# Global Information Assurance Certification Paper

**My Personal Firewall Failed, What Do I Do Now**
Archie Alimagno
November 14, 2000

**Introduction**

The proliferation of ISDN, DSL and Cable modems have precipitated the use of personal firewalls to provide a level of security that at one time only existed in corporate environments. Additionally, the publication, dissemination, and headlines of successful Internet attacks have provided the corporations, small businesses and home users with a view of how vulnerable they are when networked and especially when linked to the Internet. In a connected environment, the weakest link is the user and their workstation. As of this writing, even Microsoft's extensive resources have been unable to stop penetration of their organization. Therefore, the fundamental examination and hardening of your system is essential to protecting your employer's as well as your assets.

**Objective**

- To know the state of the operating system (OS), in this particular case an NT 4.0 workstation, when the personal firewall on that system fails or is turned off accidentally.
- To harden the OS and the browser to limit the vulnerability inherent with the system and Internet browsing.
- To limit access to trusted or authenticated users to the system.

**Hardware/Software**

The following system was utilized in this write up (practical).

| Hardware Setup | Software Setup |
|---|---|
| 433 Mhz Celeron Processor | OS: NT 4.0 Workstation |
| 256 MB RAM | SP6a with all applicable hotfixes |
| 8 MB video (800X600 res) Sis620P4 | Internet Explorer 5.5.4134.0600 |
| C: and D: HD (Maxtor 13.6 Gig) NTFS | IE 5.5 patched OS specific fixes from MS |
| 42X CD ROM, Zip 250 and 100 | MS Office 2000 w/SP1 |
| SMC EZ Card PCI (Nic) | Adobe Acrobat, Ntreskit, VPN client & Misc. Sec. Apps |
| Com21 Cable Modem (@home service) | Firewall by Zonelabs |

**System Hardening**

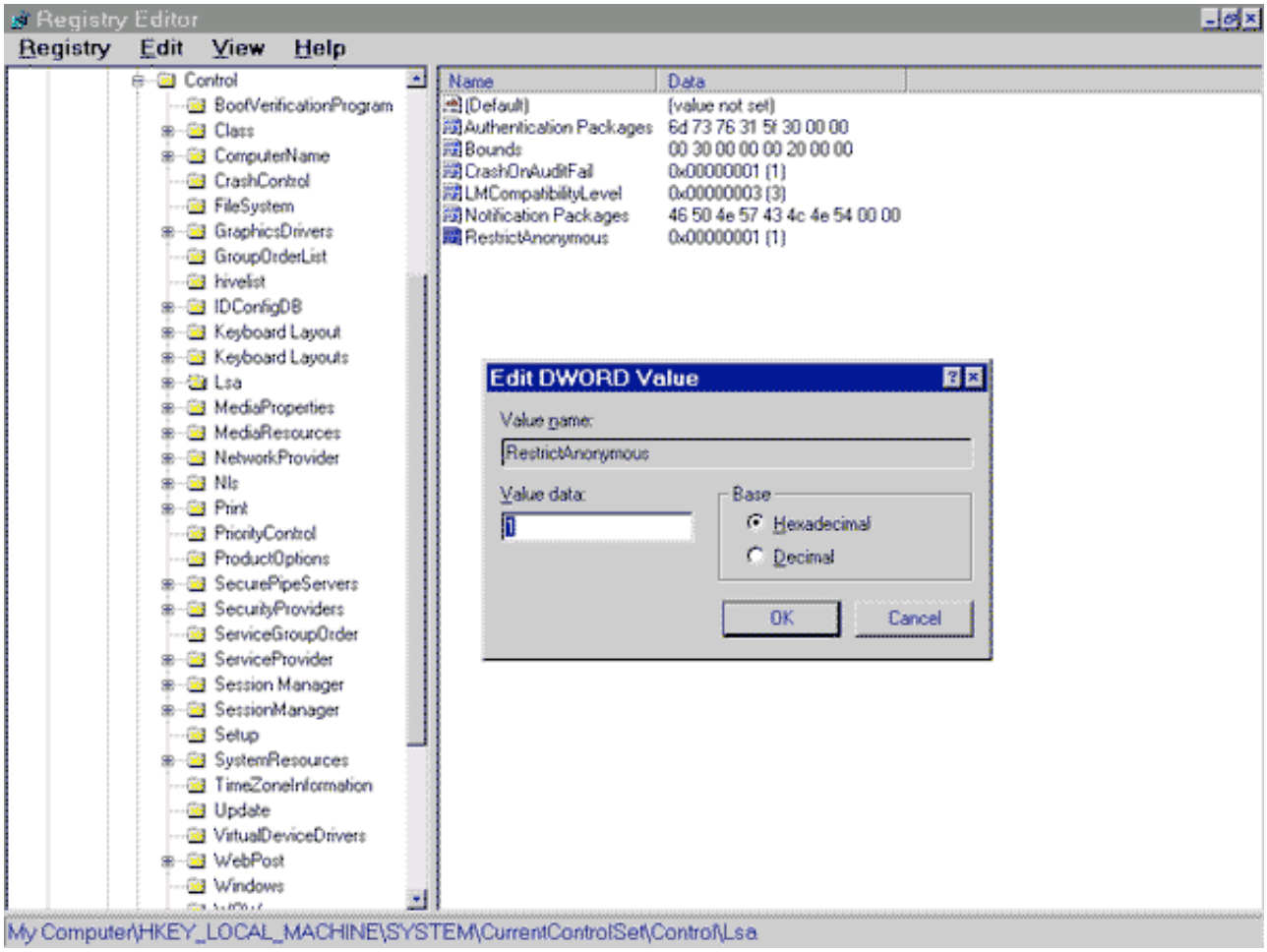
Assumptions: The reader has a technical background or is comfortable with manipulating and configuring various system settings via the system registry, control panel, or command prompt. As always, when testing the system, backup working configuration (e.g., registry, *.ini and other critical file settings for your specific host).

