GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

Check out the list of upcoming events offering
"Auditing & Monitoring Networks, Perimeters & Systems (Audit 507)"
at http://www.giac.org/registration/gsna

Small Business IT Auditing

A Practical Examination Submitted in Partial Requirement for the Global Information Assurance Certification (GIAC) program for GIAC Systems and Network Auditor (GSNA) certification v1.2.

David M. Eaves
Company Name
email@address

© SANS Institute 2000 - 2002, Author retains full rights.

Part I: Small Business IT Auditing with OS/Machine Variations 3
A. Motivation and Background 3
B. Proposed Improvements in Measurement and Practice 3
C. Listing IT Assets and Risks 4
D. Contribution: Ranking and Valuation of Assets 7
E. Contribution: Auditing RedHat Linux 7.1 9
F. Contribution: Auditing Windows 98 13
G. Contribution: Auditing the Linksys BEFSR41 15
H. Contribution: Auditing a Remote System and Web Application 17
I. Score, Remedial Action List, and Actions Taken 20
References 21

Part II: Auditing a Real World Small Business: Generic Services Corporation 22
A. Executive Summary 22
B. The Organization 22
C. IT Systems and Assets 22
D. Audit Results 24
E. Auditor and Executive Comments 26
F. Lessons Learned for Future Auditing 28
Appendix A: Benchmark and Matrixes, System #1 29
Appendix B: Benchmark and Matrixes, System #2 42
Appendix C: Benchmark and Matrixes, System #3 56
Appendix D: Benchmark and Matrixes, Remote System #1 68
Appendix E: Benchmark and Matrixes, Remote system #2 82
Appendix F: Overall Value-at-Risk Mitigation Matrix 87

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

Part I: Small Business IT Auditing with OS/Machine Variations

A. Motivation and Background

Current practice in enterprise, or firm-wide systems audit, measurement, and control is well covered in theory. Checklists abound: there are well-defined overall practices defined by CERT and ISACA, two organizations devoted to IT and systems audit practices. An example of analytic practice can be seen in [Marchany]. However most examples suffer from being too costly for most businesses, or too device-specific.

For measurement of individual assets there are numerous sources, including two specific auditing rulers available from the Center for Internet Security [CIS] (as of December, 2001), with several others in development. For general measurement, one must combine three approaches: 1) apply the principles implemented by the CIS rulers, based on OS and appliance-specific knowledge, 2) use developer or manufacturer references, and 3) supplement this measurement with more general checklist methods such as top-ten and top-twenty vulnerability scanning.

Every actual IT department and real world CIO or CEO might reasonably complain that their own situation is not adequately covered, either because of unique organizational features, or because their technology is not well documented. This essay should serve a number of purposes in both areas, as well as providing guidance for a real world small business in need of a systems security measurement benchmark.

B. Proposed Improvements in Measurement and Practice

While the two largest populations of vulnerable systems may have been covered by the latest CIS measurement techniques (Solaris and Windows 2000), there are many other popular systems and appliances attached to networks. It seems that until Windows/NT, Windows/XP, RedHat and SuSe Linux, Mac/System X, by way of systems have rulers, and until the various Cisco routers, Linksys home broadband routers, and assorted modems, Layer 4 switches, top layers, and other popular network appliances have rulers, the majority of most companies' networks will not be measurable. That does not even take into account wireless technology.

The methodology suggested by [Marchany] and others may require excessive amounts of valuable meeting time. These procedures rank and measure assets' value, risks to which they are exposed, and controls to mitigate them in such a way to focus attention on the most valuable and risky assets, and the most valuable controls. This excessive time requirement in turn can damage the credibility of the ongoing auditing process in an organization. Methodology proposed by [CERT], the Survivable Network Analysis method, was deemed to be overkill for a small business situation with few services offered and few network assets.

There are five proposed improvements to measurement and practice in this essay: 1) A time-saving, robust methodology for ranking and analyzing assets, risks, and controls, 2) a Linux (RedHat 7.1) auditing procedure based on [Laude], and on the [CIS] Solaris benchmark, 3) a Windows 98 auditing procedure based on the [CIS] Windows 2000 benchmark documentation, 4) a Linksys home router auditing procedure based on manufacturer and other documentation, and 5) a general web application auditing procedure based on [Rhoades].

There will be not one, but several proposed improvements here simply because the author needs a real world example that applies to his own firm's IT assets, and like all other CIOs and CEOs, he faces unique organization and technology features that must be accommodated. Each improvement need not be final and authoritative, since several are made. In addition, some candid feedback from the executive audience, and a review

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

of remedial actions taken and the rationale actually applied should be interesting and helpful to real world IT audit personnel.

C. Listing IT Assets and Risks

To explain the ranking methodology it is useful to provide a concrete framework by actually listing some example IT assets to which it will be applied. This list will also be used in Part II, to do the actual audit. This is based loosely on the CoBIT model of [ISACA], but simplified, without Key Goal or Performance indicators. The approach is to list actual assets, and the system or component by which they might be exposed to risks.

1. Strategic, or Research and Development Data

Asset	Location	Potential Harm
Product development code, project #1	System #1	Destruction, Disclosure, and/or Modification
Service Contracts with client-specific charges and fees	System #2	Disclosure to other clients
Email records with strategy and shareholder discussions	System #1, and remote	Disclosure of strategy, internal info, Forgery
Web site HTML and CGI code/objects.	Remote	Destruction and/or Modification

2. Network and Systems Data

Asset	Location	Potential Harm
PKI elements such as public keys, signatures from other sources	System #1	Modification, Forgery
Private keys: email, integrity-check, Secure Shell, other	System #1	Disclosure, Forgery
Server system logs, individual system logs	System #1	Destruction, and/or Modification
File system integrity databases	System #1	Destruction, and/or Modification
Password and related files with user information	System #1, System #2	Disclosure, Modification, Forgery
Device configuration, ACL's and administrative passwords/backdoors	System #1, System #3	Disclosure, Forgery

3. Private Client or Partner Data

Asset	Location	Potential Harm
Legal Disclosure Agreements with clients	System #2	Disclosure
Reports for client audits, forensic work, network design, and policy	System #2	Disclosure
Personal information from client, mailing, and customer lists	System #2	Disclosure

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

4. Public Appearance, Storefront, or Reputation: Goodwill

Asset	Location	Potential Harm
Web site appearance – proxy for perceived quality of service	Remote (the web server)	Enterprise Reputation
Product vulnerability or quality	System #1	Product Reputation
Investor relations: perceived core competency	Remote (the web server)	Enterprise Reputation

5. Service Level Obligations

Asset	Location	Potential Harm
Prepaid contractual services owed	Requires system #1	Breach of Contract Liability
Retainer service agreements	Requires system #1	Breach of Contract Liability

6. Personnel Security and Goodwill

Asset	Location	Potential Harm
Personnel private records	System #2	Disclosure
Key or essential IT personnel	Home Office	Death, Incapacitation, Personnel Loss
Creditworthiness: payroll/payables cash-flow coverage	Banking/accounts procedures	Enterprise Reputation
Inside IT personnel loyalty	Home Office	Defection, Disgruntlement

7. IT Physical Plant and Equipment

Asset	Location/ID	Potential Harm
Gateway/firewall routers and top layers	ID: System #3	Replacement and/or reconfiguration
DMZ hosts, dedicated firewalls – including shared resources	System #1	Replacement and/or reconfiguration
Server hosts – including shared resources	Remote	Replacement, recovery, and/or reconfiguration
Desktop PCs: x86/Linux	ID: System #1	Replacement, recovery, and/or reconfiguration
Laptops: x86/Windows	ID: System #2	Replacement, recovery, and/or reconfiguration
Office supplies, electronics	Home Office	Replacement
UPS and generator/backup power supply	Home Office	Replacement

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

8. Enumerating Risks

Risks, Potential Harm	Description	Damage to Asset
Disclosure – see Compromise	Information is made freely visible to any interested parties	Fraction
Destruction – see Compromise	Data destruction without backup of most recent and significant changes	Total
Modification – see Compromise	Possible Trojan Horse implant or other malicious unintended change to product/key	Fraction
Forgery – see Exploits, Compromise	Identity can be successfully misrepresented	Marginal
Enterprise Reputation	Unable to do business effectively	Fraction
Product Reputation – see Modification	Unable to sell product	Fraction
Contractual Liability	Operations disrupted: Loss/refund of services/monetary damages	Total
Death, Incapacitation, Personnel Loss*	Loss of expertise, reputation	Fraction
Defection, Disgruntlement	Intentional harm using systems expertise	Total
Systems Surveillance	Network vulnerabilities are disclosed	Marginal
Systems Exploits*, Denial of Service	One or more successful intrusion attempts	Fraction
Systems Compromise*	Root access and root-kit, owned by intruder	Total
Power Outage, Connectivity Outage	Basic infrastructure fails temporarily	Total
Civil or Natural Catastrophe	Go home and protect your family	Total

* Systems exploits imply possible disclosure of any data accessible to the user id that was used. Systems compromise implies disclosure of all data accessible to the system. Personnel loss also might be considered to be enterprise reputation, effectively.

There are three systems, one physical location (the home office), banking and accounting procedures, and a remote network as locations, or possible risk vectors to the list of assets above. The asset-risk matrix will list six routes through which the firm's IT assets are exposed to risk: Systems #1 through #3, the physical premises (office), financial procedures, and the remote network (which runs the company web application and handles some email).

Risk\Asset Set	System#1	System#2	System#3	Office	Finance	Remote
Disclosure – see Compromise			N/A		N/A	N/A
Destruction – see Compromise				N/A		

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

Modification – see Compromise				N/A	N/A	
Forgery – see Exploits, Compromise						
Enterprise Reputation			N/A	N/A		
Product Reputation – see Modification			N/A	N/A	N/A	
Contractual Liability			N/A			
Death, Incapacitation, Personnel Loss*		N/A	N/A	N/A		
Defection, Disgruntlement				N/A		
Systems Surveillance				N/A	N/A	
Systems Exploits*, Denial of Service				N/A	N/A	
Systems Compromise*				N/A		
Power Outage, Connectivity Outage						
Civil or Natural Catastrophe						

D. Contribution: Ranking and Valuation of Assets

One contribution to community knowledge in this essay will be that a simple rank-ordering scheme discussed by numerous political scientists in the context of non-transitive voting and preferences ([Condorcet], [Saari], [Sen]) can be guaranteed to produce robust collective preference orderings. For a ranking of *M* objects by *N* participants, this requires only *NM* value assignments, rather than the $NM^2/2$ value assignments required for the full-information pairwise resolution proposed by [Marchany].

When the number of systems and components goes above 30, the time saved is substantial, especially considering that this is shared meeting time being saved, with all the implications for stakeholder buy-in as well as credibility of the auditing process within the organization.

The procedure to follow assigns integer ranks of importance to each of the M systems and components listed, in increasing order for more important ones. The numbers are simply added, weighted or unweighted, to result in a robust vote score for each system. When there are 40 systems, each voter is required to assign 40 numbers unilaterally, rather than vote all together on 1600/2, or 800 separate binary comparison votes.

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

Examples based on [Marchany], Appendix A, will follow in Part II.

In this case there are only six asset categories, and only three stakeholders in the organization, so the advantage of this improvement is not clear in the example, but the way in which the procedure is applied can be shown clearly. There can be ties in the ranking order. If there were more than 30 systems, or if there were more than ten or so stakeholders, then the advantages would be significant.

