2008

Ron Woerner, CISSP, CEH

22 August 2008

NEbraska CERT Conference 2008

Computer Security and Information Assurance


Many security resources are readily available for **free**

Guidelines

- This is my interpretation and summary and not necessarily the opinion of my employer.
- Not a debate on open source versus commercial software.
- Please feel free to ask questions, make comments at any time.
- This is not a complete list. Help add to it.
- I am not responsible for the content of the links or for how you use these resources.


It’s not what you buy,
but what you do.

It's What You Do

Identify, assess, and manage risks

Establish policies and procedures

Change all default user ids and passwords

Ensure proper access control

Harden servers

Train administrators, managers and users

Why Free?

- For the good of all;
  - Government
  - Open source
- Guilt;
- Marketing;
- Try it; you'll like it.

freebeer.org

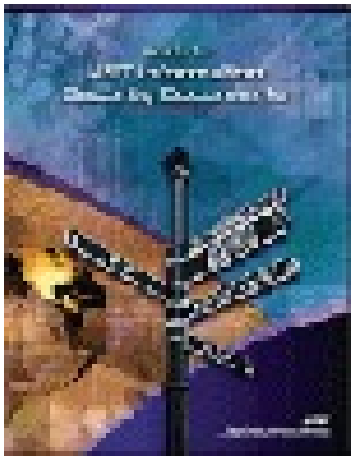
Free Information#

- Federal Government
- Security Organizations
- Vendors

Articles, Checklists, Books, White Papers, Presentations, etc.

U.S. Government

- Department of Homeland Security (http://www.ready.gov)
- NIST CSRC (http://csrc.nist.gov/)
  - Publications
    - Special publications (800 Series)
    - ITL Bulletins
  - Guide



U.S. Government

- DHS National Cyber Security Division
  - Build Security In

    (https://buildsecurityin.us-cert.gov/portal/)

U.S. Government

- National Security Agency (NSA)
  - Security Configuration Guides (http://www.nsa.gov/snac/)
    - Microsoft Vista
    - Oracle Application Server
    - Cisco Router
  - Security-enhanced Linux

U.S. Government

- U.S. Dept of Energy – Computer Incider Advisory Capability (CIAC) (http://www.ciac.org/ciac/)
  - Bulletins
  - Hoaxbusters (http://hoaxbbusters.ciac.org/)

U.S. Government - DoD

- Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE) (http://iase.disa.mil/)
  - Document Library (http://iase.disa.mil/stigs/)
- Defense Technical Information Center (DTIC) Information Assurance Technology Analysis Center (IATAC) (http://iac.dtic.mil/iatac/)

IATAC
Information Assurance
Technology Analysis Center

U.S. Government

- U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS) (http://www.cybercrime.gov/)
- U.S. Federal Trade Commission (http://www.ftc.gov/)
  - E-Commerce & the Internet (http://www.consumer.gov/)
  - Identity Theft (http://www.ftc.gov/bcp/edu/microsites/idtheft/)

Security Organizations

InfraGard
Guarding the Nation's Infrastructure

- FBI InfraGard (http://www.infragard.net/)*
  - Alerts & advisories
  - Secure email communications
  - Library
- InfraGard Members Alliance (http://www.infragardmembers.org/)

* Open only in the United States

Security Organizations

- Computer Security Institute [CSI] (http://www.gocsi.com/)
  - CSI Computer Crime & Security Survey

- CERIAS (http://www.cerias.purdue.edu/)
  - Security Seminars (http://www.cerias.purdue.edu/news_and_events/events/security_seminar/)

Security Organizations

- CERT Coordination Center (http://ww)
  - Advisories & Incident Notices
  - Security Practices & Evaluations
  - Tech Tips (http://www.cert.org/tech_tips/)
- GovernmentSecurity (http://www.governmentsecurity.org/)

Security Organizations

- SANS (http://www.sans.org/)
  - Free Resources
  - Internet Storm Center
    - Cyber Security Awareness Tip #2: Multimedi
  - Top 20 Vulnerabilities
- Center for Internet Security (CIS) (http://www.cisecurity.org)
  - Benchmarks & Tools

