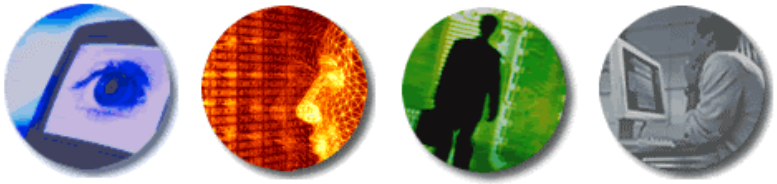
RELIABLE, RESPONSIBLE E-SECURITY

Solutionary
reliable, responsible e-security



Free Security!

Ron Woerner, CISSP

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.

Thoughts

It's not what you buy that makes you secure, but what you do.

As Bruce Schneier says, "Security is a process, **not** a product.

Many IT Security documents, tools, applications and services are available for free (or very little cost);

Agenda

- Actions that increase security
- Why Free
- Free Documents
- Free Tools
  - UNIX
  - Windows
- Education, Training & Awareness

Actions that Increase Security

- Establish policies and procedures
- Audit, test, and assess
- Change all default user ids and passwords
- Ensure proper access control
- Harden servers
  - Turn off all unnecessary services
  - Apply appropriate patches
- Run Anti-virus applications
- Train administrators, managers and users

Why Free

"There is no such thing as a free lunch."
Anonymous

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

Free Documents#

- Federal Government
- State / Local Government
- Security Organizations
- Vendors

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

Free Documents - Government

- Department of Homeland Security (http://www.ready.gov)
- NIST CSRC (http://csrc.nist.gov/)
  - Publications
    - Special publications (800 Series)
    - ITL Bulletins
  - Focus Areas
- National Infrastructure Protection Center (NIPC) (http://www.nipc.gov/)
  - CyberNotes

Free Documents - Government

- National Security Agency (NSA)
  - Security Recommendation Guides (http://www.nsa.gov/snac/)
    - Microsoft Windows (XP/2000/NT)
    - Cisco Router
    - E-mail and executable content
  - Security-enhanced Linux
- U.S. Dept of Energy Computer Incident Advisory Capability (CIAC) (http://www.ciac.org/ciac/)

Free Documents - 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
  - Identity Theft (http://www.consumer.gov/idtheft/)

Free Documents – State Gov't

- Nebraska Information Technology Commission (NITC) Security Working Group (http://www.nitc.state.ne.us/tp/workgroups/security/)
  - Policies
  - Guidelines & Instructions
- Iowa Information Technology Department Enterprise Security (http://www.iowaccess.org/government/its/security/)
- Texas Information Resources Security Office (http://www.dir.state.tx.us/security/index.htm)

Free Documents – Security Orgs

- CERT Coordination Center (http://www.cert.org/)
  - Advisories & Incident Notices
  - Security Practices & Evaluations
  - Tech Tips (http://www.cert.org/tech_tips/)
  - Survivability Research & Analysis

Free Documents – Security Orgs

- SANS (http://www.sans.org/)
  - Reading Room
  - Internet Storm Center
  - SCORE
  - Top 20 Vulnerabilities
- Center for Internet Security (CIS) (http://www.cisecurity.org)
  - Benchmarks & Tools

Free Documents – Security Orgs

- CERIAS (http://www.cerias.purdue.edu/)

- GovernmentSecurity.org (http://www.governmentsecurity.org/)

Free Documents – Vendors

- SecurityFocus (http://www.securityfocus.com/)
  - News, Columns, Infocus (tips & techniques)
  - Vulnerabilities & advisories
- Microsoft (http://www.microsoft.com/security/)
- Verisign (http://www.verisign.com/)
- Cisco (http://www.cisco.com/)
- *<Insert your favorite vendor here>*

Free# Documents – Magazines

- Information Security (http://www.infosecuritymag.com)
- SC Magazine (http://www.scmagazine.com/)
- CSO Magazine (http://www.csoonline.com/)

Must pre-qualify and be in the USA or Canada

Free Documents – Others

- SearchSecurity.com (http://searchsecurity.techtarget.com/)
- Security Super Site (http://security.ziffdavis.com/)
- eSecurity Planet (http://www.esecurityplanet.com/)

Mailing Lists

- Security Focus – Bugtraq + (http://www.securityfocus.com/archive)
- NTBugtraq (http://www.ntbugtraq.com)
- CERT Advisory Mailing List (http://www.cert.org/contact_cert/certmaillist.html)
- Bruce Schneier's Cryptogram (http://www.counterpane.com/crypto-gram.html)
- VulnWatch (http://www.vulnwatch.net/)
- Also see http://lists.insecure.org

Free Security Tools#

- 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
- Top 75 Security Tools (http://www.insecure.org/tools.html)

Applications, Programs, Scripts, etc.

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 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 of a system
  - **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/)
  - The premier 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

Free Windows Security Tools

- Microsoft (http://www.microsoft.com/technet/security/tools/tools.asp)
  - Hfnetchk – Checks patch status
  - MS Baseline Security Analyzer
  - IIS Lockdown tool
  - Slammer assessment tools
  - Checklists

Free Windows Security Tools

- Foundstone (http://www.foundstone.com/resources/freetools.htm)
  - Superscan - TCP port scanner
  - Fport - reports all open TCP/IP and UDP ports
  - Attacker – A TCP and UDP port listener
- PS tools (http://www.sysinternals.com/ntw2k/freeware/pstools.shtml)
  - Provides various information about remote windows systems.

Free Security Tools for Both

- Nmap (http://www.insecure.org/nmap/)
  - An open source utility for network exploration or security auditing.
- Ethereal (http://www.ethereal.com/)
  - "Sniffing the glue that holds the Internet together."
  - A free network protocol analyzer
- Snort (http://www.snort.org/)
  - A free, a lightweight network intrusion detection system (IDS).

Free Security Tools for Both

- Netcat (http://www.atstake.com/research/tools/network_utilities/)
  - The network swiss army knife.
- Dsniff (http://naughty.monkey.org/~dugsong/dsniff/)
  - A collection of tools for network auditing and penetration testing.
- John the Ripper (http://www.openwall.com/john/)
  - A powerful, flexible, and *fast* multi-platform password hash cracker

Free Security Tools for Both

- Nikto (http://www.cirt.net/code/nikto.shtml)
  - Web vulnerability scanner and library.
- Kismet (http://www.kismetwireless.net/)
  - A 802.11b network sniffer and network dissector
- Others???

Free Web-based Security Tools

- Sam Spade (http://www.samspade.org)
  - Network Query Tool.
- Geektools (http://www.geektools.com/)
  - Calculators, traceroute, whois, etc
- Network Calculators (http://www.telusplanet.net/public/sparkman/netcalc.htm)
  - Subnet mask and network node calculators.
- See your IP Address
  - http://www.lawrencegoetz.com/programs/ipinfo/
  - http://www.whatismyip.com/

Conclusion

- Free really isn't
- Policy is where it starts
- Be aware of what's available
- Use your (free) resources
- Share with others
  - By helping others, we strengthen ourselves.

Questions

Ron Woerner, CISSP

Ron_Woerner@excite.com