Ranking Votes	1) CEO/ President	2) Tech Director	3) Director Emeritus	Summary	Rank
System #1	6	6	4	16	1
System #2	1	3	2	6	5-tied
System #3	2	4	3	9	4
Home Office	4	1	1	6	5-tied
Financial	5	2	5	12	3
Remote Network	3	5	6	14	2

Clearly System #1 represents the most important collection of assets, followed by the remote network (including the web site), banking and accounting procedures, and System #3, the firewall router. The office's physical premises and System #2 are tied for the least important collections of assets.

Analysis of Ranked Assets, and Value of the Risks Mitigated:

Using matrix notation, consider *A* assets residing on *S* systems, each of which is exposed to *R* risks, addressable by *P* remedies, or controls. The matrix of asset values at risk *versus* remedies is ($\boldsymbol{O} \cdot \boldsymbol{D} \cdot \boldsymbol{F}$), where ***O*** is an *A* by *S* matrix of which assets reside on which systems, ***D*** is a *S* by *R* matrix of which systems are exposed to which risks (denoting what proportion of damage in each case), and ***F*** is an *R* by *P* matrix denoting which risks are mitigated by which remedies. Call this matrix the Value at Risk Mitigation matrix, or ***V***.

Let a 4 by 3 ***O*** be populated with asset value as follows:

	System #1	System #2	System #3
Asset 1: Dev Code	$250K	0	$100K
Asset 2: Good Name	0	$100K	$500K
Asset 3: Privacy Data	0	$100K	0
Asset 4: Personnel	0	0	$250K

Let a 3 by 5 ***D*** (the potential damage) be populated with risk value as follows, the Damage Done numbers (subjective, between zero and one, assigned per checklist item, including notional frequency or likelihood) apply whenever a system has not passed the benchmark for the checklist item, otherwise there are zeroes. It is important to note that in this study, no effort will be made to make these estimates of damage done (damage times frequency, or likelihood) better than subjective estimates (see [Marchany]).

	Checklist item #1	Checklist item #2	Checklist item #3	Checklist item #4	Checklist item #5
Damage Done	0.1	0.5	1.0	0.5	0.1
System #1	0	0	1.0	0	0
System #2	0.1	0.5	0	0	0
System #3 (all tests passed)	0	0	0	0	0

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

Let a 5 by 6 ***F*** be populated with ones and zeroes depending whether the fix in the column will make the checklist item pass. Fractional numbers based on subjective judgment about the checklist item should be applicable. For example:

	Patch #1	Patch #2	Password policy	UPS and premises	Dedicated firewall	Armed guards
Checklist item #1	1	0	0	0	0	0
Checklist item #2	0	1	1	0	0	0
Checklist item #3	0	0	0	1	0	1
Checklist item #4	0	0	0	0	1	1
Checklist item #5	0	0	0	1	0	1

The resulting ***V*** matrix, (***O*** · ***D*** · ***F***), should indicate the assets values mitigated by each of the corrective measures in the columns. Decisions taken are supported by this kind of analytical treatment.

	Patch #1	Patch #2	Password policy	UPS and premises	Dedicated firewall	Armed guards
Asset 1: Dev Code	0	0	0	$250	0	$250
Asset 2: Good Name	$10	$50	$50	0	0	0
Asset 3: Privacy Data	$10	$50	$50	0	0	0
Asset 4: Personnel	0	0	0	0	0	0

Each resulting column represents a fix to address risks, each row represents a list of asset values at risk that stand to be mitigated by undertaking the cost represented by the fix in each column. In a sense, each column sum should be greater than the cost of the remedy represented by that column in order for the fix to be worthwhile. In the example above both patches, a new password policy, and a UPS and premises security are appropriate and should be implemented. Armed guards are cost ineffective.

E. Contribution: Auditing RedHat Linux 7.1

There is no authoritative auditing procedure or CIS ruler available at this time to measure RedHat Linux v7.1, however we can use methods from [Laude] of a RedHat Linux 7.0 audit, and the CIS Solaris ruler to measure this system. The references in [Laude] to earlier Linux 6.x auditing are omitted because of the significant changes to Linux covered there.

A recap of tools and checklists, from [Laude] is as follows:

1. Tools:

- Swatch, log monitoring.
- Psionic logcheck, log monitoring
- Logwatch, log monitoring

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

- Tripwire, file system integrity monitoring
- AIDE, file system integrity monitoring
- Psionic PortSentry, host based intrusion detection
- Tiger, vulnerability analysis
- TARA, vulnerability analysis
- SATAN/SARA/SAINT, vulnerability analysis
- Nessus, vulnerability analysis
- Nmap, vulnerability analysis
- ISS Internet Scanner, vulnerability analysis
- Cybercop, vulnerability analysis
- Snort, traffic sniffing/monitoring
- Tcpdump, traffic sniffing/monitoring
- Ethereal, traffic sniffing/monitoring (author's own addition)
- System commands, diagnostic information about system

2. Checklists

- Securing Linux Step by Step [SANS]
- Auditing Linux [Naidu]
- Linux Security Auditing [Whelan]
- CIS Solaris ruler (author's own addition)
- <Anti-virus software> [Laude]
- <Physical security> [Laude]

The elements to be checked are listed briefly below, along with the source of the item, A= Author, C= CIS Solaris ruler documentation, L= [Laude]. Redundancies have been removed in the interest of economy, and some relatively subjective criteria have been included. Other sources such as the [CERT] checklist were minimal and a subset of these other checklists.

Checklist Item	Src	Method/Command	Benchmark
Kernel version/tool calibration	L	**uname -a**	Linux 2.4.2-2
Latest OS security patches/updates	L	**rpm –qa** compared w/patch versions recommended by RedHat	Same versions in http://www.redhat.com/support/errata/rh71-errata-security.html
Recovery boot disk	L	Make a new one: **/sbin/mkbootdisk**	Bootable disk exists
Linux 7.1 Incident handling disk	A	Insert, **ls –al**	Should have at minimum: ls, lsof, netstat, bash, tcsh, dump, all built static
Only non-privileged user accounts are bona fide employees	L	**cat /etc/passwd** should show only known non-privileged users	Only bona fide accounts
Shadowed passwords, MD5 hashed	L	**md5sum** a known password and see if it matches content in /etc/shadow	Hash matches password entry in /etc/shadow
Every user has a shadowed password	L	**pwck** shows no errors	/etc/shadow shows password entries

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

System password policy matches security policy	L	Run **chage –l** <user> for each user in /etc/passwd, **crack** to test strength.	Passwords expire, and are all nontrivial
There is anti-virus software installed	L	**rpm –qa** to verify claimed software	Installed supported product, up to date
There are no shared filesystems	L	**cat /etc/exp*, exportfs, df –k**	None
There are no setuid or setgid files	L	**find / \(-perm –4000 –perm –2000 \) –print**	None, except ??? userhelper
Is the LILO boot-prompt password protected? Is lilo.conf 600 and root?	L	**cat /etc/lilo.conf, ls –al /etc/lilo.conf**	Password set, conf is root, 600
Reboot from console with CTRL-ALT-DELETE is disabled	L	**cat /etc/inittab | grep shutdown**	Key combination does not prompt for reboot
Single user mode requires root password	L	**cat /etc/inittab | grep sulogin**	No autologin, root password required
All console logins disabled except for root and administrative user	L	**cat /etc/security/ access.conf**	Nope – users have to use the console
TCP wrappers are in use	L	**cat /etc/hosts.allow, cat /etc/hosts.deny**	Iptables, ipchains, all ports filtered
Remote telnet users are disallowed	L	**cat /etc/securetty**	None except as specifically required by policy
Only permitted ports are unfiltered, from the inside	L	**nmap –I –O –sR localhost** to see ports	Possible select service only on ftp, ftp-data, ssh ports
Only permitted services running, as seen from the inside, esp. no rpc*, lpd, named, or portmap.	L	**netstat –at** to see if any inappropriate services are running, **chkconfig --list** to see if any inappropriate services are configured	None except for X11, port 6000
No unusual or suspicious file descriptors are open	L	**lsof –i +M** to list all open file descriptors	None except X11, port 6000
Only permitted ports are accessible from the outside	L	Use **nessus** for Solaris to perform scan from remote system.	None at all
Vulnerability assessment tool shows negative database match	L	Use **nessus** for Solaris to perform assessment from remote system.	None at all, no ports open
No .rhosts or hosts.equiv files anywhere on the system	L	**find / -name .rhosts –ls, find / -name hosts.equiv –ls**	None

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

Tripwire installed and configured using encryption	L	**Which tripwire, tripwire –m c** to see if it has been initialized properly, and uses an encrypted database, and is in cron.d	Should respond that database cannot be found, See Audit, Appendix A
Sendmail configuration is secure, in case SMTP is used	L	**cat /etc/sendmail.cf | grep DAEMON** and also **| grep Privacy** to make sure no daemon mode or remote commands work	DAEMON=no is present, and PrivacyPolicy at least has … See Audit, Appendix A
Physical premises are secured	L	Terminal session times out after 10 minutes Safe contains the only records of passwords Physically locked safely when personnel absent Router is disconnected when personnel absent more than three days	Timeouts, safely locked, safely locked, and disconnected
Privileged users root, bin, daemon, gdm, xfs are present and have passwords	A	**cat /etc/passwd**	/etc/passwd shows only these and legit users
Appropriate UPS and Backups	A	Check them physically	Unplug mains, system remains up, test restoration
Groups are limited to only necessary ones, and all have passwords	A	**cat /etc/group**	See Audit, Appendix A
Iptables is running and configured appropriately	A	**iptables -L –line-number**	See Audit, Appendix A
Logging functions for cron, reboot, messages, security..	C	**tail /var/log/*** to make sure recent events have been logged. Generate some events, reboot, use ssh to test.	Known recent events, including reboot, ssh use, packets, are logged
Unusual surveillance and known exploits are noted.	A	Subjective – see systems administrator	Subjective
/etc/passwd, /etc/group, and /etc/shadow are 644, 400,root	C	**ls –al /etc** and examine permissions	`-rw-r--r--` and `-r--------`
No users or groups are uid or gid of 0	C	**cat /etc/passwd** and **cat /etc/group**	None except root
No '.' In any $PATH variable	C	Log in as each user and **echo $PATH**	None
No inappropriate or casual files exist in /root	C	**ls /root** (done as root)	Only bash, mail, xwindows-related

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

User home directories are all 755 or more restrictive	C	**ls –al /home** and examine permissions	`-rwxr-xr-x` Or more restrictive
User '.'files should all be 755 or more restrictive	C	**ls –al /home/*** and examine permissions	Same

F. Contribution: Auditing Windows 98

There is no authoritative auditing procedure or CIS ruler available to measure Windows 98, however we can use methods from the CIS Windows 2000 ruler to measure this system. Many of the tools used will be the same, or will be a Windows version of the same tool used to audit Unix systems.

The elements to be checked are listed briefly below, along with the source of the item, A= Author, C= CIS Solaris ruler documentation, S= [Scambray,McClure,Kurtz]. Items relevant only to domain controllers and network relationships are omitted, since no Windows workgroups or domains are allowed, other than local domain controllers and user authentication on isolated Windows 98 systems. Some items may have no known way to check or perform them under Windows 98/95, but would be worthwhile to keep on the list, in case an expert can contribute a method and hopefully a remedy.

