GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

DSL AND COMPUTER SECURITY ISSUES

The key to security for Digital Subscriber Lines (DSL) can also be remembered by the same acronym, DSL: DON'T STOP LOOKING (or logging).

DSL connectivity has increased in popularity from the home or small office ("SOHO") due to the need for fast, reliable transmissions between the telecommuter or branch office, and the primary corporate servers housing applications, databases, and files used to perform work. In the last 10 years, the rise of Internet connectivity for the home computer, the need for greater bandwidth (broadband=>1.544Mbps) for streaming audio and video, and the desire to have the transmission speed approximating the speed that one is used to with the T1 for the main office network has spurred the development of inexpensive alternatives to ISDN and T1 connections that only larger corporations can afford. DSL is commonly sold for a flat rate for unlimited usage, at less than $40 per month to individuals, or more for multinode sites such as small offices.

DSL is not monolithic. "xDSL" is a collective name for the varying standards, which can be symmetric (upload and download at the same speed) or asymmetric (download [downstream, D] speeds far exceed upload [upstream, U] speeds. The comparison is written as DDD/UUU in Kbps. The chosen standard may range from 2 to 25 times as fast as the standard 56Kbps dial-up modem. The rate varies based on the distance to the telephone central office, where a DSL Access Multiplexer (DSLAM), directs data traffic to the Internet (onto fiber optic channels) before hitting the PSTN voice telephone switch (thus not overloading them). It is the need and justification of expense to install DSLAMs at telephone central offices, and the need to be within a few miles proximity of the DSLAM that is holding DSL growth back. DSL's popularity also stems from the ability to use standard copper twisted-pair phone lines, often with a splitter (and microfilters to eliminate out-of-band-noise) to differentiate voice and data traffic by frequency. Unlike like coaxial cable TV, it can not only transmit Video on Demand (VoD) at a high rate of speed, but also voice traffic in most versions. Current standards include:

1. ADSL (ANSI T1.413 standard) – Asymmetric DSL, speed 1500to8000 / 64to-800Kbps – High-speed solution originally developed for Video on Demand with compression and to incorporate voice with a video channel (voice over IP) in differential or transverse mode. It is designed for fault tolerance, low error rates, and minimal time delay cost. ADSL travels on standard copper wire, allowing a shared data and voice line. ATM transmissions are used on the "trunk" portions, and give rise to "Voice over ATM". Often used for residential DSL.
2. RADSL: Rate-adaptive DSL that adjusts its transmission rate to the phone line quality.
3. DSL-Lite or G.Lite: A form of ADSL which does not require a installing a splitter to separate out voice transmissions below 4KHz, and may be plugged into an ordinary phone jack, thus more "plug-and-play". This version would be available for laptop and remote connections. Transmission at frequencies above 4KHz would not interfere with voice transmissions. Speed is 1500/384Kbps.
4. HDSL (High Bit/Data-Rate DSL): Symmetric (same speed download/upload: 1.54Mbps) Uses two copper twisted-pair lines. A replacement for T1/E1 repeater systems, due to the equivalent speed. Also originally designed for video data. No compression, and less fault tolerance. (A faster version uses 3 twisted pairs, and HDSL-2 uses only 1 pair.)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

5. SDSL: Single line, symmetric DSL. The same speed download/upload ranges between: 160Kbps to 2.3Mbps)
6. VDSL: Very high speed DSL for short-distance transmissions over copper twisted-pair telephone lines with a fiber optic "trunk" connection to the host site. Does NOT support voice traffic on the same line. Industry standards are under discussion.
7. VADSL: An asymmetric version of VDSL is in the planning stages. Standards are under discussion. Earlier also known as BDSL. This would yield extremely high speeds.
8. IDSL: A hybrid between DSL and ISDN, with a symmetric 128-144Kbps data rate, but may have bonded circuits. Can be used on fiber optics, and thus for greater distances, up to 6.6 miles. Does NOT support voice traffic on the same line. (ISDN is convertible to DSL.)
9. ISDN (Integrated Services Digital Network): Surprisingly enough, it can be categorized with DSL technology, though it was its predecessor. Unlike the other pure digital systems, ISDN relies on passage through the telephone switching systems. It was primarily developed for 2 twisted-pair voice channels or a data channel (2B+D) at the rate of 64-128Kbps. In the "olden" days of 1200 bps modems, this was "screaming" fast. The expense of the installation and monthly fee for a dedicated ISDN line vis-à-vis DSL has increased DSL popularity.
10. Voice over DSL (VoDSL): Up to 16 phone lines voice and data over one DSL connection.

