticated Users group on the "access this computer from the network" user right
- Allow only Administrators and System to have remote access to the registry
- Disable the guest account, and ensure all accounts have passwords even if they're disabled
- Replace everyone group with authenticated users group on critical system folders, files, and registry keys
- Restrict permissions on network shares
- Remove unneeded services, and don't place RAS or Web service on a domain controller
- Enable auditing of logons, logoffs, failed access attempts, and system events
- Review trust relationships between domains
- Make regular backups of the system, and keep at least one copy off-site.

Adapted from "The 60 Minute Network Security Guide" - The National Security Agency, SNAC.Guides@nsa.gov

Also see

SANS Step by Step Security Documents: (available on campus)
<http://www.its.uiowa.edu/cio/itsecurity/resources/>

Microsoft Security Program
<http://www.microsoft.com/security/>

Unix Server Guidelines

- Patch your system often
- Allow access to system services only to authorized hosts and users
- Place the system in a secure location (locked room, air conditioned, UPS, etc)
- Use encryption where possible – ie replace telnet with ssh
- Deactivate network services which are not in use on the system (pop3, imapd, ftpd, finger, bind, named, httpd, nfs etc)
- Review file permissions using least access rule (allow write access only where needed)
- NFS – review file exports, do not export / or /bin or /etc, disable altogether if not needed
- Ensure strong authentication is used, and all default passwords are changed.
- Monitor your system by regularly reviewing syslog, open ports, and running processes. Review the network configuration and scheduled processes often.
- Make regular backups of the system, and keep at least one copy off-site.

Also see

CERT's Guidelines for Securing Unix:
http://www.cert.org/tech_tips/unix_configuration_guidelines.html

University of Iowa Linux Security Page:
<http://www.its.uiowa.edu/cio/itsecurity/bestprac/linux.htm>

SANS Step by Step Security Documents: (available on campus)
<http://www.its.uiowa.edu/cio/itsecurity/resources/>

Macintosh-Specific Security Issues

- Mac OS 9 users should install/use Virex (see <http://www.its.uiowa.edu/cs/helpdesk/virus>)
- Keep up to date with Microsoft Office patches to protect against macro viruses
- Turn off CD-Rom Autoplay (see QuickTime control panel)
- Keep program linking turned off unless needed (see File Sharing control panel)
- Update to Mac OS 9.2.1 to prevent compromise & use in DoS
- If Network Assistant is installed, be sure to change the default password
- Beware of password compromises in remote control applications (VNC, Timbuktu), and keep them patched
- Beware that Mac OS X's BSD subsystem & Unix services require standard Unix security measures!
- Turn off automatic BinHex decoding in preferences for Internet Explorer 5.1 on Mac OS X.
- Consider a GUI firewall configuration utility for Mac OS X, and commercial firewall software for Mac OS 9.
- Ensure physical machine security (Optical Drive, USB, & FireWire access can be used to boot & circumvent security)
- Place servers in a secure location (locked room, air conditioned, UPS, etc)
- Make regular backups, and for servers, keep at least one copy off site.

Also see

Apple Security Updates

http://www.apple.com/support/security/security_updates.html

Mac OS X Firewall software

http://personalpages.tds.net/~brian_hill/brickhouse.html

SANS Reading Room

http://www.sans.org/infosecFAQ/mac/mac_list.htm

Macintosh Security Site

<http://www.securemac.com>

Security Incident Response - Basic Procedures

Account Breach

- Note the current date/time and the date/time of when the account owner last logged in
- Take notes about what alerted you/them to the problem, make copies of log files that apply.
- Change the password
- Report it to IT Security: call 335-6332 or email to it-security@uiowa.edu
- Assess the situation: are there institutional confidentiality or exposure issues?

System Breach

- Take notes. You won't remember your observations and actions very clearly for long.
- If destructive activity is occurring, disconnect the machine from the network, but do not shut it down.
- Make removable copies of volatile files for evidence: system and/or application logs, process lists, password files, etc. Take an image copy of the whole drive if possible.
- Report it to IT Security: call 335-6332 or email it-security@uiowa.edu
- Perform a thorough assessment of the system
- Change account passwords
- Repair or reinstall, including all current maintenance, and restore data from a recent backup that you trust the integrity of.

Also see:

SANS Step by Step Computer Incident Handling (available on campus)

<http://www.its.uiowa.edu/cio/itsecurity/pubs/i.pdf>

Procedures for Handling a Computer System compromise:

<http://www.its.uiowa.edu/cio/itsecurity/incident/incident.htm>

Responding to Intrusions

<http://www.cert.org/security-improvement/modules/m06.html>

Keep Informed:

Subscribe to Security Mailing Lists

Lists hosted at the University of Iowa

List Function:	Send message to:	Include in body of the message:
Campus Security Alerts	nsc-all-request@list.uiowa.edu	subscribe nsc-all
Helpdesk Announcements	helpdesk-announce-request@list.uiowa.edu	subscribe helpdesk-announce
Networking Information/Alerts	uiowa-netfolks-request@list.uiowa.edu	subscribe uiowa-netfolks

National/Global Mailing Lists

List Function:	Send message to:	Include in body of the message:
CERT Advisories	majordomo@cert.org	subscribe cert-advisory
CIAC	ciac-listproc@llnl.gov	subscribe ciac-bulletin
UNISOG	unisog-request@sans.org	subscribe unisog
ISS Alerts	majordomo@iss.net	subscribe alert
BugTraq (detailed Unix):	LISTSERV@NETSPACE.ORG	SUBSCRIBE BUGTRAQ
NTBugtraq (Windows):	listserv@listserv.ntbugtraq.com	subscribe ntbugtraq

Web Resource Links

University of Iowa IT Security Site

<http://www.its.uiowa.edu/cio/itsecurity/>

- Licensed security publications
- Campus Security Alerts
- Security Scanning Service
- Best Practices Documents

COAST Lab “Hotlist”

<http://www.cerias.purdue.edu/coast/hotlist/>

- Publications, papers, lists, organizations... (huge)

CERT Coordination Center

<http://www.cert.org/>

- Report Security Incidents (National)
- Technical Tips

SANS Institute

<http://www.sans.org/>

- Security Reading Room
- Internet Storm Center

Macintosh Security Site

<http://www.securemac.com/>

Microsoft Security Toolkits

<http://www.microsoft.com/security/>

Known Operating System Vulnerabilities

<http://xforce.iss.net>

University licensed full-text online computer books

<http://www.lib.uiowa.edu/eng/books.htm>