Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Protecting the Network without Breaking the Bank

Network security has been getting a lot more attention lately due to the news media reporting on Viruses, network attacks, and hackers. That makes it a little easier for Security Professionals to get managers to give us some time and resources to do our jobs, but the high cost of securing a Network may drive managers to look for ways to outsource Network Security instead of using available resources. In most instances, readily available tools can be acquired with little or no cost to enable a security professional to d...

Copyright SANS Institute
Author Retains Full Rights

AD

Protecting the Network without Breaking the Bank

Network security has been getting a lot more attention lately due to the news media reporting on Viruses, network attacks, and hackers. I even heard the term 'script-kiddy' on the National News recently. That makes it a little easier for Security Professionals to get managers to give us some time and resources to do our jobs, but the high cost of securing a Network may drive managers to look for ways to outsource Network Security instead of using available resources. In most instances, readily available tools can be acquired with little or no cost to enable a security professional to do an effective job of securing a network without spending the entire IT budget. Most businesses allow 2-3% of their budget for IT cost, and that has to include security. If you can give the business a secure network without breaking the IT budget, then MAYBE their will be more left for raises…but don't bet on it. The goal of any good security professional is for management not to have to worry about information security, but don't expect to be appreciated for doing a good job. Document everything that you do to secure the network and the cost involved. Also, give the pointed haired boss the available choices and how much the commercial products cost, as well as what you are using and the cost involved. Have a Security Policy and documented security procedures and get the management to sign them. Include in the procedures the Intrusion Detection system, Vulnerability scanning, and web use monitoring.

Security Policy

The first step in securing your network is to develop a security policy that is supported by the management. Section 5 of Sans Security Essentials 1 covers Security policy in depth, so there is no added value in rehashing the information. In addition, RFC 2196 "Site Security Handbook" developed by the Network Working Group should be read by anyone planning to develop a site security policy. Security policy should address remote access, Configuration Control, Vulnerability Scanning, and Intrusion Detection.
In the W2K news Volume 7 article "The Human Factor in Security Management," the five main challenges of maintaining a security policy are as follows:

1. Creating and updating Policy,
2. Distributing Policy,
3. Users reading current Policy,
4. User awareness and retention of Policy information and
5. Tracking status and awareness level.

A good configuration Control Policy establishing standard configurations for all systems is an important part of any Security Policy. Develop a standard configuration for each operating system that is used and ensure that all systems are configured to conform to the configuration policy. Create a procedures handbook that includes these configuration procedures, as well as procedure for creating shares and for adding and updating software. Check systems when they are added to the network and recheck them for configuration changes several times each year. Use vulnerability scanning and periodic audits to ensure that users conform to the security policy.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Access to resources

If your business involves E-Business, then planning for external access to available resources is your number one challenge. It is a good idea to invest some time and money into a Firewall. Firewalls are available from free to well over $100,000.
If you only need remote access for a satellite office or a couple of road warriors, you might consider using PC anywhere or setting up a RAS server using Protocol Address Translation. It is fairly easy to set up Port Address Translation (PAT) to route a VPN connection to a Microsoft Remote Access Server using 1723/tcp and GRE 47(Generic Routing Encapsulation).
If you need to have E-Commerce available, then there are other considerations. Many businesses have an ISP that provides Internet access and a limited amount of Web space. This provides an area for Web hosting without leaving the network vulnerable. For internal systems that need Internet access, use Network Address Translation to isolate the internal systems from Internet traffic. Most routers have built in firewalls that will provide some protection from common attacks. Just remember, the router is not only your entrance to the Internet, it can be the Internets entrance to your network. Scan your router for proper configuration and apply strict configuration policies to you routers. Don't enable SNMP if you aren't using it, and always use a generated password on the router. If a hacker compromises a router, they can divert all traffic destined for your network to another site. Scan routers for vulnerabilities, and always scan new devices added to the network.

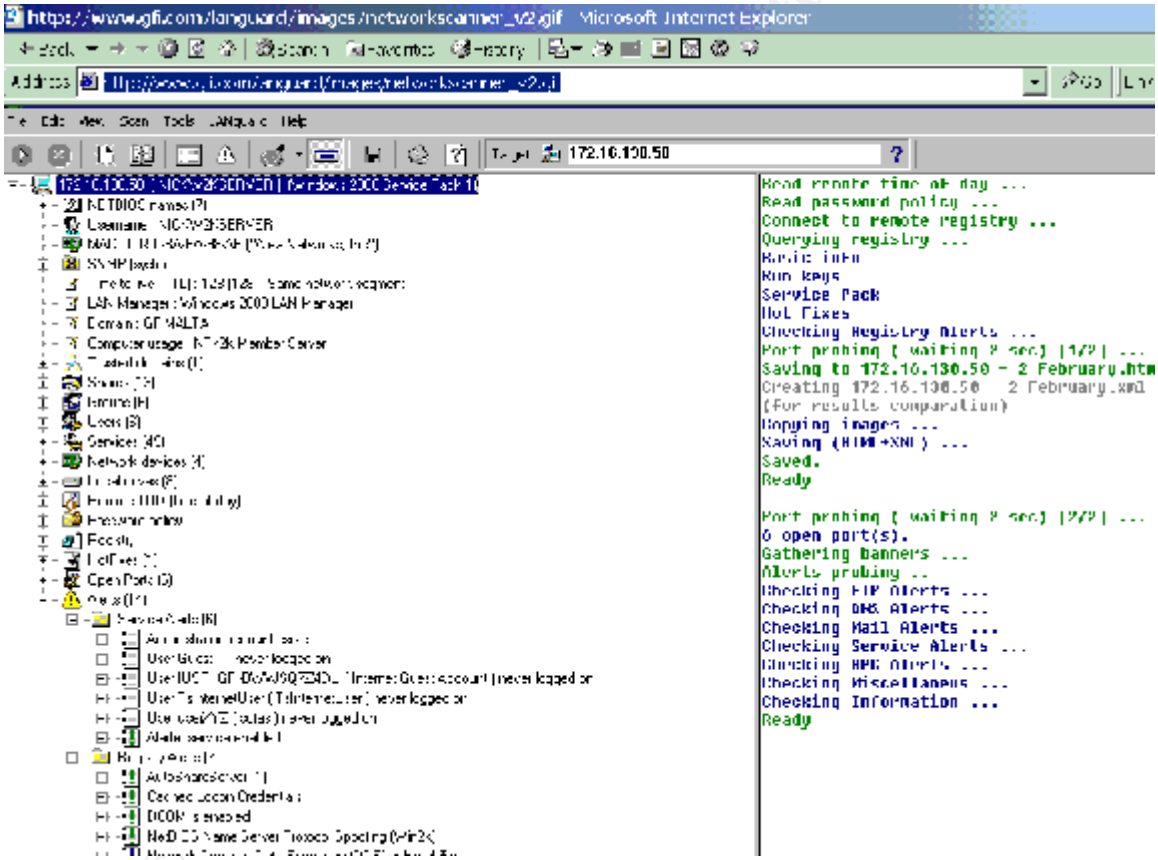
Vulnerability Scanning

Set up a schedule for scanning. The frequency of scanning should depend on the Security Posture of the Network. Using a tool like LanGuard Vulnerability Scanner commercial Version ($99) can provide a comparison of the configuration of your network and report on configuration changes or device additions since the last scan. This can save some time on running scans and let you concentrate on newly added devices or devices with configuration changes, but a complete rescan of the network should still be completed several times a year. Include in the Security Policy a requirement that each system be scanned to ensure proper configuration when connected to the network. Correct any configuration problems and rescan to ensure the system is configured properly. Then use the initial scan as a baseline to check against in order to detect configuration changes to the system. Rescan and save the new configuration baseline after any Service Patch or application install. 3 steps of a Vulnerability Scan
1.Network Discovery using Ping to map active devices on the Network
2.Port Scanning to identify open ports, Operating system, and vulnerabilities.
3.Report generation
And then there is the corrective action, scanning without corrective action is a waste of time and effort. Have a corrective action policy that gives users a deadline for correcting vulnerabilities.
Don't depend on any one product to find all the holes. A high end product like ISS System scanner may find a lot of vulnerabilities, while a free scanner such as SuperScan

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

(available from Foundstone) can easily identify open shares that provide easy access into the system.

