Global Information Assurance Certification Paper

Auditing ISA on Windows 2000 Server

Doug Dziuba
GIAC Systems and Network Auditor (GSNA)
Version 3.2 Option #1

Abstract

This audit evaluates the overall security of a Microsoft ISA firewall as it protects an organization's Internet access.

This audit reviews the firewall system in three areas. Technical, managerial, and operational are each considered in the design of the audit checklist.

Part two includes an audit checklist based on materials presented in the "state of practice" section.

For part three the audit will be conducted during off-hours for the client to minimize any potential impacts caused by the audit, though no impact is expected.

Part four summarizes the audit findings and makes recommendations for improvement in the overall system security.

Part 1: Research in Audit, Measurement Practice, and Control

Identify the System Being Audited

This audit is evaluating a Windows 2000 Server running Internet Security and Acceleration Server version 2000. This server is configured with two network interface cards and is a member of the organization's Active Directory Domain to facilitate group and user restrictions and monitoring.

This server is functioning as the single point of protection between the organization and the outside world. It provides the employees with Internet access, VPN services, access to Outlook Web Access, public access to the company's website, and limited FTP access for the website designer and the staff member who is maintaining content.

The pertinent systems are connected as detailed below (figure 1):

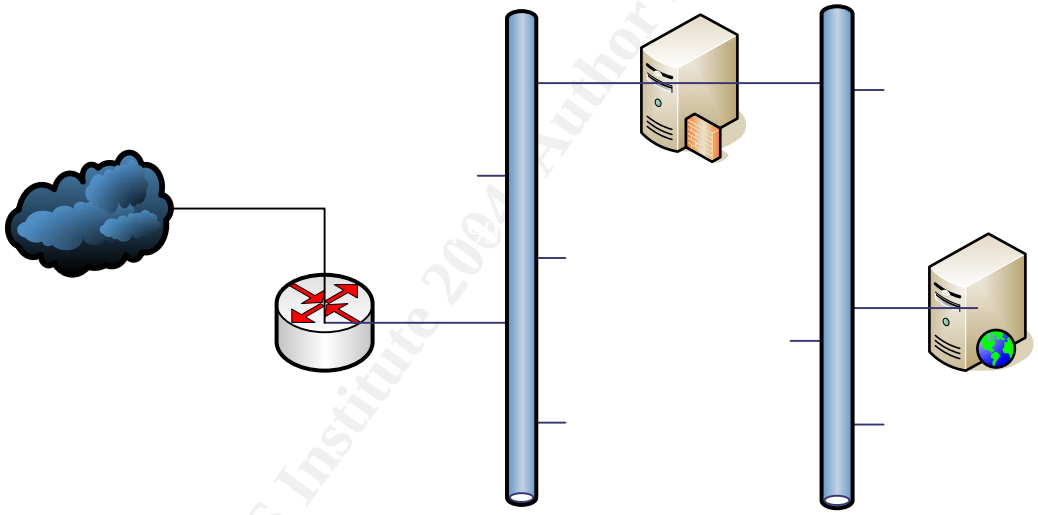


Figure 1

Most Significant Risks to the System

Since the firewall application requires an underlying operating system, the risks to the system can arise from hardware, operating system, or the firewall application itself. There are a several classes of vulnerabilities that can exist: technical (T), operational (O), or managerial (M). Additionally, the degree of exposure and the potential impact to the organization must be factored. All vulnerabilities are *not* created equal.

By understanding the class of the vulnerability, the organization can streamline its remediation activities. A technical vulnerability is a vulnerability found within

the software or hardware and can only be addressed by a software patch or the application of additional technology to mitigate the risk. These are fairly simple to fix once the vendor has created the patch. An example would be the Microsoft Security Bulletin MS04-022 (http://www.microsoft.com/technet/security/bulletin/MS04-022.mspx) from July 2004. This vulnerability in the Task Scheduler would allow remote code execution if exploited. This vulnerability can be corrected with a patch from the vendor or it can be mitigated by raising user awareness, ensuring least privilege for users, or removing the dynamic icon handler from the Windows registry.

An operational vulnerability would exist within the procedures utilized by administrators. These vulnerabilities are normally remediated by procedural changes, not necessarily policy changes. For example, in the organization's policy it requires that user accounts that have not been logged in for 30 days or greater be disabled. If the administrative procedures check for inactive user accounts every two months, then this would be an operational-based vulnerability. This would be mitigated by changing the administrative procedures followed by the administrators.

A managerial vulnerability usually centers on policy problems. These vulnerabilities are mitigated by creating or improving policy. Once the policy has been created or updated, the vulnerability immediately becomes an operational or technical vulnerability until addressed by applying the required operational or technical controls.

The most critical vulnerability is system mis-configuration. Mis-configuration is the most critical risk in this design and could cause catastrophic damage to the organization. This is in part because the firewall software (ISA Server) sits on top of Windows which must be hardened and configured securely, independent of the firewall application. Additionally, ISA Server is a very robust, configurable firewall that has many complex settings and can be difficult to troubleshoot which could lead administrators to allow more access than desired in the course of troubleshooting.

The second most critical vulnerability is poor user and password management. Since all user access and security is tied to the user's account, it simplifies administrative management but requires the administrators to be diligent in managing users and requiring strong passwords that are changed frequently. If this is not monitored, there is the potential for a user account to be compromised. If that were to happen, a hacker anywhere in the world would be able to access the system remotely through the VPN. Depending on the account compromised and the intent of the hacker, the damage could vary from data modification, data destruction, or data theft, without the organization being aware until it is too late.

Other major vulnerabilities are listed in the table below.

Vulnerability	Description	Class of vulnerability	Degree of Exposure	Potential Impact
Windows Mis-configuration	There are many steps recommended by Microsoft to harden a Windows server. Several of these require registry changes.	O	The degree of exposure will vary based on what is mis-configured.	The impact will vary depending on what is mis-configured. However, it is potentially catastrophic.
ISA Server mis-configuration	ISA Server is a complex product, especially when you desire to operate internal web resources.	O	The degree of exposure will vary based on what is mis-configured.	The impact will vary depending on what is mis-configured. Most commonly the impact will be a denial of service, but there is the potential that hackers could be given un-intended access.
Insufficient user policy and procedures	Since user access is tied to their account it is necessary to ensure least privilege for user accounts and frequent password changes and enforced password complexity rules.	M, O If the policy is absent then the policy should be created and procedures put in place to ensure compliance with the policy	The degree of exposure will vary based on which accounts can be compromised.	Impact can vary but data theft, destruction, and modification are real possibilities if an account is compromised.
MS Security Bulletin MS04-001	Vulnerability in Microsoft Internet Security and Acceleration Server 2000 H.323 Filter Could Allow Remote Code Execution	T	There is a high exposure because H.323 filter is enabled by default on servers running ISA Server 2000 computers that are installed in	This would give the attacker complete control over the system.

			integrated or firewall mode.	
MS Security Bulletin MS03-028	Flaw in ISA Server Error Pages Could Allow Cross-Site Scripting Attack	T	There is a medium exposure for this because the attacker must be aware of an ISA server and its access policy or host there own and then entice a user to visit the site.	Allows an attacker to execute code of their choice
MS04-025	This security bulletin summarizes 3 different vulnerabilities affecting the system.	T	There is medium exposure for these because in all cases the attacker must entice the user to take action, visit a web site, open a bmp or gif image. The code runs as the logged on user so applying the principal of least privilege will mitigate these.	Allows attacker to execute code of their choice or complete control of the system.
MS04-022	Task Scheduler Vulnerability	T	This is a medium exposure because user interaction is requiring for this vulnerability to be exploited.	Allows an attacker to execute code of their choice
MS03-033	Unchecked buffer in	T	This is a low to	Allows an attacker

	MDAC could cause system compromise		medium risk due to the complexity of the exploit and the attack would run with the privileges of the system exploited.	complete system control.
MS04-020	POSIX Vulnerability could lead to code execution	T	This is a low risk because this vulnerability requires physical access and valid login credentials.	This vulnerability would allow an attacker to escalate their privileges on the target system.

Current State of Practice

There is quite a bit of material available discussing how to secure a Windows 2000 Server for the Internet. Less information for the ISA Server is available. Since the underlying operating system has more possible settings to configure it makes sense that there is a lot of material available and any audit of an ISA Server based firewall will have to review thoroughly the security of the operating system in addition of the firewall configuration.

The resources listed were helpful in formulating the checklist items, understanding the technologies, and appreciating the vulnerabilities and what damage they can do to an organization.

Bragg, Roberta. Windows 2000 Network Security Design. Indianapolis: Que Publishing, 2003.
Bragg, Roberta. Windows 2000 Security. Indianapolis: New Riders, 2001.
Roberta's books help to outline what security Microsoft has built into the operating system and Microsoft's recommendations for designing secure networks with Windows 2000 systems. She discusses the topics in a manner that beginners can get it but provides enough depth that more experienced administrators will find value.

Jones, Don. Managing Windows with VBScript and WMI. Boston, Pearson Education, Inc., 2004.

This book doesn't require previous programming experience to be useful. Don introduces scripting fundamentals and continues to build on the foundation throughout the book. Scripting can allow administrators the ability to automate many management tasks, including auditing tasks.

McClure, Stuart, et al. Hacking Exposed. Berkley: Osborne,1999.
These series of books serve as a reminder how important it is to maintain proper operational security. It also highlights the ease at which some of these attacks can be made against an organization or system.

Norberg, Stefan. Securing Windows NT/2000 for the Internet. Sebastopol: O'Reilly and Associates, 2001.
This book essentially gives you a security settings checklist and the step-by-step instructions in order to set the settings.

Shinder, Shinder. ISA Server and Beyond: Real World Security Solutions for Microsoft Enterprise Networks. Rockland: Syngress Publishing, Inc., 2002.
ISA Server is a complex program that requires many options and contains many nuances especially when publishing services to the Internet. This book outlines the tasks that need to be performed and the settings that need to be set in order to configure ISA properly and securely.

Part 2: Audit Checklist

Item #	Checklist Item	Checklist Detail
1	Review user account procedures for disabling inactive accounts.	• **Reference:** Microsoft; http://www.microsoft.com/technet/security/topics/issues/w2kccscg/w2kscgce.mspx?pf=true • **Risk:** The security design of this network is dependent on user authentication and inactive user accounts could indicate that users no longer with the organization could still access the systems or the accounts could be compromised. The threat this vulnerability represent is significant to the system. The concept of least privilege is important to this environment because the security relies on the strength of the username/password combination. Poor user account management could easily lead to a system compromise.

		• **Testing Procedure:** The test for inactive user accounts is accomplished through the use of the InactiveUser script (script code can be found in the Appendix). This script will query the server and/or domain (which ever is required) for account that have not been logged in for 8 weeks or longer. • **Test Nature:** This test is *Objective*. • **Evidence:** • **Findings:**
2	Verify that service packs and hot fixes are installed.	• **Reference:** Microsoft; http://www.microsoft.com/technet/security/topics/issues/w2kccscg/w2kscgce.mspx?pf=true • **Risk:** The actual risk will vary depending on the nature of the vulnerabilities addressed by the service pack and/or hot fix. The threat that these vulnerabilities could be exploited is fairly high since this system is directly exposed to the Internet. A compromise of this asset could affect the organization's ability to use the Internet, potential data compromise, and the use of internal systems as launch pads for attacks on other organizations. • **Testing Procedure:** This is tested by running Microsoft's Baseline Security Analyzer. This tool will identify which service packs and hot fixes are not installed or not detected. It also verifies and alerts on basic security settings. • **Test Nature:** This test in *Objective* • **Evidence:** • **Findings:**
3	Verify there are no unneeded services and processes.	• **Refernece:** Securing Windows NT/2000 for the Internet • **Risk:** The more running processes there are on a system the more potential vulnerabilities can exist by creating additional vectors for attacks. There is also a system performance issue since each running process consumes system resources so disabling unused services will enhance system performance. Unused services could allow an attacker to exploit a vulnerability that you didn't know existed because you did not know to mitigate it. A successful exploit could affect just this system causing a Denial of Service or potentially causing the system to give private

