Information Security Resources

Professional Development/ Security Associations:

(ISC)^2 International Information Systems Security Certifications Consortium, Inc. – CISSP Certification
http://www.isc2.org

Information Systems Security Association (ISSA) (90 day trial membership available)
http://www.issa-intl.org/

International Computer Security Association
http://www.icsa.net/

SANS – Certifications in Intrusion Detection & Firewalling (Free Security Poster)
http://www.sans.org

IEEE Computer Society Technical Committee on Security and Privacy
http://ieee-security.org/

Legal Resources:

Case Law - Hacking/cracking, viruses, and security (Law School Web Site)
http://www.jmls.edu/cyber/index/hacking.html

Hacking Laws in the 50 States & The UK
http://www.ladysharrow.ndirect.co.uk/Virus%20Information/virus_and_hacking_law.htm

Canadian Hacking Law
http://www.happyhacker.org/hhlist/digest7b5.shtml

Canadian IT Law Index
http://www.it-can.ca/Links.html

The Computer Fraud and Abuse Act (as amended Oct. 3, 1996)
http://206.9.156.15/hacklaw.htm

FindLaw.Com - Searchable Database of Case Law by Court (Use keyword: hacking)
http://laws.findlaw.com/

Information Security Resources

Legal Resources (continued):

International Law Enforcement Resources
http://www.vaonline.org/law.html

Intrusion Detection (Network Based):

Cisco Secure IDS
http://www.cisco.com/warp/customer/cc/pd/sqsw/sqidsz/

RealSecure (Download Eval)
http://www.iss.net/cgi-bin/download/evaluation/evaluation-select.cgi

SecureNet Pro (Kane Security Monitor by RSA Networks licensed to Intrustion.com)
http://192.94.73.13

SNORT – FREE Unix Intrusion Detection System
http://www.snort.org

Intrusion Detection (Host Based):

BlackICE Pro
http://www.networkice.com/

TripWire for NT
http://www.tripwiresecurity.com

FREE Common Security Exploit & Vulnerability Matrix Poster Request Form
http://www.tripwiresecurity.com/promos/poster.cfml

Reconnaissance Tools (UNIX):

SAINT (Formerly SATAN)
http://www.wwdsi.com/saint/archive.html

Network Mapper (nmap)
http://www.insecure.org/nmap

Information Security Resources

Reconnaissance Tools (Windows):

Cisco Secure Scanner (NetSonar)
http://www.cisco.com/kobayashi/sw-center/internet/netsonar.shtml

NetCat
http://www.l0pht.com/~weld/netcat

Self-Scan (Check your own machine's vulnerabilities)
http://www.cablemodemhelp.com/portscan.htm

DNScape – DNS Dump Tool
http://www.inettools.com

SNMP Discovery Tools (Windows):

SolarWinds
http://www.solarwinds.net

Exploits by OS:

MITRE – CVE – Common Vulnerabilities & Exposures
http://www.cve.mitre.org/cve

CERT Advisories
http://www.cert.org

Insecure.Org
http://www.insecure.org/sploits.html

BlackCode (temporarily off-line, but worth it to keep trying it)
http://www.blackcode.com

Security Portal
http://www.securityportal.com

Security Focus
http://www.securityfocus.com

Information Security Resources

Exploits by OS (continued):

Packet Storm
http://packetstorm.securify.com

CyberArmy (Links to Top 50 Hacking Sites)
http://www.cyberarmy.com/t-50/index.shtml

General Security

SearchSecurity.com
http://searchsecurity.techtarget.com

Web Security
http://www.w3.org/Security

Information Security Magazine (FREE Subscription)
http://www.infosecuritymag.com

FREE Protocol Posters (Links to many Protocol Posters)
http://www.net3group.com/resources.asp

New Order
http://neworder.box.sk

CAIDA
http://www.caida.org/home/index.xml

Information Security Resources

Cracking Tools:

L0pht Crack for NT
http://www.l0pht.com/l0phtcrack

Rhino9 Cracking Suite - Legion
http://packetstorm.securify.com/groups/rhino9

DMOZ Cracking Tools Index
http://www.dmoz.org/Computers/Hacking/Cracking

Cisco Links:

Improving Security on Cisco Routers
http://www.cisco.com/warp/public/707/21.html#spoof-rpf

Security Related RFC Index
http://www.cisco.com/warp/public/625/ccie/certifications/security_qual_blueprint.html#24

CCIE – Security
http://www.cisco.com/warp/public/625/ccie/certifications/security_qual_blueprint.html#24

Security Technical Tips: Internetworking
http://www.cisco.com/warp/public/707/index.shtml

Top Issues in VPN
http://www.cisco.com/warp/customer/471/top_issues/vpn/vpn_index.shtml (CCO Login Required)

Enterprise Security Design Implementation Guide
http://www.cisco.com/warp/partner/synchronicd/cc/sol/mkt/ent/secur/
(Requires PARTNER level CCO access. Speak to your local Cisco SE to download it for you)

Cisco Secure Encyclopedia (CSEC) Requires CCO Login:
www.cisco.com/go/csec

Information Security Resources

Certificate Authority (PKI):

Configuring Microsoft Certificate Server (Windows 2000 Server)
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csvpnc/csvpnsg/idcmsft.htm

Verisign PKI White Paper
https:///www.verisign.com/cgi-in/clearsales_cgi/leadgen.htm?form_id=0152&toc=w058801560152000&email=

Books:

Internet Security Protocols – Protecting IP Traffic
Uyless Black – 2000 - Prentice Hall – ISBN: 0-13-014249-2

Hacking Exposed – Network Security Secrets & Solutions, 2E (Be sure to get the NEW 2ND Edition)
McClure, Scambray & Kurtz – 1999 – Osborne (McGraw Hill) – ISBN: 0-07-212127-0

The Cuckoo's Egg: Tracking a spy through the maze of computer espionage.
Clifford Stoll – 1989 – Doubleday – ISBN: 0385249462

Take-Down: The pursuit and capture of Kevin Mitnick, America's most wanted computer outlaw.
Tsutomu Shimomura – 1996 – Hyperion – ISBN: 0786862106

Cyberpunk: Outlaws and Hackers on the Computer Frontier
Katie Hafner, John Markoff – 1995 – Touchstone Books – ISBN: 0684818620

Network Intrusion Detection, 2E (Be sure to get the NEW 2ND Edition)
Stephen Northcutt – 2000 – New Riders Publishing - ISBN: 0735710082

Intrusion Signatures and Analysis
Stephen Northcutt - 2001 – New Riders Publishing - ISBN: 0735710635

Designing Network Security
Merike Kaeo – 1999 – Cisco Press – ISBN: 1578700434