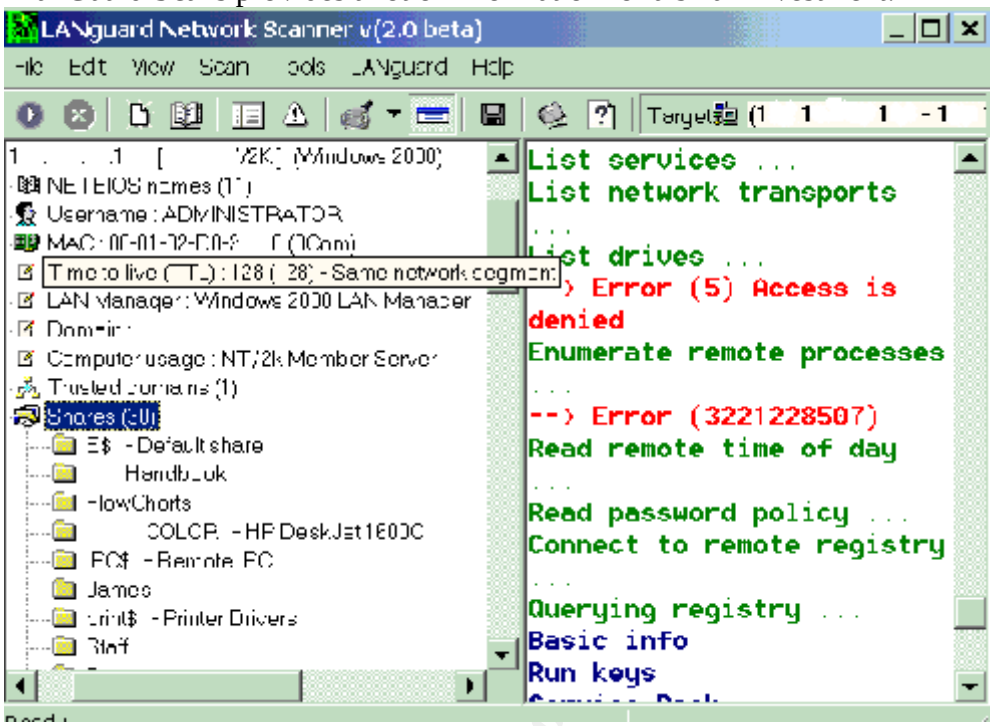
The following screenshot from GFI Ltd. Is the web site example of a LanGuard scan. LanGuard Network Scanner is available for download from the GFI site. A commercial version can be purchased for $99. LanGuard has the ability to detect shares, users, services, and sessions on a remote system. The commercial version can be used to "compare scans and identify new security holes." The example below shows a scan of a single address, 172.16.130.50, but LanGuard can scan a range of addresses. Due to the large amount of information, I do not like to scan more than one subnet at any one time. By clicking on the 'SHARES' and clicking each individual share, you check for shares configured to allow 'authenticated user' or 'everyone.' LanGuard can also check for easily guessable passwords, and open ports.



Following is a LanGuard scan of a file Server with several shares. This tool gives the scanner a lot more information than 'Super Scan' while still providing ease of use. Lan guard provides a lot of information useful in mapping the network, including Domain name, Operating system, MAC address, and netbios name, as well as whether the system is a domain controller or member server. The one complaint I have with LanGuard is that it initiates a HyperTerminal connection when you click on a Netbios share…although the netbios session 'connects' when you click on a 'Share.'

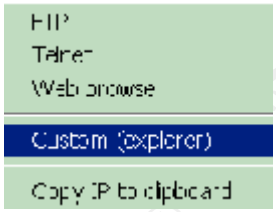
© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

LanGuard Scans provides a lot of information for a small investment:



(See Appendix)

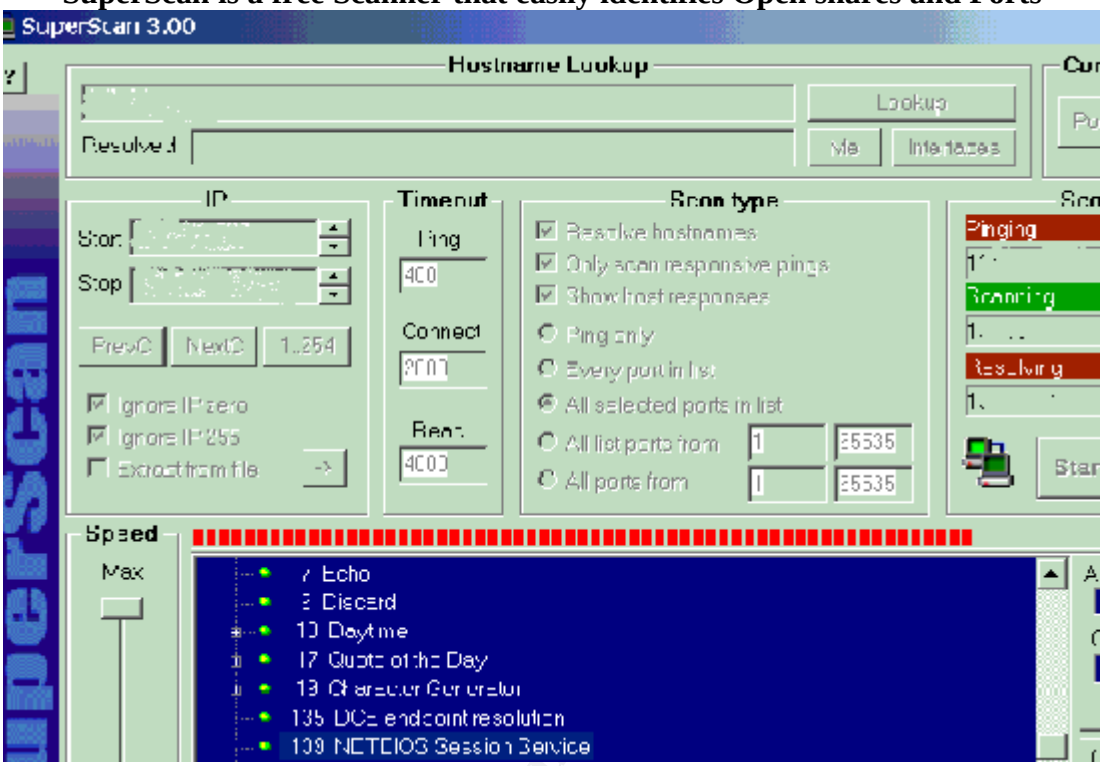
Superscan is a free scanner that is very easy to use. Download SuperScan, start the scanner and enter a starting and ending IP address for the scan. The Configure Ports setting allows you to configure which ports are scanned. The scanner first 'pings' all the addresses in the selected range, then scans each selected port in the IP address range. A + in front of a port, protocol, or service indicates additional information. In the case of 'net bios', a check indicates a net bios share exist. Simply right click on the ***139 Net bios Session Service***. A set of choices will be displayed.



By clicking the ***Custom (explorer)*** selection, the Net bios share will open. In the event that you have access to a folder or drive, this indicates 'read' access to the folder or drive. If that occurs, I always try to create a folder to check for 'write' privileges. The discovery of a writ able share is a concern. This indicates that anyone with network access has the ability to create folders and hide them if the want, and load and run anything they want from the compromised system…NOT GOOD!

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

SuperScan is a free Scanner that easily identifies Open shares and Ports



(See Appendix)

Configuration Control

A Configuration Checklist is a good procedure for ensuring configuration Control policies are being followed. Without a configuration control policy, users can install and configure systems improperly, create shares at random, and constantly introduce viruses and vulnerabilities into the network. Not having good configuration control will present a moving target for the person or persons trying to protect the network. If the user is a member of the systems Administrator group, they have the ability to change these settings, clear logs, and return to the established configuration at will. Have an Administrator group and take the ability to change these system settings away from the user.

A good practice is to start with a standard configuration. Test the configuration to make sure it is both secure and usable. We once turned off an alert that notified us that our UPS was bad, every 15 minutes the system would power down without warning. I even locked my system down while testing my checklist so that I couldn't get in and had to reload, that is a little too secure.

Provide a checklist for Operating systems and have the user sign the checklist to acknowledge that the system was configured correctly. And run a scan of the system. Include a report of the system scan with the configuration checklist and have the system user sign the checklist to verify that they are aware of configuration requirements. This would be a good time to run a scan with LanGuard to establish a Baseline configuration on the system. These settings are accessed through 'Start\Administrative Tools.'

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

An associate and myself developed the following checklist to help in the initial configuration of Windows NT and Windows 2000 Systems.