Vendors

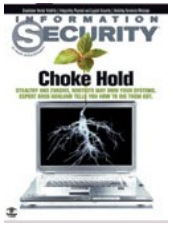
- SecurityFocus (http://www.securityfocus.com/)
  - Owned by Symantec
- Microsoft
  - General (http://www.microsoft.com/security/)
  - Technical (http://www.microsoft.com/technet/security/)
- RSA (EMC²) (http://www.rsa.com/)
- Verisign (http://www.verisign.com/)
- Cisco (http://www.cisco.com/)
- *<Insert your favorite vendor here>*

White Papers

- SearchSecurity (http://searchsecurity.techtarget.com/)
- BitPipe (http://www.bitpipe.com/data/tlist?b=ka_bp_security)
- SecurityDocs (http://www.securitydocs.com/)
- Attack Prevention (http://www.attackprevention.com/)

Magazines

Information Security
(http://www.infosecuritymag.com)



SC Magazine
(http://www.scmagazine.com/)

CSO Magazine
(http://www.csoonline.com/)

(IN)Secure Magazine
(http://www.insecuremag.com/
)

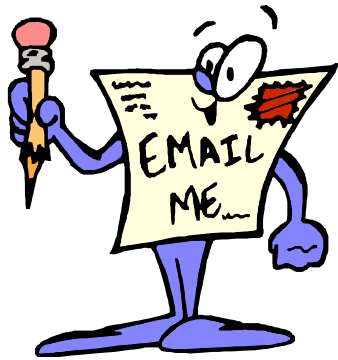
Must pre-qualify and be in the USA or Canada

Other Sources

- eWeek Security Site (http://security.ziffdavis.com/)
- eSecurity Planet (http://www.esecurityplanet.com/)
- SecurityNews Portal (http://www.securitynewsportal.com/)
- Help-Net Security (http://net-security.org/)
- SecuriTeam (http://www.securiteam.com/)
- LinuxSecurity (http://www.linuxsecurity.com/)

Mailing Lists

- US-CERT National Cyber Alert System (http://www.us-cert.gov/cas/)
- Security Focus – Bugtraq + (http://www.securityfocus.com/archive)
- Bruce Schneier's Cryptogram (http://www.counterpane.com/crypto-gram.html)
- VulnWatch (http://www.vulnwatch.org/)
- Also see http://seclists.org/



Blogs & Podcasts

- SecurityCatalyst (http://www.securitycatalyst.com/blog/)
- Network Security Blog (http://www.mckeay.net/)
- StillSecure, after all these years (http://ashimmy.typepad.com/)
- PaulDotCom (http://www.pauldotcom.com/)
- IT Toolbox Security Blogs (http://blogs.ittoolbox.com/security/)
- Digital Common Sense: IT Security Podcasts (http://ipadventures.com/)
- RSA Speaking of Security (http://www.rsa.com/blog/blog.aspx)

Free Security Tools#

Applications, Programs, Scripts, etc.

- These utilities provide a variety of security testing, auditing and hardening functions.
- They are generally divided into two "flavors:"
  - UNIX/Linux
  - Windows NT/2000/XP/2003

Evaluating Security Tools

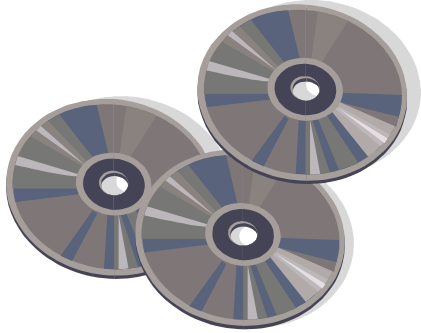
- Is source code available for this tool?
- Is this tool easy to install?
- Is this tool reasonably easy to use?
- Is this tool reliable?
- Is this tool maintained?
- Is this tool portable across different OS implementations?
- Does this tool do any harm?