Checklist Item	Src	Method/Command	Benchmark
Password policy is correct and enforced, min 7 length, nontrivial, and 90-day exp.	C	Using the Settings, Network dialog, the Primary Network Logon is "Biometrics Client"	Poledit.exe, Local Computer, Windows 98 Network, Password, Minimum password length. No local aging possible, enforce manually
Windows 98 is installed multi-user, ***no/local*** Windows network or domain, DHCP only, peripherals only on individual systems	A	Control Panel, Network, Identification shows local Workgroup and Computer name, check Printers, right mouse-button, Share… each	Not Shared
Account lockouts enabled for more than 20 logon attempts	C	Attempt 20 logons	Fails to log on
Security event logs appear to function correctly	C	Examine /Program Files/ESLogs/*.html	Shows latest logon, boot, other events
Task scheduler is only available to administrator	C	Attempt CTRL-ALT-DEL as user	Button disabled
ROM-BIOS password is set	A	Hard boot and try to edit CMOS/BIOS	Fails without password
Refuse startup without network logon	C	Press cancel on login dialog when prompted for boot logon	Cancel repeats logon prompt
CD/floppy autorun is disabled	A	Insert any CD with autorun.inf	No action taken
Inetd is disabled, with no services offered	A	Run task manager, check task bar	No inetd process

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

Log backups and restores	C	Check system logs	Backups are logged
Lock (screensaver) console after 10 minutes of no activity	C	Let system alone for 10 minutes as each user	System requires re-login
Clear virtual memory pagefile on shutdown	C	Not known for Windows 98	Not known for Windows 98
Remove last username from logon screen	C	"Don't show last user at logon" is checked	See Audit, Appendix B
Logon banners have legally binding warning text	C	"Logon banner" is checked and has text.	Test shows up on logon
Installation of drivers is prohibited except for admin	C	Policy for local users, Windows 98 System, Control Panel, System	Unknown for Windows 98
Rename the administrator account	C	Check Control Panel, Users	No such user as administrator
Only recognized user accounts allowed, no guest	C	Check Control Panel, Users	No unrecognized users defined
System has local firewall software installed and configured correctly	A	Check firewall control panel for ACLs	All ports filtered/drop except connections established locally
Biometric logon declines any nonmatching fingerprint for 5 lockouts, or 100 attempts.	A	Exhaust 100 logon attempts with incorrect fingerprint	Refuses all attempts
Browser security settings refuse all unsigned, prompts for signed applets/ActiveX, allows active scripting.	A	Open IE 5.5, select Tools, Internet Options, Security tab. Check all levels, each user.	All settings are correct for all zones: See Audit, Appendix B
All file and print sharing is disabled by policy	S	Policy has all file and print sharing disabled	Poledit.exe has items disabled: See Audit, Appendix B
Any exceptions to file sharing have share names ending with '$'	S	Examine shared resources	Examine all shares: all names begin with "$"
All dialup access is disabled by policy, or DUN 1.3 used	S	Policy has all dialup access/service disabled	Poledit.exe has items disabled: See Audit, Appendix B
Remote registry services are not installed	S	Policy Connect… to local host name is refused	No such services are available locally
Reputable antivirus software is installed and configured correctly	S	Check antivirus software control panel or UI.	McAfee, Symantec, Microsoft, PC-cillin, others?
Disable password caching for Windows 98	S	Policy has password caching turned off	Poledit.exe has items disabled: See Audit, Appendix B
Vulnerability assessment tool shows negative database	A	Use **nessus** for Linux to perform assessment	Nessus report shows no known

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

match		from inside firewall.	vulnerabilities
Registry is not writeable by non-privileged users	A	Use poledit.exe, Local User, Windows 98 System, Restrictions	Disable Registry Editing Tools is checked
LAN has UPS/power, backups performed regularly	A	Check physically	Functions unplugged long enough to power down, backups have recent changes

G. Contribution: Auditing the Linksys BEFSR41

There are no authoritative auditing procedures or CIS rulers available to measure any of the Linksys home Cable and DSL routers. In this case, an assortment of methods from [Northcutt], and manufacturer documentation must be used to measure this system. As of November 30, 2001, web references about the Linksys BEFSR41 can be found at the following links.

http://www.mactechnologies.com/pages/tftpinst.html#linksys

http://www.practicallynetworked.com/support/linksys_router_help.htm

http://www.linksys.com/products/product.asp?prid=20&grid=23

This device can be treated as more or less a black box firewall combined with a web server and a tftp server available to the LAN addresses. There may or may not be other services running but hidden, available to either the LAN side or the WAN side, but documentation mentions only the web interface and a tftp update interface, presumably with the server component on the router and client in the update package. Since both web services and tftp services are prone to security vulnerabilities, more in-depth testing than is within the scope of this audit is strongly recommended by the author, and in a laboratory context. The router here is intended only to 1) provide NAT for an internal network, 2) forward all IP traffic to the designated DMZ host (system #1), and 3) filter out most unroutable and malformed IP packets.

The elements to be checked are listed briefly below, along with the source of the item, N= [Northcutt], A= Author, L= Linksys Corporation or related source, (e.g. Mac Technologies, the software contractor). Note that some tests are pertinent to the LAN ports, while others are relevant to the WAN side of the appliance.

Checklist Item	Src	Method/Command	Benchmark
Latest patches are installed	N	BEFSR41 4-port Cable/DSL router,	All patches on or before current date are installed
Vulnerability assessment tool shows negative database match	N	Use **nessus** for Solaris to perform assessment from remote system.	WAN side, LAN side each show no known vulnerabilities
Router has no users other than one administrator, this has a nontrivial password	N	Attempt to log in as default and admin, using same passwords, run brute force login attack.	Negative login

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

Have correct ISP-specified host, domain, and IP address or DHCP, and name servers	L	See ISP installation documentation.	Checks out with ISP, can ping name servers, DMZ firewall allowing
Remote login is disabled (unless ADSL requires it)	L	See Setup panel in web interface	Disabled
Subnet mask is minimal for actual number of systems	L	See Setup panel in web interface	As small as possible, 248 for 3-4 addresses
Router cannot force factory defaults restoration	A	Sniff http request to restore defaults, send on new unauthenticated session	HTTP 403, or 407
Number of DHCP users is minimal for network	A	See DHCP panel in web interface	Number of IP/NAT devices, including the router
Log viewing interface views in and out access logs	L	Compare with LogViewer application from www.linksys.com, compare with third sniffer product logs	All traffic is logged, and logs can be archived
If ZoneAlarm or PC-cillin is in use from the Linksys router, then they are enforced, and only the DMZ firewall is exempted.	L	See Security panel in web interface	Security panel shows license key, enforcement checked, and no exemptions except firewall NAT IP
Port filtering implements secure ACLs, MAC addresses are filtered too	A	See Filters panel in web interface	Outbound ACL requirements implemented by port
There is no port forwarding in place for this router	L	See Forwarding panel in web interface	No ports forwarded
All Dynamic routing is disabled, gateway mode, not router mode	L	See Dynamic Routing panel in web interface	TX, RX both disabled, gateway mode
Static WAN routes exist only for static ISP gateways, or none if using DHCP for WAN side	L	See Static Routing panel in web interface	Each route in select box shows empty. Routing table has only three routes, WAN inbound and outbound, and LAN
DMZ Host is set to the Linux host address for System #1	A	See MDZ Host panel in web interface	192.168.1.n, for designated host n
Internal (LAN) addresses are away from 1 and 255, making surveillance more difficult	A	See Setup panel in web interface, LAN IP Address section	Start at 192.168.1.39 for example, requires static LAN routes

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

(Note: Last item in checklist contradicts items for minimal subnet mask, DHCP use, and minimum number of DHCP users – it may be of dubious value)

The web user interface for the Linksys Cable/DSL router is mostly quite intuitive, but sometimes idiosyncratic, for example, where the access control list is managed from the Filters panel: there are five port ranges that can be prohibited, and these appear from the logic to apply to outbound IP traffic, not inbound. An additional stateful firewall is required for meaningful active security. This is provided by the DMZ host, System #1.

H. Contribution: Auditing a Remote System and Web Application

There is no authoritative auditing procedure or CIS ruler available for web applications and user-interactive web sites in general, and so it will be necessary to apply methods described in [Rhoades], web application testing techniques [Nguyen] and the author's own software development experience to measure the corporate web application and the remote network that supports company email and auxiliary services. A simple application of the CIS ruler will be made to the Solaris 5.6 operating systems that run the remote network.

Unfortunately the remote system is under the control of a not-for-profit organization, and operates several other web sites for the benefit of other entities. This means that any functioning in any of the other organizations' web sites represent a security opening to the web server, and therefore a risk to the company's web site assets. All virtual hosts sharing the same system, especially web server, will generally have to be tested for security, to the extent that any system compromise is possible via any of them. The elements to be checked are listed briefly below, along with the source of the item, R= [Rhoades], A= Author, S= [Scambray, McClure, Kurtz], N= [Nguyen]

Remote system #1: DMZ host and web server

Checklist Item	Src	Method/Command	Benchmark
CIS Solaris 5.6 ruler score of 85 percent or better	A	www.cisecurity.com, download the tarfile & run sara	75 percent or better
Vulnerability assessment tool shows negative database match	A	Use **nessus** for Linux to perform assessment from local system.	No security holes
SSH is actually secure	A	Use sniffer – e.g. hunt to read actual TCP content, esp. password	All communications other than prompts are unreadable

Remote system #2: IMAP/SMTP (email) server

Checklist Item	Src	Method/Command	Benchmark
CIS Solaris 5.6 ruler score of 75 percent or better	A	www.cisecurity.com, download the tarfile & run cis	75 percent or better
Vulnerability assessment tool shows negative database match	A	Use **nessus** for Linux to perform assessment from local system.	No security holes
IMAP is actually secure	A	Use sniffer – e.g. hunt to read actual TCP content, esp. password	All communications other than prompts are unreadable

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

Web Applications:

Checklist Item	Src	Method/Command	Benchmark
The web server product cannot be identified easily	R	telnet to port 80	No or inaccurate banners
No default install materials remain available	R	Try “default.*” in URL in all possible forms	All 404’s, not found
Available web map is correct	R	Try each location	All 400’s, all there
No well known executables are installed in, linked to document root	R	Try appending perl, perl.exe, python, python.exe, csh, to each path in the site	No responses, all 404’s
Site server is set to resist mirroring applications	R	Mirror the site, multiple times if necessary	Lockouts after many requests, difficulty
Robots.txt is set properly in each document root	R	ls –al in the document root folder, from inside	Robots.txt says no robots
HTML contains no unintended name tags or comments	R	Examine served HTML, look for action, method, name, <!--, <script, javascript, //, other usual suspects	No inappropriate comments, subjective, some may be acceptable
HTML and javascript are obfuscated or compressed	R	Examine served HTML	Hard to read in vi or notepad
If HTTPS, encryption level requires 128 bit RSA or better	R	Use Netscape, turn off SSL v2 encryption ciphers from lowest up	Requires only 128 bit or better
Attempts to manipulate boundary and extreme values of candidate application variables do not reveal important or private information	R	List relevant application variables (“name=”) and values (“value=”), note application roles, submit test suite forms to see error codes and results	Error messages are generic and have no debug information, or application info
Browser cache does not cache private information	R	Maximize cache, examine cached pages	No private form responses, or pages with private info
If Certificate Authentication, agency is trustworthy, and only one session is allowed	R	Try to spoof signer, or show it can be forged, try multiple concurrent auths	Multiple session authentications fail, with no information revealed
If CA, then the way the certificate is authenticated is secure	R	MD5 signatures and PGP public signatures match (best effort)	Unbroken chain of authentication
If form-based authentication, the form, or at least the action is HTTPS	R	Sniff the login. Check the url of the form, and the form’s action attribute	No passwords or other private info is plaintext

