Global Information Assurance Certification Paper

Open File Shares: An Unexpected Business Risk
Jaime Carpenter
June 21, 2001

Over the past few days, well O.K. the last month, I have been stressed over what topic to write about for my GSEC practical. Many topics have come to mind. I have found that as I now focus on writing my practical my topic has finally crystallized into a topic that we are currently working through at my company: Open File Shares.

Background

The purpose of this report is to talk about the risk of open file shares to a business, reiterate the importance of a security policy on file sharing, show you some tools to use to assess the security posture of your network, and finally outline basic steps to take to secure your network.

In this report an open file share or network share is defined as either a Peer-to-Peer or Client/Server NetBIOS/SMB type of shared folder or directory of files that has been improperly secured or not secured at all. At a minimum, the open file share would allow unintended read access to information stored in the shared directory. The worst case of an open file share allows full read/write access to information stored in the shared directory.

The Risk

File sharing in general is seen as a major benefit of networking. The risk arises when a PC, workstation or server is improperly configured and data is exposed. Imagine a manager of a payroll department who saves a spreadsheet containing information about this year's raises on the hard drive of his PC only to be called in to the CEO's office later to explain how the information was leaked! This is an example of how confidentiality can be compromised and often the owner of the information has no idea that the data is at risk.

Unexpected exposure of confidential information is not the only risk. Data integrity and availability can be affected by the spread of viruses like Funlove. In my company we have been hit hard by the Funlove virus, which can propagate itself via open file shares. "Periodically the virus scans any network shares with write access, and infects any EXE, SCR and OCX files on any shared network drives."(1) Our help desk and workstation support team have been fighting the battle of eradication of this virus for months. Each instance of the virus infection requires hours of recovery work and sometimes a complete reload of the desktop OS. Since January 1, 2001, there have been 50 Funlove infections reported to our help desk.

A recent eWeek article claims that the number 1 threat to security today is from internal sources rather than external sources. According to the respondents of a survey quoted in the article, "57 percent said the breaches were caused by inside users accessing unauthorized resources"(2). Open file shares are certainly one way this type of unauthorized access can occur.

The need for a good Security Policy

Because of these risks, it is paramount that you establish a security policy on file sharing. In the article "Best Practices in Network Security"(3), Fredrick M. Avolio says that it is important to establish a root security policy that includes:

- Root security policy overview
- Security architecture guide
- Incident-response procedures
- Acceptable use policies
- System admin procedures
- Other management procedures (data classification and storage)

The Root security policy overview should contain the overall security philosophy of your company. It is the basis or foundation on which the other policies are derived. It is essential that you have the commitment of senior management to support your security policies because "if senior management is not committed to information security, your best efforts are wasted"(3).

The security architecture guide needs to show how file sharing is used in your company. A small company may implement a peer-to-peer technology while a large company may have a mix of peer-to-peer and client/server or just client/server. Whichever suites your need, it is important to spell it out clearly in your policy. File sharing will also need to be covered in the acceptable use policies, system admin procedures and other management procedures (like data classification and storage).

In your policies you must also clearly spell out the consequences of a policy violation. It may be only a reprimand or it could lead to termination of employment. It is a good idea to check with your human resources and/or legal departments on the language used in your policies.

Tools

There are three network scanning tools that I have chosen to demonstrate in this paper.

- **SMBScanner 1.0** available at: http://hispahack.ccc.de/smb.htm
- **Legion v2.1** available at: http://packetstorm.securify.com/groups/rhino9/
- **ISS Internet Scanner** available at: https://www.iss.net/cgi-bin/download/evaluation/evaluation-select.cgi

Test Lab Setup

Here is the test lab setup I will use to demonstrate the scanning tools. (This is not a recommended security setup, just an example)