Free Security Tools Lists

- Top 100 Security Tools (http://sectools.org/)

- Talisker Security Wizardry Portal (http://securitywizardry.com/radar.htm)
- Network Security Toolkit (http://www.networksecuritytoolkit.org/nst/links.html)

Free Security Tools – Bootable CDs



- Network Security Toolkit [NST] (http://www.networksecuritytoolkit.org/)
- Ubuntu Trinux (http://code.google.com/p/ubuntutrinux/)
- Knoppix (http://www.knoppix.org/)
- OWASP Live CD (LabRat) (http://www.owasp.org/index.php/Category:OWASP_Live_CD_Project)
- Backtrack 2 (http://www.remote-exploit.org/)
- Pentoo (http://www.pentoo.ch/)
- Helix (http://www.e-fense.com/helix/)

See SecurityDistro.com (http://www.securitydistro.com/)

Free Windows Security Tools

- Microsoft (http://www.microsoft.com/technet/security/tools/)
  - MS Baseline Security Analyzer (MBSA)
  - Windows Defender (antispyware)
  - Malicious Software Removal Tool
  - Security Assessment Tool
  - Windows Powershell
- PS tools (http://www.microsoft.com/technet/sysinternals/Utilities/PsTo
  - Formerly SysInternals
- Microsoft Security and Compliance Guides (http://www.microsoft.com/technet/security/topics/)

Free Windows Security Tools

- Ultimate List of Free Windows Software from Microsoft (http://bhandler.spaces.live.com/blog/cns!70F64BC910C9F7F3!1231.entry)
  - Security
  - And more
- Open Source Windows (http://www.opensourcewindows.org/)

Free Windows Security Tools

- Foundstone (a McAfee Company)
  (http://www.foundstone.com/us/resources-free-tools.asp)
  - Superscan - TCP port scanner
  - Fport - reports all open TCP/IP and UDP ports
  - Attacker – A TCP and UDP port listener
- Bayden Systems‘ (http://www.bayden.com/)
  - Slickrun
- HexEdit (http://www.expertcomsoft.com/download.htm)

Free Windows Security Tools

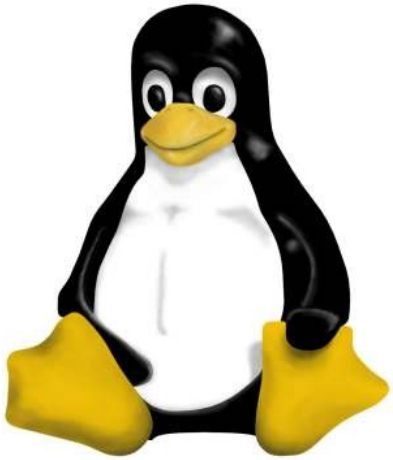
- WinFingerprint (http://sourceforge.net/projects/winfingerprint/)
  - Windows Enumeration
- KeePass (http://sourceforge.net/projects/keepass/)
  - Windows Password Manager
- ClamWin (http://sourceforge.net/projects/clamwin/)
  - Windows Anti-Virus

Free Windows Security Tools

- JoeWare tools (http://www.joeware.net/freetools/index.htm)
  - GetUserInfo – Get User Account Information
  - AdFind – Command line AD & ADAM LDAP query tool
  - SecData – Dump security info for users and computers
- LDP – LDAP enumeration
- Cain & Abel (http://www.oxid.it/)

  A password recovery tool

Free UNIX/Linux Security Tools



- Native UNIX/Linux Commands:
  - **netstat** – network status
  - **ifconfig** – network interface information
  - **ps** – print or process status
  - **lsof** – lists open files
  - **Nslookup/dig/host/dnsquery** – lookup the name/IP address
  - **traceroute** – look at network path to another server
  - **ipchains/iptables** – Linux firewall application
  - **whois** – Determine ownership of domains