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

If secure form-based auth is used, then additional token or other factor is used	R	Check the login form	Smartcard, time token, or biometric id
If HTTP basic authentication is used, the initial URL is HTTPS	R	Sniff the login to make sure, check the url	HTTPS
Generally, there is no ability to authenticate at different scopes, global, session, and request, as different users, except as specified	R	Try to use several different sets of credentials concurrently each from the other	Only one scope at which authentication is done.
There is no ability for concurrent logon from different addresses	R	Try to do this from different addresses	Authentication fails with minimal info message
If any auth error, report all verifiable user names, and if possible, passwords	R	Brute force it if there is any way to confirm existence from error messages returned	Lockout preferable, or generic error message
There is an authentication lockout and renewal policy	R	More than n invalid auth attempts lock users out	Locked out pending email request, or similar
For heavy traffic sites, sign-on timeouts and load balancing is in proper order	R	Use Webcracker to open many concurrent sessions	No lockups that are not intentional (see above, mirroring)
If auth is used, then sign-off does actually sign the user off	R	Try to access previous resources from a signed-off session, sign off multiple times	Access denied as though never authenticated
Any application variables used for session tracking are encrypted or obfuscated	R	Determine the session tracking mechanism, if any, See if it can be predicted.	Impervious to astute analysis, subjective
Any cookies containing sensitive information are encrypted and have full identifying information included	R	Examine all cookies, and sniff their transit to confirm	All encrypted
If there is auth used, and if the session tracking is predictable, then concurrency from different IP's disallowed	R	Try to simulate a session id from a different address while logged on from the first	Multiple sessions from different IPs forbidden
Session inactivity timeouts are reasonably short	R	Leave a session inactive	Less than about 15 minutes
Form submissions are all POSTs rather than GETs	R	Examine all form action attributes	No GETs
Web sites allowing user input perform filtering for CSS and other malicious code	R	Procedures for serving user-defined HTML and customization	All user input is filtered rigorously, subjective

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

Product-specific vulnerabilities are scanned for esp. IIS, ColdFusion, JRun	S	See www.cisecurity.org or http://packetstorm.decepticons.org for the latest product scanners	Product ruler exists and has 75 or 90 percent level results.
Server request logs are monitored for surveillance, DoS, and legitimate use patterns	A	Subjectively, the level of attention is sufficient to preempt intrusion and adapt to usage	Daily intrusion check, monthly usage review

I. Score, Remedial Action List, and Actions Taken

The audit report on each of the systems above will include a referral to an appendix containing the audit results and benchmark comparisons. There should also be an appendix containing an overall ***V*** or Value at Risk Mitigation matrix to indicate which corrective measures should be taken. The score on the checklist will be reported and discussed briefly, and a list of remedial actions for the checklist enumerated. A paragraph on recommended actions taken for each system will be made at the end of each system's section in the report, and an overall comment made by both auditor and executive for remedial actions taken will be made in summary.

© SANS Institute 2000 - 2002, Author retains full rights.

References

CIS – "Solaris Benchmark and ruler", Center for Internet Security
http://www.cisecurity.org/bench_solaris.html, PDF-format documentation from tarfile

CIS – "Windows 2000 Benchmark and ruler", Center for Internet Security
http://www.cisecurity.org/bench_win2000.html, PDF-format documentation from zipfile

CERT – "Unix Security Checklist" and "Survivable Network Analysis Method" articles
http://www.cert.org/tech_tips/usc20_essentials.html, http://www.cert.org/archive/html/analysis-method.html

Condorcet, Marie-Jean-Antoine-Nicolas, marquis de "Foundations of Social Choice and Political Theory", trans. and ed. by Iain McLean and Fiona Hewitt Aldershott, UK: Edward Elgar, 1994

Laude, Mary, "Auditing RedHat Linux 7.0", SANS GSNA Practical Exam, August 10, 2001.
http://www.giac.org/GSNA.php and select Mary Laude for PDF download

ISACA, CobiT methodology documentation, http://www.isaca.org/cobit.htm

Nguyen, Hung "Testing Applications on the Web", Wiley 2001, ISBN 0-471-39470-X

Marchany, Randy "Applying Risk Analysis Techniques to Information Systems Assets" SANS course notes and reference, October, 2001, www.sans.org

Northcutt, Stephen "Auditing Routers and Firewalls" SANS course notes and reference, October, 2001, www.sans.org

Rhoades, David "Auditing Web-Based Applications" SANS course notes and reference, October, 2001, www.sans.org

Saari, Donald, e.g. http://www.unc.edu/depts/cmse/math/Saari.html assorted articles between 1970-1990 on voting, non-transitivity

Scambray, McClure, Kurtz "Hacking Exposed" McGraw Hill 2001, ISBN 0-07-212748-1

Sen, Amartya "The Impossibility of a Paretian Liberal", 1970, Journal of Political Economy 78(1): 152-57

Further reading on voting, rank-ordering, non-transitive voting schemes, robust voting, etc. – Requires academic affiliation, or fee-based membership:
American Political Science Review http://www.jstor.org/journals/00925853.html
American Journal of Political Science http://www.jstor.org/journals/00030554.html

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

Part II: Auditing a Real World Small Business:

Generic Services Corporation

A. Executive Summary

The exposure of IT assets for Generic Services Corporation (a fake name to satisfy GIAC examination criteria) is at an acceptably low level, being primarily exposed due to lack of control over physical premises, certain kinds of web hacking, general lack of adequate local firewall and antivirus capability, and lack of Windows 98 system event logging. These weaknesses in the overall security schema are mitigated by adequate external network security. There is no compelling issue or gaping security hole anywhere.
Other remedial measures such as purchase of a safe, purchase of reliable UPS capability, possible web site relocation, and compromise recovery capability (i.e. incident handling capability) appear to be of significant value in reducing the overall risks to this corporation for loss or revelation of critical data, interruption of operations, and defacement or damage to web assets. These measures are cost effective, and should be implemented.
The overall present value of the entire enterprise's future, however big or small, is at stake due to the core function of the business being network security itself. The only significant assets of the firm are those in the IT department, unlike some other businesses. Consequently, however small the amount of value at risk that is mitigated by these corrective measures appears to be, it represents a critical measure of success for this entire company. It is imperative therefore that all or most of the corrective measures described in the matrixes in Appendix F be implemented.

B. The Organization

Generic Services Corporation is a closely held Delaware "S" corporation founded in 1994, and has done no business between Fiscal Years 2000 and 2001. The author was fortunate enough (perhaps) to be able to purchase this corporation along with all its assets and prior relationships for a small sum. Currently, operations are being revived with both prior and new clients, and the business of the company is being defined and focused.

The founders of this corporation are 1) a US Naval Academy graduate (1963) who later taught the first computer science courses there, 2) one of the original DARPA systems administrators who had discovered and helped eliminate the Morris worm threat (the first known Internet worm in 1988), and 3) a penetration and exploit expert who is currently employed attacking and testing defense department networks. All three remain principals and co-owners.

The business has in the past included custom software and services, mixed together as needed for any specific project. However, the new management has decided to focus the firm's attention on security services and standard service offerings. Some of these are installation, while others involve more general business practice consulting and expert legal testimony. The network certification and auditing offering, however, is new, and will feature GIAC-certified audit personnel, CIS rulers, and any other broad standards that are available. The flagship example of this auditing service will be this essay.

(write to email@address for more information)

C. IT Systems and Assets

The company has few and simple assets compared to a large, complex operation in the same business, such as Symantec, or Counterpane, and it would be the author's desire to show a more comprehensive example of enterprise IT auditing procedure. However,

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

the assets here should be representative enough to make a helpful example for small businesses, where this function is sorely needed, but who also need to spend minimal resources on non-revenue generating activities such as auditing.

These assets are grouped into two collections, by physical locale: Locally, there are one Pentium Linux system (System #1, custom built with 233Mhz, Ethernet and USB, 12G disk), functioning as a firewall, product development machine, and service attack/ evaluation machine ("attack dog"), and one Pentium laptop (System #2, Dell Inspiron 7000 with 133Mhz, 9GB disk, and PCMCIA) for operations needs. A shared monitor and keyboard will be considered part of the laptop system. One Linksys cable/DSL router (BEFSR41), cabling, and printer constitute most of the office equipment and supplies assets, plus there are some miscellaneous other supplies. Local assets also include some PKI elements: private keys and trusted signatures of other entities.

Assets and the systems they occupy are enumerated as follows:

Asset	Location	Size of Possible Harm to Asset (1,000's of $)
Product development code, project #1	System #1	$100K
Service Contracts with client-specific charges and fees	System #2	$250K
Email records with strategy and shareholder discussions	System #1, and remote #2	$1,000K
Web site HTML and CGI code/objects.	Remote #1	$100K
Server system logs, individual system logs	System #1	$100K
File system integrity databases	System #1	$100K
Password and related files with user information	System #1, System #2	$1,000K
Device configuration, ACL's and administrative passwords/backdoors	System #1, System #3	$100K
Web site appearance – proxy for perceived quality of service	Remote (the web server)	$250K
Personnel private records	System #2	$10K
Gateway/firewall routers and top layers	ID: System #3	<$1K
Desktop PCs: x86/Linux	ID: System #1	$2K
Laptops: x86/Windows	ID: System #2	$2K
Office supplies, electronics	Home Office	$2K

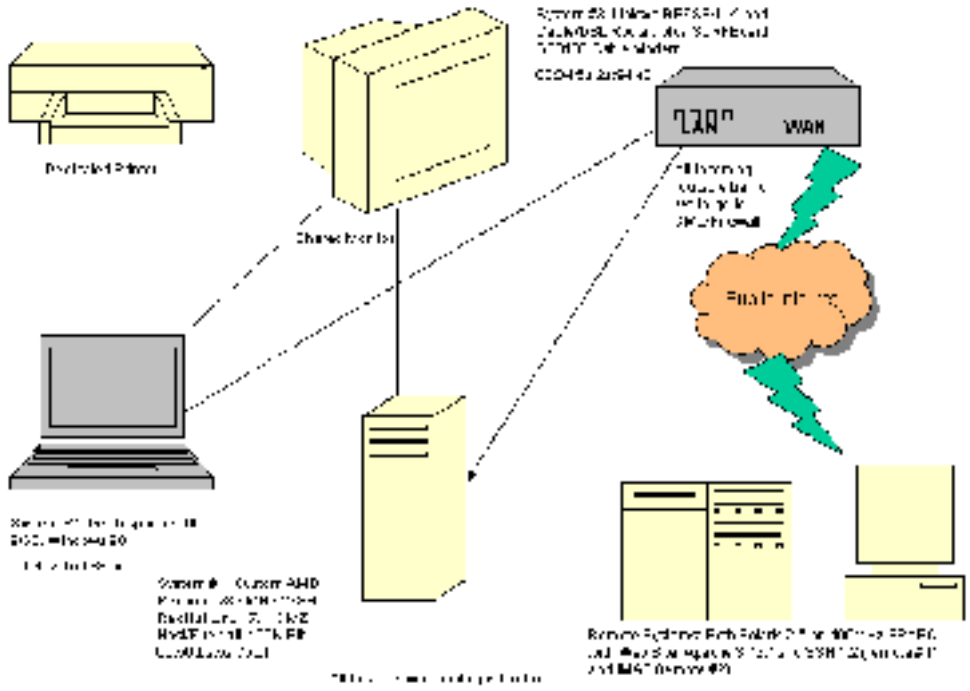
From the enumeration of assets, the systems to be audited will #1, #2, #3, and remote systems #1 and #2, plus a brief coverage of the home office premises. Attention to this latter premises checklist will be omitted from this audit. The asset estimates to some extent may double-count enterprise asset value predicated on those informational assets. However it is assumed that the risks to these assets are independent of each other, and can be mitigated independently.