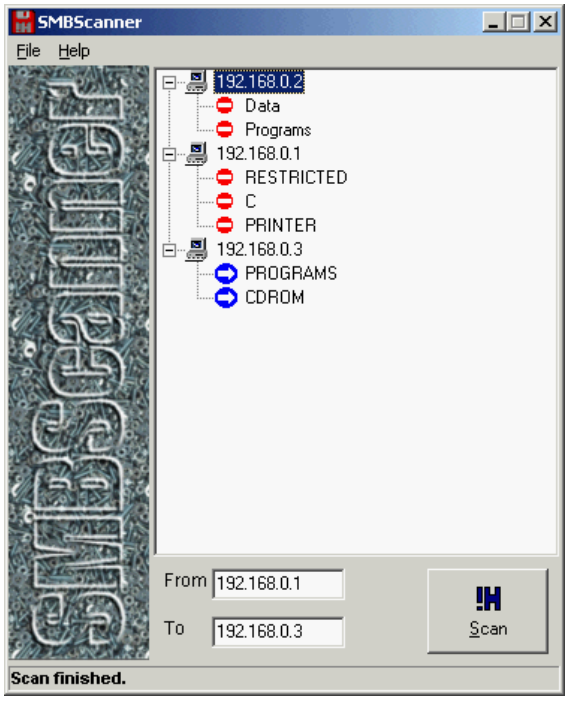
IP Address	Name	Operating System	Share Name	Access Type
192.168.0.1	WINKIN	Windows 98	C	Password/Full
			RESTRICTED	Password/Full
			PRINTER	Full
			HIDDEN$	Full
192.168.0.2	BLINKIN	Windows 2000 Pro	ADMIN$	Admin
			C$	Admin
			DATA	Everyone/Full
			PROGRAMS	Everyone/Read
192.168.0.3	NOD	Windows 95	PROGRAMS	Read
			CDROM	Read

SMBScanner 1.0

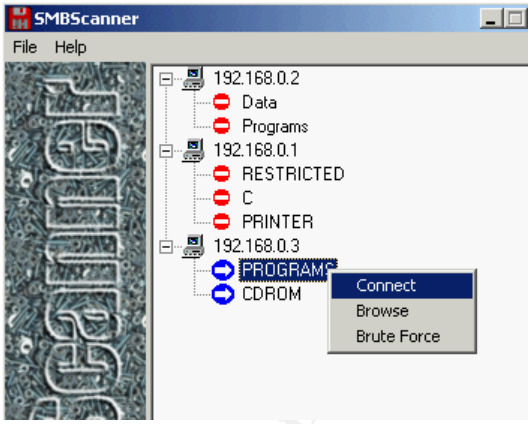
The first tool is SMBScanner 1.0. Although I don't understand Spanish, the translated web page states: "SmbScanner does not have limitation and it is not necessary to pay for use rights.")(4). I understood that to mean "Free".

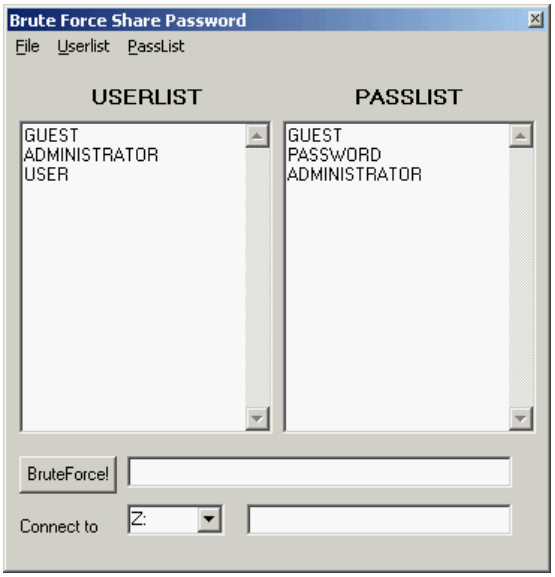
Setup was easy enough. I downloaded the zip file, extracted the files to a directory and I was ready to go.

Running the program displays a dialog that allows you to enter an IP address range to scan. Enter the IP address range to scan and click the Scan button. When the scan completes you will be given a tree view of hosts where file shares were found. You will notice that this tool does not display hidden shares (a share with a $ sign at the end of the name). There is also no option to export or save a list of the scan results.