		information to an attacker. • **Test Procedure:** This test is conducted by a combination of methods. The first thing is to review the security policy to verify which services the system needs to perform in its intended capacity. DumpSec will be utilized to gather a listing of running processes on the system and the following command will be run at the command prompt to determine what services are listening on the network: *netstat –a > c:\netstatresults.txt*. In addition, a port scanner will be employed to verify what ports are active remotely. The port scanner that will be used will be GFI LANGuard N.S.S. Each check will be conducted from the local side and the external side. • **Test Nature:** This test is *Objective*, either the service is running or it isn't. However, the processes that are considered unneeded may be *Subjective* if there is not a security policy in place. • **Evidence:** • **Findings:**
4	Verify secure password storage and cached user credentials.	• **Refernece:** Securing Windows NT/2000 for the Internet • **Risk:** Since access to the entire environment is controlled through usernames and passwords it is vital to protect the passwords. If the passwords were compromised it could lead to a complete system compromise. The logon process stores passwords is what is called an LM hash which is a very weak encryption strategy is useful for backward compatibility but is no longer required is most environments. The LM hash should be disabled in favor of NTLMv2. Additionally, the local machine will cache the logons credentials in case the domain server can't be contacted the user will still be able to log on. The risk is if an administrator logs onto the system those credentials are cached on the local machine. • **Test Procedure:** The procedure to test this is through the use of an automated tool: GFI's LANGuard N.N.S. • **Test Nature:** This test is *Objective*. • **Evidence:** • **Findings:**
5	Restrict null session	• **Reference:** Microsoft;

	access.	http://www.microsoft.com/technet/security/topics/issues/w2kccscg/w2kscgce.mspx?pf=true • **Risk:** The primary risk is giving the attacker a lot of information about the system and the network though the use of connecting through a null session. • **Test Procedure:** This is tested for by running the command (net use \\firewall\ipc$ /user: “” “”) at the command prompt of a remote desktop system. If the command completes successfully then null sessions are permitted. • **Test Nature:** This test is *Objective*. • **Evidence:** • **Findings:**
6	Verify least privilege for users and groups	• **Reference:** SANS: Advanced System Audit: Windows NT/2000. • **Risk:** Since the system are reliant on usernames and passwords as the primary security it is important to know what users have access too and ensure that they do not have access to data that they do not need in case their user account ever becomes compromised. • **Test Procedure:** This is tested by running DumpSec on the system, writing the results to a file. With the results the permissions are checked against the user list and the job responsibilities of the users. • **Test Nature:** This test is *Objective*. • **Evidence:** • **Findings:**
7	Verify removal of POSIX and OS/2 Subsystems	• **Reference:** Microsoft; http://www.microsoft.com/technet/security/topics/issues/w2kccscg/w2kscgce.mspx?pf=true • **Risk:** The risks presented by having these subsystems loaded, primarily they require the use of the LM password hash and are subject to their own vulnerabilities (http://support.microsoft.com/default.aspx?scid=kb;en-us;875496) with varying levels of risk. • **Test Procedure:** This is tested by visually inspecting the system registry for the presence of the key SubSystems in the following registry: HKLM\SYSTEM\Current

		ControlSet\Control\Session Manager. • **Test Nature:** This test is *Objective*. • **Evidence:** • **Findings:**
8	Verify ruleset "agrees with" the security policy and test enforcement.	• **Reference:** A theme throughout the reference material above it that system settings and rulesets should be set in accordance with organization policy. • **Risk:** There are a couple of potential risks with rulesets that don't "agree with" the security policy. Primarily the risk could be more access than intended is granted to the anonymous user or the local user. Additionally there is additional processor utilization required to process more rules. Additionally, with rules that don't "agree" if another firewall administrator reviewed the rules and finds non-compliant rules they may disable or remove those rules causing access to cease to function as expected. Further having non-compliant rules will usually add to the ruleset and long rulesets are difficult to manage and troubleshoot and could lead to unintended consequences, such as, an allow rule allowing an activity that is expressly forbidden in a later rule. • **Test Procedure:** This is tested several ways. First a visual inspection of the ruleset comparing it to the security policy and any change control process to ensure that the ruleset complies and is sufficiently documented. HPING will be utilized in concert with a sniffer to detect if the firewall rules are allowing unauthorized traffic to the internal network. Appendix II illustrates the audit network environment. • **Test Nature:** This test is *Objective*. • **Evidence:** • **Findings:**
9	Confirm that logs are inaccessible to unauthorized individuals.	• **Reference:** Microsoft; http://www.microsoft.com/technet/security/topics/issues/w2kccscg/w2kscgce.mspx?pf=true • **Risk:** If the logs are accessible to unauthorized users it is possible that an attacker could compromise the system and then hide their tracks by modifying the system logs.

		• **Test Procedure:** • **Test Nature:** This test is *Objective*. • **Evidence:** • **Findings:**
10	Perform vulnerability assessment.	• **Reference:** Personal experience. It isn't practical to operate security in a void. Knowing that the system patches and hot fixes are up-to-date is not enough. You must be aware there may be additional known vulnerabilities that may exist with the installed services that the system requires for proper operation. You need to know if these exists so you can either mitigate them or accept them. • **Risk:** If there are additional risks that you are unaware of the system and protected network could be compromised. While many vulnerabilities are technical in nature and can only be corrected through the proper deployment of a vendor patch there are many that are related to improper configuration or combination of services that could lead to vulnerabilities. • **Test Procedure:** This assessment is performed by using two separate automated vulnerability assessment tools. The reason is that each tool is designed a little differently and will often look at the target systems a little differently and can highlight different vulnerabilities and help to reduce false positives if both scanner interpret the data the same way. • **Test Nature:** This test is *Objective*. • **Evidence:** • **Findings:**
11	NetBIOS disabled on external interface	• **Reference:** Microsoft Security Guidance Kit • **Risk:** Servers in the perimeter network should have all unnecessary protocols disabled including NetBIOS and server message block (SMB). Web servers and Domain Name System (DNS) servers do not require NetBIOS or SMB. These protocols should both be disabled to counter the threat of user enumeration. User enumeration is a type of information gathering exploit in which an attacker attempts to obtain system specific information to plan further attacks. The SMB protocol will return rich information about a computer even to unauthenticated users using "null"

		sessions. The information that can be retrieved includes domain and trust details, shares, user information (including groups and user rights), registry keys, and more. Disabling NetBIOS is not sufficient to prevent SMB communication. This is because in the absence of standard NetBIOS ports, SMB will use Transmission Control Protocol (TCP) port 445, which is referred to as SMB Direct Host. As a result, explicit steps must be taken to separately disable both NetBIOS and SMB. • **Test Procedure:** This test is performed by visual inspection in the Network and Dial-up Connections applet. The external facing interface should have the Client for Microsoft Networks and File and Print Sharing for Microsoft Networks. Also the inspection will include verifying that NetBIOS over TCP/IP is disabled from the Device Manager. • **Test Nature:** This test is *Objective*. • **Evidence:** • **Findings:**
12	Verify local address table only includes addresses on the local network	• **Reference:** Microsoft Creating an Access Policy Checklist (http://www.microsoft.com/resources/documentation/isa/2000/enterprise/proddocs/en-us/isadocs/cmt_chckforward.mspx) • **Risk:** By not configuring the LAT correctly it can result in a client request for an internal IP address being routed to the Internet or being redirected through the Firewall service. It can also advertise local routing information out to the Internet. • **Test Procedure:** This item is checked by reviewing the local address table as it is configured in the ISA properties. • **Test Nature:** This test is *Objective*. • **Evidence:** • **Findings:**
13	Harden the TCP/IP Stack Against Denial of Service Attacks	• **Reference:** Windows 2000 Security Configuration Checklist from the Microsoft Security Guidance Kit • **Risk:** This isn't a security risk that could lead to a direct system compromise but could lead to a denial of service that would affect all of the Internet services.

		• **Test Procedure:** This item is checked by reviewing for the existence of the following values in the HKLM\System\CurrentControlSet\Services\Tcpip\Parameters **Values:** 1. DisableSourceIPRouting 2. EnableDeadGWDetect 3. EnableICMPRedirect 4. EnablePMTUDiscovery 5. EnableSecurityFilters 6. KeepAliveTime • **Test Nature:** This test is *Objective*. • **Evidence:** • **Findings:**

Part 3: Conduct the Audit

The audit was conducted on the described system and the results of the audit are presented below:

Audit Results

Checklist Item 1: Fail

<table>
<tr><th>Item #</th><th>Checklist Item</th><th>Checklist Detail</th></tr>
<tr><td>1</td><td>Review user account procedures for disabling inactive accounts.</td><td>
Evidence: The InactiveUsers script yielded the following results:
<table>
<tr><td>abethia</td><td>Inactive for:</td><td>18</td><td>Weeks</td></tr>
<tr><td>admin</td><td>Inactive for:</td><td>82</td><td>Weeks</td></tr>
<tr><td>IWAM_HOMENET</td><td>Inactive for:</td><td>82</td><td>Weeks</td></tr>
<tr><td>IUSR_HOMENET</td><td>Inactive for:</td><td>82</td><td>Weeks</td></tr>
<tr><td>nhardy</td><td>Inactive for:</td><td>82</td><td>Weeks</td></tr>
<tr><td>EUSER_EXSTOREEVENT</td><td>Inactive for:</td><td>82</td><td>Weeks</td></tr>
<tr><td>TsInternetUser</td><td>Inactive for:</td><td>82</td><td>Weeks</td></tr>
<tr><td>Krobertson</td><td>Inactive for:</td><td>24</td><td>Weeks</td></tr>
</table>
Findings: The system has user accounts that are inactive but are still enabled. Due to low staff turnover there are very few user accounts that are inactive from users that have left the organization. Most of the user accounts that are inactive are system generated accounts with “guest” privileges. There are several user accounts that should be disabled immediately; namely, admin and nhardy. The admin account was an account setup for Novell server access and nhardy is a consultant who helped deploy this firewall server. The Novell server is no longer in the environment and is safe to disable or remove.
</td></tr>
</table>

Checklist Item 2: Pass

<table>
<tr><th>Item #</th><th>Checklist Item</th><th>Checklist Detail</th></tr>
<tr><td>2</td><td>Verify that service packs and hot fixes are installed.</td><td>
Evidence: MBSA Scan results:
<table>
<tr><td>Computer name:</td><td>local\FIREWALL</td></tr>
<tr><td>IP address:</td><td>10.10.1.23</td></tr>
<tr><td>Security report name:</td><td>local - FIREWALL (9-28-2004 12-48 PM)</td></tr>
<tr><td>Scan date:</td><td>9/28/2004 12:48 PM</td></tr>
<tr><td>Security update database version:</td><td>2004.9.14.0</td></tr>
<tr><td>Office update</td><td>11.0.0.6914</td></tr>
</table>
</td></tr>
</table>

		Security assessment: Strong Security (All checks were passed.) **Security Updates** Score / Issue / Result Check passed / Windows Security Updates / No critical security updates are missing. Check passed / Office Updates / No critical security updates are missing. Check passed / MDAC Security Updates / No critical security updates are missing. Check passed / MSXML Security Updates / No critical security updates are missing. • **Findings:** MBSA scans report that all critical and security updates have been installed on this system

Checklist Item 3: Fail

Item #	Checklist Item	Checklist Detail
3	Verify there are no unneeded services and processes.	• **Evidence:** The following services are shown to be running by DumpSec:

FriendlyName	Name	Status
3Com EtherLink XL B/C Adapter Driver	EL90BC	Running
AFD Networking Support Environment	AFD	Running
Alerter	Alerter	Running
Audio Stub Driver	audstub	Running
Automatic Updates	wuauserv	Running
Background Intelligent Transfer Service	BITS	Running
Beep	Beep	Running
Cdfs	Cdfs	Running
CD-ROM Driver	Cdrom	Running
COM+ Event System	EventSystem	Running
Computer Browser	Browser	Running
DfsDriver	DfsDriver	Running
DHCP Client	Dhcp	Running
DHCP Server	DHCPServer	Running
Direct Parallel	Raspti	Running
Direct Parallel Link Driver	Ptilink	Running
Disk Driver	Disk	Running
Diskperf	Diskperf	Running
Distributed File System	Dfs	Running
Distributed Link Tracking Client	TrkWks	Running
Distributed Link Tracking Server	TrkSvr	Running
Distributed Transaction Coordinator	MSDTC	Running