Operating System (NT 4.0 Workstation w/SP6a): First and foremost protect the RestrictAnonymous key in your registry. For the sake of learning, do everything manually, that is use the Regedit/Regedt32, to solidify your knowledge when setting the various keys outlined in this practical instead of using some type of utility that may do it for you (i.e. Ntreskit - C2 config.exe, TweakIU or X-teq). It also provides you with invaluable practice before implementing some of the techniques that you will learn on this practical.

Add the following:

Data Type: Reg_Dword
Value Name: RestrictAnonymous
Value: 1

Once you have set this key, you will have limited the type of attacks that can be perpetrated to your system. This one key is a gold mine for attackers. For the sake of space and time, the subsequent recommendations for hardening your system(s) will not have the screenshot of the actual changes.




Please note some of the other settings in this hive that you should consider adding for added security:

- Set CrashOnAuditFail (Reg_Dword=1)
- Set LMCompatibility (Reg_Dword=3)

Services: Run Winmsd.exe to determine the state of the system; all other services are set to manual. Set server, workstation, tcp/ip netbios helper and computer browser to MANUAL. Again, review all services that are started and limit it to those that are required by your system and applications. While it is not covered in this practical, reviewing the services area for IIS is critical. One should consider a bastion host (hardened OS with minimal services and firewall) when putting it on the DMZ as a server.

Microsoft Diagnostics Report (Services-Summary)

| | | |
|---|---|---|
| DHCP Client (TDI) | Running | Automatic |
| EventLog (Event log) | Running | Automatic |
| TrueVector Basic Logging Client | Running | Automatic |
| Remote Procedure Call (RPC) | Running | Automatic |
| TrueVector Internet Monitor | Running | Automatic |

Bindings: All adapters for WINS client should be disabled. That means that netbios interface, server and workstation are unbound from the adapter. You can find these settings in control panel. Click on network (it is the last tab). Go to adapters and check WINS setting and disable the items noted above. Steve Gibson provides a very detailed and lengthy explanation of this procedure (http://grc.com/su-rebindingnt.htm).

You should also remove the host from the network browse list. If your system can't be browsed, then it would be harder for an attacker to assess your system for weaknesses. Open up your registry and go to:

HKLM\currentcontrolset\services\lanmanserver\parameters\

Add the following:

Data Type: Reg_Dword
Value Name: Hidden
Value: 1

Internet Explorer 5.5 Browser
Next in our step - protect our browser. While some would argue that only the purest would disable the Active X and Java functionality. However, it must be considered especially if you are a security professional that will conduct research on hacker techniques, their tools and go into their Internet sites.

To highlight the point that it is extremely easy to execute code that can infiltrate and damage your system through your browser, you can review Georgi Guninski's advisory at http://guninski.com. Once you examine this information, you will be surprised to find how open your system can be through your browser. You would be a firm believer that in customizing your Internet security setting.

Here are the steps to take in customizing your Internet Security Settings:

- Start IE 5.5, go to the Tools and drill down to Internet Options. If you are a keyboard person, use the Alt T, then O.
- Click on Security Tab (make sure you are on the Internet Zone), and then click on Custom Level.
- Disable the first 3 ActiveX controls and plug-ins, make the next one administrator approved, and then enable ActiveX controls marked safe for scripting.
- Microsoft VM - Java Permissions, disable.
- Access data sources across domains, disable
- Active Scripting, disable
- Scripting of Java applets, disable
- User Authentication, prompt user for user name and password
- Click OK after all the changes has been completed.