Once you have the list of hosts, you can right click on a share and you will be given the choice to connect, browse or brute force the share.





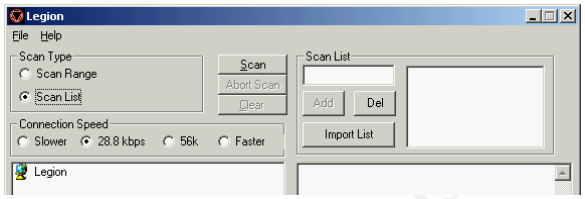
The brute force option uses a userlist file and a passlist file to attack a password protected share. There is a sample of each included with the program. They are text files named user.dat and pass.dat. You can create your own files or modify the ones provided. However you will have to use a text editor to edit the files, because the brute force dialog will not allow editing even though it appears that it will.

Legion v2.1

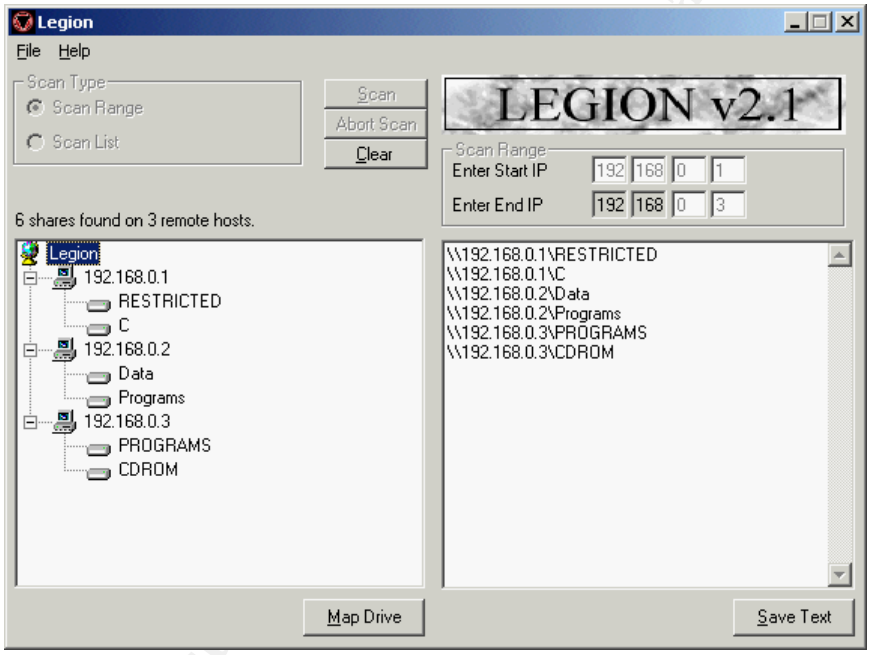
The next tool is Legion v2.1. This is a very well known scanning tool. Legion v2.1 was mentioned in the SANS Security Essentials class I attended, in the book "Hacking Exposed: Network Security Secrets and Solutions"(5) and in one of my searches there was even a link to a tutorial for Legion v2.1 on a hackers website!(6)

After downloading the zip file, just extract the setup files and run setup.exe to install. Legion is shareware and if you use the program beyond the 14-day evaluation period you are expected to pay $25 for continued use.

You have a few more options with Legion v2.1 beyond just IP address range scanning. The startup dialog gives you options for Scan Type and Connection Speed. The Scan Type allows you to use a range or a predefined list of IP addresses. Connection Speed allows you to adjust what type of line speed you have on your network connection.



I chose to use the Scan Range option. Enter a range of IP addresses then click Scan (you are limited to scanning only 64 subnets at a time). When the scan is complete, you will be given a dialog that shows a tree view of the hosts where shares were found. A nice feature is the ability to save a listing of shares to a text file, which is very useful for reporting. Legion v2.1 also does not display hidden shares.