		Dmload	dmload	Running		
		DNS Client	Dnscache	Running		
		DNS Server	DNS	Running		
		EFS	EFS	Running		
		Event Log	Eventlog	Running		
		Fastfat	Fastfat	Running		
		File Replication Service	NtFrs	Running		
		Fips	Fips	Running		
		Floppy Disk Controller Driver	Fdc	Running		
		Floppy Disk Driver	Flpydisk	Running		
		Game Port Enumerator	gameenum	Running		
		Generic Packet Classifier	Gpc	Running		
		i8042 Keyboard and PS/2 Mouse Port Driver	i8042prt	Running		
		i81x	i81x	Running		
		IntelIde	IntelIde	Running		
		Intersite Messaging	IsmServ	Running		
		IP Network Address Translator	IpNat	Running		
		IP Traffic Filter Driver	IpFilterDriver	Running		
		IPSEC driver	IPSEC	Running		
		IPSEC Policy Agent	PolicyAgent	Running		
		Kerberos Key Distribution Center	kdc	Running		
		Keyboard Class Driver	Kbdclass	Running		
		KSecDD	KSecDD	Running		
		License Logging Service	LicenseService	Running		
		Logical Disk Manager	dmserver	Running		
		Logical Disk Manager Driver	dmio	Running		
		Messenger	Messenger	Running		
		Microcode Update Driver	Update	Running		
		Microsoft ACPI Driver	ACPI	Running		
		Microsoft MPU-401 MIDI UART Driver	ms_mpu401	Running		
		Microsoft Search	MSSEARCH	Running		
		Microsoft System Audio Device	sysaudio	Running		
		Microsoft USB Standard Hub Driver	usbhub	Running		
		Microsoft USB Universal Host Controller Driver	uhcd	Running		
		Microsoft WINMM WDM Audio Compatibility Driver	wdmaud	Running		
		Mnmdd	mnmdd	Running		
		MountMgr	MountMgr	Running		
		Mouse Class Driver	Mouclass	Running		
		MRxSmb	MRxSmb	Running		
		Msfs	Msfs	Running		
		Mup	Mup	Running		
		NDIS Proxy	NDProxy	Running		
		NDIS System Driver	NDIS	Running		
		Net Logon	Netlogon	Running		
		NetBIOS Interface	NetBIOS	Running		
		NetBios over Tcpip	NetBT	Running		
		Network Connections	Netman	Running		

Npfs	Npfs	Running		
NT LM Security Support Provider	NtLmSsp	Running		
Ntfs	Ntfs	Running		
Null	Null	Running		
Parallel class driver	Parallel	Running		
Parallel port driver	Parport	Running		
PartMgr	PartMgr	Running		
ParVdm	ParVdm	Running		
PCI Bus Driver	PCI	Running		
Plug and Play	PlugPlay	Running		
PnP ISA/EISA Bus Driver	isapnp	Running		
Print Spooler	Spooler	Running		
Protected Storage	ProtectedStorage	Running		
QoS Packet Scheduler	PSched	Running		
Rdbss	Rdbss	Running		
Remote Access Auto Connection Driver	RasAcd	Running		
Remote Access IP ARP Driver	Wanarp	Running		
Remote Access NDIS TAPI Driver	NdisTapi	Running		
Remote Access NDIS WAN Driver	NdisWan	Running		
Remote Procedure Call (RPC)	RpcSs	Running		
Remote Procedure Call (RPC) Locator	RpcLocator	Running		
Remote Registry Service	RemoteRegistry	Running		
Removable Storage	NtmsSvc	Running		
RunAs Service	seclogon	Running		
Security Accounts Manager	SamSs	Running		
Serenum Filter Driver	serenum	Running		
Serial port driver	Serial	Running		
Server	lanmanserver	Running		
Service for AC'97 Driver (WDM)	ichaud	Running		
Software Bus Driver	swenum	Running		
Srv	Srv	Running		
Standard IDE/ESDI Hard Disk Controller	atapi	Running		
System Event Notification	SENS	Running		
Task Scheduler	Schedule	Running		
TCP/IP NetBIOS Helper Service	LmHosts	Running		
TCP/IP Protocol Driver	Tcpip	Running		
VgaSave	VgaSave	Running		
VIA VT86C100A PCI Fast Ethernet Adapter NT Driver	FETNDIS	Running		
Volume Manager Driver	Ftdisk	Running		
WAN Miniport (L2TP)	Rasl2tp	Running		
WAN Miniport (PPTP)	PptpMiniport	Running		
Windows Management Instrumentation	WinMgmt	Running		
Windows Management Instrumentation Driver Extensions	Wmi	Running		
Windows Time	W32Time	Running		
Workstation	lanmanworkstation	Running		

The netstat results show which processes are listening for remote connections:

Active	Connections		
Protocol	Local Address	Foreign Address State	
TCP	firewall:kerberos	firewall.local.homenet.com:0	LISTENING
TCP	firewall:epmap	firewall.local.homenet.com:0	LISTENING
TCP	firewall:ldap	firewall.local.homenet.com:0	LISTENING
TCP	firewall:microsoft-ds	firewall.local.homenet.com:0	LISTENING
TCP	firewall:kpasswd	firewall.local.homenet.com:0	LISTENING
TCP	firewall:593	firewall.local.homenet.com:0	LISTENING
TCP	firewall:ldaps	firewall.local.homenet.com:0	LISTENING
TCP	firewall:1026	firewall.local.homenet.com:0	LISTENING
TCP	firewall:1029	firewall.local.homenet.com:0	LISTENING
TCP	firewall:1037	firewall.local.homenet.com:0	LISTENING
TCP	firewall:3002	firewall.local.homenet.com:0	LISTENING
TCP	firewall:3003	firewall.local.homenet.com:0	LISTENING
TCP	firewall:3004	firewall.local.homenet.com:0	LISTENING
TCP	firewall:3069	firewall.local.homenet.com:0	LISTENING
TCP	firewall:3080	firewall.local.homenet.com:0	LISTENING
TCP	firewall:3129	firewall.local.homenet.com:0	LISTENING
TCP	firewall:3146	firewall.local.homenet.com:0	LISTENING
TCP	firewall:3226	firewall.local.homenet.com:0	LISTENING
TCP	firewall:3259	firewall.local.homenet.com:0	LISTENING
TCP	firewall:3268	firewall.local.homenet.com:0	LISTENING
TCP	firewall:3269	firewall.local.homenet.com:0	LISTENING
TCP	firewall:3372	firewall.local.homenet.com:0	LISTENING
TCP	firewall:3431	firewall.local.homenet.com:0	LISTENING
TCP	firewall:4135	firewall.local.homenet.com:0	LISTENING
TCP	firewall:33770	firewall.local.homenet.com:0	LISTENING
TCP	firewall:33822	firewall.local.homenet.com:0	LISTENING
TCP	firewall:34323	firewall.local.homenet.com:0	LISTENING
TCP	firewall:34325	firewall.local.homenet.com:0	LISTENING
TCP	firewall:34327	firewall.local.homenet.com:0	LISTENING
TCP	firewall:35655	firewall.local.homenet.com:0	LISTENING
TCP	firewall:35979	firewall.local.homenet.com:0	LISTENING
TCP	firewall:36086	firewall.local.homenet.com:0	LISTENING
TCP	firewall:36326	firewall.local.homenet.com:0	LISTENING
TCP	firewall:domain	firewall.local.homenet.com:0	LISTENING
TCP	firewall:netbios-ssn	firewall.local.homenet.com:0	LISTENING
TCP	firewall:netbios-ssn	LDZIUBA:1272 ESTAB	LISHED
TCP	firewall:ldap	firewall.local.homenet.com:3	3822 ESTABLISHED
TCP	firewall:ldap	firewall.local.homenet.com:3	6326 FIN_WAIT_2
TCP	firewall:1026	firewall.local.homenet.com:3	259 ESTABLISHED
TCP	firewall:1026	firewall.local.homenet.com:3	431 ESTABLISHED
TCP	firewall:1026	FIREWALL2:3553 ESTAB	LISHED
TCP	firewall:3259	firewall.local.homenet.com:1	026 ESTABLISHED
TCP	firewall:3431	firewall.local.homenet.com:1	026 ESTABLISHED
TCP	firewall:4135	DFX3XG21:microsoft-ds ESTAB	LISHED
TCP	firewall:33822	firewall.local.homenet.com:l	dap ESTABLISHED
TCP	firewall:34323	v4-ori.windowsupdate.microso	ft.com:http CLOSE_WAIT
TCP	firewall:34325	207.46.253.188:http CLOSE	_WAIT
TCP	firewall:36086	firewall.local.homenet.com:l	dap CLOSE_WAIT

		TCP	firewall:36326	firewall.local.homenet.com:l	dap CLOSE_WAIT
		TCP	firewall:domain	firewall.local.homenet.com:0	LISTENING
		TCP	firewall:ldap	firewall.local.homenet.com:3	002 ESTABLISHED
		TCP	firewall:ldap	firewall.local.homenet.com:3	003 ESTABLISHED
		TCP	firewall:ldap	firewall.local.homenet.com:3	3770 ESTABLISHED
		TCP	firewall:3002	firewall.local.homenet.com:l	dap ESTABLISHED
		TCP	firewall:3003	firewall.local.homenet.com:l	dap ESTABLISHED
		TCP	firewall:33770	firewall.local.homenet.com:l	dap ESTABLISHED
		TCP	firewall:35979	firewall.local.homenet.com:l	dap CLOSE_WAIT
		TCP	firewall:netbios-ssn	firewall.local.homenet.com:0	LISTENING
		UDP	firewall:bootpc	*:*	
		UDP	firewall:epmap	*:*	
		UDP	firewall:microsoft-ds	*:*	
		UDP	firewall:1028	*:*	
		UDP	firewall:1040	*:*	
		UDP	firewall:1043	*:*	
		UDP	firewall:3001	*:*	
		UDP	firewall:3008	*:*	
		UDP	firewall:3134	*:*	
		UDP	firewall:3135	*:*	
		UDP	firewall:3256	*:*	
		UDP	firewall:3493	*:*	
		UDP	firewall:3924	*:*	
		UDP	firewall:4383	*:*	
		UDP	firewall:5057	*:*	
		UDP	firewall:domain	*:*	
		UDP	firewall:bootps	*:*	
		UDP	firewall:bootpc	*:*	
		UDP	firewall:kerberos	*:*	
		UDP	firewall:ntp	*:*	
		UDP	firewall:netbios-ns	*:*	
		UDP	firewall:netbios-dgm	*:*	
		UDP	firewall:389	*:*	
		UDP	firewall:kpasswd	*:*	
		UDP	firewall:isakmp	*:*	
		UDP	firewall:2535	*:*	
		UDP	firewall:domain	*:*	
		UDP	firewall:3133	*:*	
		UDP	firewall:36433	*:*	
		UDP	firewall:bootps	*:*	
		UDP	firewall:bootpc	*:*	
		UDP	firewall:kerberos	*:*	
		UDP	firewall:ntp	*:*	
		UDP	firewall:netbios-ns	*:*	
		UDP	firewall:netbios-dgm	*:*	
		UDP	firewall:389	*:*	
		UDP	firewall:kpasswd	*:*	
		UDP	firewall:isakmp	*:*	
		UDP	firewall:2535	*:*	
		• **Findings:** There are many services that are probably unneeded and can be disabled without affecting the			

		system's performance in its intended activity—in fact it may help by reducing the memory and processor needs for the unneeded services. The services that should be disabled are: 1. Alerter 2. Audio Stub Driver 3. Automatic Updates 4. Background Intelligent Transfer Service 5. Beep 6. CDFS 7. CD-Rom Driver 8. DHCP Client 9. Direct Parallel 10. Direct Parallel Link Driver 11. Distributed File System 12. Distributed Link Tracking Client 13. Distributed Link Tracking Server 14. EFS 15. Game Port Enumerator 16. Intersite Messaging 17. Microsoft System Audio Device 18. Microsoft USB Standard Hub Driver 19. Microsoft USB Universal Host Controller Driver 20. Microsoft WINMM WDM Audio Compatibility Driver 21. Parallel class driver 22. Parallel port driver 23. Remote Registry Service

Checklist Item 4: Fail

Item #	Checklist Item	Checklist Detail
4	Verify secure password storage and cached user credentials.	• **Evidence:** Due to space limitations the evidence for this item can be found in Figure 2 at the end of this checklist. • **Findings:** Passwords are stored in the insecure LM password hash.

Checklist Item 5: Fail

Item #	Checklist Item	Checklist Detail
5	Restrict null session access.	• **Evidence:** C:\>net use \\firewall\ipc$ /user: "" "" The command completed successfully. • **Findings:** A null user can connect to this server. This allows the person connecting to survey a lot of information about this system.

Checklist Item 6: Pass

Item #	Checklist Item	Checklist Detail
6	Verify least privilege for users and groups	• **Evidence:** The share permissions from DumpSec followed by the user rights at the server level.