The primary sources of risk to these assets are from outside hacking and exploits, network surveillance that might reveal private information, and compromise of physical premises, allowing access to consoles, CD Rom drives, hard drives that could be removed, devices that could be planted, and access to physical machines and sensitive data storage on their physical media. Any of these sources of risk can potentially harm or reveal the assets listed above.

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

A network diagram describing the systems and their relationship follows:

The remote systems contain the production web site and the site's HTML code. The IT systems to be audited are system #1, system #2, system #3, and remote systems #1 and #2, including the web sites run by remote system #1.



D. Audit Results

1. System #1

The Linux DMZ host, development box, and attack dog, currently attains a score of 30 out of 38, or about 79 percent on the unweighted checklist. Being an internal audit, permission was available to correct some items during the course of the audit, if in the administrator's subjective judgment it would take little time to do so. Prior to these corrections, the unweighted score would have been less than 58 percent.

Remaining corrective actions to be taken include purchase of a safe and a reliable UPS system, more frequent backups, an incident handling disk with statically compiled applications, setting a LILO password and an Xwindows inactivity timeout, and some setuid related systems administration adjustments. The estimated amount of cost, time, and effort to perform these corrections is on the order of $1000, taking about 6-8 employee days.

These actions are supported by the fact that they reduce risks significantly to strategically sensitive email records, and system-compromising assets such as passwords. The most important remedial actions to take are purchase of a safe

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

for premises password security (and other security), and creation of an incident handling disk. See Appendix A for more details of the audit.

2. System #2

The Windows 98 operations and user applications machine currently attains a score of 19 out of 29, or just over 65 percent on the unweighted checklist. Prior to correction of some items during the course of the audit, the unweighted score would have been about 48 percent.

Corrective actions still remaining to be taken on System #2 include Local firewall and antivirus software, Task scheduler restrictions, driver installation restrictions, system event logging, pagefile clearing on shutdown, more frequent backups, and purchase of a UPS. The order of cost, time, and effort required to correct these is on the order of $500 and five to seven days of employee days to address these items.

Most important and cost effective of these items is the local firewall and antivirus software, and system logging, while the user restrictions seem most questionable as far as risk mitigation and time spent. See Appendix B for more details of the audit of System #2, the Windows 98 laptop.

3. System #3

The Linksys BEFSR41 home 4-port Cable/DSL router is a home network appliance that is fast growing in popularity, mainly because of its low cost and its turnkey nature. It may seem *ex ante* similar to writing a book report on an ABC's textbook (an exercise in pure procedure without any added value), but it is important to know the security implications for the network as a whole, and the organization's IT assets.

Upon auditing, this system scores twelve out of sixteen possible checklist items, or 75 percent. None of the items discovered out of compliance could be addressed during the course of the audit. It is anticipated that changing items that *can* be fixed could add some small degree of extra security while costing approximately 1 to 2 days of employee time. See Appendix C for more details of the audit of System #3, the Linksys router.

In summary, while unarguably cost effective, there are also a number of logging deficiencies and LAN side vulnerabilities and deficiencies. However, there seem to be no glaring problems on the WAN side of the device. Product note: Beware of using this device within a wireless context, or as a general router, and thoroughly investigate the Linksys wireless appliances in future for the same reasons. Do not use this device as the DMZ host and expect to have meaningful security.

4. Remote System #1, plus Web Site

There are SSH, SMTP, and HTTP services, which all appear to be reasonably secure with the exception of the obsolete web server version. The web application uses no HTTPS, authentication, or cookies, and is not vulnerable as such on any of these counts, however two other web sites run as different virtual hosts by the same server are somewhat at risk due to the custom CGI in use for administrative login. Application testing for these additional web applications is outside the scope of this audit, and this risk is irreducible unless web hosting arrangements are altered.

This system scores 60 percent, or 12 out of 20 on an unweighted checklist. This may overweight some of the web application testing at the expense of the overall system checklist testing. For example it may be that the CIS Solaris ruler or Nessus scan results should be weighted more heavily than whether or not the web site's cookies are encrypted. A concern here is that the CIS Solaris ruler

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

was not permitted by the remote network owner and operator, and so internal measures of security are unknown. See Appendix D for more details of the audit of remote system #1, the SSH/SMTP/HTTP server.

5. Remote System #2

Remote system #2 represents minimal risks, as it is used exclusively for email service via IMAP. The IMAP service is protected by two firewalls permissioned for individual IP access, and so vulnerability is low. However system internal security conditions inside the perimeter could not be ascertained by using the CIS Solaris ruler or an internal vulnerability scan, due to the network owner's hesitancy to grant root access.
Overall the system scores passes on two out of three checklists (67 percent), failing the CIS checklist, passing the external Nessus scan, and passing the IMAP traffic sniffing test. Due to the minimal nature of the services provided, this scanning is deemed sufficient to decide whether to keep or replace this email service. The only other solution is to request an updated IMAP daemon from the system owner.

E. Auditor and Executive Comments

The management in this case has represented a benchmark for the desired level of cooperation and participation in this audit, and cannot be thanked enough for their assistance. It cannot be anticipated that in future audits or those of other companies or departments that this level of cooperation can again be expected. There are still remaining risks to be contended with that are outside the scope of the IT department, for example, finances, personnel loyalty, leased premises, and business conditions. All of these can have an impact on information assets and their safety, and are left uncovered by this technology audit.

It is imperative for the ongoing survivability of this company that its only significant assets, those in the IT department, should be protected at all costs up to a significant fraction of the firm's entire net present value.

Assuming that all the recommended corrective measures described in the matrixes in Appendix F are implemented, the remaining risks to the corporation's IT assets will be a small fraction of the value of those assets, expressed on an annual basis. To recap, these measures are: 1) Placing written passwords in a safe (to be purchased), 2) Xwindows screensaver timeout, 3) setuid issues clarified, 4) LILO password set, 5) An incident handling disk for Linux 7.1, 6) A UPS (to be purchased), 7) local Windows 98 firewall and antivirus software (to be purchased), 8) Windows task scheduler and driver install restrictions, 9) Windows 98 system/event logging, 10) Windows pagefile clearing on shutdown, 11) Outbound router ACL's, 12) static LAN routes, 13) secure DNS servers, 14) Apache update, 15) Web site corrections (robots.txt, comments, and compressed HTML), and 16) an updated IMAP server.

The practices currently in place at Generic Services Corporation are, with the exception of some logging, backups, and screen saver timeouts, current state-of-the-art for any reasonably prudent commercial IT department, and we endorse those practices, conditional on the remedial measures described above having been taken.

Comment dated December 13, 2001:

David M Eaves

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

Executive response:
All remedial measures described in Appendix F have been, or will be taken within 30 days of this comment, except for updating IMAP and Apache on the remote systems and the router modifications. However, a singular situation exists with respect to the remote systems. These are run by one of the firm's founders, whose good will is essential to maintaining some business relationships. These relationships, like the risks, are also worth an amount comparable to the entire present value of all future earnings of the firm. The remote network owner may be from time to time temporarily unavailable, preventing remote systems security issues from being dealt with quickly, we can only anticipate a reasonably timely correction of such issues as they may arise.
It is recognized that assets, particularly web assets on these remote systems are at risk, but they will simply have to remain at risk until such time as additional features are added to the corporate web site (e.g. credit card acceptance for software downloads) that represent some additional risk, which requires more secure hosting premises. The same situation applies to email services provided (also hosted for free). The fact that both of these services are provided free of charge does not mitigate the risk that these remote systems pose to our information assets, and as revenue and ongoing relationships permit (or as medical conditions may require), Generic Services Corporation will move those assets elsewhere.

December 14, 2001, Generic Services Corporation

© SANS Institute 2000 - 2002, Author retains full rights.

F. Lessons Learned for Future Auditing

- Procedurally, it should be emphasized that firewall settings must accommodate any external vulnerability scanning activity. The scanning system must completely permission the subject system for returning traffic, while the subject system must set their permissions to treat the scanning system as it does any other system on the Internet. Planning for this in advance can prevent the need to re-scan repeatedly, saving large amounts of time.
- The analysis methodology may multiply count the value of corrective measures that apply to more than one system. This should be investigated.
- Security is easy when few publicly available services are offered. With more services offered comes more risk.
- The analysis methodology proposed is multiply counting the risk reductions, by asset, and might usefully account for those risks' statistical independence.
- Many methodologies exist and can be used for a process template, it is only important to select and use –one- that is sufficient for the desired purposes. The author wasted weeks trying to select one from among many. This seems best for most small IT departments.
- The major source of risk to assets turns out to be less from Internet intrusion than from other older and more well known sources: premises intrusion and personnel defection. More emphasis should be placed here, even for a technology audit.
- Top ten and top twenty scanning should still probably supplement these benchmarks, as an additional scoring or checklist item. It was judged here that these would probably have been done as part of Nessus' vulnerability scanning, but to be sure, and to corroborate, the CIS top twenty scanner could easily have been deployed, and was not.
- This has been educational, but now what needs to happen is that a "mini-CobiT" or some sanctioned lightweight audit procedure like this needs to be developed for smaller commercial IT orgs.