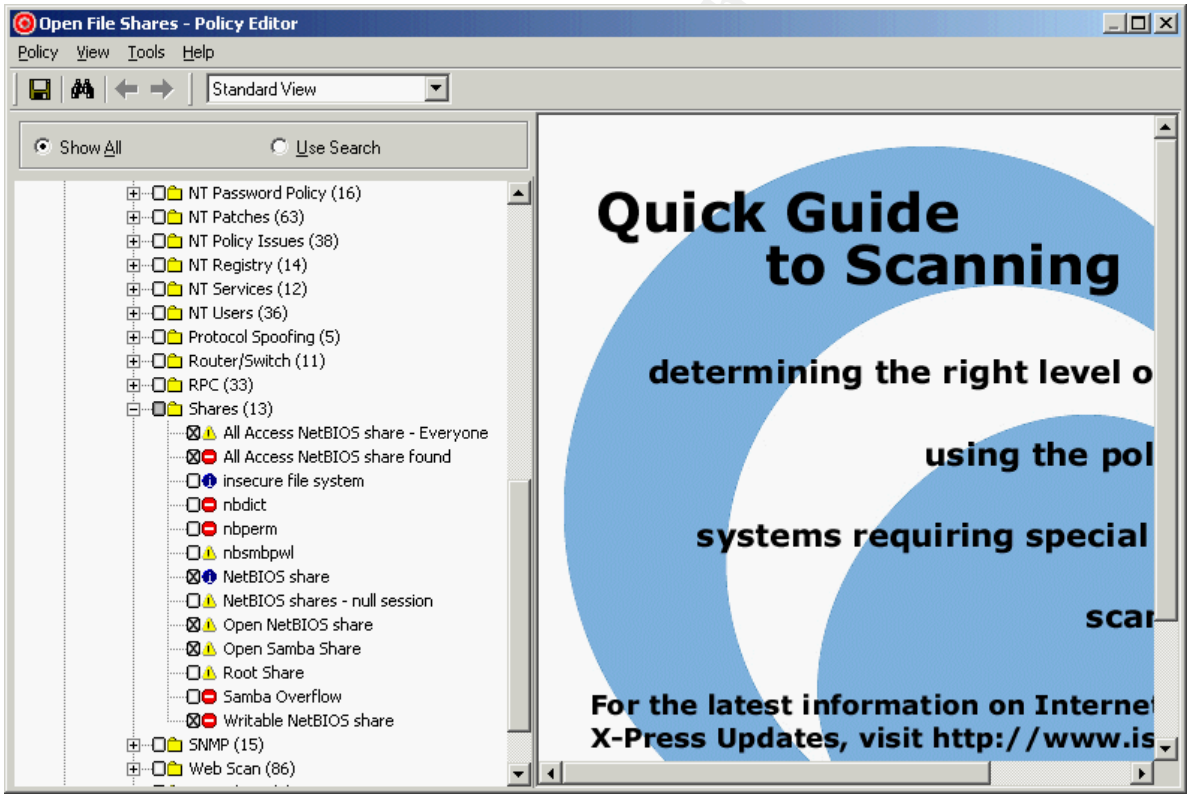
ISS Internet Scanner

The most powerful scanning tool of those covered in this report is Internet Security Systems' Internet Scanner. This is a full-featured vulnerability and threat assessment tool. You can download a trial copy but you will be limited on both time and features. Internet Scanner uses an expiring key to limit the number of addresses that you may scan and also ensure that you have properly licensed the product.

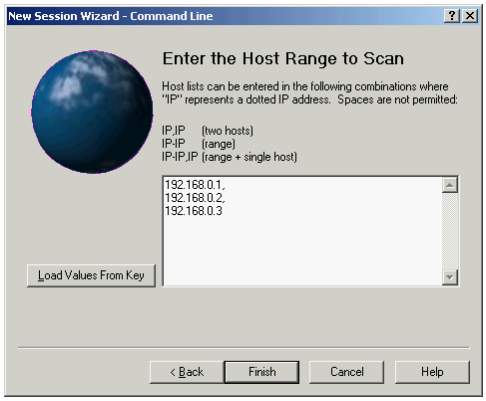
ISS Internet Scanner works by scanning a range of IP addresses using policies, which are made up of exploits or checks, to assess the vulnerabilities of the host(s) found. You can create your own policies based on your environment. Use caution when creating your own policies because Internet Scanner can also perform denial of service checks that will in fact cause a denial of service on a host.