The DSL used by small and home offices should be contrasted with another popular option: cable modems. Both allow "always on" connectivity, require static IP addresses, and pricing options are similar. (A previous GSEC paper addressed cable modems.) Cable modems differ, however, in that they utilize the coaxial cabling provided by Cable TV firms to achieve high speed data transfer. Voice traffic is not included. The connection for a cable modem is akin to a "Network Neighborhood", in that all homes on a particular cable wiring on a street all exist on a common circuit, and are essentially trusted shares on that circuit, thus allowing an alarming access to the resources found on other computers on that circuit! As the number of users and utilization by their transmissions grow on the circuit, speed may decrease and bottleneck. Cable modems therefore link multiple nodes on a circuit to the cable provider, with little inherent security, and have scalability issues.

Satellite systems are dedicated, but often allow only one-way communication. Downloads are at about 384Kbps, but upload are at a slow 33.6Kbps, and so will not be discussed further.

DSL connectivity is provided between a single point of entry and the telephone central office. While multiple users may exist behind that point of entry, e.g., behind a small 2-interface router and DSL modem, there is a "virtual private circuit" created between the two points, without vying for resources with other connections. This connection can be further secured by authentication with a trusted host after passing through the telephone central office onto the Internet to its destination. Finally, the major attraction is the development of extranets using VPN technology and protocols that will allow for secure connectivity and transmissions between two points (tunneling), when one exists outside the trusted network. This gives rise not only to the potential to secure connections with the home or small office, but also to the ability to conduct e-commerce with customers and business-to-business transactions without compromising security.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Security for the DSL environment is dependent on the user as well as the technology. A "24 x 7" connectivity with a static IP address via a modem to an internal network makes for a juicy target.

1. Protect by means of a VPN solution incorporating 128-bit encryption and secure tunneling to a corporate site. The IPSec standard protocol is preferable to PPTP and other protocols. It should be noted that compatibility issues exist between the Microsoft Proprietary IPSec used in Windows 2000 and the generic IPSec standard used in certain current VPN solutions. IPSec can only be used in Native Mode Windows 2000 implementations, not Mixed Mode. Additionally, MS VPN utilizes PPTP tunneling with DUN 1.3 or 1.4 (Dial Up Networking).
2. See the VTAC article (6) and DSL Forum for discussion of PPP (PPPoA, PPPoE) dynamic IP-addressing security. This is disputed in the DSL Zone "Tweaks.html" article (7) section on Security (p. 10). See Day (26) on bridged, routed and PPPoA/PPPoE connection security.
3. SSL should be enabled for v3.0 only, by unchecking the box for v2.0 in the Browser (e.g., Internet Explorer: Tools, Internet Options, Advanced, then unchecking the 3 boxes: Use SSL 2.0, Use PCT 1.0, and Use TLS 1.0).
4. The most recent operating system and application service packs and patches must be applied and logged. Communication with IT security or periodic vendor website review is essential.
5. Provide Perimeter Defense with a router that has IOS Firewall software and a strong script for packet filtering. Use of conduits, a warning banner, secure encrypted passwords, non-default password-strength community names, and directional ACLs should be implemented. A proxy server software (often incompatible with router firewall software) is another alternative. 2 NIC cards (internal and external) are another alternative for sharing resources.
6. For the individual user, a personal firewall and encryption solution should be added to the user's PC. For portables and laptops, hard disk encryption should be added. This expense is less than $150 per user. More robust small office versions with more functionality and configuration options exist, allowing sophisticated security for $300 to $500. Protection for Java applets and Active X controls should be included.
7. In the small office or networked home office, a mini-NATting solution can hide additional devices behind 1 IP address. Commercial software is available for this.
8. A beta version of Microsoft's IE 5.5 has additional privacy and cookie protection built in, and is available for download from the IE Explorer downloads page. Third-party privacy software exist, often in conjunction with antivirus, encryption and personal firewall solutions.
9. Turn off File and Print Sharing via the Control Panel, Network, File and Print Sharing button. Both options for giving others access to your files and letting others print to your printer should be changed to unchecked boxes, unless in a shared office environment.
10. Remove additional unnecessary services and shut down unneeded port services. NetBIOS (unless Scope ID set for file and print sharing), NetBEUI (unless you truly must "file and print share", and then unbound from TCP/IP), and IPX/SPX and NWLINK (unless a Novell office) protocols, as well as ICMP, NetBIOS services, and remote services not needed should be removed, or configured for specific source and destination IP addresses.
11. FTP, if allowed inbound, should not allow anonymous FTP, not permit traversing directory structures above the allowed folder(s), not be world-writeable or readable, nor allow an insecure password for the above. Hidden directories may be used. Restrict telnet and FTP to specific administrators inbound from specific IP addresses or ranges, or use SSH (Port 22). SSH is an encrypted session—including the password, which should overcome telnet issues.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Clear text passwords are an issue for FTP, telnet, and POP mail services. Refer to A.P. Lawrence article (12).