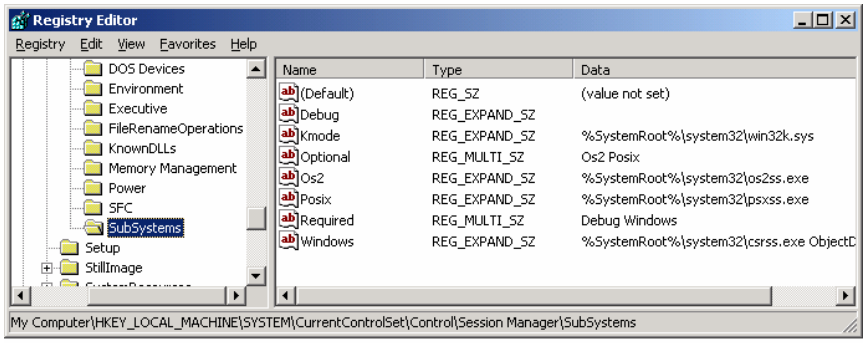
Share and path	Account	Own
My Documents=C:\Documents and Settings\Administrator\My Documents (disktree)	LOCAL\Administrators	all
IPC$= (special admin share)		admin-only (no dacl)
D$=D:\ (special admin share)		admin-only (no dacl)
NETLOGON=C:\WINNT\SYSVOL\sysvol\local.homenet.com\SCRIPTS (disktree)	Everyone	read
NETLOGON=C:\WINNT\SYSVOL\sysvol\local.homenet.com\SCRIPTS (disktree)	LOCAL\Administrators	all
Firewall Client=C:\Program Files\Microsoft ISA Server\CLIENTS (disktree)		unprotected (no dacl)
ADMIN$=C:\WINNT (special admin share)		admin-only (no dacl)
SYSVOL=C:\WINNT\SYSVOL\sysvol (disktree)	Everyone	read
SYSVOL=C:\WINNT\SYSVOL\sysvol (disktree)	LOCAL\Administrators	all
SYSVOL=C:\WINNT\SYSVOL\sysvol (disktree)	Authenticated Users	all
C$=C:\ (special admin share)		admin-only (no dacl)

User Right	Account
SeNetworkLogonRight	BUILTIN\Administrators
SeNetworkLogonRight	LOCAL\IUSR_HOMENET
SeNetworkLogonRight	LOCAL\IWAM_HOMENET
SeNetworkLogonRight	NT AUTHORITY\Authenticated Users
SeNetworkLogonRight	Everyone
SeTcbPrivilege	
SeMachineAccountPrivilege	NT AUTHORITY\Authenticated Users
SeBackupPrivilege	BUILTIN\Backup Operators
SeBackupPrivilege	BUILTIN\Server Operators
SeBackupPrivilege	BUILTIN\Administrators
SeChangeNotifyPrivilege	BUILTIN\Administrators
SeChangeNotifyPrivilege	NT AUTHORITY\Authenticated Users
SeChangeNotifyPrivilege	Everyone
SeSystemtimePrivilege	BUILTIN\Server Operators
SeSystemtimePrivilege	BUILTIN\Administrators

SeCreatePagefilePrivilege	BUILTIN\Administrators
SeCreateTokenPrivilege	
SeCreatePermanentPrivilege	
SeDebugPrivilege	BUILTIN\Administrators
SeRemoteShutdownPrivilege	BUILTIN\Server Operators
SeRemoteShutdownPrivilege	BUILTIN\Administrators
SeAuditPrivilege	
SeIncreaseQuotaPrivilege	BUILTIN\Administrators
SeIncreaseBasePriorityPrivilege	BUILTIN\Administrators
SeLoadDriverPrivilege	BUILTIN\Administrators
SeLockMemoryPrivilege	
SeBatchLogonRight	LOCAL\IUSR_HOMENET
SeBatchLogonRight	LOCAL\IWAM_HOMENET
SeBatchLogonRight	NT AUTHORITY\SYSTEM
SeServiceLogonRight	
SeInteractiveLogonRight	BUILTIN\Backup Operators
SeInteractiveLogonRight	BUILTIN\Print Operators
SeInteractiveLogonRight	BUILTIN\Server Operators
SeInteractiveLogonRight	BUILTIN\Account Operators
SeInteractiveLogonRight	BUILTIN\Administrators
SeInteractiveLogonRight	LOCAL\IUSR_HOMENET
SeInteractiveLogonRight	LOCAL\TsInternetUser
SeSecurityPrivilege	BUILTIN\Administrators
SeSecurityPrivilege	LOCAL\Exchange Enterprise Servers
SeSystemEnvironmentPrivilege	BUILTIN\Administrators
SeProfileSingleProcessPrivilege	BUILTIN\Administrators
SeSystemProfilePrivilege	BUILTIN\Administrators
SeAssignPrimaryTokenPrivilege	
SeRestorePrivilege	BUILTIN\Backup Operators
SeRestorePrivilege	BUILTIN\Server Operators
SeRestorePrivilege	BUILTIN\Administrators
SeShutdownPrivilege	BUILTIN\Backup Operators
SeShutdownPrivilege	BUILTIN\Print Operators
SeShutdownPrivilege	BUILTIN\Server Operators
SeShutdownPrivilege	BUILTIN\Account Operators
SeShutdownPrivilege	BUILTIN\Administrators
SeTakeOwnershipPrivilege	BUILTIN\Administrators

- **Findings:** This checklist item passes but some modification to the permissions and rights should be considered. The Everyone group should probably not be given any rights instead that could be changed to authenticated users to minimize the risk associated with visiting people with laptop from gaining any kind of system access without having valid network credentials.

Checklist Item 7: Fail

Item #	Checklist Item	Checklist Detail
7	Verify removal of POSIX and OS/2 Subsystems	• **Evidence:**  • **Findings:** Both the POSIX and OS/2 subsystems are present on this system and should be removed.

Checklist Item 8: Pass

Item #	Checklist Item	Checklist Detail
8	Verify ruleset “agrees with” the security policy and test enforcement.	• **Evidence:** HPING results /hping2-rc3 root# /usr/sbin/hping --syn --destport 80 216.56.xxx.xxx HPING 216.56.xxx.xxx (en0 216.56.xxx.xxx): S set, 40 headers + 0 data bytes ^C --- 216.56.xxx.xxx hping statistic --- 5 packets tramitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms /hping2-rc3 root# /usr/sbin/hping -S -A -c 5 -p 80 216.56.xxx.xxx HPING 216.56.xxx.xxx (en0 216.56.xxx.xxx): SA set, 40 headers + 0 data bytes --- 216.56.xxx.xxx hping statistic --- 5 packets tramitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms /hping2-rc3 root# /usr/sbin/hping --icmp --icmptype 13A -c 5 216.56.xxx.xxx HPING 216.56.xxx.xxx (en0 216.56.xxx.xxx): icmp mode set, 28 headers + 0 data bytes --- 216.56.xxx.xxx hping statistic --- 5 packets tramitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms /hping2-rc3 root# /usr/sbin/hping -S -p 80 -c 5 216.56.xxx.xxx HPING 216.56.xxx.xxx (en0 216.56.xxx.xxx): S set, 40 headers + 0 data bytes --- 216.56.xxx.xxx hping statistic --- 5 packets tramitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms /hping2-rc3 root# /usr/sbin/hping -S -p 21 -c 5 216.56.xxx.xxx HPING 216.56.xxx.xxx (en0 216.56.xxx.xxx): S set, 40 headers + 0 data bytes len=46 ip=216.56.xxx.xxx ttl=128 DF id=12577 sport=21 flags=SA seq=0 win=65535 rtt=0.9 ms len=46 ip=216.56.xxx.xxx ttl=128 DF id=12578 sport=21 flags=SA seq=1 win=65535 rtt=0.6 ms len=46 ip=216.56.xxx.xxx ttl=128 DF id=12579 sport=21 flags=SA seq=2 win=65535 rtt=0.6 ms len=46 ip=216.56.xxx.xxx ttl=128 DF id=12580 sport=21 flags=SA seq=3

		win=65535 rtt=0.6 ms len=46 ip=216.56.xxx.xxx ttl=128 DF id=12581 sport=21 flags=SA seq=4 win=65535 rtt=0.6 ms --- 216.56.xxx.xxx hping statistic --- 5 packets tramitted, 5 packets received, 0% packet loss round-trip min/avg/max = 0.6/0.7/0.9 ms • **Findings:** The firewall rules agree with the security policy and the firewall is properly enforcing the security rules.

Checklist Item 9: Fail

Item #	Checklist Item	Checklist Detail
9	Confirm that logs are inaccessible to unauthorized individuals.	• **Evidence:** Due to space limitations the evidence for this item can be found in Figure 2 at the end of this checklist. • **Findings:** GFI's LANguard reports that guest users have access to the System, Application, and Security logs. This can allow unauthorized changes to the logs that can hide unauthorized access.

Checklist Item 10: Pass, see findings

Item #	Checklist Item	Checklist Detail
10	Perform vulnerability assessment.	• **Evidence:** See Appendix 3 • **Findings:** From the internal perspective there are many vulnerabilities. However, from the external perspective there is only one vulnerability of any significance: it may be possible to case a denial of service with FTP but since the firewall proxies the incoming FTP requests there may not be an actual security hole with respect to the actual FTP server. Overall from an external perspective the system is secure from a technical perspective.

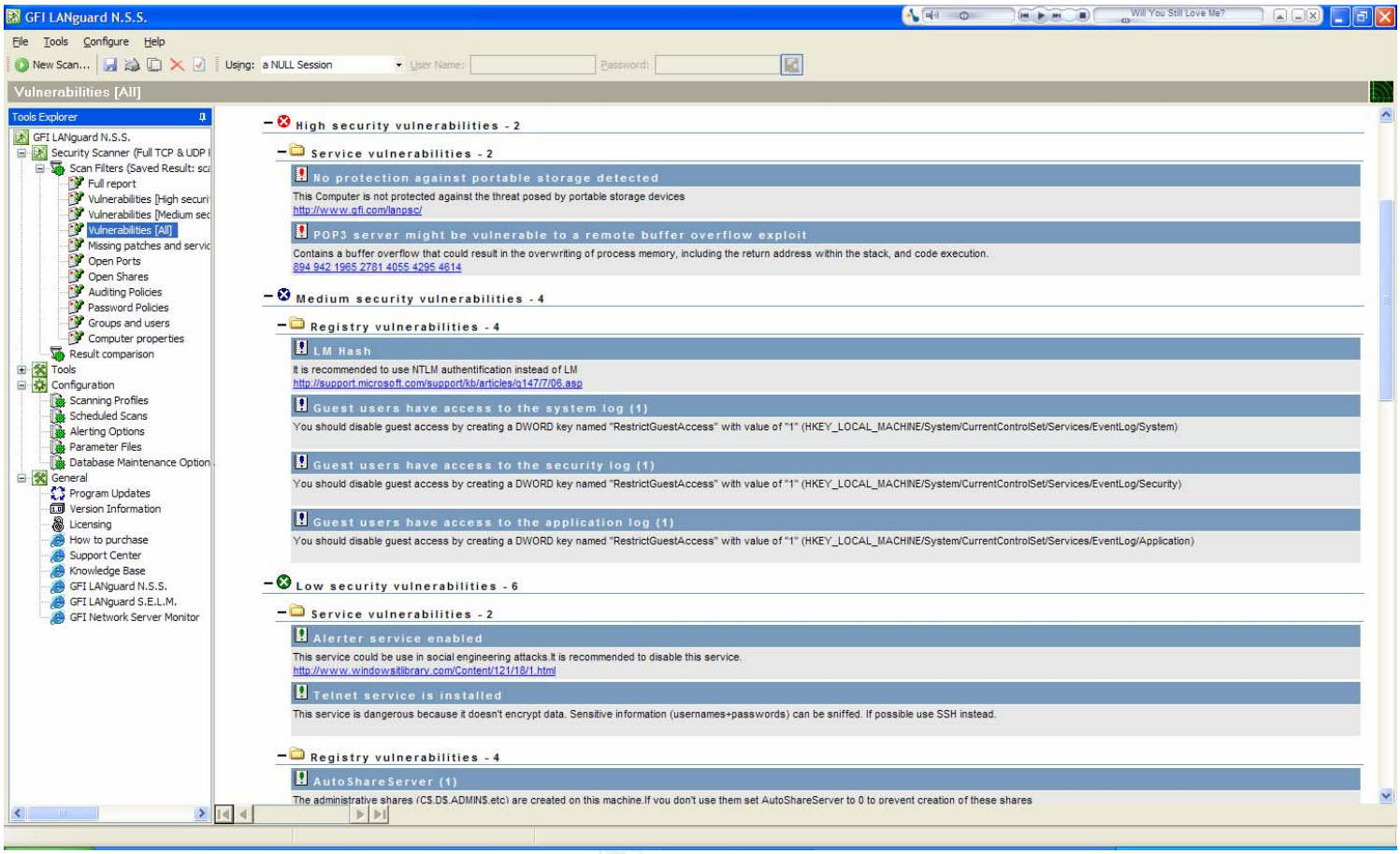


Figure 2

Part 4: Audit Report

Executive Summary

This audit reviewed the security of the organization's firewall and the primary objective was to verify the technical security from outside attackers. The audit looked at the security settings of the system from both the internal and the external perspectives. Portions of the audit were conducted during off hours in order to minimize the effects of any unplanned service interruption.

The audit was conducted with a combination of tools, scripts, and visual inspection. The tools used primarily included; GFI's LANguard N.S.S., Somarsoft's DumpSec, HPING, Ethereal, and a customized script from Managing Windows with VBScript and WMI. The audit checklist development relied heavily on the vendor's checklists.

Overall the audit objectives were met. The result of the audit shows that the security from the outside is solid, but there is a lack of internal security. This is

very typical in many organizations the have a hard, crunchy outside and a soft chewy inside.

