

Security resource list for administrators

As new and more dangerous network security threats proliferate, administrators need to know as much as possible about these threats and about the vulnerabilities that leave networks open to attack. The better armed net admins are with knowledge of threats and security measures, the better able they'll be to secure their networks and fend off attacks.

The following links are to Web sites that can offer valuable information about securing your networks, including updates on new threats and vulnerabilities and how to deal with them, as well as downloads of utilities and information about products that can help you secure your networks.

Many of the links in this document were provided by [Global Knowledge](#) in Network Security I courseware, David Ford, course director.

Security organization and information sites

SecurityPortal (<http://www.securityportal.com>)

SecurityPortal offers various security information and services. The site is currently down for upgrades, and users are being redirected to security solution provider [RedSiren Technologies](#).

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

Yes, Microsoft's Web site offers important tips and other information to help you secure your network. In addition to valuable information, Microsoft provides security services.

TruSecure Corp (<http://www.trusecure.com>)

TruSecure is a security solutions provider that also certifies security products. TruSecure has established the TruSecure ICSA Certified Security Associate (T.I.C.S.A.) certification for IT professionals.

U.S. Dept. of Justice CCIPS (<http://www.cybercrime.gov/>)

The Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice Web site presents detailed information about policy regarding computer crime, procedures for reporting computer crime, and news relating to computer crime cases.

National Infrastructure Protection Center (NIPC) (<http://www.nipc.gov>)

The NIPC assesses and investigates threats to critical infrastructures and provides warnings about threats and vulnerabilities.

NTBugtraq (<http://www.ntbugtraq.com>)

NTBugtraq is a mailing list devoted to security exploits and bugs in Windows NT, Windows 2000, and Windows XP.

SecurityFocus Online (<http://online.securityfocus.com/cgi-bin/sfonline/forums.pl>)

SecurityFocus is a collection of security-related mailing lists. You can subscribe to the newsletter, which offers information about exploits, vulnerabilities, and threats, and you can take advantage of the mailing list to solicit information from members.

Computer Incident Advisory Capability (CIAC) (<http://www.ciac.org/ciac/>)

The U.S. Department of Energy's CIAC Web site offers news about new computer threats, hoaxes, and vulnerabilities, along with procedures for reporting incidents such as network attacks.

Forum of Incident Response and Security Teams (FIRST) (<http://www.first.org>)

FIRST is an international coalition formed to share information about network security threats and to work out responses to incidents. You can sign up for mailing lists and become a member. The annual membership fee is \$550.00. FIRST holds an annual forum to discuss security issues.

Computer Emergency Response Team Coordination Center (CERT/CC) (<http://www.cert.org>)

CERT/CC is a center that specializes in Internet security issues at Carnegie Mellon's Software Engineering Institute. At its Web site, you'll find information about Internet vulnerabilities, security alerts, and information about fixing vulnerabilities.

Common Vulnerabilities and Exposures (CVE) (<http://www.cve.mitre.org/>)

CVE is a dictionary of information security vulnerability and exposure terms.

The National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) (<http://csrc.ncsl.nist.gov>)

The CSRC is the Web site for the Computer Security Division (CSD) of the NIST's Information Technology Laboratory. The CSD's mission is to research and raise awareness of new IT vulnerabilities and to develop cost-effective security measures.

Information Systems Security Association (ISSA) (<http://www.issa.org>)

ISSA is an international organization of IT security professionals established to educate its members about security issues and measures and to publish the findings of its forums on security-related issues.

International Information Systems Security Certification Consortium (ISC2) (<http://www.isc2.org>)

The ISC2 Web site provides information about becoming a Certified Information Systems Security Professional (CISSP).

High Technology Crime Investigation Association (HTCIA) (<http://www.htcia.org>)

The HTCIA is an international organization established to set standards for investigating technology crimes.

Center for Education and Research in Information Assurance and Security (CERIAS) (<http://www.cerias.purdue.edu/>)

CERIAS is Purdue University's center for research on information security issues. It offers a wealth of information on vulnerabilities and threats.

Security product links

The following list represents products that can help you better secure your network. This is not an endorsement of the products but a list of those that are well known.

Firewalls

- Check Point FireWall-1 (<http://www.checkpoint.com/products/protect/index.html>)
- Cisco Secure PIX 500 series (<http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/>)
- Symantec VelociRaptor (<http://enterprisesecurity.symantec.com/products/products.cfm?productID=49>)
- Secure Computing's Sidewinder (<http://www.securecomputing.com/index.cfm?sk=232>)
- BorderWare Firewall Server (<http://www.borderware.com/>)
- Elron Software's Internet Manager (IM) Firewall (<http://www.elronsw.com/productfamily/firewall.shtml>)
- CyberGuard LX, FS, KS, and SL VPN/firewall appliances (http://www.cyberguard.com/SOLUTIONS/product_intro.cfm)
- WatchGuard Firebox series (<http://www.watchguard.com/products/wgls.asp>)
- SonicWALL appliances (<http://www.sonicwall.com/>)

Be sure to check out products from Network Associates (<http://www.networkassociates.com>) as well.