**Testing Security Measures**

If you can't validate your results, then all the work that you have done seems unfulfilling. However, having hard data provides confidence and assurance that at this time, your system is relatively secure and certainly much more so than the average user.

All testing have been conducted locally and remotely while the ZoneAlarm personal firewall is turned-off. Additionally, I have also had colleagues to remotely assess my system using their favorite security and footprinting tools. Finally, online services from GRC.com and Secure-me.net have scanning services to add the final unbiased information security assessment on the target system.

SuperScan (version 2.06 - See Appendix for screen shot): This is an extremely fast tool to review what ports are open (and it's free). The program is very elegant and simple in its design yet very powerful. The net result is that the scanner did not show any open ports. However, it did resolve the IP address.

Cerberus Information Security (version 5.0.02 - See Appendix for screen shot): Another useful tool to determine vulnerabilities. It provides another simple and elegant approach to system scanning of over 300 vulnerabilities. The results were similar; no vulnerabilities showed up.

SolarWinds 2000 (IP Browser - See Appendix for screen shot): The entire SolarWinds suite is a beautiful tool (somewhat expensive though). To check snmp vulnerability, I use the IP Browser. It provides a graphic interface that is easy to read and use. As an alternative, you may use the NT resource kit for enumerating tools that you should get familiar with. This is a wonderful resource and you should have it in your toolkit.

ISS Internet Scanner (version 6.1 - See Appendix for screen shot): A powerful commercial scanning tool; again expensive for a regular user, but valuable in the hands of the information security professional. This scanner adds the functionality of configuring the scanner. Various types of reports can be built to your system (from denial of service attacks to accounts and service information as well as many others). It can be utilized to examine how policies are set, what to look for and how to correct non-compliant items via a technician report.

L0phtCrack (version 2.5): To assist in determining password strength, run this tool against your SAM. Your passwords should be strong so that it runs for days (if not months depending on your security policy) before your password is revealed. However, if your SAM has been dumped to a remote computer, then it will just take time before your password is cracked. The lessons learned here are protect your SAM, backup your system and safeguard your registry settings.

**Maximizing Performance**

I have now hardened my system. My firewall is up. Why is my system slower? Did I complete the security measures only to find out that I now have a slower system? Can't I have both? Yes you can.

As a fanatic to system efficiency, I would hesitate to harden my system if the overhead is too high (requiring better and faster hardware) or the performance hit is excessive. To compensate for the minor degradation, please examine the performance tweaks outlined below. The schema will be to modify the registry and general system settings. Since you (hopefully) modified the registry already, the information will be succinct. It will show the hive and the key to add or modify. Let's get started.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem
Data Type: Reg_Dword
Value Name: NtfsDisableLastAccessUpdate
Value: 1

If you have a large number of directories this setting will allow you better performance when using explorer or DIR command, etc.