Audit Findings

The core finding of the audit is that the internal security policy is not developed sufficiently to adequately protect the organization's IT resources. The organization is adequately protected from external technical attacks from outside attackers. Typical reconnaissance activities will not reveal overmuch about the environment and is well protected from basic scripted and automated attacks. However, the audit showed that the internal security and policies are lacking and can leave the organization open to attacks from disgruntled employees, and password guessing attacks from the use of simple passwords with infrequent password changes. The problem with maintaining weak passwords is the amount of damage an attacker could do with a compromised username and password combination. If an attacker were to compromise a username and password, they would have the same level of access as that person. By not enforcing the prompt removal and/or disabling of user accounts exacerbates the potential for compromise by disgruntled users or general attackers. Checklist item 1 shows that there are currently several accounts that should be disabled or removed.

Abethia	Inactive for:	18	Weeks
Admin	Inactive for:	82	Weeks
IWAM_HOMENET	Inactive for:	82	Weeks
IUSR_HOMENET	Inactive for:	82	Weeks
Nhardy	Inactive for:	82	Weeks
EUSER_EXSTOREEVENT	Inactive for:	82	Weeks
TsInternetUser	Inactive for:	82	Weeks
Krobertson	Inactive for:	24	Weeks

Very critical in maintaining security and system performance is timely installation of service packs and hotfixes. Checklist item 2 finds that the system is current with all of the Microsoft recommended service packs and hotfixes.

Computer name:	local\FIREWALL
IP address:	10.10.1.23
Security report name:	local - FIREWALL (9-28-2004 12-48 PM)
Scan date:	9/28/2004 12:48 PM
Security update database version:	2004.9.14.0
Office update database version:	11.0.0.6914
Security assessment:	Strong Security (All checks were passed.)

Unneeded services and processes can create potential security holes and utilize more system resources on the system which hinders optimal performance. The following services could be disabled:

1. Alerter
2. Audio Stub Driver
3. Automatic Updates
4. Background Intelligent Transfer Service
5. Beep
6. CDFS
7. CD-Rom Driver
8. DHCP Client
9. Direct Parallel
10. Direct Parallel Link Driver
11. Distributed File System
12. Distributed Link Tracking Client
13. Distributed Link Tracking Server
14. EFS
15. Game Port Enumerator
16. Intersite Messaging
17. Microsoft System Audio Device
18. Microsoft USB Standard Hub Driver
19. Microsoft USB Universal Host Controller Driver
20. Microsoft WINMM WDM Audio Compatibility Driver
21. Parallel class driver
22. Parallel port driver
23. Remote Registry Service

Keep in mind that these services should be disabled during off-peak hours and tested to ensure that the disabled services do not have a negative impact on system operations.

As eluded to at the beginning of this section strong passwords and password storage is imperative. Checklist item 4 (see also figure 2) finds that passwords are stored in the weak LM hash.

Generally, the audit found that security has been omitted in the internal environment. Checklist items 5, 6, and 7 show that anyone physically connected to the network would be able to get complete system reconnaissance. Checklist item 9 shows that users with guest access would be able to access the logs, see figure 2.

The vulnerability assessment (see Appendix 3) shows that there are major vulnerabilities to the system from an internal system scan but no major vulnerabilities from an external perspective.

Audit Recommendations

Essentially, the core recommendation is that internal policy and procedures should be modified to increase the internal security posture. Critical is the password management procedures. The password management can be handled through system policies and will add no additional costs to maintaining the system, outside of the administrator's time to set up the policies initially.

It is also recommended that the registry changes required to address checklist items 5, 7, and 9 be performed. These changes are one time changes and do not add to the cost of maintaining the system and should be implemented immediately.

Appendix 1: Test Script Used

Inactive Users

```
Dim dDate
Dim oUser
Dim oObject
Dim oGroup
Dim iFlags
Dim iDiff
Dim iResult
Const UF_ACCOUNTDISABLE = &H0002

'Set this to TRUE to enable Logging only mode –
'no changes will be made
CONST LogOnly = TRUE

'Point to oObject containing users to check
Set oGroup = GetObject("WinNT://firewall/Domain Users")
On error resume next
For each oObject in oGroup.Members

 'Find all User Objects Within Domain Users group
 '(ignore machine accounts)
 If (oObject.Class = "User") And _
  (InStr(oObject.Name, "$") = 0) Then
  Set oUser = GetObject(oObject.ADsPath)
 End If

 dDate = oUser.get("LastLogin")
 dDate = Left(dDate,8)
```

```
 dDate = CDate(dDate)

'find difference in weeks between then and now
 iDiff = DateDiff("ww", dDate, Now)

 'if 8 weeks or more then disable the account
 If iDiff >= 8 Then
  iFlags = oUser.Get("UserFlags")
 End If

 If (iFlags AND UF_ACCOUNTDISABLE) = 0 Then

  ' Only disable accounts if LogOnly set to FALSE
  If LogOnly = False Then
   oUser.Put "UserFlags", iFlags OR UF_ACCOUNTDISABLE
   oUser.SetInfo
  End if

  sName = oUser.Name
  iResult = Log(sName,iDiff)
 End If
Next

Set oGroup = Nothing
MsgBox "All Done!"

Function Log(sUser,sDate)

 'Constant for Log file path
 CONST StrLogFile = "C:\UserMgr1.txt"

 Set oFS = CreateObject("Scripting.FileSystemObject")
 Set oTS = oFS.OpenTextFile(strLogFile, 8, True)
 oTS.WriteLine("Account:" & vbTab & sUser & vbTab & _
  "Inactive for:" & vbTab & sDate & vbTab & "Weeks" & _
  vbTab & "Disabled on:" & vbTab & Date & vbTab & "at:" & _
  vbTab & Time)
  oTS.Close
  Set oFS = Nothing
  Set oTS = Nothing

End Function
```

Appendix 2: Network Layout for Audit

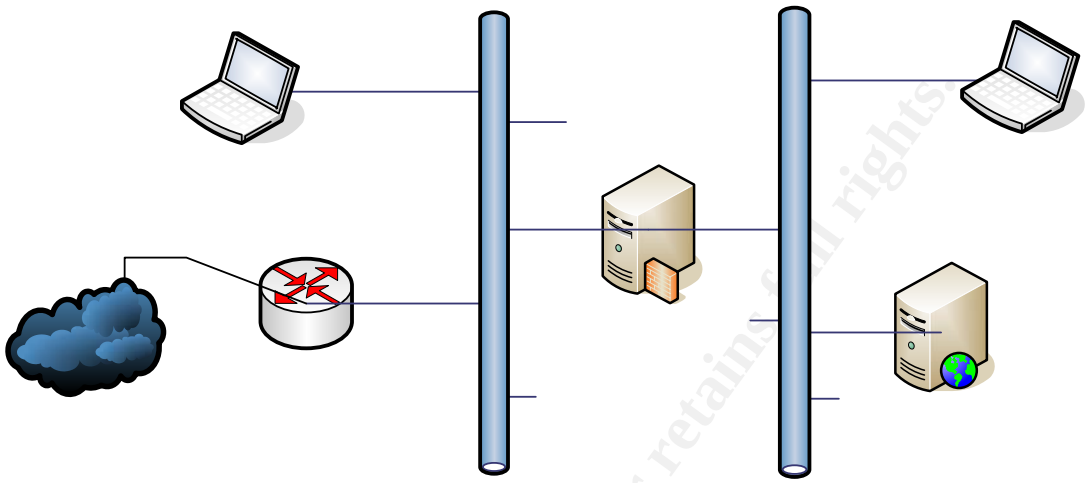


Figure 3

Vulnerability assessment tool and Hping

Internet

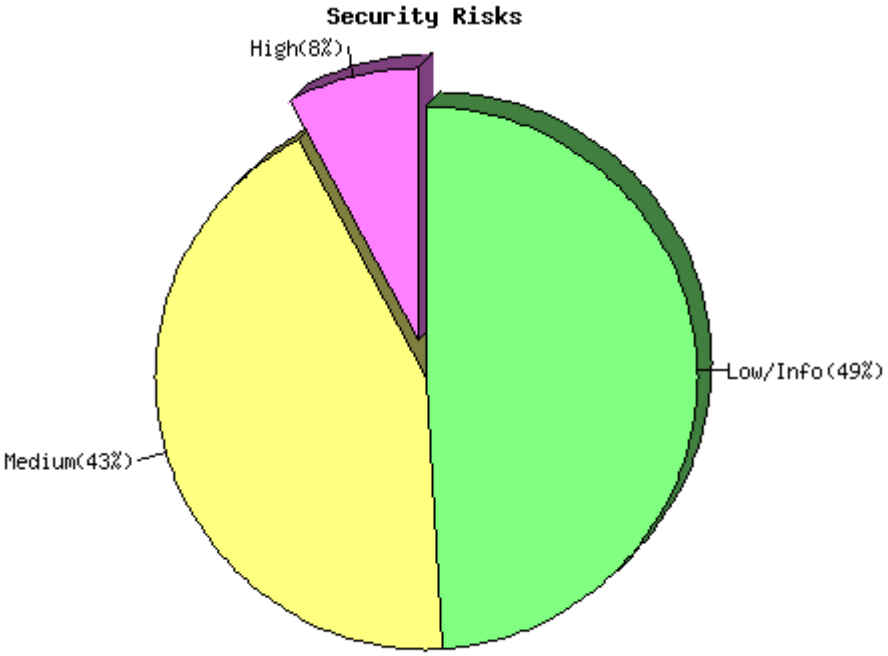
Cisco Edge Router

Appendix 3: Vulnerability Analysis Report

Internal Perspective:

firewall

Repartition of the level of the security problems :



[Back to the index]

List of open ports :

- *domain (53/tcp) (Security warnings found)*
- *kerberos (88/tcp)*
- *netbios-ssn (139/tcp) (Security notes found)*
- *epmap (135/tcp) (Security warnings found)*
- *ldap (389/tcp) (Security warnings found)*
- *microsoft-ds (445/tcp) (Security hole found)*
- *kpasswd (464/tcp)*
- *http-rpc-epmap (593/tcp)*
- *ldaps (636/tcp) (Security notes found)*
- *cap (1026/tcp) (Security notes found)*
- *csoftragent (3004/tcp) (Security notes found)*
- *ls3 (3069/tcp) (Security notes found)*
- *stm_pproc (3080/tcp) (Security notes found)*
- *bears-02 (3146/tcp) (Security notes found)*

- *netport-id (3129/tcp) (Security notes found)*
- *isi-irp (3226/tcp) (Security notes found)*
- *msft-gc-ssl (3269/tcp) (Security notes found)*
- *msft-gc (3268/tcp)*
- *tip2 (3372/tcp) (Security notes found)*
- *general/tcp (Security warnings found)*
- *general/icmp (Security warnings found)*
- *domain (53/udp) (Security notes found)*
- *bootps (67/udp) (Security notes found)*
- *general/udp (Security notes found)*
- *ntp (123/udp) (Security notes found)*
- *netbios-ns (137/udp) (Security warnings found)*
- *unknown (1029/tcp) (Security notes found)*
- *unknown (1037/tcp) (Security notes found)*
- *unknown (1028/udp) (Security notes found)*

[back to the list of ports]

Warning found on port domain (53/tcp)

The remote name server allows recursive queries to be performed
by the host running nessusd.

If this is your internal nameserver, then forget this warning.

If you are probing a remote nameserver, then it allows anyone
to use it to resolve third parties names (such as www.nessus.org).
This allows hackers to do cache poisoning attacks against this
nameserver.

If the host allows these recursive queries via UDP,
then the host can be used to 'bounce' Denial of Service attacks
against another network or system.

See also : http://www.cert.org/advisories/CA-1997-22.html

Solution : Restrict recursive queries to the hosts that should
use this nameserver (such as those of the LAN connected to it).

If you are using bind 8, you can do this by using the instruction
'allow-recursion' in the 'options' section of your named.conf

If you are using bind 9, you can define a grouping of internal addresses
using the 'acl' command

Then, within the options block, you can explicitly state:
'allow-recursion { hosts_defined_in_acl }'

For more info on Bind 9 administration (to include recursion), see:
http://www.nominum.com/content/documents/bind9arm.pdf

If you are using another name server, consult its documentation.

Risk factor : High
CVE : CVE-1999-0024
BID : 136, 678
Nessus ID : 10539

[back to the list of ports]

Information found on port domain (53/tcp)

A DNS server is running on this port. If you do not use it, disable it.

Risk factor : Low
Nessus ID : 11002

[back to the list of ports]

Information found on port netbios-ssn (139/tcp)

An SMB server is running on this port
Nessus ID : 11011

[back to the list of ports]

Warning found on port epmap (135/tcp)

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

Solution : filter incoming traffic to this port.
Risk factor : Low
Nessus ID : 10736

[back to the list of ports]

Warning found on port ldap (389/tcp)

Improperly configured LDAP servers will allow any user to connect to the server and query for information.