12. Chat/ICQ, NetMeeting, AOL/Netscape Instant Messenger (Port 5190), CuCme and other live channels with vulnerabilities should be removed or at minimum disabled when not in use.
13. Ensure that current antivirus software is licensed and used, with virus signature update by scheduled web update or pushed from the corporate server.
14. Insist on a strong password policy, enforced by network-based password filter/strength monitoring for user accounts, with expiration and cycle depth for passwords coded into the user profile.
15. User education on social engineering, taping passwords to monitors, and bringing software in from home or the Internet should be part of the Acceptable Use and Computer Security training provided annually.
16. PCAnywhere: Remote configuration and troubleshooting software, also used for file transfer must be guarded in use. It should not be placed in the Startup folder, nor configured with the password to be remembered automatically. Further, the host should not be allowed to communicate with the client without authentication by username and password. The administrator should further be required to input an additional administrator password to perform such updates. A previous GSEC paper, knowledge base articles on Norton's website, and security forums address PCAnywhere vulnerabilities.
17. Broadcast traffic, RIP, and PCAnywhere pings to scan for other PCAnywhere hosts announce to the world that you exist, as well as increasing load and utilization. Minimize the time periods to the level that will not cause traffic degradation, or have default broadcast configurations removed so system reconnaissance and mapping is not a "giveaway".
18. Email transmissions should be secured with password protection on attachments. User education against clear-text email transmissions should be followed up with the use of encryption through the email software (e.g., Exchange) or a 3rd party solution. Avoid webmail, which transmits clear-text passwords. (See also POP discussion.) As encryption and X.509 digital signature/certificate technology is part of a PKI solution with VPN implementation, this should be extended to the email system used. It may actually then be harder to get email TO the remote site encrypted than FROM the remote site!
19. With the advent of the Palm VII from 3Com, and similar handhelds that support WAP (wireless) transmission protocols, wireless DSL is possible, and security complexity increases. This is the basis for another paper.
20. Coordination with your IT Security and Network Administration departments should be developed for periodic security and network performance evaluations. This should include looking for vulnerabilities and system compromise (e.g., breached systems with "hidden file space" hiding hacker tools or data files). Monitoring may be possible in sophisticated organizations. (There are also websites for testing the vulnerability of the website: http://www.secureme.net, http://grc.com for Shields Up, and http://www.antionline.com. These should be used with caution and supervision so that crucial services are not "broken".)
21. Linux has developed sufficiently that not only does it have its UNIX-linked vulnerabilities and versions of software developed for its platforms that can have security weaknesses, but it also has Linux firewalls. IP-chaining is possible (like NATs). Any such computer should be reviewed per such standards for Linux and UNIX varieties, and have firewall software on it.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