Example Configuration Setting for Windows NT

1. Set up Hard Drive with NTFS file system.
2. Shares of the root and operating system restricted to Administrative Purposes.
3. Create Local users group: (Insert Domain\UIDS that need access to the computer
4. Remove the OS2 and Posix files/ directories.
5. No shared passwords for all accounts
6. Generated passwords are used for each separate account
7. The Guest account is disabled / Guest password set
8. All default accounts have been removed or passwords changed (guest, Administrator)
9. The screen saver has been enabled for 10-minute delay and password protected

User Manager/Policies

Password Policy:

Maximum Password Age: Expires in 180 days
Minimum Password Length: 8 Characters
Account lockout duration: 40 minutes
Account Lockout Threshold: 5 invalid attempts
Reset Lockout count after: 30minutes
Minimum Password Age: 3 days
Password Uniqueness: 10 passwords

Audit Policy:

Logon and Logoff: Success and Failure
File and Object Access Failure
Use of User Rights: Success and Failure
User and Group Management Failure
Security Policies Changes Success and Failure

User Rights Assignments

Access this computer from the network: Administrators, Local User Group
Backup files and directories: Administrators, Backup Operators
Bypass Traverse Checking: Administrators
Change system time: Administrators
Create a Pagefile: Administrators
Create a token object: Administrators
Create permanent shared objects: Administrators
Debug Programs: Administrators
Force shutdown from a remote system: Administrators
Generate security Audits: Administrators
Increase Quotas: Administrators
Increase Scheduling Priority: Administrators
Load and Unload Device drivers: Administrators
Log on as a service: Administrators
Log on locally: Administrators, Local User Group

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Manage auditing and security log: Administrators
Modify firmware environment values: Administrators
Profile single process: Administrators
Profile system performance: Administrators
Restore files and directories: Administrators
Shutdown the system: Administrators, Local User Group
Take ownership of files and other objects: Administrators

10. SERVICES

Alerter Service	manual	
Clipbook	Disable	
COM+ Event System	Started	Automatic
Computer Browser	Started	Automatic
DHCP Client	(determined by network configuration)	
Directory Replicator	Manual	
Event Log	Started	Automatic
Messenger	Manual	
Net Logon	Started	Automatic
Network DDE	Manual	
Network DDE DSDM	Manual	
NT LM Security Support Provider	Manual	
Plug and Play	Started	Automatic
Protected Storage	Started	Automatic
Remote Procedure Call (RPC) Service	Started	Automatic
Remote Procedure Call (RPC) Locator	Manual	
Server	Started	Manual
Spooler	Started	Automatic
System Event Notification	Started	Automatic
Task Scheduler	Manual	
TCP/IP NetBIOS Helper	Started	Automatic
Telephony	Disable	
Uninterruptible Power Supply	Automatic	
Windows Installer	Manual	
Workstation	Started	Automatic

Apply the following settings to the registry

11. Restrict Anonymous:

Add a value named "Restrict Anonymous" with REG_DWORD value of 1 to the key.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

12. Hidden Shares:

Remove Hidden Administrative Shares (C$, D$, etc.)….Add a value named "AutoShareWks" with REG_DWORD value of 0 to the key.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

13. BIOS password is set if available
14. After completing setup, have Network Manager conduct a Security Scan of the system.

(The Restrict Anonymous setting is one of the SANS "The Twenty most critical Internet Security Vulnerabilities.")
This checklist follows recommended settings from Microsoft, SANS, and the NSA Windows NT Configuration Guide. We disabled services that we determined were not used and tried to follow recommended NT configuration guidelines. It is always best to turn off unused services, but test the system after turning off a service to avoid turning off something you need. Keep up with service Packs and patches to the OS, and, if possible, provide a way to Push service packs to the users desktop when they login.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

(In Windows 2000 Administrator tools is located in the Control Panel)

See Appendix

Example Configuration Setting for Windows 2000

1. Set up Hard Drive with NTFS file system.
2. Shares of the root and operating system restricted to Administrative Purposes.
3. Create Local users group: (Insert Domain\UIDS that need access to the computer and keep to a minimum.
4. No shared passwords for all accounts
5. Unique generated passwords are used for each account
6. The Guest account is disabled / Guest password set
7. All default accounts have been removed or passwords changed (guest, Administrator)
8. The screen saver has been enabled for 10-minute delay and password protected

The following policies are set

ACCOUNT POLICIES:

(Password Policy)

Enforce Password History	10 passwords remembered
Maximum Password Age	180 Days
Minimum Password Age	3 Days
Minimum Password Length	8 Character

(Account Lockout Policy)

Account Lockout Duration	1440 minutes
Account Lockout Threshold	5 invalid Logon Attempts
Reset Lockout count after	30 minutes

LOCAL POLICIES:

(Audit Policy)

Audit Account Logon Events	Success/Failure
Audit Account Management	Failure
Audit Logon Events	Success/Failure
Audit object access	Failure
Audit Policy Change	Failure
Audit Privileged Use	Success/Failure

(User Rights Assignment)

Access this computer from the network	Administrators, Local User Group
Back up files and directories	Administrators
Bypass traverse checking	Administrators
Change the system time	Administrators
Create a Pagefile	Administrators
Debug programs	Administrators
Force shutdown from a remote system	Administrators
Generate security audits	Administrators
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Log on locally	Administrators, Local User Group
Manage auditing and security log	Administrators

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Modify firmware environment values	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Restore files and directories	Administrators
Shut down the system	Administrators
Take ownership of files or other objects	Administrators

(**Security Options)**

Additional restrictions for anonymous connections:	Do not allow enumeration of SAM accounts and shares
Allow system to be shut down without having to log on	Disabled
Allowed to eject removable NTFS media	Administrators
Amount of idle time required before disconnecting session	10 minutes
Audit the access of global system objects	Disabled
Audit use of Backup and Restore privilege	Disabled
Automatically log off users when logon time expires (local)	Enabled
Clear virtual memory Pagefile when system shuts down	Enabled
Digitally sign client communication (always)	Disabled
Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (always)	Disabled
Digitally sign server communication (when possible)	Disabled
Disable CTRL+ALT+DEL requirement for logon	Disabled
Do not display last user name in logon screen	Disabled
LAN Manager Authentication Level	Send LM & NTLM use NTLMv2 session security
Number of previous logons to cache	3 logons
Prevent system maintenance of computer account password	Disabled
Prevent users from installing printer drivers	Disabled
Prompt user to change password before expiration	14 days
Recovery Console: Allow automatic administrative logon	Disabled
Restrict CD-ROM access to locally logged-on user only	Enabled
Restrict floppy access to locally logged-on user only	Enabled
Strengthen default permissions of global system objects	Enabled
Unsigned driver installation behavior	Warn but allow installation
Unsigned non-driver installation behavior	Silently succeed

11. SERVICES

Alerter Service	Disable
Application Management	Manual
Clip book	Disable
COM+ Event System	Manual
Computer Browser	Automatic
DHCP Client	Disable
Distributed Link Tracking Client	Manual
Distributed Transaction Coordinator	Manual
Event Log	Automatic
Event Log Watch	Automatic
Fax Service	Disable
Indexing Service	Disable
Internet Connection Sharing	Disable
IPSEC Policy Agent	Automatic
Logical Disk Manager	Manual
Logical Disk Manager Administrative Service	Manual
Messenger	Manual

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Net Logon	Automatic
NetMeeting Remote Desktop Sharing	Disable
Network Connections	Manual
Network DDE	Manual
Network DDE DSDM	Manual
NT LM Security Support Provider	Manual
Performance Logs and Alerts	Manual
Plug and Play	Automatic
Print Spooler	Automatic
Protected Storage	Automatic
QoS RSVP	Disable
Remote Access Auto Connection Manager	Manual
Remote Access Connection Manager	Automatic
Remote Procedure Call (RPC)	Automatic
Remote Procedure Call (RPC) Locator	Manual
Remote Registry Service	Disable
Removable Storage	Automatic
Routing and Remote Access	Disabled
RunAs Service	Manual
Security Accounts Manager	Automatic
Server	Manual
Smart Card	Manual
Smart Card Helper	Manual
SMTP	Manual
System Event Notification	Automatic
Task Scheduler	Manual
TCP/IP NetBIOS Helper Service	Automatic
Telephony	Disable
Telnet (Client Setting)	Disable
Uninterruptible Power Supply	Automatic
Utility Manager	Manual
Windows Installer	Manual
Windows Management Instrumentation	Manual
Windows Time	Manual
Workstation	Automatic

Apply the following settings to the registry

12. **Hidden Shares:**

Remove Hidden Administrative Shares (C$, D$, etc.)….Add a value named "AutoShareWks" with REG_DWORD value of 0 to the key.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

13. BIOS password is set if available
14. **AN EMERGNECY REPAIR DISK**.

i. Go to "Start/Programs/Accessories/System Tools/Backup". Run this command anytime you change the configuration of the system.

(BIOS passwords protect the system from booting to a floppy where the Admin password could be hacked and the system compromised.)

An important part of this Configuration Control Checklist is the controls on who can access the computer from the network. By limiting access to a specific group of authenticated users we have provided a primary line of defense from external access. The default right of 'Everyone' makes the system accessible to anyone who gains access to the network. 'Authenticated Users' improves access control somewhat, but it still gives any user authenticated to the domain access to the system. By creating a group and limiting access to the group of users that you may want to share resources with, you are limiting the availability of the system and its shares to a designated group of users.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Further access controls on individual shares can restrict access to individual members of the access group, but a default share will not be open to the world.
To test access to shares, scan the system while logged into the network as an authenticated user that is not a member of any access group (create a new user that is only a member of the users group.) If the scan (SuperScan is quick and easy for this check) uncovers accessible shares then you have something shared to 'authenticated users' or 'everyone.' If you think the temp worker doing the filing has a 'need to know' for all the Personnel information, or for all the information on the Bid Proposal for the next big contract, then I guess it's okay to have uncontrolled shares.