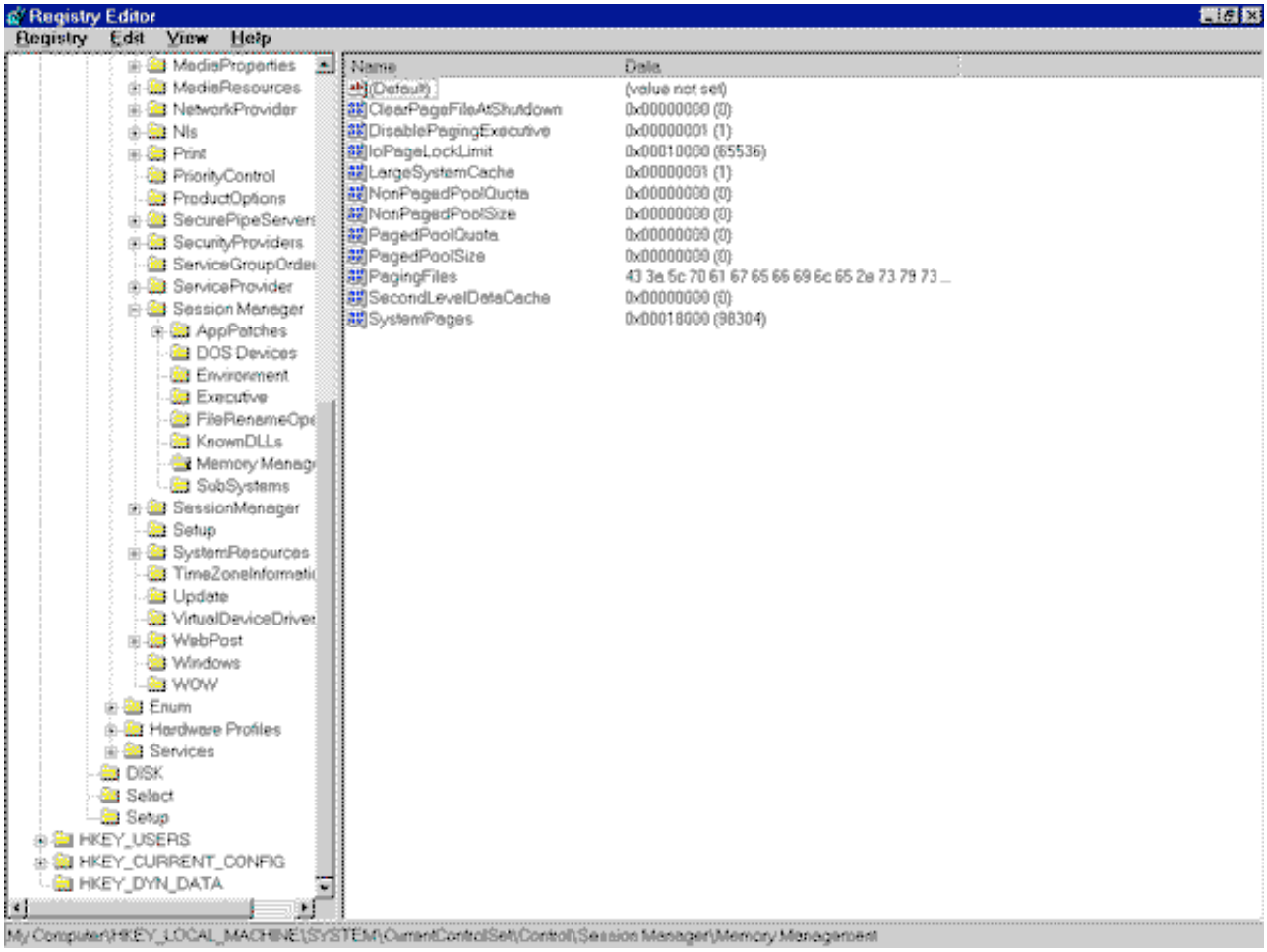
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management
Data Type: Reg_Dword
Value Name: SecondLevelDataCache
Value: 0

If you have a direct-mapped L2 cache, which is not properly detected, set the value in decimal. For example, if you have 512K cache, set the entry to 512 in decimal (Hexadecimal 200).

If you have lots of memory (over 256Mb or more), set DisablePagingExecutive, then type REG_DWORD, to 1. This will allow drivers and the kernel code to be kept in memory. The default is 0 which pages drivers and kernel code when needed. Since you are still in this area you may consider the following as well:

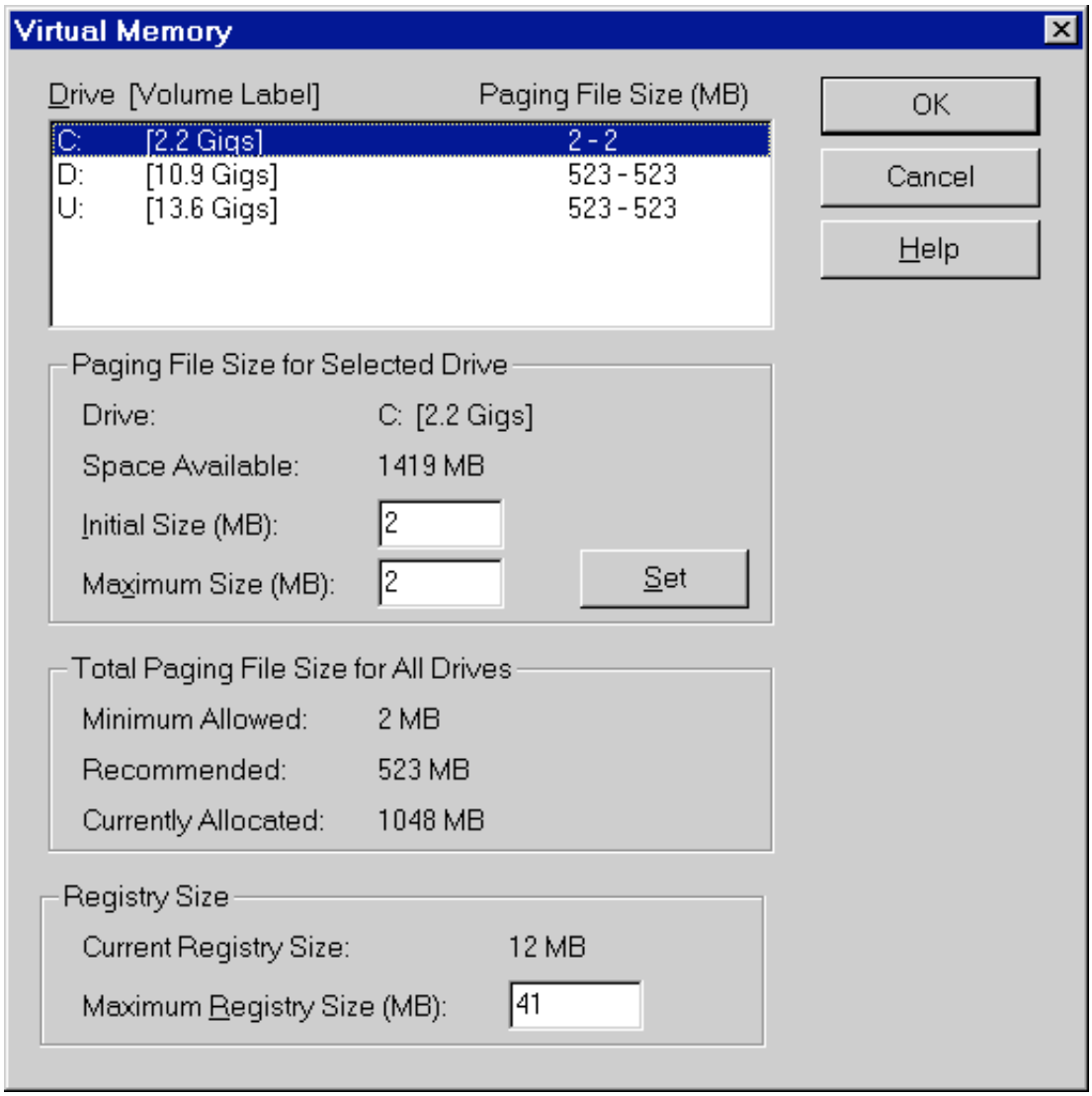
ClearPageFileAtShutdown and set REG_DWORD, to 1. This will clear your page file. However it will add anywhere from 15 to over 60 seconds to clear your pagefile.

IoPageLockLimit and set Reg_Dword to 65536 FOR computers with 256MB of memory or more. It will create a problem if you set it for this level if your memory is not 256MB or more. For 128+ MB, set it to 16384.




To ensure that your memory utilization is optimized, make sure that your virtual memory setting (right mouse click on my computer, go to properties, then to performance tab) is the set to the amount of memory that you have (i.e. For 128 MB of memory set size to 128 initial and 128 maximum). I would also put this in your D:\ drive or your fastest drive.

See my settings as an example:




**Conclusion**

While the average user may not undertake the painstaking review of how their system is setup; Information Security Professionals or those who want to get into this field, must review all facets of configuration carefully. Systems can be well protected and optimize to perform very well even with a hardened system. While the information provided herein concentrates on the cable modem user (typically home or telecommuter), most of the recommendation can be implemented on a corporate setting.

From my vantage point as an information security trainer (and also setting setup standards on workstations and servers), the weakest link seems to be the users in almost 100 percent of the cases that I have reviewed. Therefore, after providing them with systems that are secure it is up to you and I to educate, train and retrain staff to ensure that information security is always on their mind when conducting business or casually browsing the web.

**References (Internet links)**

Microsoft Corporation. "Windows NT Configuration Checklist" Last Updated April 5, 2000
URL: http://www.microsoft.com/TechNet/security/c2config.asp

Gibson, Steve. "Shields Up - Internet Connection Security for Windows Users" Updated-NA
URL: http://grc.com/su-rebindingnt.htm

Team DSL Reports. "Secure-me.net" Last Updated November 1, 1999
URL: http://www.secure-me.net/

Guninski, Georgi. "IE 5.5/Outlook java security vulnerability - reading arbitrary files and URLs" Advisory #24, 2000
URL: http://guninski.com/javacodebase1-desc.html

Cooper, Russ. "How to Survive A Hack Attack" November 23, 1998
http://www.zdnet.com/windows/stories/main/0,4728,2168256,00.html

Farmer, Dan. "Shall We Dust Moscow?" December 18, 1996
http://www.fish.com/survey/introduction.html