Solution: Disable NULL BIND on your LDAP server

In addition, the LDAP bind function in Exchange 5.5 has a buffer overflow that allows a user to conduct a denial of service or execute commands in all versions prior to Exchange server SP2. Coupled with a NULL BIND, an anonymous user can mount a remote attack against your server.

Note: no test was done to see what version of Exchange server is running, nor attempt to verify the service pack.

Solution: see http://www.microsoft.com/technet/security/bulletin/ms99-009.mspx
Risk factor: Medium
CVE : CVE-1999-0385
BID : 503
Nessus ID : 10723

[back to the list of ports]

Warning found on port ldap (389/tcp)

Improperly configured LDAP servers will allow the directory BASE
to be set to NULL. This allows information to be
culled without any prior knowledge of the directory
structure. Coupled with a NULL BIND, an anonymous
user can query your LDAP server using a tool such
as 'LdapMiner'

Solution: Disable NULL BASE queries on your LDAP server

Risk factor : Medium
Nessus ID : 10722

[back to the list of ports]

Warning found on port ldap (389/tcp)

The server's directory base is set to NULL. This allows information to be enumerated
without any prior knowledge of the directory struture.

The following information was pulled from the server via a LDAP request:
NTDS Settings,CN=FIREWALL,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=local,DC=homenet,DC=com

Solution: If pre-Windows 2000 compatibility is not required, remove pre-Windows 2000 compatibility as follows:
net localgroup 'Pre-Windows 2000 Compatible Access' everyone /delete

Risk Factor: Medium

Nessus ID : 12105

[back to the list of ports]

Vulnerability found on port microsoft-ds (445/tcp)

The remote Windows Internet Naming Service (WINS) is vulnerable to a flaw which could allow an attacker to execute arbitrary code on this host.

To exploit this flaw, an attacker would need to send a specially crafted packet with improperly advertised lengths.

Solution : http://www.microsoft.com/technet/security/bulletin/ms04-006.mspx
Risk factor : Low (Windows NT, Windows 2000) / High (Windows 2003)
CVE : CAN-2003-0825
BID : 9624
Nessus ID : 12051

[back to the list of ports]

Vulnerability found on port microsoft-ds (445/tcp)

The registry key HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
is writeable by users who are not in the admin group.

This key contains a value which defines which program should be run when a user logs on.

As this program runs in the SYSTEM context, the users who have the right to change the value of this key
can gain more privileges on this host.

Solution : use regedt32 and set the permissions of this key to :

- admin group : Full Control
- system : Full Control
- everyone : Read

Risk factor : High
CVE : CAN-1999-0589
Nessus ID : 10429

[back to the list of ports]

Vulnerability found on port microsoft-ds (445/tcp)

XMLHTTP Control Can Allow Access to Local Files.

A flaw exists in how the XMLHTTP control applies IE security zone settings to a redirected data stream returned in response to a request for data from a web site. A vulnerability results because an attacker could seek to exploit this flaw and specify a data source that is on the user's local system. The attacker could then use this to return information from the local system to the attacker's web site.

Impact of vulnerability: Attacker can read files on client system.

Affected Software:

Microsoft XML Core Services versions 2.6, 3.0, and 4.0.
An affected version of Microsoft XML Core Services also ships as part of the following products:

Microsoft Windows XP
Microsoft Internet Explorer 6.0
Microsoft SQL Server 2000

(note: versions earlier than 2.6 are not affected
files affected include msxml[2-4].dll and are found
in the system32 directory. This might be false
positive if you have earlier version)

See http://www.microsoft.com/technet/security/bulletin/ms02-008.mspx

Risk factor : High
CVE : CVE-2002-0057
BID : 3699
Nessus ID : 10866

[back to the list of ports]

Vulnerability found on port microsoft-ds (445/tcp)

The remote host has a version of Outlook express which has a bug in its MHTML URL processor, which may allow an attacker to execute arbitrary code on this host.

To exploit this flaw, an attacker would need to send a malformed email to a user of this host using Outlook, or would need to lure him into visiting a rogue website.

Solution : http://www.microsoft.com/technet/security/bulletin/ms04-013.mspx
Risk factor : High
CVE : CAN-2004-0380
BID : 9105, 9107, 9658
Other references : IAVA:2004-A-0009
Nessus ID : 12208

[back to the list of ports]

Warning found on port microsoft-ds (445/tcp)

The remote registry can be accessed remotely using the login / password combination used for the SMB tests.

Having the registry accessible to the world is not a good thing as it gives extra knowledge to a hacker.

Solution : Apply service pack 3 if not done already, and set the key HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg to restrict what can be browsed by non administrators.

In addition to this, you should consider filtering incoming packets to this port.

Risk factor : Low
CVE : CAN-1999-0562
BID : 6830
Nessus ID : 10400

[back to the list of ports]

Warning found on port microsoft-ds (445/tcp)

The domain SID can be obtained remotely. Its value is :

LOCAL : 5-21-1214440339-842925246-1060284298

An attacker can use it to obtain the list of the local users of this host
Solution : filter the ports 137 to 139 and 445
Risk factor : Low

CVE : CVE-2000-1200
BID : 959
Nessus ID : 10398

[back to the list of ports]

Warning found on port microsoft-ds (445/tcp)

The host Security Identifier (SID) can be obtained remotely. Its value is :

LOCAL : 5-21-1214440339-842925246-1060284298

An attacker can use it to obtain the list of the local users of this host
Solution : filter the ports 137-139 and 445
Risk factor : Low

CVE : CVE-2000-1200
BID : 959
Nessus ID : 10859

[back to the list of ports]

Warning found on port microsoft-ds (445/tcp)

Here is the list of the SMB shares of this host :

My Documents -
IPC$ - Remote IPC
D$ - Default share
NETLOGON - Logon server share
ADMIN$ - Remote Admin
SYSVOL - Logon server share
C$ - Default share

This is potentially dangerous as this may help the attack
of a potential hacker.

Solution : filter incoming traffic to this port
Risk factor : Medium
Nessus ID : 10395

[back to the list of ports]

Warning found on port microsoft-ds (445/tcp)

The domain SID could be used to enumerate the names of the users
of this domain.
(we only enumerated users name whose ID is between 1000 and 1200
for performance reasons)

This gives extra knowledge to an attacker, which
is not a good thing :
- Administrator account name : Administrator (id 500)
- Guest account name : Guest (id 501)
- TsInternetUser (id 1000)
- DHCP Users (id 1001)
- DHCP Administrators (id 1002)
- FIREWALL$ (id 1003)
- DnsAdmins (id 1104)
- DnsUpdateProxy (id 1105)
- ddziuba (id 1106)
- adziuba (id 1107)
- WDDZIUBA$ (id 1109)
- admin (id 1110)
- HOMENET$ (id 1113)
- H_ADZIUBA$ (id 1114)
- H-ADZIUBA$ (id 1115)
- DFX3XG21$ (id 1116)
- Exchange Domain Servers (id 1117)
- Exchange Enterprise Servers (id 1118)
- EUSER_EXSTOREEVENT (id 1121)
- 9BB8D441-B798-4E26-A (id 1122)
- LDZIUBA$ (id 1124)
- LDZIUBAMAC$ (id 1125)
- FIREWALL2$ (id 1126)

Risk factor : Medium
Solution : filter incoming connections this port

CVE : CVE-2000-1200
BID : 959
Nessus ID : 10399

[back to the list of ports]

Warning found on port microsoft-ds (445/tcp)

The remote host is missing a cumulative security update for Outlook Express which fixes a denial of service vulnerability in the Outlook Express mail client.

To exploit this vulnerability, an attacker would need to send a malformed message to a victim on the remote host. The message will crash her version of Outlook, thus preventing her from reading her e-mail.

Solution : http://www.microsoft.com/technet/security/bulletin/ms04-018.mspx
Risk factor : Medium
CVE : CAN-2004-0215
BID : 10711
Nessus ID : 13643

[back to the list of ports]

Warning found on port microsoft-ds (445/tcp)

There are 42 services running on this host :
Alerter [Alerter]
Background Intelligent Transfer Service [BITS]
Computer Browser [Browser]
Distributed File System [Dfs]
DHCP Client [Dhcp]
DHCP Server [DHCPServer]
Logical Disk Manager [dmserver]
DNS Server [DNS]
DNS Client [Dnscache]
Event Log [Eventlog]
COM+ Event System [EventSystem]
Intersite Messaging [IsmServ]
Kerberos Key Distribution Center [kdc]
Server [lanmanserver]
Workstation [lanmanworkstation]
License Logging Service [LicenseService]
TCP/IP NetBIOS Helper Service [LmHosts]
Messenger [Messenger]
Distributed Transaction Coordinator [MSDTC]
Microsoft Search [MSSEARCH]
Net Logon [Netlogon]
Network Connections [Netman]
File Replication Service [NtFrs]
NT LM Security Support Provider [NtLmSsp]
Removable Storage [NtmsSvc]
Plug and Play [PlugPlay]
IPSEC Policy Agent [PolicyAgent]
Protected Storage [ProtectedStorage]
Remote Registry Service [RemoteRegistry]
Remote Procedure Call (RPC) Locator [RpcLocator]
Remote Procedure Call (RPC) [RpcSs]
Security Accounts Manager [SamSs]
Task Scheduler [Schedule]
RunAs Service [seclogon]
System Event Notification [SENS]
Print Spooler [Spooler]
Distributed Link Tracking Server [TrkSvr]
Distributed Link Tracking Client [TrkWks]
Windows Time [W32Time]
Windows Management Instrumentation [WinMgmt]
Windows Management Instrumentation Driver Extensions [Wmi]
Automatic Updates [wuauserv]
You should turn off the services you do not use.
This list is useful to an attacker, who can make his attack
more silent by not portscanning this host.

Solution : To prevent the listing of the services for being
obtained, you should either have tight login restrictions,
so that only trusted users can access your host, and/or you
should filter incoming traffic to this port.

Risk factor : Low
Nessus ID : 10456

[back to the list of ports]

Warning found on port microsoft-ds (445/tcp)

The remote host seems to be a Primary Domain Controller
or a Backup Domain Controller.

This can be told by the value of the registry
key ProductType under
HKLM\SYSTEM\CurrentControlSet\Control\ProductOptions

This knowledge may be of some use to an attacker and help
him to focus his attack on this host.

Solution : filter the traffic going to this port
Risk factor : Low
CVE : CAN-1999-0659
Nessus ID : 10413

[back to the list of ports]

Warning found on port microsoft-ds (445/tcp)

Here is the browse list of the remote host :

DFX3XG21 -
FIREWALL -
FIREWALL2 -
HOMENET - Samba Server

This is potentially dangerous as this may help the attack
of a potential hacker by giving him extra targets to check for

Solution : filter incoming traffic to this port
Risk factor : Low

Nessus ID : 10397

[back to the list of ports]

Warning found on port microsoft-ds (445/tcp)

The messenger service is running. This service allows
NT users to send pop-ups messages to each others.

This service can be abused by who can
trick valid users into doing some actions that may
harm their accounts or your network (social
engineering attack)

Solution : Disable this service.

Risk factor : Low

How to disable this service under NT 4 :
- open the 'Services' control panel
- select the 'messenger' service, and click 'Stop'
- click on 'Startup...' and change to radio button of the
field 'Startup Type' from 'Automatic' to 'Disabled'

Under Windows 2000 :
- open the 'Administration tools' control panel
- open the 'Services' item in it
- double click on the 'messenger' service
- click on 'stop'
- change the drop-down menu value from the field 'Startup Type'
from 'Automatic' to 'Disabled'

CVE : CAN-1999-0630
Nessus ID : 10458

[back to the list of ports]

Warning found on port microsoft-ds (445/tcp)

The alerter service is running. This service allows
NT users to send pop-ups messages to each others.

This service can be abused by an attacker who can
trick valid users into doing some actions that may
harm their accounts or your network (social
engineering attack)

Solution : Disable this service.

Risk factor : Low

How to disable this service under NT 4 :
- open the 'Services' control panel
- select the 'Alerter' service, and click 'Stop'
- click on 'Startup...' and change to radio button of the
field 'Startup Type' from 'Automatic' to 'Disabled'

Under Windows 2000 :
- open the 'Administration tools' control panel
- open the 'Services' item in it
- double click on the 'Alerter' service
- click on 'stop'
- change the drop-down menu value from the field 'Startup Type'
from 'Automatic' to 'Disabled'

CVE : CAN-1999-0630
Nessus ID : 10457

[back to the list of ports]

Warning found on port microsoft-ds (445/tcp)

The registry key
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount
is non-null. It means that the remote host locally caches the passwords
of the users when they log in, in order to continue to allow the users
to log in in the case of the failure of the PDC.