Passwords

In Security Essentials Steven Northcutt stated that he didn't rely much on passwords, because they can be cracked, but a good password will slow down even a good hacker. Along with a good password, you need a good password policy. Passwords should be generated and not made up, and be composed of letters and numbers. Password generator programs are available from various Security Sites, such as Freshmeat.net. Most of these password generators run on Linux or BCD, an easy password generator for Windows based machines is 'Advanced Password Generator' from Segobit.com. If possible, passwords should be generated from a common server and pushed to all systems that the user needs to access. This results in a single password for access to all systems. Passwords should be 6 to 8 characters and include both numbers and letters. I noticed recently when looking at the dictionary used for some vulnerability scanner that checked for easily guessed passwords that 'oicu812' was in the dictionary for password guessing, so a random password generator should be used to avoid easily guessable passwords. Passwords should be set to expire at a maximum of 180-day intervals.

Intrusion Detection

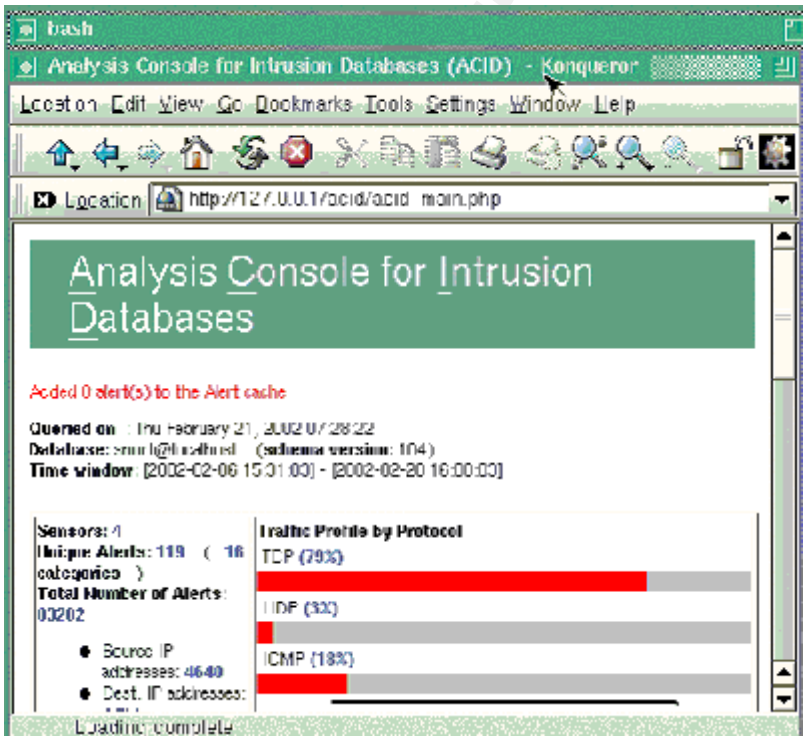
Part of the 'Defense-In-Depth' approach to Network Security is the idea of not relying on a 'Silver Bullet' to solve Network security concerns. Just because you have a Firewall doesn't mean that you are safe. A Firewall should be accompanied by an Intrusion Detection system, not only for the network, but also for the critical Host on the Network. The first place to locate an Intrusion Detection System monitor is on the outside of the firewall to see who is 'knocking on the door.' This monitor will tell you what port scans and probes are being ran against your address space, even if the scan is blocked by the Firewall. A second Intrusion Detection Monitor should be placed inside of the Firewall to detect what gets through. This internal monitor should be equipped to alert a Network Support staff member in the event of a successful intrusion through the Firewall, even during non-working hours. By comparing the intrusions identified by the Internal Monitor to the port scans and probes on the External monitor, the configuration of the Firewall can be analyzed for its effectiveness. Monitoring of Firewall logs is also an integral part of the overall Intrusion Detection plan. However, Firewall logs can be extremely large. Utilizing an Intrusion Detection system to identify suspicious activity can help in sorting out Firewall logs that need further scrutiny.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

A good thing about an Internal Intrusion Detection Monitor is that it can monitor what's going out, as well as what's coming in. Reports from the internal Monitor can be used for identifying Waste, Fraud, and abuse of network resources, as well as monitoring breeches of the Firewall, spy ware reporting, and mis-configured devices or operating systems. The Intrusion Detection Monitor can also be useful in identifying systems infected with a Virus. We recently identified systems infected with the NIMDA virus by their network traffic. The 'SNORT' box running internal to the firewall identified the signature of the Nimda virus on an internal system.

There are several Free Intrusion Detection systems available, but it is important to select an Intrusion Detection system that has some support structure that will provide updates when new intrusion techniques and vulnerabilities are discovered. A good source for tools is the Foundstone site (www.foundstone.com) and www.freshmeat.net . Most of the free Intrusion Detection systems are Unix/Linux based, so, if you are an NT person, you may have to get a Linux or UNIX guru to help set things up. If you have a UNIX guru available, you can get them to set up Cygwin/Xfree86 X-window software http://sources.redhat.com/cygwin/ and get the screen from the Snort or other Linux IDS system onto the NT box. Cygwin is a Unix environment, developed by RedHat, for Windows. This is also useful in enabling monitoring of the IDS by different people in the support staff.

Cygwin window from a SNORT IDS:



According to 'COAST' at Purdue University, a good Intrusion Detection System should include the following:

(http://www.cerias.purdue.edu/coast/intrusion-detection/detection.html)

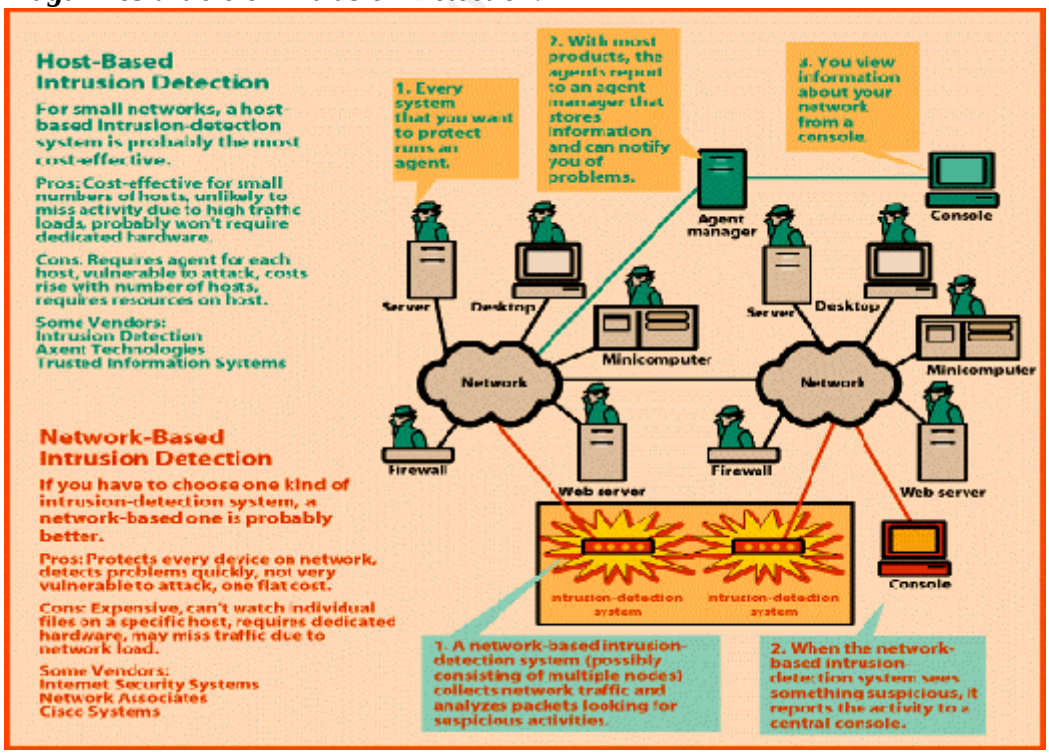
© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Characteristics of a Good Intrusion Detection System

An intrusion detection system should address the following issues, regardless of what mechanism it is based on:

1. *It must run continually without human supervision. The system must be reliable enough to allow it to run in the background of the system being observed. However, it should not be a "black box". That is, its internal workings should be examinable from outside.*
2. *It must be fault tolerant in the sense that it must survive a system crash and not have its knowledge-base rebuilt at restart.*
3. *On a similar note to above, it must resist subversion. The system can monitor itself to ensure that it has not been subverted.*
4. *It must impose minimal overhead on the system. A system that slows a computer to a crawl will simply not be used.*
5. *It must observe deviations from normal behavior.*
6. *It must be easily tailored to the system in question. Every system has a different usage pattern, and the defense mechanism should adapt easily to these patterns.*
7. *It must cope with changing system behavior over time as new applications are being added. The system profile will change over time, and the IDS must be able to adapt.*
8. *Finally, it must be difficult to fool.*

*According to **Byte magazine**: 'If you have to choose one type of Intrusion-Detection System, a Network-based one is probably better.' Following is an illustration from **Byte Magazines** article on Intrusion Detection.*



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Host based Intrusion Detection systems: according to COAST: 'an Intrusion Detection System detects intrusions by looking for activity that is different from a users' or systems' normal behavior'. Many host based Intrusion Detection systems use the system audit logs and matches signatures of know intrusions. Coast has an extensive list of Intrusion Detection systems. An important feature is some sort of centralized monitoring capability such as a central console. All the Intrusion Detection Systems in the world won't help secure your network if no one ever looks at the alerts and logs.