Broughton, John. "Cable Modem and DSL Security Issues and Solutions" April 2000
http://istpub.berkeley.edu:4201/bcc/Apr_May2000/sec.dsl.html

**References (Publications):**

Norhtcutt, Stephen. "Network Intrusion Detection, An Analyst Handbook" June 1999
Published by New Riders

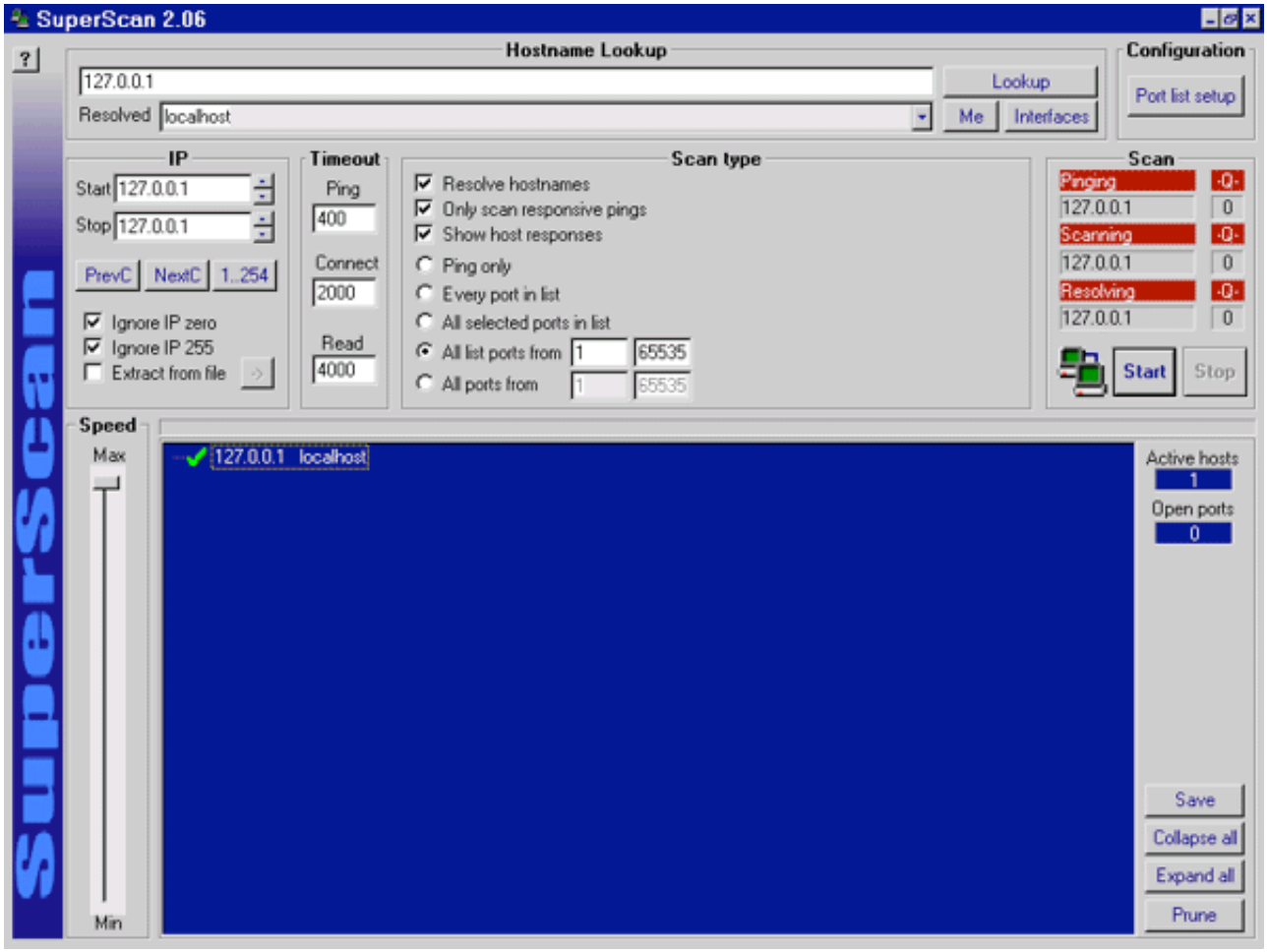
Scambray, Joel and McClure, Stewart and Kurtz, George "Hacking Exposed" 2nd Edition
October 2000 Published by McGraw Hill