22. Macintoshes and other Apple computers must use antivirus and "Net-barrier" or "DoorStop" firewall software for that platform. Platform-specific security should be applied.
23. OS/2 software firewalls include InJoy, SafeFire, and Zampa.
24. The Guest Account on NT servers and workstations should be disabled. Default IIS IUSR_<username> and IWAM_<username> accounts that are members of the Guest group should be either moved to a WWWUsers group created or configured to "authenticate from the network only".
25. NT workstations and Servers shall comply with MS C2 configuration, and preferably SANS "Securing NT" guidelines. An administrator account on an NT workstation (or server) shall not be allowed to have a blank password, or password with no expiration and unlimited logon attempts. Additional user management, registry configuration, and system lockdown information specific to these platforms are addressed in these documents.
26. Users should still backup sensitive or important files and configurations. A tape or "zip" drive is wise, or at minimum a secured user home directory on a network file server. If the registry is backed up, hide that folder or secure by NTFS file permissions if possible.
27. Sensitive information files such as password (.pwl) or financial data files (even Quicken, MS Money, and stock portfolio software) may be hidden to discourage hackers, or secured by NTFS file permissions, if possible. Copies of these saved to disk should be kept securely under lock and key available to no more than two supervisors.
28. If the system can authenticate to the host network, network shares and trust relationships should be reviewed for security. Shared folders should not be used if a network directly secured by group permissions is available.
29. Any remotely-hosted web servers or computers having personal web server / IIS / Front Page software should also meet the above criteria, and be secured against anonymous login.
30. Educate users on incident handling procedures. This should include contact call lists for IT security, Network Administration/Remote Access, and a form for describing a problem found either with the DSL system, or with an intrusion attempt. Contact with the DSL provider should be by the primary or secondary contact in the IT department, with a last-resort provision for a top supervisor or technical super-user to contact the DSL provider when IT cannot be reached. A follow-up report to IT should be made as soon as possible with all problem description and service call information included.
31. Consider separating any home office software, email, and connectivity to a separate computer from your personal PC. Not only will this be more compliant with most corporate acceptable use policies, it will protect your personal and financial information and correspondence from both corporate and hacker "prying eyes". A functional system, including software, can be built for under $1000, including "switch boxes" to share a printer, for example. (Home networks co-mingling personal and business computers should be thoroughly discussed with corporate IT security before implementing or attaching to a corporate network, due to the risks involved in both directions).
32. When not in use, turn the Internet connection or the computer off. While it sounds antithetical to the reason for having DSL, common sense dictates it is by far the best way to secure your connection from external intrusion.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

BIBLIOGRAPHY:

(1) Various. "Corporate Internet Security White Paper: Internet Security Issues" The DSL Forum. March 15, 2000. Updated March 24, 2000. URL: http://www.adsl.com/security_index.html (August 29, 2000)

(2) Various. "EasyStreet DSL Security Info or Is Your Computer a Zombie?" EasyStreet DSL. 2000. URL: http://support.easystreet.com/easydsl/dslsecurity.html (May 10, 2000).

(3) Various. "Work Place Security Extends to Employee's Homes?" EEye.com 1999. URL: http://www.eeye.com/database/columns/security/ds10091998.html. (July 10, 2000).

(4) Broughton, John, "Cable Modem and DSL Security Issues and Solutions" University of California at Berkeley, IST publication, April-May, 2000, URL: http://istpub.berkeley.edu:4201/bcc/Apr_May2000/sec.dsl.html (August 29, 2000)

(5) Paone, Joe, "DSL/Cable Security Guide, Part 1: Pitfalls of an always-on connection" SysOpt.com. January 19, 2000. URL: http://sysopt.earthweb.com/articles/cabdslsec-part1/index.html. (August 29, 2000). Good screen shots in Parts 2 and 3 (substitute in URL).