Free UNIX/Linux Security Tools

- Nessus* (http://www.nessus.org/)
  - Open Source vulnerability assessment tool.
- Hping2 (http://www.hping.org/)
  - A network probing utility like ping on steroids
- SARA (http://www.www-arc.com/sara/)
  - Security Auditor's Research Assistant
  - See also: SATAN, SANTA
- OSSEC (http://www.ossec.net/)
  - An Open Source Host-based Intrusion Detection System

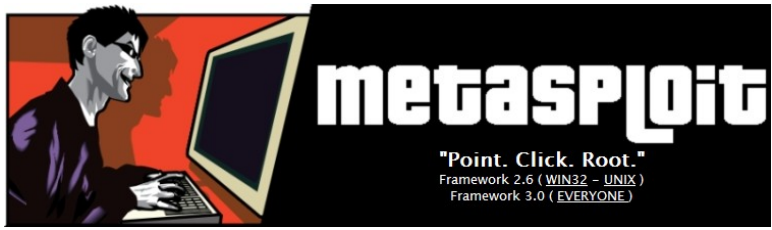
* Now Tenable

Free Security Tools for Both

- Nmap (http://insecure.org/nmap/)
  - A utility for network exploration or security auditing.
- Wireshark (http://www.wireshark.org/)
  - “Sniffing the glue that holds the Internet together.”
  - Network protocol analyzer
- Snort (http://www.snort.org/)
  - Network intrusion detection system (IDS).
- Heme – Hex Editor (http://sourceforge.net/projects/heme/)

Free Security Tools for Both

- Metasploit Framework (http://www.metasploit.org/)
  - An advanced open-source platform for developing, testing, and using exploit code."
  - Four steps:
    1. Choose a platform/application
    2. Choose an exploit
    3. Choose a shell code
    4. Exploit



Free Security Tools for Both

- Netcat (http://www.vulnwatch.org/netcat/)
  - The network swiss army knife.
- Dsniff (http://naughty.monkey.org/~dugsong/dsniff/)
  - A collection of tools for network auditing and pen testing.
- Truecrypt (http://www.truecrypt.org/)
  - Disk encryption software
- John the Ripper (http://www.openwall.com/john/)
  - A powerful, flexible, *fast* multi-platform password hash cracker

Free Network Security Tools

- IPCop (http://ipcop.org/)
  - Linux network protection
- SmoothWall (http://www.smoothwall.org/)
  - Turns a PC into a Linux Firewall appliance.
- Comodo (http://www.personalfirewall.comodo.com/)
  - Personal Firewall for Windows
- OpenVPN (http://openvpn.net/)
  - A full-featured SSL VPN

Free Wireless Security Tools

- Kismet (http://www.kismetwireless.net/)
  - A 802.11(a/b/g) network sniffer and network dissector
- Network Stumbler (http://netstumbler.com/)
- AirSnort (http://airsnort.shmoo.com/)
- Bluetooth hacking (http://trifinite.org/)

Free Forensics Tools

- Deft (http://deft.yourside.it/)

  Digital Evidence & Forensic Toolkit – a Bootable CD

- The Coroner's Toolkit (TCT) (http://www.porcupine.org/forensics/tct.html)

  A collection of programs for a post-mortem analysis of a UNIX system.

- Forensic Acquisition Utilities (http:// www.gmgsystemsinc.com/fau/)