Firewall

A firewall is an important part of any network protection system. Firewalls can be anything from a border router running ingress egress filtering, to a high-end device such as the CISCO PIX or SonicWall Pro. For a small office environment, utilizing a small router with an integrated firewall can be very affordable and offer an acceptable level of protection. Cable/ DSL routers with integrated Firewalls are available from less than $100. The Siemans Speedstream DSL router offers Attack recognition and logging, as well as the ability to block common attacks. And the Asante Friendly-net DSL router provides packet-filtering capabilities. These inexpensive routers utilize Network Address Translation to provide a layer of protection from Internet traffic as well as the Firewall capabilities.

Network Address Translation can be used to shield internal systems from Internet traffic while providing access to Internet resources. Of course, you may need to access some systems from the Internet to provide for Remote access or Web access for your customers and remote users. This can be easily accomplished through the use of Network Port Address Translation. By configuring the port for VPN or Web traffic to map to a particular internal address, external services can be provided through the router without greatly compromising security. Most routers support Port Address Translation (PAT), or Network Address Port Translation (NAPT) to provide access to systems with Internal IP addresses by mapping traffic on a particular port to a designated internal address. As mentioned earlier, you can set up NAPT to an internal system running Microsoft Remote Access Server by configuring the router to map TCP/1723 and GRE/47 to an internal address such as 192.168.100.7. The client simply configures the Microsoft VPN client to 'dial' the Globally Unique IP address of the router, and the NAPT routes the VPN connection to the internal system running the RAS service. It works great and it's included with Microsoft NT server.

If you already have an Internet connection and just want an inexpensive firewall, IP Chains running on Linux is easily configured to provide Firewall protection for your network and a lot of on line documentation exist to help configure the system. A good source for configuring Linux IpChains is ***SANS Track2: Firewalls, Perimeter Protection and Virtual Private Networks 2.2 Firewalls 101: Perimeter Protection with Firewalls.*** The course manual contains an example of how to block the 'Sans top 10 Most Critical Internet Security Threats.' But first, secure your Linux box. A good reference is the "Securing Linux Step-by-step" located in section III of the Security Essentials Course material. Scan the system for vulnerabilities, set up the IP Chains firewall, and then scan the system again. Included in the bibliography is a link to a Linux Firewall How-To page that takes you step by step through the configuration of a Linux IP Chains firewall.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Conclusion:

Business needs vary depending on the size and nature of the business. Computer networks are as diverse as are businesses, each having differing resources and requirements. The added attention given to computer networks and computer security may drive business managers to seek external support for computer security services. By evaluating the needs of your network, and developing a Site Security Plan which includes a Site Security Policy, Perimeter Protection Policy, and an Intrusion detection policy, the Information Technology Staff may be able to present management with an economical alternative to outsourcing computer security services. There are many free or inexpensive tools available to the security professional to help develop a viable security protection plan without breaking the IT budget. By utilizing good configuration control, vulnerability scanning, intrusion detection, and perimeter protection, the IT staff can provide business with a fairly secure and usable network utilizing free or inexpensive security tools. But the job of protecting the information and the network cannot be accomplished by any one tool or security appliance. A service that may not be considered a security risk today could be in the news tomorrow. SNMP was considered a tool for network management that did not pose a significant risk to the network until February of 2002 when an SNMP exploit grabbed the attention of network security professionals worldwide. Although SANS included SNMP in "The Twenty most critical Internet Security Vulnerabilities" published in January 2002, the announcement of the SNMP exploit on February 12, 2002 brought special attention to this vulnerability. Just as virus scanners must be updated with new virus definition files to continue to protect against new and ever changing virus threats, security policy must consider the ever changing threats against Firewalls, network devices, and Operating systems. Simply developing and implementing a security policy will not guarantee that your site will remain safe. Without constantly accessing vulnerabilities, applying updates and patches on not only operating systems, but also network devices, firewalls, and security tools, the network security professional will have a false sense of security as the network becomes more and more vulnerable to new threats. Not only must the Network security professional develop and implement a Security Policy, but he or she must include in the policy a mechanism for auditing and updating the policy to insure than the Network Protection Plan keeps up with the evolving threats from the internet as well as from internal and yet undetermined threats to information security. A security audit is a very important tool in accessing the security of the network, but, like tools and firewalls, can be extremely costly. Since the premise of this paper is to secure the network without breaking the bank, finding an economic means of accessing the security of the network will be an important addition to this paper. One way of checking network security would be to select some of the IT group to be an auditing team with the goal of breaking in to the network or systems on the network. Of course, management approval for these tests is a must. Also, pick a time when network traffic is low, weekend or off shift. And divide your group into two teams, one to break in, and the other to catch the 'hackers.' The result will be a security audit that is not only free, but also fun.

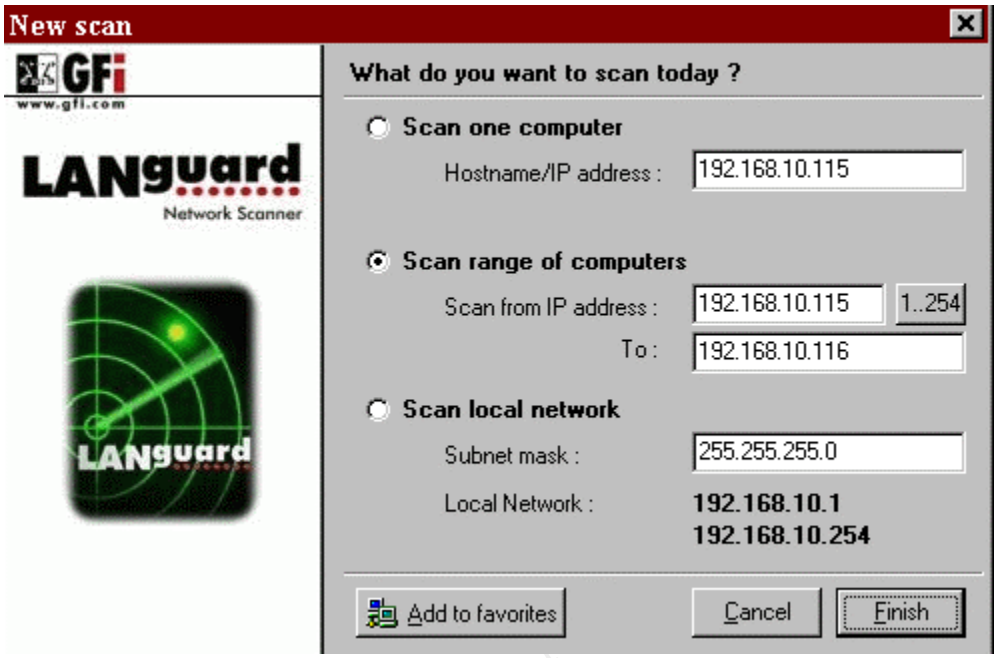
Keeping a network secure is a task that presents new challenges every day. By utilizing available tools, keeping up with new threats and available patches, we can mitigate the risk to our network and computing systems in an economic manner.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

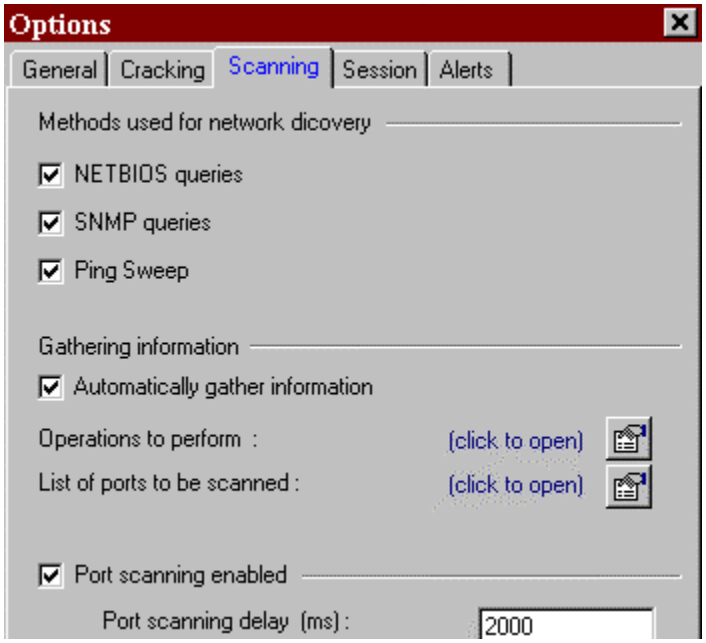
Appendix

Languard

Languard has alot more options than the freeware Superscan product. The first screen allows you to select the address of the system or systems to scan.