(6) Thompson, Jim, Originally on Internet.com, "DSL Brings High Speeds and Security Issues", Vermont Telecommunications Application Center (VTAC), Unknown. URL: http://www.vtac.org/businessapplications/dslsecurity.htm (August 29, 2000)

(7) Beckler, D., "System Tweaks" The DSL Zone. Unknown. URL: http://www.easystreet.com/~dbeckler/tweaks.html (August 29, 2000). 34 pages of excellent How-to information; faxes; detailed pages on security of DSL and cable modems. Must-read.

(8) Beckler, D., "Broadband Internet Security Basics" The DSL Zone. Unknown. URL: http://www.easystreet.com/~dbeckler/security.html (August 29, 2000). 4 pages, more on security of DSL and cable modems. . Links to antivirus, personal and network firewall sites.

(9) Wilson, Carol, "CheckPoint, Ramp Ink DSL Security Deal" Inter@ctive Week, ZDNet. April 19, 2000. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2551707,00.html. (August 29, 2000)

(10) Various, "Intel to Become First Company to Offer Advanced Internet Security Software from Network ICE with its High Speed DSL Modem" Network ICE. March 30, 2000. URL: http://www.networkice.com/html/march%5F30%5F%5F2000.html. (August 29, 2000).

(11) Various. "Windows 9x Network/DSL Security" StarNet. Unknown. URL: http://www.azsstarnet.com/service/dsl/security/fnps.html (August 29, 2000). Security with NetBEUI when you must have File and Print Sharing. Additional links off http://www.azstarnet.com/service/dsl show configuration of Intel and Cisco DSL modems.

(12) Tony@APLawrence, "DSL and Cable Modem Security" A.P. Lawrence. February 2000. URL: http://aplawrence.com/Security/dslsecure.shtml. (August 29, 2000). Excellent article with technical detail on vulnerabilities, based on SCO OSR5, but applicable. SSH info.

(13) Various, "DSL Reports: Secure-Me – Automated Security Testing" Net Access Corp. 2000. URL: http://www.secure-me.net August 29, 2000.

(14) Crowe, Elizabeth Powell, "Net Surfer Column: DSL Security: Is It a Problem? Yes and No" Computer User, November 23, 1999 URL: A set of links beginning at: http://www.computeruser.com/magazine/national/1722/nets1722.html (August 29, 2000).

(15) Aspinwall, Jim, "Prying Eyes: Is your always-on connection safe?" Computer User, January 25, 2000 URL: http://www.computeruser.com/magazine/national/1802/covr1802.html (August 29, 2000) A

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

set a links for the article beginning at that URL. Final link is to a comparison chart of Personal Firewall products, "Do Personal Security Products Work?".
(16) Mitchell, Bradley "Computer Networking: DSL Crib Sheet" About.com , 2000. URL: http://compnetworking.about/com/compute/compnetworking/library/weekly/aa063000a.htm (August 29, 2000. A set of links for the article, beginning at that URL.
(17) Karve', Anita, "DSL Finds Its Killer App" Network Magazine. November 1, 1999. URL: http://www.networkmagazine.com/article/NMB20000426S0003 (August 29, 2000). Excellent article on VoDSL, and how DSL may become indispensable.
(18) Riggs, Brian, "DSL Suppliers Boost Security Features" CMP. December 20, 1999, URL: http://www.techweb.com/wire/story/TWHB19991220S0005 (August 29, 2000).
(19) Reiner, Dave "Do you have a fast Internet Connection? Are you being hacked or cracked right now?" About.com. February 29, 2000. URL: http://bismarck.about.com/citiestowns/midwestus/bismarck/library/weekly/aa022900a.htm (August 29, 2000)
(20) Hsaio, Aron "Focus on Linux: Workstation Security Primer #85" About.com. April 28, 2000 URL: http://linux.about.com/compute/library/weekly/aa042800c-al.htm (August 29, 2000).
(21) Wilmore, John D., , "DSL vs. Cable" BeyondInfinity . November 7, 1999. URL: http://beyondinfinity.net/dsl_vs.cable.htm (August 29, 2000)
(22) Various, "Security Tips for Windows, Linux,, NT, Novell" BeyondInfinity. Unknown. URL: http://www.beyondinfinity.net/opportunity.html (August 29, 2000)
(23) Various, "General Frequently Asked Questions" Flashcom.com Unknown. URL: http://www.flashcom.com/support/faqs.html (September 5, 2000).
(24) Various, "DSL Glossary" Flashcom.com. Unknown. URL: http://www.flashcom.com/support/glossary.html (September 5, 2000).