Free Web Testing Tools

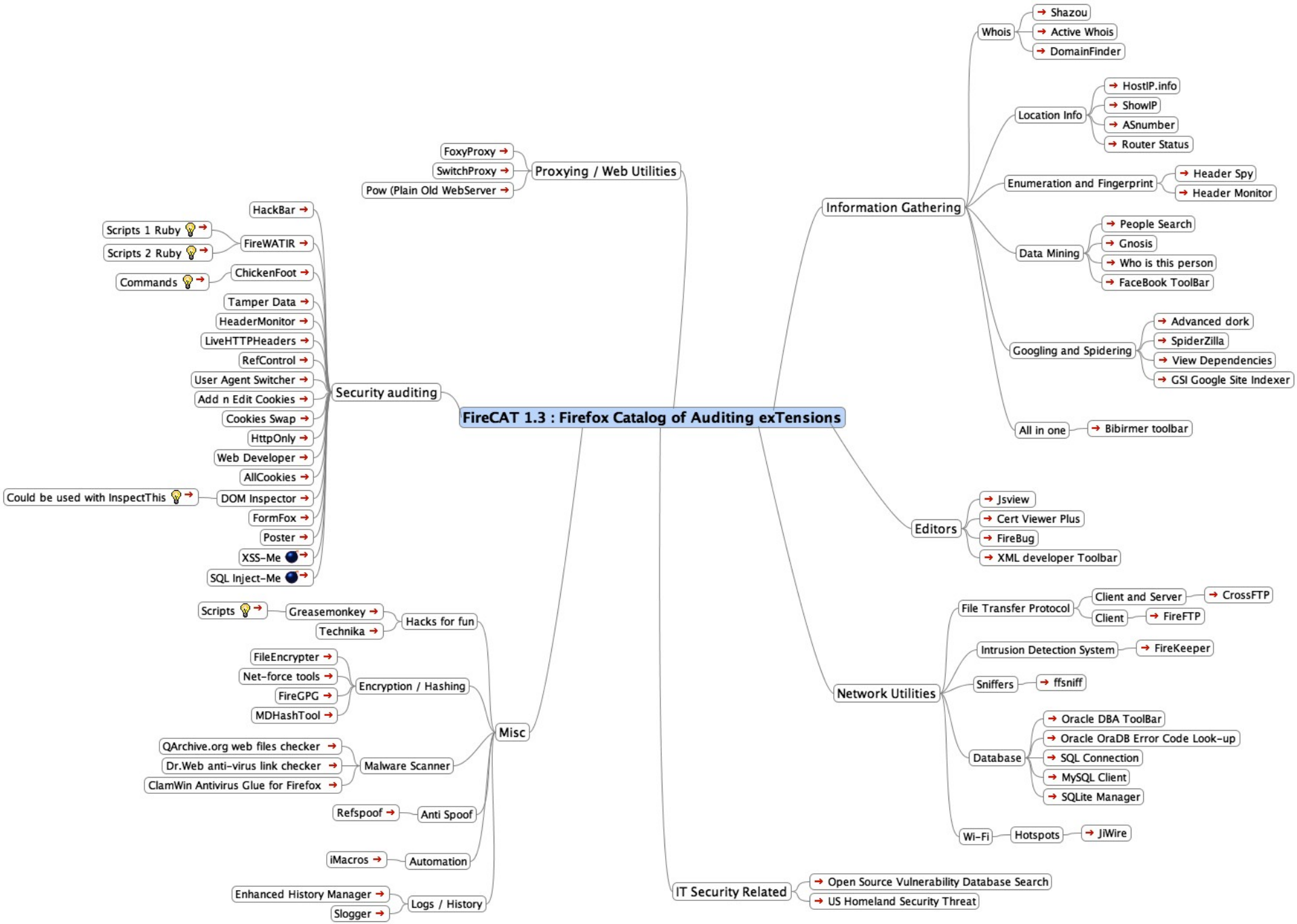
- Microsoft
  - Fiddler HTTP Debugging Proxy (http://www.fiddlertool.com/fiddler/)
  - IE Developer Toolbar
- OWASP (http://www.owasp.org/index.jsp)
  - WebGoat & WebScarab
- Nikto (http://www.cirt.net/code/nikto.shtml)
  - Web vulnerability scanner and library.
- Paros (http://www.parosproxy.org/index.shtml)

Free Web Testing Tools

- Bayden Systems' (http://www.bayden.com/)
  - TamperIE – HTTP form-tampering
- Google (http://www.google.com)
  - Google Hacking Database (http://johnny.ihackstuff.com/ghdb.php)
- TouchGraph Google (http://www.touchgraph.com/TGGoogleBrowser.html)