Anonymous. "Maximum Security 2nd Edition" September 1998
Published by Sams

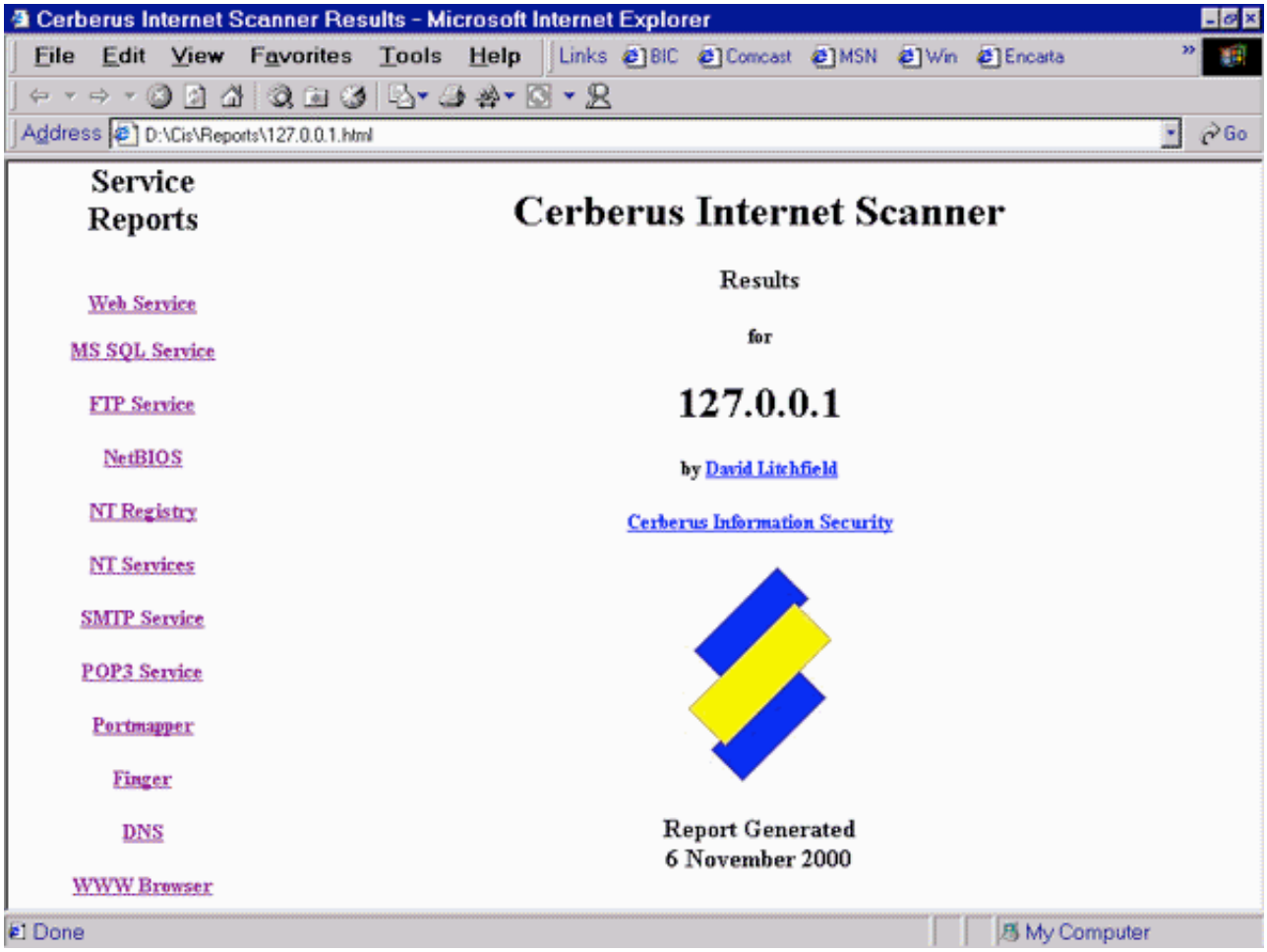
Husted, Robert and Kuslich, JJ. "Server-Side JavaScript" 1998
Published by Addison-Wesley

McClean, Ian. "Windows 2000 Security - Little Black Book" 2000
Published by Coriolis