Intrusion detection systems (IDS)

- Symantec Intruder Alert (acquired with Axent) (<http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=48&PID=11649525&EID=0>)

- Symantec NetProwler (acquired with Axent)
(<http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=50&PID=11649525&EID=0>)
- Cisco IDS series (<http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/>)
- Enterscept Security Technologies' Enterscept (<http://www.clicknet.com/products/enterscept/>)
- Internet Security Systems RealSecure Network Sensor
(http://www.iss.net/products_services/enterprise_protection/rsnetwork/sensor.php)
- NFR Security's Network Intrusion Detection (NID) (<http://www.nfr.net/products/>)
- Intrusion Inc.'s SecureNet products
(<http://www.intrusion.com/products/productcategory.asp?lngCatId=4>)
- Tripwire, Inc.'s intrusion detection and data integrity products (<http://www.tripwire.com/>)
- Psionic's TriSentry Suite (freeware) (<http://www.psionic.com/products/index.html>)

Scanners (vulnerability assessment and auditing tools)

- Symantec NetRecon
(<http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=46&PID=11649525&EID=0>)
- Internet Security Systems (ISS) scanning products
(http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/index.php)
- Cisco Secure Scanner (<http://www.cisco.com/warp/public/cc/pd/sqsw/nesn/>)
- McAfee CyberCop ASaP (<http://www.mcafee2b.com/services/cybercop-asap.asp>)
- NetIQ's Security Analyzer (<http://www.netiq.com/solutions/security/default.asp>)
- Nessus (freeware) (<http://www.nessus.org>)
- HP Webenforcer (<http://www.hp.com/security/products/webenforcer/>)

Authentication

- Netegrity SiteMinder (<http://www.netegrity.com/products/?leveltwo=SiteMinder>)
- IBM Tivoli Access Manager (<http://www.tivoli.com/products/solutions/security/access.html>)
- *RedCreek Ravlin series (<http://www.redcreek.com/products/index.html>)
- *SonicWALL Authentication Service (<http://www.sonicwall.com/authentication-service/solutions.html>)
- RSA SecurID (<http://www.rsasecurity.com/products/securid/index.html>)
- Entrust GetAccess (<http://www.entrust.com/getaccess/index.htm>)
- Funk Software's Steel-Belted Radius (http://www.funk.com/radius/enterprise/enterprise_radius.asp)
- ActivCard (<http://www.activcard.com>)
- CRYPTOCARD CRYPTOLogon, CRYPTOWeb, and CRYPTOAdmin
(<http://www.cryptocard.com/index.cfm?CID=8&NAVCID=8&PageName=Solutions%20for%20your%20Network>)
- Gemplus GemSAFE products (<http://www.gemplus.com/index.html>)
- Vasco Digipass series
(<http://www.vasco.com/products/range.html?VSID=5e65eb874a61e5e501501b1bbdaf9f53#Digipass>)

*Red Creek acquired Internet Dynamics, which offered Conclave, and was later acquired by SonicWALL. Thus, RedCreek and Internet Dynamics products may be pulled under the SonicWALL umbrella.

Antivirus and content filtering software

- Trend Micro antivirus products (<http://www.antivirus.com/products/>)
- Symantec (Norton) AntiVirus Enterprise Edition
(<http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=64&PID=1117941&EID=0>)
- McAfee VirusScan (<http://www.mcafee.com/myapps/default.asp?>)
- SonicWALL Complete Anti-Virus (<http://www.sonicwall.com/anti-virus/index.html>)
- SurfControl SuperScout (<http://www.surfcontrol.com/business/products/>)
- GFI Mail essentials (<http://www.gifax.com/mes/index.html>)

- Tumbleweed's Secure Mail (http://www.tumbleweed.com/en/products/solutions/protect_enterprise/mail.html)
- Elron's Internet Manager (<http://www.elronsw.com>)

Hacker sites

Hacker sites offer good information about the latest threats and newly discovered vulnerabilities. They also offer freeware downloads of scanners and other utilities that you can use to identify vulnerabilities—so that you can see what hackers see. Don't download and install anything without scanning it first, though. While these sites can help you beef up your security arsenal, you should still proceed with caution.

AntiOnline (<http://www.antionline.com/index.php>)

For information and news about vulnerabilities and threats, AntiOnline is one of the best of the hacker sites. It includes a wealth of downloads from antivirus programs to exploits and scanners. AntiOnline also offers an extensive list of links divided into a number of categories so you can find more sites about security and hacking.

2600 Magazine The Hacker Quarterly home page (<http://www.2600.com>)

This site offers news and information from the hacker community.

Phrack Magazine (<http://www.phrack.org>)

Here's another hacker publication offering news and information.

Hackers.com (<http://www.hackers.com>)

Hackers.com offers information about vulnerabilities, threats, and exploits, as well as advice on securing networks.

L0pht Heavy Industries at @Stake (<http://www.atstake.com/research/redirect.html>)

This site features information about vulnerabilities and threats, along with downloads for auditing network security, including LC4, a password auditing and recovery application.

Cult of the Dead Cow (<http://www.cultdeadcow.com>)

Cult of the Dead Cow offers news and comments about issues of hacking and security. You can also download files from the site, including Back Orifice and Whisker.

Def Con (<http://www.defcon.org>)

This Web site promotes the annual hacker convention and offers links to a variety of downloads, including cracks, scanners, and other tools.