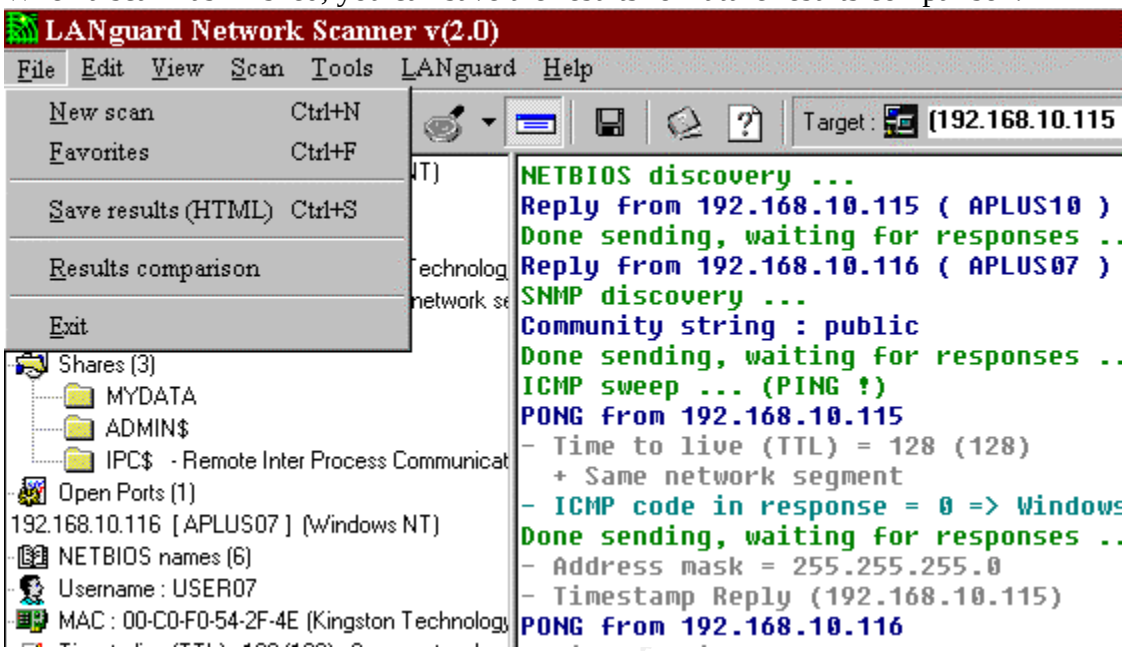


After selecting the range, LanGuard alows you to configure the scan by selecting Scan/options and configure the scan options you want.



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

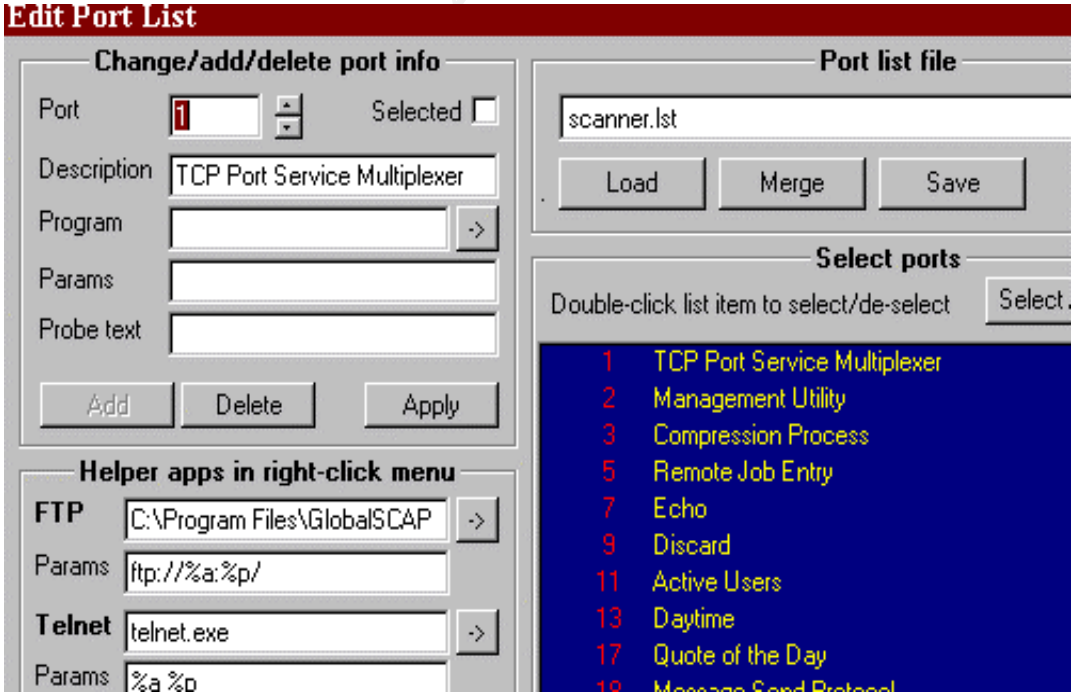
When a scan has finished, you can save the results for future results comparison.



Results comparison is only available in the commercial product. Output can be saved in HTML format.

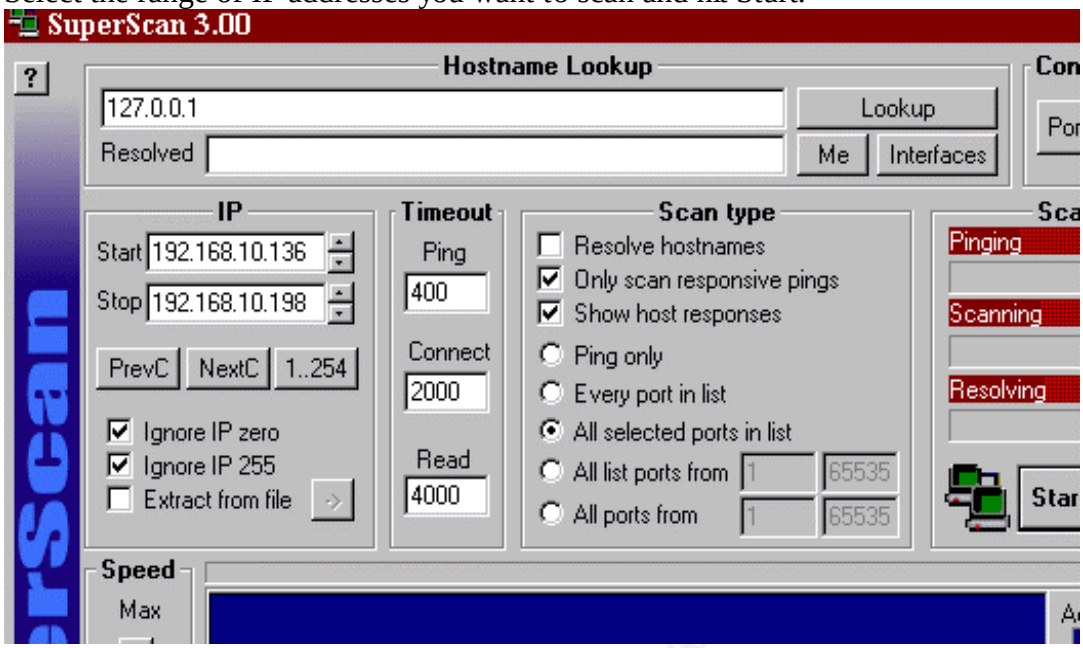
Superscan

Configure the Ports you want to include in the scan. Common ports include 21(FTP),23 (Telnet),80 (HTTP, and 139(NetBios session)and 161 (SMTP).