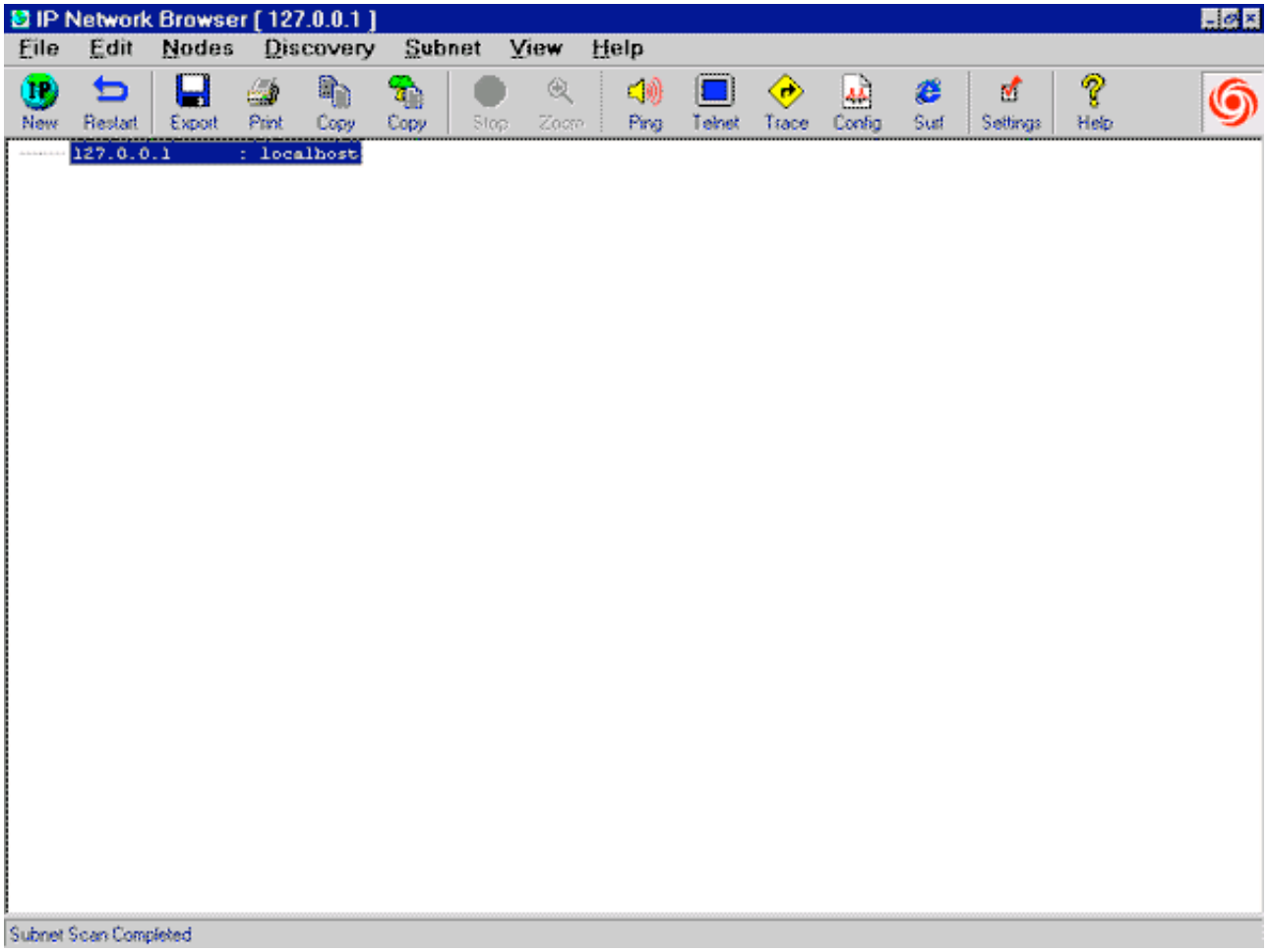
**Appendix**




SuperScan Report




CIS Report




IP Network Browser from SolarWinds 2000

**Network Vulnerability Assessment Report**
Sorted by Vulnerability Severity (11/05/2000)

**Report Description**

This report displays the organization's susceptibility to attack in relation to its policy and vulnerability conditions. Specifically, this report identifies network vulnerabilities and suggested corrective action. Vulnerabilities are classified as high, medium and low. High-risk vulnerabilities are those, which provide unauthorized access to the host, and possibly, the network. Medium risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploitation of higher risk vulnerabilities. Low risk vulnerabilities are those, which provide access to sensitive, yet non-lethal, network data. It is recommended that all high-risk vulnerabilities be corrected as soon as possible.

**Session Name:** Session1
**Session ID:** 16
**File Name:** Session1_001105
**Template:** L1 Inventory
**Comment:** Termination
**Status:** Finished

**Scan Summary Information**
Hosts Scanned: 1 Scan Start: Scan End: 2000/11/05 22:07:53
Hosts Active: 1 Elapsed: 2000/11/05 22:10:21
Hosts Inactive: 00:02:28

Vulnerability Name Severity

Description:

Fix
IP Address DNS Name Additional Info More Info
Session ID