After you have installed the program, you will need to create a policy to use. For this report, I created a policy called Open Shares and included only a few of the checks available for shares. To create the policy, follow these steps:

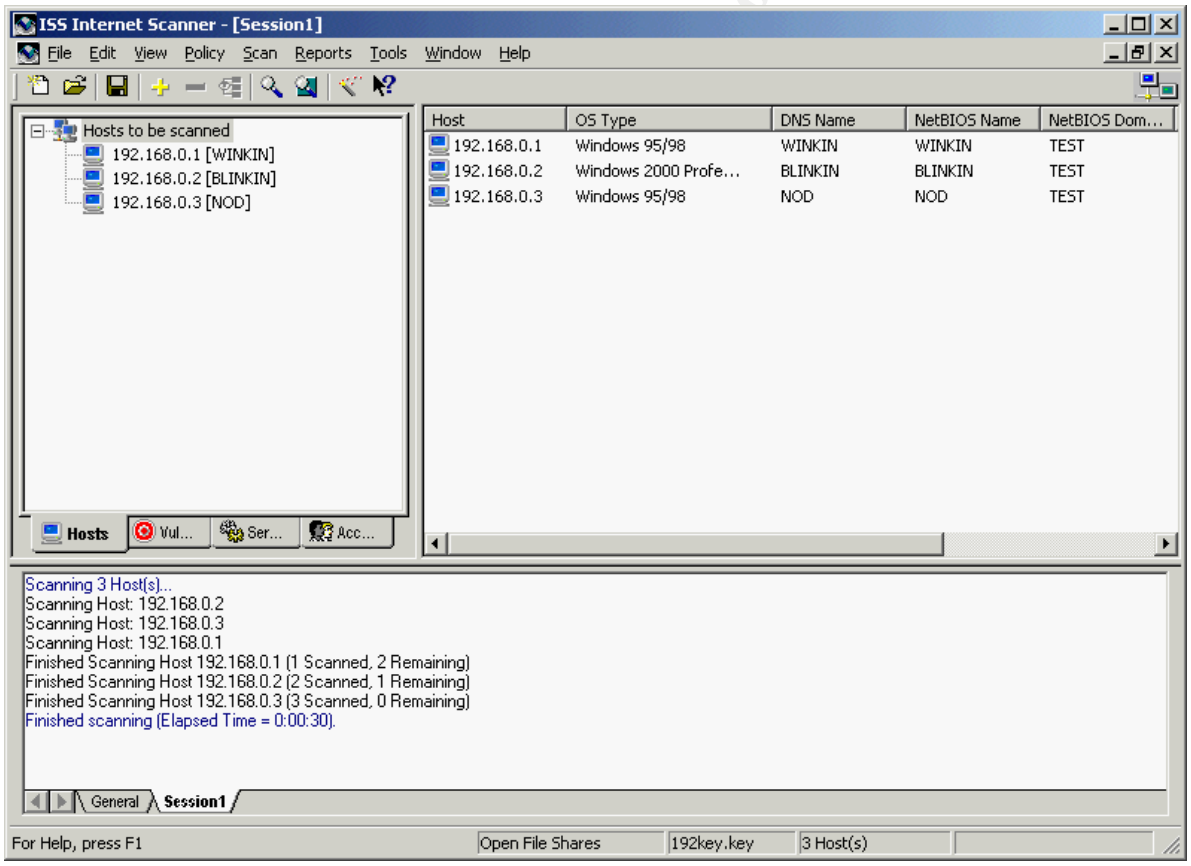
1. Choose Policy on the Internet Scanner menu
2. Choose New (this will step you through a wizard like creation tool)
3. Select the "Blank" policy as the base for your new policy
4. Give the policy a name: Open File Shares
5. When the policy editor starts choose Vulnerabilities, Standard, Shares
6. Enable the checks for
    a. All Access NetBIOS share – Everyone
    b. All Access NetBIOS share found
    c. NetBIOS share
    d. Open NetBIOS share
    e. Open Samba Share
    f. Writable NetBIOS Share