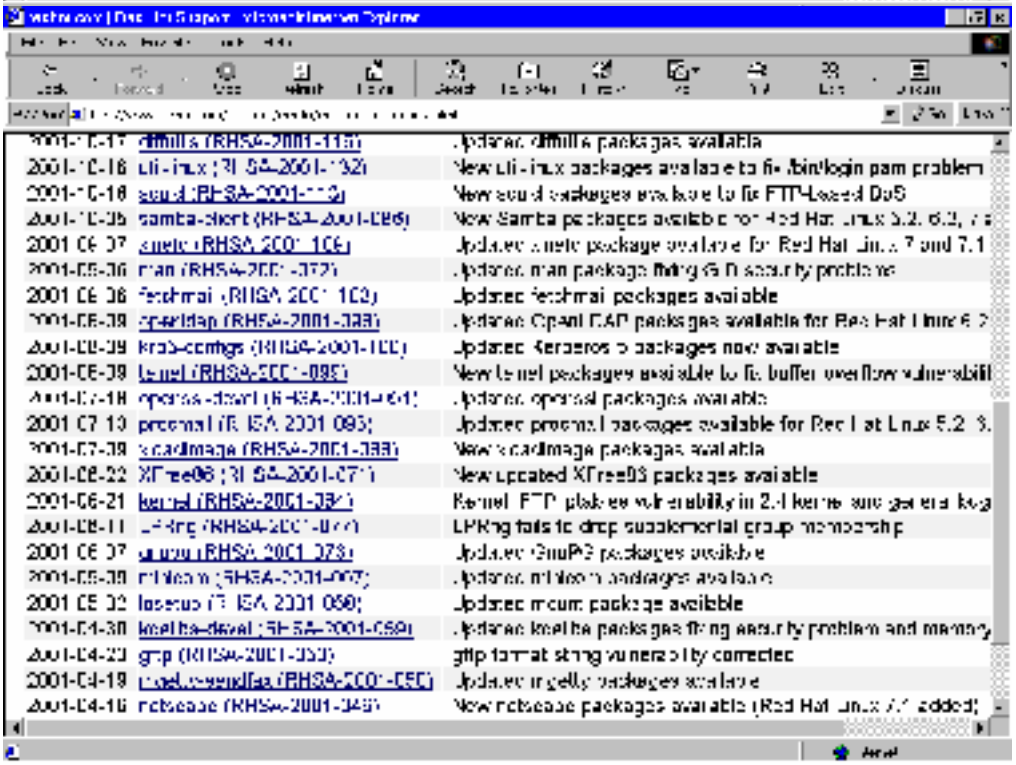
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix A: Benchmark and Matrixes, System #1

```
> uname -a
Linux <hostname>.<domainname> 2.4.2-2 #1 Sun Apr 8 20:41:30 EDT 2001 i686 unknown

Installed packages follow. List formatting (rpm -qa) is not preserved:

yp-tools-2.4-7, gftp-2.0.7b-3, mount-2.10r-5, gnome-games-devel-1.2.0-10, nkf-1.92-4, e2fsprogs-devel-
1.19-4, gqview-0.8.1-3, vim-minimal-6.0-0.27, dump-0.4b21-3, db1-1.85-5, magicdev-0.3.5-3, hotplug-
2001_02_14-15, tclx-8.2.0-53, docbook-dtd30-sgml-1.0-10, compat-libstdc++-6.2-2.9.0.14, byacc-1.9-18,
cdecl-2.5-17, gtk-engines-0.10-12, dhcpcd-1.3.18pl8-10, gcc-g77-2.96-81, nscd-2.2.2-10, gnome-objc-
1.0.2-11, python-xmlrpc-1.4-1, procps-2.0.7-8, ncurses-devel-5.2-8, sysklogd-1.4-7, emacs-X11-20.7-34,
dia-0.86-4, net-tools-1.57-6, minicom-1.83.1-5, esound-devel-0.2.22-1, netpbm-9.9-5, locale_config-
0.2-4, dev86-0.15.0-5, sendmail-cf-8.11.2-14, libstdc++-devel-2.96-81, efax-0.9-8, openssh-clients-
2.5.2p2-5, gpm-1.19.3-16, sed-3.02-9, libtermcap-devel-2.0.8-26, pwdb-0.61.1-1, rpm-4.0.2-8, gpm-
devel-1.19.3-16, textutils-2.0.11-7, readline-devel-4.1-9, rootfiles-7.0-4, kernel-headers-2.4.2-2,
libjpeg-devel-6b-15, file-3.33-1, psmisc-19-4, sh-utils-2.0-13, rep-gtk-gnome-0.15-3, gnome-applets-
1.2.4-3, glib-devel-1.2.9-1, ical-2.2-21, librep-0.13.3-1, util-linux-2.10s-12, flex-2.5.4a-13,
readline-4.1-9, indent-2.2.6-1, procmail-3.14-6, modemtool-1.22-3, libole2-0.1.7-2, libgal3-0.4.1-3,
gnome-utils-1.2.1-5, tix-4.1.0.6-53, mktemp-1.5-8, cpio-2.4.2-20, binutils-2.10.91.0.2-3, gzip-1.3-12,
gnome-pim-1.2.0-9, cproto-4.6-7, ncurses-5.2-8, emacs-20.7-34, docbook-dtd41-sgml-1.0-10, extace-
1.4.4-2, groff-1.16.1-7, python-devel-1.5.2-30, wget-1.6-2, ltrace-0.3.10-5, rhn_register-1.3.1-1,
guile-1.3.4-12, chkconfig-1.2.22-1, pygnome-1.0.53-7, gnome-libs-devel-1.2.8-11, netcfg-2.36-3, krb5-
libs-1.2.2-4, setuptool-1.7-2, ORBit-devel-0.5.7-3, rmt-0.4b21-3, initscripts-5.83-1, gnome-objc-
devel-1.0.2-11, kbdconfig-1.9.12-1, gnome-pim-devel-1.2.0-9, texinfo-4.0-20, iptables-1.2.1a-1,
tmpwatch-2.7.1-1, db2-2.4.14-5, openssh-2.5.2p2-5, tripwire-2.3-47, quota-3.00-4, ppp-2.4.0-2, hdparm-
3.9-6, pump-0.8.11-1, XFree86-tools-4.0.3-5, ucd-snmp-4.2-12, gnorpm-0.96-1, pam_krb5-1.31-1,
pciutils-devel-2.1.8-19, mailx-8.1.1-20, sgml-common-0.5-5, fileutils-4.0.36-4, netpbm-progs-9.9-5,
audiofile-devel-0.1.11-1, make-3.79.1-5, db2-devel-2.4.14-5, gd-devel-1.8.3-7, pygnome-libglade-0.6.6-
7, pnm2ppa-1.04-1, less-358-16, db3-utils-3.1.17-7, ncftp-3.0.2-1, libgtop-1.0.10-3, freetype-devel-
2.0.1-4, raidtools-0.90-20, gmp-devel-3.1.1-3, perl-5.6.0-12, alchemist-0.16-3, glade-0.5.9-5,
cracklib-2.7-8, ORBit-0.5.7-3, pam-0.74-22, 4Suite-0.10.1-1, expat-devel-1.95.1-1, control-center-
devel-1.2.2-8, bind-utils-9.1.0-10, python-1.5.2-30, newt-devel-0.50.22-2, imlib-1.9.8.1-2, termcap-
11.0.1-8, umb-scheme-3.2-18, mkxauth-1.7-15, gtk+-devel-1.2.9-4, gmc-4.5.51-32, logrotate-3.5.4-1,
groff-perl-1.16.1-7, gcc-2.96-81, libtool-1.3.5-8, rep-gtk-libglade-0.15-3, dip-3.3.7o-22, kudzu-
0.98.10-1, control-center-1.2.2-8, arpwatch-2.1a10-39, rep-gtk-0.15-3, slang-1.4.2-2, ftp-0.17-7,
gnome-core-devel-1.2.4-16, njamd-0.8.0-3, zlib-1.1.3-22, filesystem-2.0.7-1, time-1.7-13, netscape-
communicator-4.76-11, imlib-devel-1.9.8.1-2, gtop-1.0.11-3, man-pages-1.35-5, vim-common-6.0-0.27,
XFree86-twm-4.0.3-5, kernel-source-2.4.2-2, bash-2.04-21, sharutils-4.2.1-7, rxvt-2.7.5-15, openssh-
askpass-2.5.2p2-5, cpp-2.96-81, libtiff-devel-3.5.5-10, losetup-2.10r-5, gtk+-1.2.9-4, ypbind-1.7-6,
bdflush-1.5-16, xisdnload-1.38-39, bzip2-1.0.1-3, tk-8.3.1-53, gd-1.8.3-7, db3-3.1.17-7, xscreensaver-
3.29-3, libtool-libs-1.3.5-8, wvdial-1.41-12, gnome-games-1.2.0-10, gnome-audio-1.0.0-12, diffutils-
2.7-21, telnet-0.17-10, ImageMagick-5.2.7-2, rhn_register-gnome-1.3.1-1, bzip2-devel-1.0.1-3, strace-
4.2.20010119-3, ed-0.2-19, libxml-1.8.10-1, autoconf-2.13-10, setup-2.4.7-1, grep-2.4.2-5, switchdesk-
3.9.5-1, gdk-pixbuf-0.8.0-7, Mesa-3.4-13, cyrus-sasl-devel-1.5.24-17, gimp-devel-1.2.1-5, kudzu-devel-
0.98.10-1, lrzsz-0.12.20-7, man-1.5h1-20, setserial-2.17-2, utempter-0.5.2-4, control-panel-3.18-4,
libglade-0.14-3, kernel-2.4.2-2, internet-config-0.40-1, printconf-gui-0.2.12-1, db1-devel-1.85-5,
libpng-devel-1.0.9-1, Xaw3d-devel-1.5-9, redhat-logos-1.1.2-3, gawk-3.0.6-1, mkbootdisk-1.4.2-1,
gnome-libs-1.2.8-11, docbook-dtd31-sgml-1.0-10, Mesa-devel-3.4-13, gmp-3.1.1-3, LPRng-3.7.4-22,
libgnomeprint11-0.25-9, desktop-backgrounds-1.1-4, mpage-2.5.1-5, tar-1.13.19-4, gnupg-1.0.4-11, rp-
pppoe-2.6-5, perl-SGMLSpm-1.03ii-4, gdk-pixbuf-devel-0.8.0-7, lsof-4.51-1, rusers-0.17-10, aumix-2.7-
2, libghttp-devel-1.0.8-2, mc-4.5.51-32, sudo-1.6.3p6-1, slocate-2.5-5, nfs-utils-0.3.1-5, pmake-1.45-
1, libungif-4.1.0-7, glibc-common-2.2.2-10, tcsh-6.10-5, anacron-2.3-16, rpm-devel-4.0.2-8,
libtermcap-2.0.8-26, rwho-0.17-10, SysVinit-2.78-15, devfsd-2.4.2-2, gedit-0.9.4-3, krb5-devel-1.2.2-
4, gal-0.4.1-3, tcl-8.3.1-53, timeconfig-3.2-1, patch-2.5.4-9, switchdesk-gnome-3.9.5-1, mailcap-
2.1.4-2, lilo-21.4.4-13, xchat-1.6.3-4, rpm-build-4.0.2-8, tksysv-1.3-2, talk-0.17-9, rsh-0.17-2.5,
gcc-c++-2.96-81, libxml-devel-1.8.10-1, lokkit-0.43-6, glib-1.2.9-1, krbafs-1.0.5-1, xtt-fonts-
0.19990222-9, tamago-4.0.6-4, qt-2.3.0-3, pygtk-libglade-0.6.6-7, words-2-16, libglade-devel-0.14-3,
statserial-1.1-20, mingetty-0.9.4-16, gq-0.4.0-2, docbook-dtd40-sgml-1.0-11, gdbm-1.8.0-5, xsri-1.0-8,
libstdc++-2.96-81, timetool-2.8-1, docbook-utils-0.6-13, redhat-release-7.1-1, gettext-0.10.35-31,
mouseconfig-4.21-1, ee-0.3.12-3, chkfontpath-1.9.5-1, bison-1.28-5, rcs-5.7-14, esound-0.2.22-1,
expect-5.31-53, gnome-print-0.25-9, indexhtml-7.1-2, Xconfigurator-4.9.27-1, XFree86-xdm-4.0.3-5,
libpcap-0.4-39, netscape-common-4.76-11, libunicode-0.4-4, gnumeric-0.61-9, basesystem-7.0-2, urw-
fonts-2.0-12, pythonlib-1.28-1, cyrus-sasl-1.5.24-17, stat-2.2-2, finger-0.17-7, VFlib2-2.25.1-12,
MAKEDEV-3.1.0-14, Xaw3d-1.5-9, openjade-1.3-13, eject-2.0.2-7, gnome-core-1.2.4-16, openssh-askpass-
gnome-2.5.2p2-5, openldap-2.0.7-14, stunnel-3.13-3, XFree86-libs-4.0.3-5, ucd-snmp-utils-4.2-12, nmap-
2.53-1, libjpeg-6b-15, XFree86-75dpi-fonts-4.0.3-5, gnome-users-guide-1.2-3, vixie-cron-3.0.1-62,
imlib-cfgeditor-1.9.8.1-2, openssl-0.9.6-3, gdbm-devel-1.8.0-5, openssl-devel-0.9.6-3, XFree86-100dpi-
fonts-4.0.3-5, rpm-python-4.0.2-8, authconfig-4.1.6-1, rsync-2.4.6-2, ntsysv-1.2.22-1, pidentd-3.0.12-
4, memprof-0.4.1-3, cracklib-dicts-2.7-8, at-3.1.8-16, m4-1.4.1-4, cvs-1.11-3, ctags-4.0.3-1, pygtk-
0.6.6-7, psutils-1.17-10, popt-1.6.2-8, gdb-5.0rh-5, glibc-devel-2.2.2-10, up2date-2.5.2-1, modutils-
2.4.2-5, ash-0.3.7-1, db3-devel-3.1.17-7, diffstat-1.27-5, bug-buddy-1.2-3, pump-devel-0.8.11-1,
which-2.12-1, screen-3.9.8-3, isdn4k-utils-3.1-39, whois-1.0.6-1, newt-0.50.22-2, libungif-devel-
4.1.0-7, iproute-2.2.4-10, ipchains-1.3.10-7, fortune-mod-1.0-13, freetype-2.0.1-4, rp3-1.1.10-1,
gnome-audio-extra-1.0.0-12, up2date-gnome-2.5.2-1, libghttp-1.0.8-2, openldap-clients-2.0.7-14,
printconf-0.2.12-1, ghostscript-fonts-5.50-3, info-4.0-20, tcp_wrappers-7.6-18, libpng-1.0.9-1,
usermode-1.42-1, sgml-tools-1.0.9-9, pam-devel-0.74-22, iputils-20001110-1, autofs-3.1.7-14, gdm-
2.0beta2-45, bc-1.06-2, tkinter-1.5.2-30, e2fsprogs-1.19-4, passwd-0.64.1-4, sawfish-0.36-7, openldap-
devel-2.0.7-14, sendmail-8.11.2-14, dosfstools-2.2-8, arts-2.1.1-5, emacs-nox-20.7-34, expat-1.95.1-1,
```