Solution : use regedt32 and set the value of this key to 0
Risk factor : Low
Nessus ID : 11457

[back to the list of ports]

Information found on port microsoft-ds (445/tcp)

A CIFS server is running on this port
Nessus ID : 11011

[back to the list of ports]

Information found on port microsoft-ds (445/tcp)

It was possible to log into the remote host using a NULL session.
The concept of a NULL session is to provide a null username and
a null password, which grants the user the 'guest' access

To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and
Q246261 (Windows 2000).
Note that this won't completely disable null sessions, but will
prevent them from connecting to IPC$
Please see http://msgs.securepoint.com/cgi-bin/get/nessus-0204/50/1.html

All the smb tests will be done as "/" in domain LOCAL
CVE : CAN-1999-0504, CAN-1999-0506, CVE-2000-0222, CAN-1999-0505, CAN-2002-1117
BID : 494, 990, 11199
Nessus ID : 10394

[back to the list of ports]

Information found on port microsoft-ds (445/tcp)

The remote native lan manager is : Windows 2000 LAN Manager
The remote Operating System is : Windows 5.0 Server
The remote SMB Domain Name is : LOCAL

Nessus ID : 10785

[back to the list of ports]

Information found on port ldaps (636/tcp)

The service closed the connection after 0 seconds without sending any data
It might be protected by some TCP wrapper

Nessus ID : 10330

[back to the list of ports]

Information found on port cap (1026/tcp)

Distributed Computing Environment (DCE) services running on the remote host
can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge
about the remote host.

Here is the list of DCE services running on this port:

UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
Endpoint: ncacn_ip_tcp:10.10.1.2[1026]
Annotation: MS NT Directory DRS Interface

UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
Endpoint: ncacn_ip_tcp:210.159.52.32[1026]
Annotation: MS NT Directory DRS Interface

UUID: f5cc5a7c-4264-101a-8c59-08002b2f8426, version 21
Endpoint: ncacn_ip_tcp:10.10.1.2[1026]
Annotation: MS NT Directory XDS Interface

UUID: f5cc5a7c-4264-101a-8c59-08002b2f8426, version 21
Endpoint: ncacn_ip_tcp:210.159.52.32[1026]
Annotation: MS NT Directory XDS Interface

UUID: f5cc5a18-4264-101a-8c59-08002b2f8426, version 56
Endpoint: ncacn_ip_tcp:10.10.1.2[1026]
Annotation: MS NT Directory NSP Interface

UUID: f5cc5a18-4264-101a-8c59-08002b2f8426, version 56
Endpoint: ncacn_ip_tcp:210.159.52.32[1026]
Annotation: MS NT Directory NSP Interface

UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
Endpoint: ncacn_ip_tcp:10.10.1.2[1026]
Named pipe : lsass
Win32 service or process : Netlogon
Description : Net Logon service

UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
Endpoint: ncacn_ip_tcp:210.159.52.32[1026]
Named pipe : lsass
Win32 service or process : Netlogon
Description : Net Logon service

Solution : filter incoming traffic to this port.
Risk factor : Low
Nessus ID : 10736

[back to the list of ports]

Information found on port csoftragent (3004/tcp)

Distributed Computing Environment (DCE) services running on the remote host
can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge
about the remote host.

Here is the list of DCE services running on this port:

UUID: 130ceefb-e466-11d1-b78b-00c04fa32883, version 2
Endpoint: ncacn_ip_tcp:10.10.1.2[3004]
Annotation: NTDS ISM IP Transport

UUID: 130ceefb-e466-11d1-b78b-00c04fa32883, version 2
Endpoint: ncacn_ip_tcp:210.159.52.32[3004]
Annotation: NTDS ISM IP Transport

Solution : filter incoming traffic to this port.
Risk factor : Low
Nessus ID : 10736

[back to the list of ports]

Information found on port ls3 (3069/tcp)

Distributed Computing Environment (DCE) services running on the remote host
can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge
about the remote host.

Here is the list of DCE services running on this port:

UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1
Endpoint: ncacn_ip_tcp:10.10.1.2[3069]
Named pipe : atsvc
Win32 service or process : mstask.exe
Description : Scheduler service

UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1
Endpoint: ncacn_ip_tcp:210.159.52.32[3069]
Named pipe : atsvc
Win32 service or process : mstask.exe
Description : Scheduler service

UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1
Endpoint: ncacn_ip_tcp:10.10.1.2[3069]

UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1
Endpoint: ncacn_ip_tcp:210.159.52.32[3069]

Solution : filter incoming traffic to this port.
Risk factor : Low
Nessus ID : 10736

[back to the list of ports]

Information found on port stm_pproc (3080/tcp)

Distributed Computing Environment (DCE) services running on the remote host
can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge
about the remote host.

Here is the list of DCE services running on this port:

UUID: 4da1c422-943d-11d1-acae-00c04fc2aa3f, version 1
Endpoint: ncacn_ip_tcp:10.10.1.2[3080]

UUID: 4da1c422-943d-11d1-acae-00c04fc2aa3f, version 1
Endpoint: ncacn_ip_tcp:210.159.52.32[3080]

Solution : filter incoming traffic to this port.
Risk factor : Low
Nessus ID : 10736

[back to the list of ports]

Information found on port bears-02 (3146/tcp)

Distributed Computing Environment (DCE) services running on the remote host
can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge
about the remote host.

Here is the list of DCE services running on this port:

UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5
Endpoint: ncacn_ip_tcp:10.10.1.2[3146]
Named pipe : dnsserver
Win32 service or process : dns.exe
Description : DNS Server

UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5
Endpoint: ncacn_ip_tcp:210.159.52.32[3146]
Named pipe : dnsserver
Win32 service or process : dns.exe
Description : DNS Server

Solution : filter incoming traffic to this port.
Risk factor : Low
Nessus ID : 10736

[back to the list of ports]

Information found on port netport-id (3129/tcp)

Distributed Computing Environment (DCE) services running on the remote host
can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge
about the remote host.

Here is the list of DCE services running on this port:

UUID: 6bffd098-a112-3610-9833-46c3f874532d, version 1
Endpoint: ncacn_ip_tcp:10.10.1.2[3129]

UUID: 6bffd098-a112-3610-9833-46c3f874532d, version 1
Endpoint: ncacn_ip_tcp:210.159.52.32[3129]

UUID: 5b821720-f63b-11d0-aad2-00c04fc324db, version 1
Endpoint: ncacn_ip_tcp:10.10.1.2[3129]

UUID: 5b821720-f63b-11d0-aad2-00c04fc324db, version 1
Endpoint: ncacn_ip_tcp:210.159.52.32[3129]

Solution : filter incoming traffic to this port.
Risk factor : Low
Nessus ID : 10736

[back to the list of ports]

Information found on port isi-irp (3226/tcp)

Distributed Computing Environment (DCE) services running on the remote host
can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge
about the remote host.

Here is the list of DCE services running on this port:

UUID: f5cc59b4-4264-101a-8c59-08002b2f8426, version 1
Endpoint: ncacn_ip_tcp:10.10.1.2[3226]
Annotation: NtFrs Service

UUID: f5cc59b4-4264-101a-8c59-08002b2f8426, version 1
Endpoint: ncacn_ip_tcp:210.159.52.32[3226]
Annotation: NtFrs Service

UUID: d049b186-814f-11d1-9a3c-00c04fc9b232, version 1
Endpoint: ncacn_ip_tcp:10.10.1.2[3226]
Annotation: NtFrs API

UUID: d049b186-814f-11d1-9a3c-00c04fc9b232, version 1
Endpoint: ncacn_ip_tcp:210.159.52.32[3226]
Annotation: NtFrs API

UUID: a00c021c-2be2-11d2-b678-0000f87a8f8e, version 1
Endpoint: ncacn_ip_tcp:10.10.1.2[3226]
Annotation: PERFMON SERVICE

UUID: a00c021c-2be2-11d2-b678-0000f87a8f8e, version 1
Endpoint: ncacn_ip_tcp:210.159.52.32[3226]
Annotation: PERFMON SERVICE

Solution : filter incoming traffic to this port.
Risk factor : Low
Nessus ID : 10736

[back to the list of ports]

Information found on port msft-gc-ssl (3269/tcp)

The service closed the connection after 0 seconds without sending any data
It might be protected by some TCP wrapper

Nessus ID : 10330

[back to the list of ports]

Information found on port tip2 (3372/tcp)

A MSDTC server is running on this port
Nessus ID : 10330

[back to the list of ports]

Warning found on port general/tcp

The remote host does not discard TCP SYN packets which
have the FIN flag set.

Depending on the kind of firewall you are using, an
attacker may use this flaw to bypass its rules.

See also : http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html
http://www.kb.cert.org/vuls/id/464113

Solution : Contact your vendor for a patch
Risk factor : Medium
BID : 7487
Nessus ID : 11618

[back to the list of ports]

Warning found on port general/tcp

The remote host accepts loose source routed IP packets.

The feature was designed for testing purpose.
An attacker may use it to circumvent poorly designed IP filtering
and exploit another flaw. However, it is not dangerous by itself.

Solution : drop source routed packets on this host or on other ingress
routers or firewalls.

Risk factor : Low
Nessus ID : 11834

[back to the list of ports]

Warning found on port general/tcp

The remote host uses non-random IP IDs, that is, it is
possible to predict the next value of the ip_id field of
the ip packets sent by this host.

An attacker may use this feature to determine traffic patterns
within your network. A few examples (not at all exhaustive) are:

1. A remote attacker can determine if the remote host sent a packet
in reply to another request. Specifically, an attacker can use your
server as an unwilling participant in a blind portscan of another
network.

2. A remote attacker can roughly determine server requests at certain
times of the day. For instance, if the server is sending much more
traffic after business hours, the server may be a reverse proxy or
other remote access device. An attacker can use this information to
concentrate his/her efforts on the more critical machines.

3. A remote attacker can roughly estimate the number of requests that
a web server processes over a period of time.

Solution : Contact your vendor for a patch
Risk factor : Low
Nessus ID : 10201

[back to the list of ports]

Information found on port general/tcp

10.10.1.2 resolves as firewall.
Nessus ID : 12053

[back to the list of ports]

Information found on port general/tcp

The remote host is running Microsoft Windows 2000 Server
Nessus ID : 11936

[back to the list of ports]

Warning found on port general/icmp

The remote host answers to an ICMP timestamp request. This allows an attacker
to know the date which is set on your machine.

This may help him to defeat all your time based authentication protocols.

Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk factor : Low
CVE : CAN-1999-0524
Nessus ID : 10114

[back to the list of ports]

Information found on port domain (53/udp)

A DNS server is running on this port. If you do not use it, disable it.

Risk factor : Low
Nessus ID : 11002

[back to the list of ports]

Information found on port domain (53/udp)

The remote DNS server answers to queries for third party domains which do not have the recursion bit set.

This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.

For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of aforementioned financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more...

For a much more detailed discussion of the potential risks of allowing DNS cache information to be queried anonymously, please see:
http://community.sidestep.pt/~luis/DNS-Cache-Snooping/DNS_Cache_Snooping_1.1.pdf

Risk factor : Low
Nessus ID : 12217

[back to the list of ports]

Information found on port bootps (67/udp)

Here is the information we could gather from the remote DHCP server. This allows an attacker on your local network to gain information about it easily :

Master DHCP server of this network : 10.10.1.2
IP address the DHCP server would attribute us : 10.10.1.35
netmask = 255.0.0.0
DHCP server(s) identifier = 10.10.1.2
router = 10.10.1.1
domain name server(s) = 10.10.1.2 , 216.231.41.22 , 216.231.41.1
domain name = local.homenet.com

Solution : remove the options that are not in use in your DHCP server
Risk factor : Low

Nessus ID : 10663

[back to the list of ports]

Information found on port general/udp

For your information, here is the traceroute to 10.10.1.2 :
10.10.1.31
10.10.1.2

Nessus ID : 10287

[back to the list of ports]

Information found on port ntp (123/udp)

A NTP (Network Time Protocol) server is listening on this port.

Risk factor : Low
Nessus ID : 10884

[back to the list of ports]

Warning found on port netbios-ns (137/udp)

The following 9 NetBIOS names have been gathered :
FIREWALL = This is the computer name registered for workstation services by a WINS client.
FIREWALL = Computer name
LOCAL = Workgroup / Domain name
LOCAL = Workgroup / Domain name (Domain Controller)
LOCAL
LOCAL = Workgroup / Domain name (part of the Browser elections)
FIREWALL = This is the current logged in user registered for this workstation.
FIREWALL$ = This is the current logged in user registered for this workstation.
ADMINISTRATOR = This is the current logged in user registered for this workstation.
The remote host has the following MAC address on its adapter :
00:01:02:29:c7:79

If you do not want to allow everyone to find the NetBios name
of your computer, you should filter incoming traffic to this port.