LATE ADDITIONS: "MUST-READS":
(25) Lane, Jim "Personal Broadband Services: DSL and ATM" Virata. URL: http://www.virata.com/pdf/virata_dsl2.pdf (September 6, 2000). 98 pages on xDSL.
(26) Day, Randy "Securing DSL" InfoSecurity Magazine. January 2000. URL: http://www.infosecuritymag.com/jan2000/broadband.htm (September 6, 2000). Discussion of bridging, routing, and PPPoA/PPPoE in moderate technical detail. IPSec is not discussed. (For more information, also see http://www.tuketu.com/dsl/xdsl.htm by Randy Day, with security part.)
(27) Paradyne (Foreword: Gage, Beth, Telechoice Inc.) "The DSL Sourcebook, 2nd Edition" 1997, Revised 1999. Paradyne Corporation. URL: http://www.paradyne.com/sourcebook_offer/sb_html.html (September 6, 2000). 111 pages.
(28) Various "Research: DSL" Network World Fusion online magazine/website, 2000. URL: http://www.nwfusion.com/dsl/ (September 6, 2000). Repository of DSL links and research.

Numerous other sites exist covering aspects of DSL functionality and security, as well as vendors and equipment sites. Many have excellent tutorials and FAQ pages. See Appendix A for a few well-rounded, additional background information and resource sites. The list is by no means exhaustive. See Appendix B for known specific DSL vulnerabilities.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

APPENDIX A:
BACKGROUND INFORMATION ON DSL: WELL-ROUNDED EXAMPLE SITES

Industry Standards Group: The DSL Forum:

(1) Various. "General Introduction to Copper Access Technologies" The DSL Forum. 1998. URL: http://www.adsl.com/general_tutorial.html (August 29, 2000).
(2) Various. "Technical Frequently Asked Questions" The DSL Forum. Updated September 1998. URL: http://www.adsl.com/tech_faqs.html (August 29, 2000).
(3) Various. "VDSL Frequently Asked Questions" The DSL Forum. Updated June 12, 1998 URL: http://www.adsl.com/vdsl_faq.html (August 29, 2000).
(4) Various. "Frequently Asked Questions" The DSL Forum.. Updated June, 1999. URL: http://www.adsl.com/faq.html (August 29, 2000).
(5) Various. "ADSL Tutorial" The DSL Forum. 2000. URL: http://www.adsl.com/adsl_tutorial.html (August 29, 2000).
(6) Various. "VDSL Tutorial" The DSL Forum. Early Draft. URL: http://www.adsl.com/vdsl_tutorial.html (August 29, 2000).
(7) Various. "Glossary" The DSL Forum. Updated April 25, 1997. URL: http://www.adsl.com/adsl_glossary.html (August 29, 2000).
(8) Various. "Technical Report: ADSL Forum System Reference Model " The DSL Forum. 1997. URL: http://www.adsl.com/adsl_reference_model.html (August 29, 2000).

There are also pages for a comprehensive linked list of vendors and DSL forum members.