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

```
libtiff-3.5.5-10, glibc-2.2.2-10, crontabs-1.9-2, slang-devel-1.4.2-2, libmng-1.0.0-2, audiofile-
0.1.11-1, findutils-4.1.6-2, automake-1.4-8, docbook-style-dsssl-1.59-10, apmd-3.0final-29, shadow-
utils-20000826-4, rdate-1.0-7, gcc-objc-2.96-81, zlib-devel-1.1.3-22, xinitrc-3.6-1, traceroute-1.4a5-
25, dev-3.1.0-14, ncompress-4.2.4-21, krb5-workstation-1.2.2-4, portmap-4.0-35, ksymoops-2.4.0-3,
nss_ldap-149-1, gv-3.5.8-11, xpdf-0.92-3, pciutils-2.1.8-19, mkinitrd-3.0.10-1, console-tools-
19990829-34, libgtop-devel-1.0.10-3, XFree86-devel-4.0.3-5, xloadimage-4.1-16, a2ps-4.13b-13,
syslinux-1.52-1, netpbm-devel-9.9-5, shapecfg-2.2.12-5, ghostscript-5.50-17, XFree86-4.0.3-5, XFree86-
xfs-4.0.3-5, nessus-common-1.0.8-1
==== Recommended installs ====
==== End recommended packages ====
```



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

```
Package summary test:
Pass: Numerous package updates are moot, since these services are
not running, but openssl-devel (2001-07-13), man (2001-09-06), xinetd
(2001-09-07), util-linux (2001-10-06), kernel (2001-10-19), sendmail-cf
(2001-10-22), ucd-snmp-devel (2001-10-31), kernel (2001-11-02), and
openssh-askpass (2001-11-30) all have potential security impacts, and
should all be installed. Remedy - download and install these immediately.


Bootable disk -- Pass: Bootable disk exists, floppy 1.44M


Incident handling disk -- Not pass: No incident handling disk exists


/etc/passwd is as follows:
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
gdm:x:42:42::/home/gdm:/bin/bash
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
nobody:x:99:99:Nobody::
deaves:x:500:100:David Eaves:/home/deaves:/bin/bash

Not pass: User Nobody is unneeded, as no web server is present,
and it has home directory of root "/". Remove this user.


Passwords are not MD5 hashed, another hashing mechanism is in use.
Pass: It works, and appears to be the standard Unix secure mechanism for one-way
encryption.


/etc/shadow not shown here. Every user has a password entry in that file,
and every user corresponds to a user defined in /etc/passwd, and vice
versa.

Pass: all users have passwords


Every user has a shadowed password, and no other problems:
> pwck
user adm: directory /var/adm does not exist
user gdm: directory /home/gdm does not exist
user nobody: directory  does not exist
pwck: no changes

Not pass: home directories for users adm and gdm, (adm is unnecessary
and should be removed) (gdm provides assistance for the Linux Xwindows
desktop environment, GNOME) are described, but do not exist. They are
not necessary in either case for proper functioning of those services.


Password aging and nontrivial password as policy compliance.
> chage deaves

Changing the aging information for deaves
Enter the new value, or press return for the default

        Minimum Password Age [0]:
        Maximum Password Age [99999]:
        Last Password Change (YYYY-MM-DD) [2001-10-22]:
        Password Expiration Warning [7]:
        Password Inactive [-1]:
        Account Expiration Date (YYYY-MM-DD) [1969-12-31]:

Not pass: The policy may be observed, but it is neither tracked nor
enforced. All passwords are nontrivial, partial pass.
```

© SANS Institute 2000 - 2002, Author retains full rights.

No antivirus software installed -- Not pass. Purchase McAfee for Linux or PC-cillin

No shared or mounted filesystems:

```
> cat /etc/exp*
> exportfs
> df -k
Filesystem           1k-blocks      Used Available Use% Mounted on
/dev/hda1               248895     62917    173128  27% /
/dev/hda9              8901756    503904   7945624   6% /home
/dev/hda8              1011928       240    960284   1% /tmp
/dev/hda5              5044156    919440   3868484  20% /usr
/dev/hda6              2016016     17064   1896540   1% /var
>
```

Pass:

No setuid or setgid files that are not necessary:

```
find / \( -perm -4000 -perm -2000 \) -print
/usr/sbin/userhelper
find: /proc/3751/fd/4: No such file or directory
/etc/rc.d/init.d/boot
```

Not pass: Why is /etc/init.d/boot setuid? It need not be. /usr/sbin/userhelper should remain setuid -- Level of risk to be investigated. Remove setuid and move boot script functions to start pump and eth0 interface to earlier before Xwindows is started as a non-privileged user.

Linux loader (LILO) is password protected, and lilo.conf is invisible to nonprivileged users

Not pass: No password is set, and /etc/lilo.conf is world readable. Set this password to a new password, and make it 600

CTRL-ALT-DEL reboot from console is disabled

```
> cat /etc/inittab | grep shutdown
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
# of power left.  Schedule a shutdown for 2 minutes from now.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"
```

Not pass: it appears to be defined for normal shutdown see man inittab. Comment out this line from inittab.

Single user mode boot requires root password

Not pass: No notation in /etc/inittab to restrict runlevel 1 to only root user, However inittab is root owned and default runlevel cannot be changed without changing it. Impact - low.

All console logins are disabled except for root and deaves:

Not pass: Users not disabled are bin, daemon, adm, gdm, xfs, and nobody. Pedantic, low risk.

TCP wrappers are in use:

```
> cat /etc/rc.iptables
iptables -N tcpin
iptables -N udpin
iptables -N ip-unknown
iptables -A INPUT -p all -s 127.0.0.0 -d 0.255.255.255 -j LOG --log-level info
```

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

```
iptables -A INPUT -p all -s 127.0.0.0 -d 0.255.255.255 -j DROP
iptables -A INPUT -p all -s 192.168.0.0 -d 0.0.255.255 -j LOG --log-level info
iptables -A INPUT -p all -s 192.168.0.0 -d 0.0.255.255 -j DROP
iptables -A INPUT -p all -s 172.16.0.0 -d 0.15.255.255 -j LOG --log-level info
iptables -A INPUT -p all -s 172.16.0.0 -d 0.15.255.255 -j DROP
# Stop all reverse-web-client SYN-ACK and ACK-RST scanning
iptables -A INPUT -p tcp --source-port 80 -m state --state INVALID,NEW -j LOG --log-level
info
iptables -A INPUT -p tcp --source-port 80 -m state --state INVALID,NEW -j DROP
iptables -A INPUT -p all -s 0.255.255.255/8 -j LOG --log-level info
iptables -A INPUT -p all -s 0.255.255.255/8 -j DROP
iptables -A INPUT -p icmp -s <DMZ LAN address> -d <DMZ LAN address> --icmp-type echo-
request -j ACCEPT
iptables -A INPUT -p icmp -d <DMZ LAN address> --icmp-type echo-reply -j ACCEPT
iptables -A INPUT -p icmp -d <DMZ LAN address> --icmp-type destination-unreachable -j
ACCEPT
iptables -A INPUT -p icmp -d <DMZ LAN address> --icmp-type time-exceeded -j ACCEPT
iptables -A INPUT -p icmp -d localhost --icmp-type echo-reply -j ACCEPT
iptables -A INPUT -p icmp -d localhost --icmp-type destination-unreachable -j ACCEPT
iptables -A INPUT -p icmp -d localhost --icmp-type time-exceeded -j ACCEPT
iptables -A INPUT -p icmp -j LOG --log-level info
iptables -A INPUT -p icmp -j DROP
iptables -A INPUT -p tcp -j tcpin
iptables -A INPUT -p udp -j udpin
iptables -A INPUT -j ip-unknown
iptables -P FORWARD DROP
# To prevent spoofing our addresses to incriminate us...
iptables -A OUTPUT -p tcp --destination-port 80 -s <DMZ LAN address> --tcp-flags
SYN,ACK,PSH,FIN,RST SYN -j ACCEPT
iptables -A OUTPUT -p tcp --destination-port 80 -s <DMZ LAN address> -m state --state
ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp --destination-port 80 -s <DMZ LAN address> --tcp-flags
SYN,ACK,PSH,FIN,RST FIN,ACK,PSH -j ACCEPT
iptables -A OUTPUT -p tcp --destination-port 80 -j LOG --log-level info
iptables -A OUTPUT -p tcp --destination-port 80 -j DROP
# inbound TCP rules
# all local-to-local only nessus traffic
iptables -A tcpin -p tcp -s localhost --source-port 1241 -d localhost -j ACCEPT
iptables -A tcpin -p tcp -s localhost --destination-port 1241 -d localhost -j ACCEPT
# all local-to-local only Xwindows traffic
# DANGER!! -- if this chain gets flushed, these go first, freezing Xwindows.
# You MUST append these rules to the end of the chain before flushing it.
iptables -A tcpin -p tcp -s localhost --source-port 6000 -d localhost -j ACCEPT
iptables -A tcpin -p tcp -s localhost --destination-port 6000 -d localhost -j ACCEPT
# all local-to-local only HTTP traffic
iptables -A tcpin -p tcp -s localhost --source-port 80 -d localhost -j ACCEPT
iptables -A tcpin -p tcp -s localhost --destination-port 80 -d localhost -j ACCEPT
# inbound HTTP responses from anywhere, but only for established locally
#iptables -A tcpin -p tcp --source-port 80 -d <DMZ LAN address> --tcp-flags
SYN,ACK,PSH,FIN,RST SYN,ACK -j ACCEPT
iptables -A tcpin -p tcp --source-port 80 -d <DMZ LAN address> -m state --state
ESTABLISHED -j ACCEPT
# inbound FTP responses from anywhere, but only for established locally
#iptables -A tcpin -p tcp --source-port 20 -d <DMZ LAN address> --tcp-flags
SYN,ACK,PSH,FIN,RST SYN,ACK -j ACCEPT
iptables -A tcpin -p tcp --source-port 20 -d <DMZ LAN address> -m state --state
ESTABLISHED -j ACCEPT
#iptables -A tcpin -p tcp --source-port 21 -d <DMZ LAN address> --tcp-flags
SYN,ACK,FIN,RST SYN,ACK -j ACCEPT
iptables -A tcpin -p tcp --source-port 21 -d <DMZ LAN address> -m state --state
ESTABLISHED -j ACCEPT
# inbound SMTP responses only from <remote system #2>, and only established locally
#iptables -A tcpin -p tcp -s 192.86.83.250 --source-port 25 -d <DMZ LAN address> --tcp-
flags SYN,ACK,PSH,FIN,RST SYN,ACK -j ACCEPT
iptables -A tcpin -p tcp -s 192.86.83.250 --source-port 25 -d <DMZ LAN address> -m state
--state ESTABLISHED -j ACCEPT
# inbound IMAP responses only from <remote system #2>, and only established locally
#iptables -A tcpin -p tcp -s 192.86.83.250 --source-port 143 -d <DMZ LAN address> --tcp-
flags SYN,ACK,PSH,FIN,RST SYN,ACK -j ACCEPT
iptables -A tcpin -p tcp -s 192.86.83.250 --source-port 143 -d <DMZ LAN address> -m state
--state ESTABLISHED -j ACCEPT
```