Free Web Testing Tools

- FireCat – Firefox Catalog of Auditing Extensions (http://www.security-database.com/toolswatch/FireCAT-1-3-released-ExploitMe.h)


FireCAT 1.3 : Firefox Catalog of Auditing exTensions
Information Gathering
Whois
Shazou
Active Whois
DomainFinder
Location Info
HostIP.info
ShowIP
ASnumber
Router Status
Enumeration and Fingerprint
Header Spy
Header Monitor
Data Mining
People Search
Gnosis
Who is this person
FaceBook ToolBar
Googling and Spidering
Advanced dork
SpiderZilla
View Dependencies
GSI Google Site Indexer
All in one
Bibirmer toolbar
Editors
Jsview
Cert Viewer Plus
FireBug
XML developer Toolbar
Network Utilities
File Transfer Protocol
Client and Server
CrossFTP
Client
FireFTP
Intrusion Detection System
FireKeeper
Sniffers
ffsniff
Database
Oracle DBA ToolBar
Oracle OraDB Error Code Look-up
SQL Connection
MySQL Client
SQLite Manager
Wi-Fi
Hotspots
JiWire
IT Security Related
Open Source Vulnerability Database Search
US Homeland Security Threat
Misc
Hacks for fun
Scripts
Greasemonkey
Technika
Encryption / Hashing
FileEncrypter
Net-force tools
FireGPG
MDHashTool
Malware Scanner
QArchive.org web files checker
Dr.Web anti-virus link checker
ClamWin Antivirus Glue for Firefox
Anti Spoof
Refspoof
Automation
iMacros
Logs / History
Enhanced History Manager
Slogger
Proxying / Web Utilities
FoxyProxy
SwitchProxy
Pow (Plain Old WebServer
Security auditing
HackBar
FireWATIR
Scripts 1 Ruby
Scripts 2 Ruby
ChickenFoot
Commands
Tamper Data
HeaderMonitor
LiveHTTPHeaders
RefControl
User Agent Switcher
Add n Edit Cookies
Cookies Swap
HttpOnly
Web Developer
AllCookies
DOM Inspector
Could be used with InspectThis
FormFox
Poster
XSS-Me
SQL Inject-Me

Free Web App Tools

- Foundstone Software Application Security Services (SASS)
  (http://www.foundstone.com/us/resources/freetools.asp)
  - CodeScout
  - HackPack
  - Hacme Casino/Bank/Books/Travel
  - WSDigger
- ModSecurity – Open Source Web Application Firewall
  (http://www.modsecurity.org/)

Hack Sites#

Use at your own risk…

- Ethical Hacker
  (http://www.ethicalhacker.net/)
- Security Tracker (http://www.securitytracker.com/)
- Hackers Center (http://www.hackerscenter.com/)

Free Web-based Security Tools

- Geektools (http://www.geektools.com/)
  - Calculators, traceroute, whois, etc
- Security Tools Online (http://www.securitytoolsonline.com/)
- IP Address (http://www.ipadress.com)
- See your IP Address
  - http://www.lawrencegoetz.com/programs/ipinfo/
  - http://www.whatismyip.com/
- Web Archives – Wayback machine (http://www.archive.org/)

Consumer Web Security

- McAfee SiteAdvisor (http://www.siteadvisor.com/)
- Comodo Verification Engine (http://www.vengine.com/)
- LinkScanner (http://explabs.com/)
- Bluecoat K9 Web Protection (http://www.k9webprotection.com/)

Protecting Our Families

- **NetSmartz** (http://www.netsmartz.org/)
- **NCSA StaySafeOnline** (http://staysafeonline.org/)
- **SafeKids** (http://www.safekids.com/)
- **GetNetWize** (http://www.getnetwise.org/)
- **i-SAFE (http://www.isafe.org)**
- **Microsoft** (http://www.staysafe.org)