Risk factor : Medium
CVE : CAN-1999-0621
Nessus ID : 10150

[back to the list of ports]

Information found on port unknown (1029/tcp)

Distributed Computing Environment (DCE) services running on the remote host
can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge
about the remote host.

Here is the list of DCE services running on this port:

UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
Endpoint: ncacn_http:10.10.1.2[1029]
Annotation: MS NT Directory DRS Interface

UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
Endpoint: ncacn_http:210.159.52.32[1029]
Annotation: MS NT Directory DRS Interface

UUID: f5cc5a7c-4264-101a-8c59-08002b2f8426, version 21
Endpoint: ncacn_http:10.10.1.2[1029]
Annotation: MS NT Directory XDS Interface

UUID: f5cc5a7c-4264-101a-8c59-08002b2f8426, version 21
Endpoint: ncacn_http:210.159.52.32[1029]
Annotation: MS NT Directory XDS Interface

UUID: f5cc5a18-4264-101a-8c59-08002b2f8426, version 56
Endpoint: ncacn_http:10.10.1.2[1029]
Annotation: MS NT Directory NSP Interface

UUID: f5cc5a18-4264-101a-8c59-08002b2f8426, version 56
Endpoint: ncacn_http:210.159.52.32[1029]
Annotation: MS NT Directory NSP Interface

UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
Endpoint: ncacn_http:10.10.1.2[1029]
Named pipe : lsass
Win32 service or process : Netlogon
Description : Net Logon service

UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
Endpoint: ncacn_http:210.159.52.32[1029]
Named pipe : lsass
Win32 service or process : Netlogon
Description : Net Logon service

Solution : filter incoming traffic to this port.
Risk factor : Low
Nessus ID : 10736

[back to the list of ports]

Information found on port unknown (1037/tcp)

Distributed Computing Environment (DCE) services running on the remote host
can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge
about the remote host.

Here is the list of DCE services running on this port:

UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
Endpoint: ncacn_ip_tcp:10.10.1.2[1037]

UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
Endpoint: ncacn_ip_tcp:210.159.52.32[1037]

UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
Endpoint: ncacn_ip_tcp:10.10.1.2[1037]

UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
Endpoint: ncacn_ip_tcp:210.159.52.32[1037]

UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
Endpoint: ncacn_ip_tcp:10.10.1.2[1037]

UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
Endpoint: ncacn_ip_tcp:210.159.52.32[1037]

UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
Endpoint: ncacn_ip_tcp:10.10.1.2[1037]

UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
Endpoint: ncacn_ip_tcp:210.159.52.32[1037]

Solution : filter incoming traffic to this port.
Risk factor : Low
Nessus ID : 10736

[back to the list of ports]

Information found on port unknown (1028/udp)

Distributed Computing Environment (DCE) services running on the remote host
can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge
about the remote host.

Here is the list of DCE services running on this port:

UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
Endpoint: ncadg_ip_udp:10.10.1.2[1028]
Annotation: MS NT Directory DRS Interface

UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
Endpoint: ncadg_ip_udp:210.159.52.32[1028]
Annotation: MS NT Directory DRS Interface

UUID: f5cc5a7c-4264-101a-8c59-08002b2f8426, version 21

Endpoint: ncadg_ip_udp:10.10.1.2[1028]
Annotation: MS NT Directory XDS Interface

UUID: f5cc5a7c-4264-101a-8c59-08002b2f8426, version 21
Endpoint: ncadg_ip_udp:210.159.52.32[1028]
Annotation: MS NT Directory XDS Interface

UUID: f5cc5a18-4264-101a-8c59-08002b2f8426, version 56
Endpoint: ncadg_ip_udp:10.10.1.2[1028]
Annotation: MS NT Directory NSP Interface

UUID: f5cc5a18-4264-101a-8c59-08002b2f8426, version 56
Endpoint: ncadg_ip_udp:210.159.52.32[1028]
Annotation: MS NT Directory NSP Interface

UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
Endpoint: ncadg_ip_udp:10.10.1.2[1028]
Named pipe : lsass
Win32 service or process : Netlogon
Description : Net Logon service

UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
Endpoint: ncadg_ip_udp:210.159.52.32[1028]
Named pipe : lsass
Win32 service or process : Netlogon
Description : Net Logon service

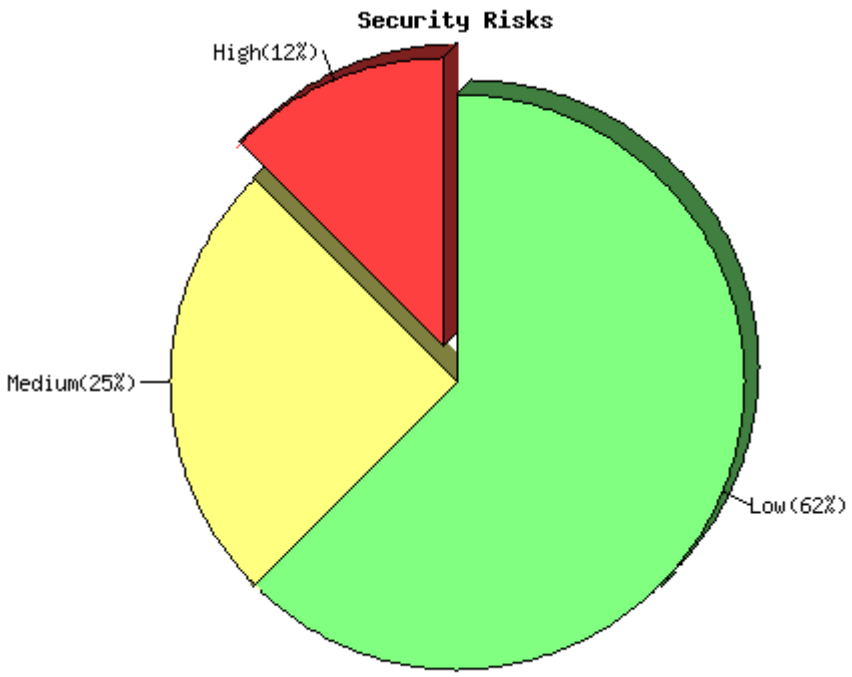
Solution : filter incoming traffic to this port.
Risk factor : Low
Nessus ID : 10736

This file was generated by Nessus, the open-sourced security scanner.

External Perspective

Firewall

Repartition of the level of the security problems :



[Back to the index]
List of open ports :

- *ftp (21/tcp) (Security hole found)*
- *smtp (25/tcp) (Security notes found)*
- *pop3 (110/tcp) (Security notes found)*
- *h323hostcall (1720/tcp) (Security notes found)*
- *general/udp (Security notes found)*
- *general/tcp (Security warnings found)*

[back to the list of ports]

Vulnerability found on port ftp (21/tcp)

It was possible to disable the remote FTP server
by connecting to it about 3000 times, with
one connection at a time.

If the remote server is running from within [x]inetd, this
is a feature and the FTP server should automatically be back
in a couple of minutes.

An attacker may use this flaw to prevent this
service from working properly.

Solution : If the remote server is GoodTech ftpd server,

download the newest version from http://www.goodtechsys.com.
BID : 2270
Risk factor : High
CVE : CAN-2001-0188
BID : 2270
Nessus ID : 10690

[back to the list of ports]

Information found on port ftp (21/tcp)

An unknown service is running on this port.
It is usually reserved for FTP
Nessus ID : 10330

[back to the list of ports]

Information found on port ftp (21/tcp)

An unknown service runs on this port.
It is sometimes opened by this/these Trojan horse(s):
Back Construction
Blade Runner
Cattivik FTP Server
CC Invader
Dark FTP
Doly Trojan
Fore
FreddyK
Invisible FTP
Juggernaut 42
Larva
MotIv FTP
Net Administrator
Ramen
RTB 666
Senna Spy FTP server
The Flu
Traitor 21
WebEx
WinCrash

Unless you know for sure what is behind it, you'd better
check your system

*** Anyway, don't panic, Nessus only found an open port. It may
*** have been dynamically allocated to some service (RPC...)

Solution: if a trojan horse is running, run a good antivirus scanner
Risk factor : Low
Nessus ID : 11157

[back to the list of ports]

Information found on port smtp (25/tcp)

An unknown service is running on this port.
It is usually reserved for SMTP
Nessus ID : 10330

[back to the list of ports]

Information found on port smtp (25/tcp)

An unknown service runs on this port.
It is sometimes opened by this/these Trojan horse(s):
Ajan
Antigen
Barok
BSE
Email Password Sender - EPS
EPS II
Gip
Gris
Happy99
Hpteam mail
I love you
Kuang2
Magic Horse
MBT (Mail Bombing Trojan)
Moscow Email trojan
Naebi
NewApt worm
ProMail trojan
Shtirlitz
Stealth
Stukach
Tapiras
Terminator
WinPC
WinSpy

Unless you know for sure what is behind it, you'd better
check your system

*** Anyway, don't panic, Nessus only found an open port. It may
*** have been dynamically allocated to some service (RPC...)

Solution: if a trojan horse is running, run a good antivirus scanner
Risk factor : Low
Nessus ID : 11157

[back to the list of ports]

Information found on port smtp (25/tcp)

For some reason, we could not send the 42.zip file to this MTA
BID : 3027
Nessus ID : 11036

[back to the list of ports]

Information found on port pop3 (110/tcp)

An unknown service is running on this port.
It is usually reserved for POP3
Nessus ID : 10330

[back to the list of ports]

Information found on port pop3 (110/tcp)

An unknown service runs on this port.
It is sometimes opened by this/these Trojan horse(s):
ProMail trojan

Unless you know for sure what is behind it, you'd better
check your system

*** Anyway, don't panic, Nessus only found an open port. It may
*** have been dynamically allocated to some service (RPC...)

Solution: if a trojan horse is running, run a good antivirus scanner
Risk factor : Low
Nessus ID : 11157

[back to the list of ports]

Information found on port h323hostcall (1720/tcp)

H323 is a protocol used all over the Internet. It is used for
Voice Over IP (VoIP), Microsoft NetMeeting, and countless other
applications. Nessus was able to determine that the remote device
supports the H323 protocol. It is in your best interest to run a
separate audit against this IP to determine the potential risk
introduced by this application.

Risk factor : None
Nessus ID : 12243

[back to the list of ports]

Information found on port general/udp

For your information, here is the traceroute to 216.56.xxx.xxx :
216.56.45.13
216.56.xxx.xxx

Nessus ID : 10287

[back to the list of ports]

Warning found on port general/tcp

The remote host uses non-random IP IDs, that is, it is
possible to predict the next value of the ip_id field of
the ip packets sent by this host.

An attacker may use this feature to determine traffic patterns
within your network. A few examples (not at all exhaustive) are:

1. A remote attacker can determine if the remote host sent a packet
in reply to another request. Specifically, an attacker can use your
server as an unwilling participant in a blind portscan of another
network.

2. A remote attacker can roughly determine server requests at certain
times of the day. For instance, if the server is sending much more
traffic after business hours, the server may be a reverse proxy or
other remote access device. An attacker can use this information to

concentrate his/her efforts on the more critical machines.

3. A remote attacker can roughly estimate the number of requests that
a web server processes over a period of time.

Solution : Contact your vendor for a patch
Risk factor : Low
Nessus ID : 10201

[back to the list of ports]

Warning found on port general/tcp

The remote host might be vulnerable to a sequence number approximation
bug, which may allow an attacker to send spoofed RST packets to the remote
host and close established connections.

This may cause problems for some dedicated services (BGP, a VPN over
TCP, etc...).

Solution : See http://www.securityfocus.com/bid/10183/solution/
Risk factor : Medium
CVE : CAN-2004-0230
BID : 10183
Other references : OSVDB:4030, IAVA:2004-A-0007
Nessus ID : 12213

[back to the list of ports]

Warning found on port general/tcp

The remote host does not discard TCP SYN packets which
have the FIN flag set.

Depending on the kind of firewall you are using, an
attacker may use this flaw to bypass its rules.

See also : http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html
http://www.kb.cert.org/vuls/id/464113

Solution : Contact your vendor for a patch
Risk factor : Medium
BID : 7487
Nessus ID : 11618

[back to the list of ports]

Warning found on port general/tcp

The remote host accepts loose source routed IP packets.
The feature was designed for testing purpose.
An attacker may use it to circumvent poorly designed IP filtering
and exploit another flaw. However, it is not dangerous by itself.

Solution : drop source routed packets on this host or on other ingress
routers or firewalls.

Risk factor : Low
Nessus ID : 11834

[back to the list of ports]

Information found on port general/tcp

Remote OS guess : Microsoft Windows Millennium Edition (Me), Windows 2000 Professional or Advanced Server, or Windows XP

CVE : CAN-1999-0454
Nessus ID : 11268

This file was generated by Nessus, the open-sourced security scanner.