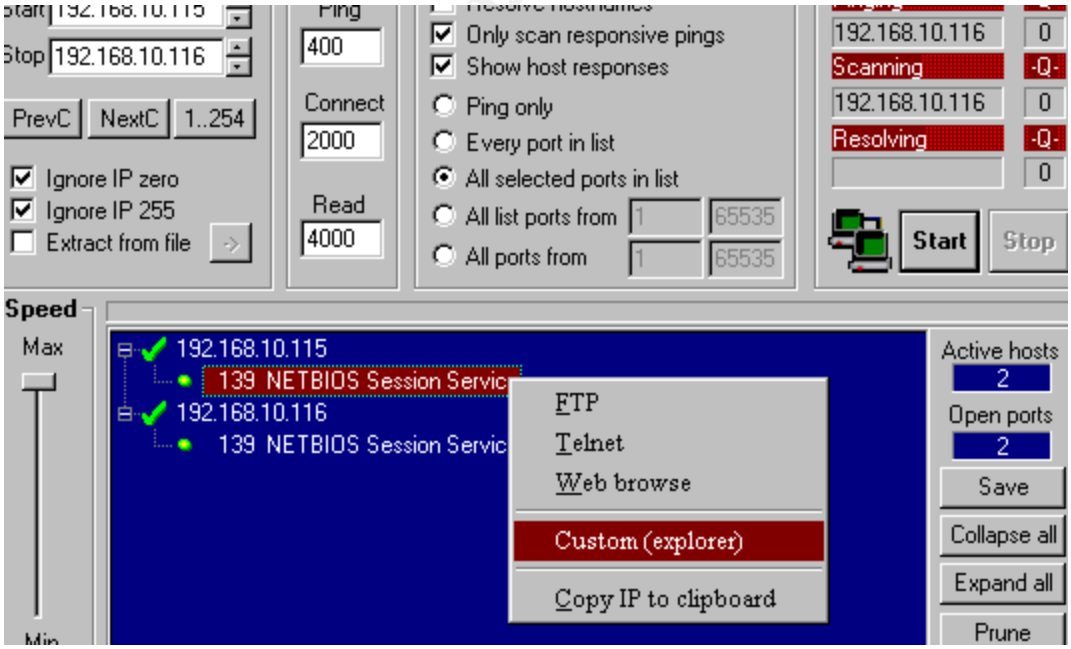


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Select the range of IP addresses you want to scan and hit Start.



SuperScan Pings addresses in the range first, then test selected ports on responsive systems.
Then checks for the configured ports. Open ports are displayed for further selection.
Right click to open a selection box to select how to attempt to open the port, FTP, Telnet, Web, Custom (explorer), or copy IP to Clipboard.

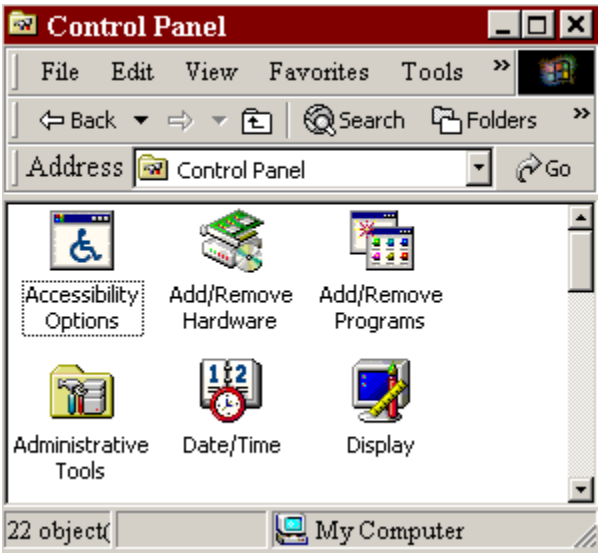


The drawback with Superscan is that it does not have the reporting capabilities that commercial scanners have. But for a free scanner, it makes checking the network for open shares cheap and easy.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Configuring Windows 2000 Professional with the Security Checklist

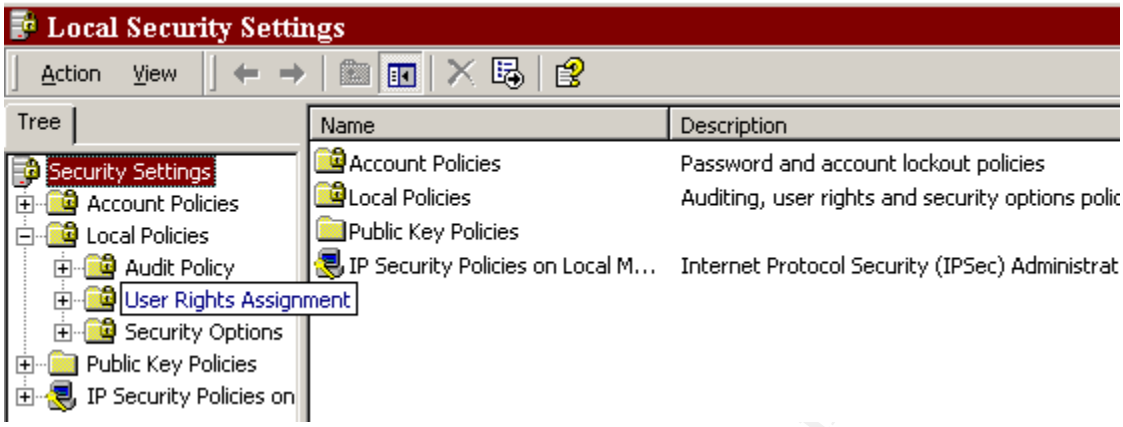
Windows 2000 Professional moved Administrator Tools into the Control Panel.



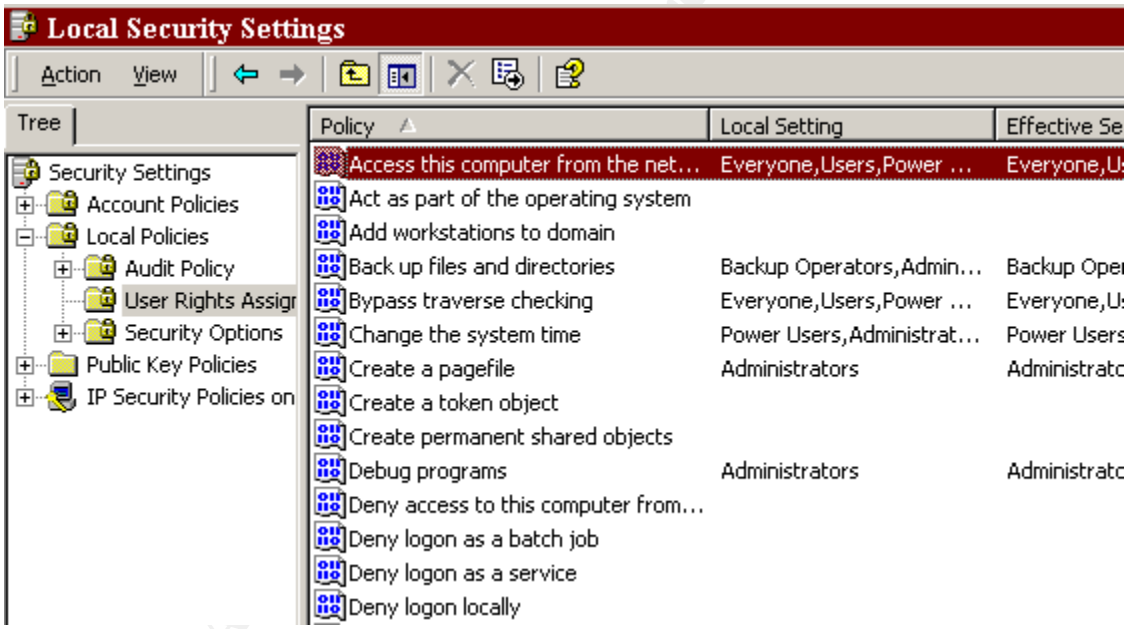
Open Admin Tools.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Select Local Security Settings.