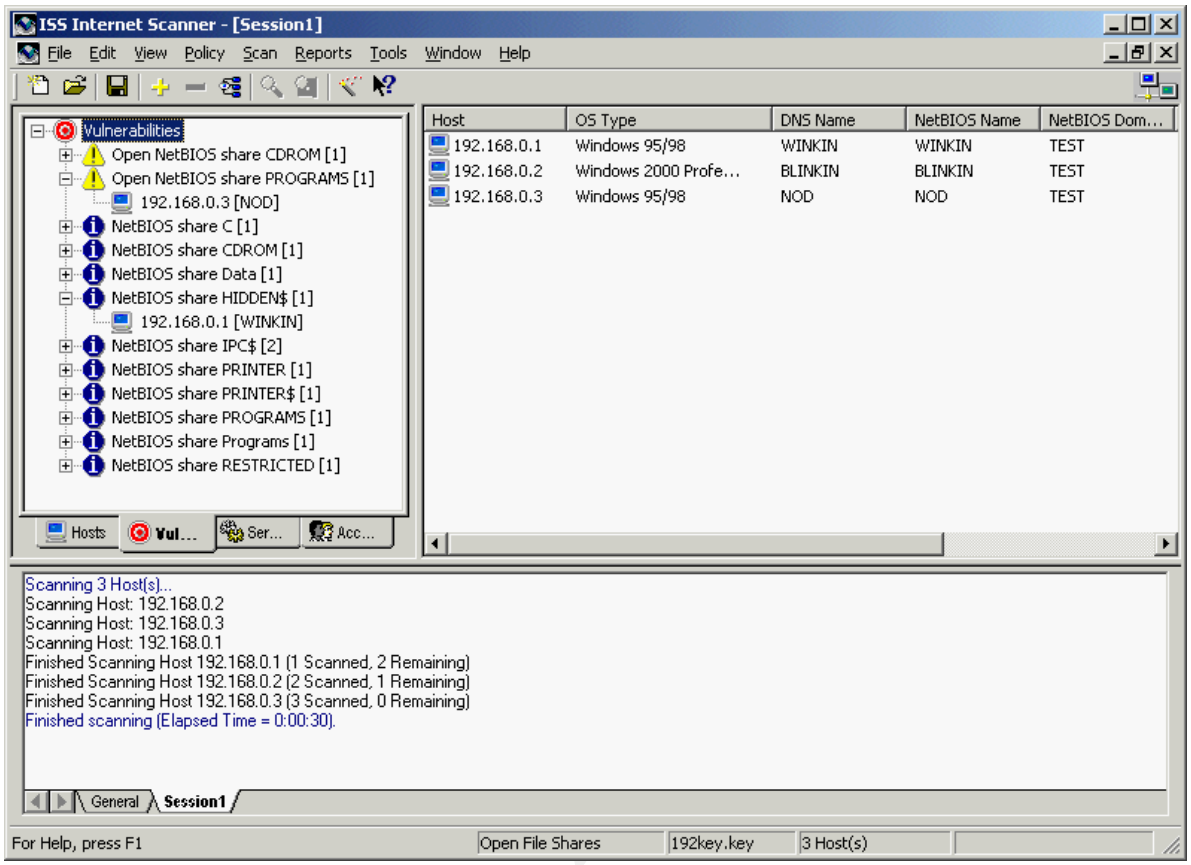
After you have created your policy, you will be ready to perform your scan. Choose File, New Session from the menu. Select your newly created Open File Shares policy, add a session comment, then specify the hosts. There are three options to use to specify the hosts: Use Host File, Use Command Line Facility or Ping valid hosts in your key. For simplicity I chose Use Command Line Facility and entered the IP addresses of the Test Lab hosts.