Vendor Site for the Public: Efficient Networks (formerly FlowPoint):

(1) Various. "Types of DSL" Efficient Networks. 2000. URL: http://www.efficieint.com/tlc/dsltypes.html (August 29, 2000). Excellent comparison chart.
(2) Various. "Glossary" Efficient Networks. 2000. URL: http://www.efficient.com/tlc/glossa-c.html (August 29, 2000). 7 pages of Glossaries.
(3) Various. "What is DSL?" Efficient Networks. 2000. URL: http://www.efficient.com/tlc/whatdsl.html (August 29, 2000).
(4) Various. "History of DSL " Efficient Networks. 2000. URL: http://www.efficient.com/tlc/history.html (August 29, 2000).
(5) Various. "DSL Equipment" Efficient Networks. 2000. URL: http://www.efficient.com/tlc/equipment.html (August 29, 2000).
(6) Various. "Whitepapers" Efficient Networks. 2000. URL: http://www.efficient.com/tlc/whitepapers/ (August 29, 2000). A series of whitepapers about DSL, voice and data transmission, and VPN technology. Also see /tlc/appnotes.html.

Books:

Besides the book pages, and major online booksites (www.bookpool.com, www.amazon.com, www.alphacraze.com, www.a1books.com http://www.booksamillion.com/ , www.barnesandnoble.com, www.fatbrain.com, and the multi-site www.evenbetter.com book section, there is a website for DSL books: http://www.everythingdsl.com/books.html.

Note: You may need to search by type of DSL, e.g. , ADSL, VDSL, even xDSL.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

APPENDIX B:
SHORT LIST OF WELL-KNOWN PRODUCT-SPECIFIC VULNERABILITIES:

1. Burris, Chris, et al, "Re: FlowPoint DSL router vulnerability"
2. URL: http://www2.merton.ox.ac.uk/~security/bugtraq-199908/0154.html August 29, 2000. FlowPoint DSL Routers before v3.0.8 had Buffer Overflow/Denial of Service. Flowpoint is now called Efficient Networks.
3. Xforce, ISS, "ISS Security Alert Summary, April 15, 1999, Volume 3 Number 9". April 15, 2000. URL: http://xforce.iss.net/alerts/vol-3_num-9.php#default-flowpoint (August 28, 2000)
4. Microsoft Product Security, Malformed IPX Ping Packet Vulnerability: (Patch Available)" URL: http://www.securiteam.com/windowsntfocus/Malformed_IPX_Ping_Packet_vulnerability__Patch_available_.html August 5, 2000. Only if using a cable modem or DSL connection., with Windows 95, 98 or 98SE.
5. Siverly, Andrew R., Beyond-Security's Securiteam.com "Cayman DSL Router are not Password Protected" March 12, 2000 URL: http://www.securiteam.com/securitynews/Cayman_DSL_router_are_not_password_protected_by_default.html (August 29, 2000.) Used by SBC Communications.
6. Cassius@hushmail.com, Beyond-Security's Securiteam.com "Cayman 3220-H DSL Router Vulnerable to a DoS Long Username Password" May 7, 2000 URL: http://www.securiteam.com/exploits/Cayman_3220-H_DSL_Router_vulnerable_to_a_DoS__long_username_password_.html August 29, 2000.
7. Mitre CVE, "The Cayman 3220-H DSL router allows remote attackers to cause a denial of service via oversized ICMP echo (ping) requests." July 12, 2000. URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0418 (August 29, 2000)
8. Friedl, Stephen, Beyond-Security's Securiteam.com "Netopia DSL Router Vulnerability" May 13, 2000. URL: http://www.securiteam.com/exploits/Netopia_DSL_Router_Vulnerability.html August 29, 2000.
9. Padin, Ed (email to Security Focus) "Re: Linksys 4-port Router NAT/Firewall. August 25, 2000. URL: http://www.securityfocus.com/templates/archive.pike?list=82&mid=78532 . August 29, 2000. (UDP scan with nmap tool on Linksys router for RAS/PPOE on a Bell Atlantic DSL connection found it wide open.)
10. Temmingh, Roelof, et al, Beyond-Security's Securiteam.com "Default Passwords Sometimes Stay for Good" May 13, 2000. URL: http://www.securiteam.com/securitynews/Default_passwords_sometimes_stay_for_good.html July 7, 2000. A large list of default passwords, sorted by the different products.
11. Additional exploits, not specific to use of DSL connections, can be found by a search on DSL in the various vulnerability databases. Additionally, vendors may post alerts and remedies on their websites.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.