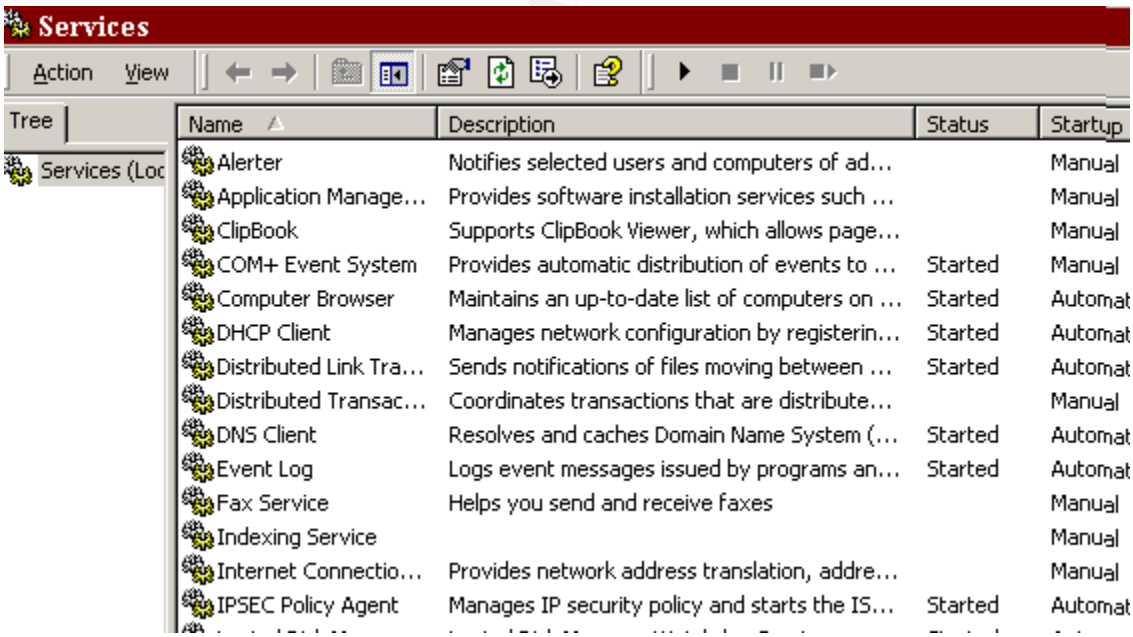
Use the CheckList to secure the Windows 2000 Installation.
The default settings gives 'Everyone' access to your system.



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

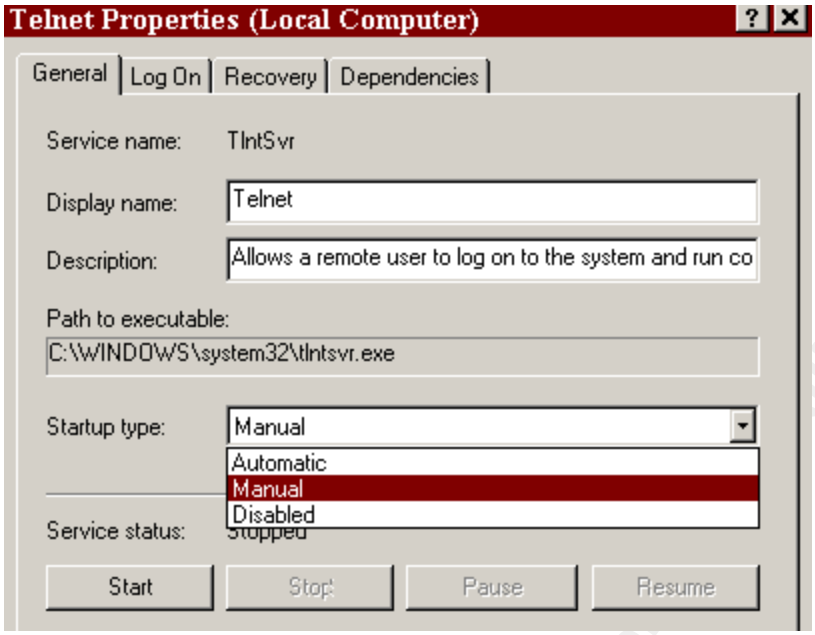
Services can also be accessed through the Administrative Tools.

Unneeded Services should be disabled. .

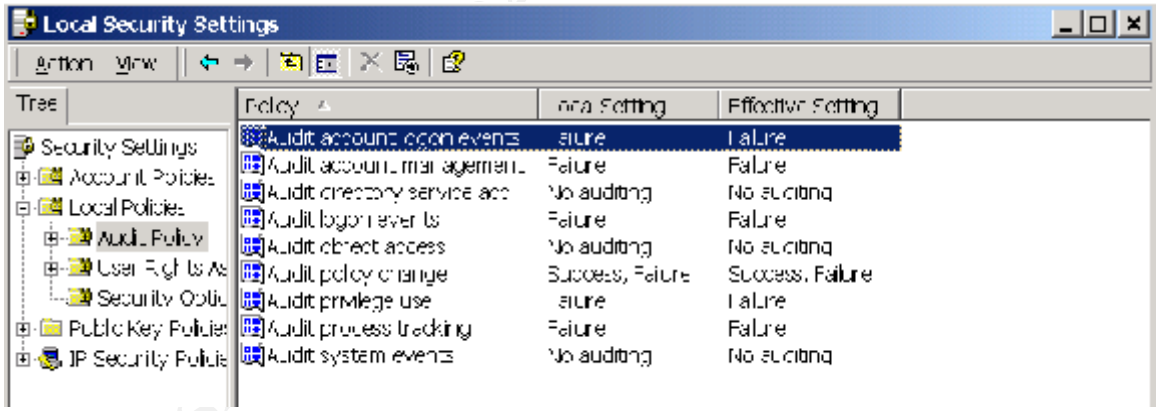


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Setting a service to Manual means it will start if needed.
Disable a service if you will not be using it!



Set your auditing policy through the Local Security Policy in Administrative tools.



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References:

Fraser,B. (editor) Network Working Group Request for Comments:2196 "Site Security Handbook" September 1997 URL:
http://www.ietf.org/rfc/rfc2196.txt?number=2196

Conry-Murray, Andrew "Vulnerability Assessment Tools" Network Magazine 4 May 2001 URL:
http://www.networkmagazine.com/article/NMG20010321S0005

Feb 25, 2002 Vol 7 Num 16 Issue 347 "New Microsoft Security Freeware" URL:
http://www.w2knews.com

Bahadur, Gary "Using Freeware Vulnerability Scanners" 4 Jan 2001 URL:
http://www.foundstone.com/knowledge/free_tools.html

Roesch, Martin "Snort: 19 April 1999 URL:
http://www.freshmeat.net/

SegoBit Software 26 Feb. 2002, Advanced Password Generator" URL:
http://www.segobit.com

GFI Ltd.
http://www.gfi.com/languard/lanscan.htm

Price, Katherine "Intrusion Detection" 23 Sept. 2000 URL:
http://www.cerias.purdue.edu/coast/intrusion-detection/detection.html

Grennan, Mark "Firewall and Proxy Server How To" 26 Feb. 2000 URL:
http://www.ibiblio.org/mdw/HOWTO/Firewall-HOWTO.html

Udell, Jon : Host-and Network Based Intrusion Detection" Jan 2002 URL:
http://www.byte.com/art/9805/img/058rs1b2.htm

Redhat Cygwin Team " What is Cygwin"
http://sources.redhat.com/cygwin

The SANS Institute Track2: Firewalls, Perimeter Protection and Virtual Private Networks 2.2 page 123-138

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: October 10th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Tysons Corner 2015	**Tysons Corner, VAUS**	**Oct 12, 2015 - Oct 17, 2015**	**Live Event**
SANS Gulf Region 2015	**Dubai, AE**	**Oct 17, 2015 - Oct 29, 2015**	**Live Event**
SANS Cyber Defense San Diego 2015	**San Diego, CAUS**	**Oct 19, 2015 - Oct 24, 2015**	**Live Event**
SANS Tokyo Autumn 2015	**Tokyo, JP**	**Oct 19, 2015 - Oct 31, 2015**	**Live Event**
SANS Sydney 2015	**Sydney, AU**	**Nov 09, 2015 - Nov 21, 2015**	**Live Event**
SANS South Florida 2015	**Fort Lauderdale, FLUS**	**Nov 09, 2015 - Nov 14, 2015**	**Live Event**
SANS London 2015	**London, GB**	**Nov 14, 2015 - Nov 23, 2015**	**Live Event**
Pen Test Hackfest Summit & Training	**Alexandria, VAUS**	**Nov 16, 2015 - Nov 23, 2015**	**Live Event**
SANS Hyderabad 2015	**Hyderabad, IN**	**Nov 24, 2015 - Dec 04, 2015**	**Live Event**
SANS Cape Town 2015	**Cape Town, ZA**	**Nov 30, 2015 - Dec 05, 2015**	**Live Event**
SANS San Francisco 2015	**San Francisco, CAUS**	**Nov 30, 2015 - Dec 05, 2015**	**Live Event**
Security Leadership Summit & Training	**Dallas, TXUS**	**Dec 03, 2015 - Dec 10, 2015**	**Live Event**
SANS Cyber Defense Initiative 2015	**Washington, DCUS**	**Dec 12, 2015 - Dec 19, 2015**	**Live Event**
SANS Las Vegas 2016	**Las Vegas, NVUS**	**Jan 09, 2016 - Jan 14, 2016**	**Live Event**
SANS Dubai 2016	**Dubai, AE**	**Jan 09, 2016 - Jan 14, 2016**	**Live Event**
SOS: SANS October Singapore 2015	**OnlineSG**	**Oct 12, 2015 - Oct 24, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**