After you enter in the IP addresses to scan and click Finish your session will be defined. Now from the ISS Internet Scanner menu choose Scan, Scan Now. When the scan has completed you will see a screen much like the one below.



On the left of the screen there are 4 tabs: Hosts, Vulnerabilities, Services and Accounts. Click on the Vulnerabilities tab and expand the tree view. ISS Internet Scanner did find the hidden share HIDDEN$, but it does not show the Windows 2000 Professional administrative shares ADMIN$ and C$



ISS Internet scanner also has predefined reports that show varying levels of detail. There are reports for Line Management that contain the vulnerabilities found and a brief description and there are Technician reports that show the vulnerabilities along with fix information.

Basic steps to take to secure your network

Now that you have seen an overview of scanning tools, you are ready to secure your network. Remember to get permission from your management, in writing, BEFORE you use any scanning tools on your network. If your company uses a change management system, you may need to document your activity so that system administrators will be on alert and expect the scan.

Here are some basic steps to take:

1. Get permission to perform your security scan
2. Document the planned scanning activity
3. Select your target IP address range or ranges to scan
4. Scan the target IP addresses
5. Verify your results against your security policy (the tools demonstrated would show if shares exist, but you will need to confirm whether or not they are properly secured)

6. Report your findings to the appropriate system admin personnel or to management (unless you are directly responsible for closing any vulnerabilities found)
7. Get an expected closure date for any vulnerabilities found (unless you are directly responsible for closing any vulnerabilities found)
8. Close any vulnerabilities found by disabling file sharing, adding passwords or other access controls
9. Rescan to ensure that the vulnerabilities have been closed

Other tools

Symantec NetRecon information at:
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=46&PID=6277422

PGP CyberCop ASaP available at:
http://www.mcafeeasap.com/content/cybercop_asap/default.asp

SMB Scanner Pro available at: http://www.tzsoftware.com/software/smbscanpro/index.shtml

DumpSec (formerly known as DumpAcl) available at: http://www.somarsoft.com/

References

(3) Avolio, Frederick M. "Best Practices in Network Security". Network Computing. March 20, 2000.
URL: http://www.nwc.com/1105/1105f2.html

Daviel, Andrew. "Network Security"
URL: http://vancouver-webpages.com/security/index.html

"File And Printer Sharing And The Internet"
URL: http://lockdown.batcave.net/issues/index.html

(2) Fisher, Dennis. "Insiders are main computer security threat". eWeek. June 20, 2001.
URL: http://www.zdnet.com/eweek/stories/general/0,11011,2777325,00.html

Greenberg, Binyamin. "Implementing a Secure Network". Nightfall Security Solutions, LLC.
URL: http://nightfallsecurity.com/whitepapers/securenetwork.html

(6) kM. "Lesson 3". www.hackersclub.com
URL: http://www.hackersclub.com/km/newbies/lesson3/index2.html

Kossuth, Joanne. "A Review of Peer-to-Peer Network Insecurities in Business Applications: Should you take the Risk". February 17, 2001.

URL: http://www.sans.org/infosecFAQ/win/review.htm

(1) McAfee. Virus Information Library Profile.
URL: http://vil.nai.com/vil/virusChar.asp?virus_k=10419

(5) McClure, Stuart, Joel Scambray and George Kurtz. Hacking Exposed: Network Security Secrets & Solutions. Berkeley: Osborne/McGraw-Hill, 1999. 63.

(4) Translated version of http://hispahack/ccc/de/smb.htm. Google.
URL:
http://translate.google.com/translate?hl=en&sl=es&u=http://hispahack.ccc.de/smb.htm&prev=/search%3Fq%3Dsmb%2Bscanner%26hl%3Den%26safe%3Doff