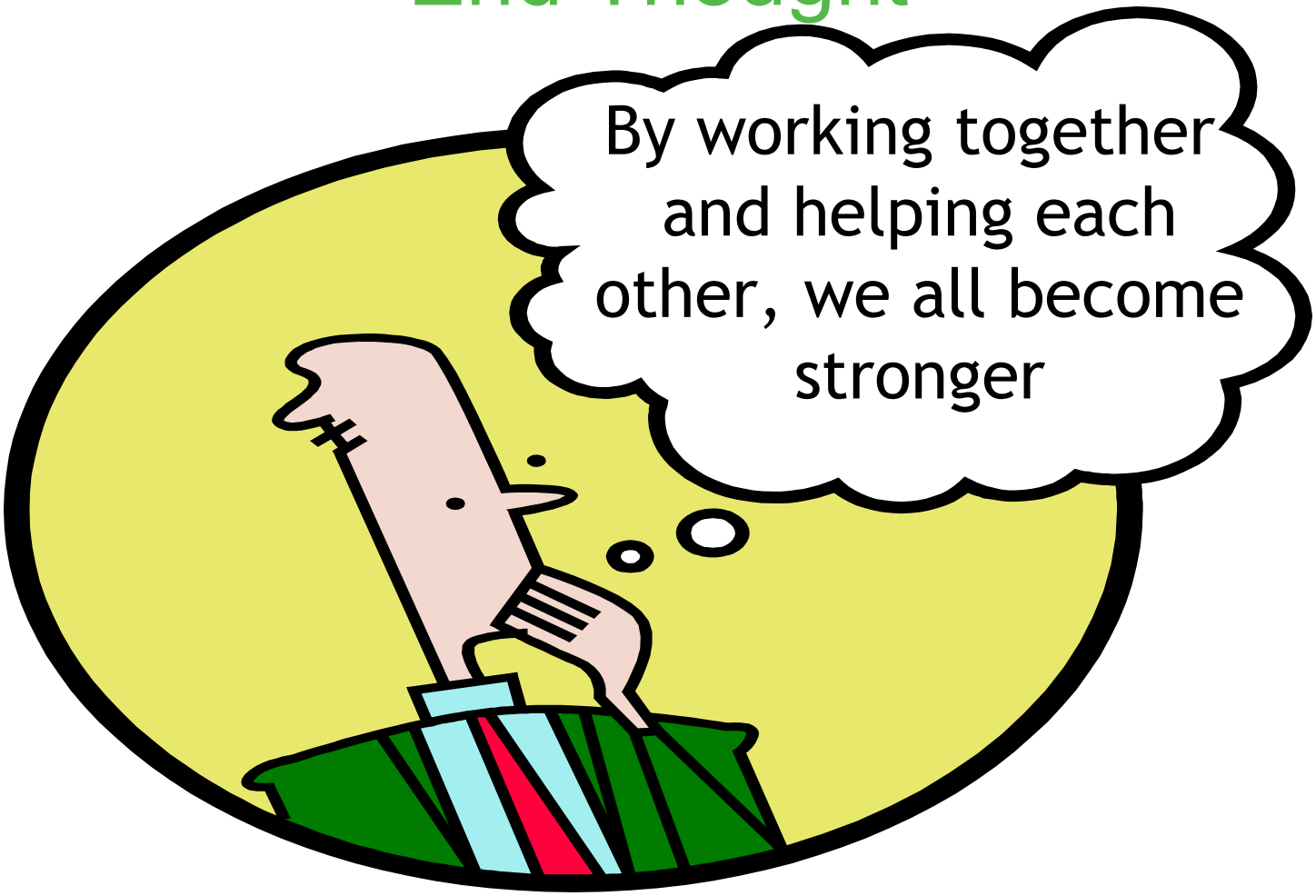
Homework
&
Test
Time


It’s not what you buy,
but what you do.

Conclusion

- Free really isn't
- Policy is where it starts
- Be aware of what's available
- Use your (free) resources
- Share with others

End Thought


By working together and helping each other, we all become stronger

Ron Woerner, CISSP

Ron[dot]Woerner[at]tdameritrade[dot]com