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

```
# inbound SSH responses only from <remote system #1>, and only established locally
#iptables -A tcpin -p tcp -s 192.86.83.nnn --source-port 22 -d <DMZ LAN address> --tcp-
flags SYN,ACK,PSH,FIN,RST SYN,ACK -j ACCEPT
iptables -A tcpin -p tcp -s 192.86.83.nnn --source-port 22 -d <DMZ LAN address> -m state
--state ESTABLISHED -j ACCEPT
# inbound whois responses only from whois.arin.net, and only established locally
#iptables -A tcpin -p tcp -s 192.149.252.21 --source-port 43 -d <DMZ LAN address> --tcp-
flags SYN,ACK,PSH,FIN,RST SYN,ACK -j ACCEPT
iptables -A tcpin -p tcp -s 192.149.252.0/26 --source-port 43 -d <DMZ LAN address> -m
state --state ESTABLISHED -j ACCEPT
# don't bother to log incoming http requests, it's all just code red and nimda vectors
iptables -A tcpin -p tcp -d <DMZ LAN address> --destination-port 80 -j DROP
# don't bother to log incoming security scans from AT&T Broadband authorized security
iptables -A tcpin -p tcp -s 24.0.0.203 --destination-port 119 -j DROP
iptables -A tcpin -p tcp -j LOG --log-level info
iptables -A tcpin -p tcp -j DROP
# Lesson learned!! -- when flushed, this chain freezes XWindows -- append these first
#iptables -A tcpin -p tcp ! -s localhost ! --source-port 6000 ! -d localhost -j DROP
#iptables -A tcpin -p tcp ! -s localhost ! --destination-port 6000 ! -d localhost -j DROP
# inbound UDP rules
# all DNS response traffic from the two designated name servers
#iptables -A udpin -p udp -s 24.5.207.179 --source-port 53 -d <DMZ LAN address> -j ACCEPT
iptables -A udpin -p udp -s 192.86.83.250 --source-port 53 -d <DMZ LAN address> -j ACCEPT
iptables -A udpin -p udp -s 216.148.227.68 --source-port 53 -d <DMZ LAN address> -j
ACCEPT
# drop without logging all other local SNMP
iptables -A udpin -p udp -s 192.168.1.0/24 --destination-port 161 -j DROP
iptables -A udpin -p udp -s 192.168.1.0/24 --destination-port 162 -j DROP
# don't log the usual dog-in-heat group-sex broadcasts from Windows
iptables -A udpin -p udp -s 192.168.1.0/24 -d 192.168.1.0/24 --destination-port 138 -j
DROP
# log all the remaining udp toxic waste
iptables -A udpin -p udp -j LOG --log-level info
iptables -A udpin -p udp -j DROP
# inbound IGMP and other IP-type packets
# drop network local IGMP without logging it
iptables -A ip-unknown -p igmp -s 192.168.100.1 -j DROP
# log all the strangest packets that fail other rules, before dropping them
iptables -A ip-unknown -j LOG --log-level info
iptables -A ip-unknown -j DROP
```

Pass: The DMZ LAN address has been edited out for public exposure.
Some FTP ACCEPT rules could be consolidated, and some of the SNMP DROP
rules -- low priority. Impact is router efficiency.
IPtables is installed and running effectively as a firewall

Remote telnet users are disallowed:

Pass: /etc/securetty has not been cut down to a minimum, but no
telnet services are running

Only permitted ports are unfiltered, as seen from the inside, esp. rpc:

```
> nmap -I -O -P0 -sR 192.168.1.3

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Warning:  No TCP ports found open on this machine, OS detection will be MUCH less
reliable
All 1523 scanned ports on <DMZ LAN address> (192.168.1.3) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
Nmap run completed -- 1 IP address (1 host up) scanned in 1883 seconds
```

Pass:

Only permitted services running, as seen from from the inside

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

```
> netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:x11                   *:*                     LISTEN
tcp        0      0 localhost.localdoma:x11 localhost.localdom:1031 ESTABLISHED
tcp        0      0 localhost.localdoma:x11 localhost.localdom:1046 ESTABLISHED
tcp        0      0 localhost.localdoma:x11 localhost.localdom:1045 ESTABLISHED
tcp        0      0 localhost.localdoma:x11 localhost.localdom:1028 ESTABLISHED
tcp        0     32 localhost.localdoma:x11 localhost.localdom:1044 ESTABLISHED
tcp        0      0 localhost.localdoma:x11 localhost.localdom:1027 ESTABLISHED
tcp        0      0 localhost.localdom:1027 localhost.localdoma:x11 ESTABLISHED
tcp        0      0 localhost.localdom:1031 localhost.localdoma:x11 ESTABLISHED
tcp        0      0 localhost.localdom:1028 localhost.localdoma:x11 ESTABLISHED
tcp        0      0 localhost.localdom:1039 localhost.localdoma:x11 ESTABLISHED
tcp        0      0 localhost.localdom:1037 localhost.localdoma:x11 ESTABLISHED
tcp        0      0 localhost.localdom:1036 localhost.localdoma:x11 ESTABLISHED
tcp        0      0 localhost.localdoma:x11 localhost.localdom:1043 ESTABLISHED
tcp        0      0 localhost.localdom:1043 localhost.localdoma:x11 ESTABLISHED
tcp        0      0 localhost.localdom:1041 localhost.localdoma:x11 ESTABLISHED
tcp        0      0 localhost.localdom:1040 localhost.localdoma:x11 ESTABLISHE
tcp        0      0 localhost.localdom:1046 localhost.localdoma:x11 ESTABLISHED
tcp        0      0 localhost.localdom:1045 localhost.localdoma:x11 ESTABLISHED
tcp        0    132 localhost.localdom:1044 localhost.localdoma:x11 ESTABLISHED
tcp        0      0 localhost.localdom:1048 localhost.localdoma:x11 ESTABLISHED
tcp        0      0 localhost.localdoma:x11 localhost.localdom:1041 ESTABLISHED
tcp        0      0 localhost.localdoma:x11 localhost.localdom:1040 ESTABLISHED
tcp        0      0 localhost.localdoma:x11 localhost.localdom:1039 ESTABLISHED
tcp        0      0 localhost.localdoma:x11 localhost.localdom:1037 ESTABLISHED
tcp        0      0 localhost.localdoma:x11 localhost.localdom:1036 ESTABLISHED
tcp        0      0 localhost.localdoma:x11 localhost.localdom:1048 ESTABLISHED
```

Pass: the only service running is the X11 server, on port 6000, although it has numerous sessions open (xterm instances).

No unusual or suspicious file descriptors are seen using lsof:

```
> lsof -l +M

COMMAND   PID   USER   FD   TYPE DEVICE SIZE NODE NAME
X         659   root    1u  IPv4    970       TCP *:x11 (LISTEN)
X         659   root   11u  IPv4   1285       TCP localhost.localdomain:x11-
>localhost.localdomain:1027 (ESTABLISHED)
X         659   root   12u  IPv4   1296       TCP localhost.localdomain:x11-
>localhost.localdomain:1028 (ESTABLISHED)
X         659   root   13u  IPv4   1402       TCP localhost.localdomain:x11-
>localhost.localdomain:1036 (ESTABLISHED)
X         659   root   14u  IPv4   1408       TCP localhost.localdomain:x11-
>localhost.localdomain:1037 (ESTABLISHED)
X         659   root   15u  IPv4   1322       TCP localhost.localdomain:x11-
>localhost.localdomain:1031 (ESTABLISHED)
X         659   root   16u  IPv4   1423       TCP localhost.localdomain:x11-
>localhost.localdomain:1039 (ESTABLISHED)
X         659   root   17u  IPv4   1514       TCP localhost.localdomain:x11-
>localhost.localdomain:1040 (ESTABLISHED)
X         659   root   18u  IPv4   1528       TCP localhost.localdomain:x11-
>localhost.localdomain:1041 (ESTABLISHED)
X         659   root   20u  IPv4   1556       TCP localhost.localdomain:x11-
>localhost.localdomain:1043 (ESTABLISHED)
X         659   root   21u  IPv4   1561       TCP localhost.localdomain:x11-
>localhost.localdomain:1044 (ESTABLISHED)
X         659   root   22u  IPv4   1564       TCP localhost.localdomain:x11-
>localhost.localdomain:1045 (ESTABLISHED)
X         659   root   23u  IPv4   1568       TCP localhost.localdomain:x11-
>localhost.localdomain:1046 (ESTABLISHED)
X         659   root   24u  IPv4   1864       TCP localhost.localdomain:x11-
>localhost.localdomain:1048 (ESTABLISHED)
```

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

```
gnome-ses 687 deaves    4u  IPv4   1283       TCP localhost.localdomain:1027-
>localhost.localdomain:x11 (ESTABLISHED)
gnome-smp 759 deaves    3u  IPv4   1294       TCP localhost.localdomain:1028-
>localhost.localdomain:x11 (ESTABLISHED)
magicdev  761 deaves    3u  IPv4   1320       TCP localhost.localdomain:1031-
>localhost.localdomain:x11 (ESTABLISHED)
sawfish   774 deaves    3u  IPv4   1406       TCP localhost.localdomain:1037-
>localhost.localdomain:x11 (ESTABLISHED)
xscreensa 779 deaves    3u  IPv4   1400       TCP localhost.localdomain:1036-
>localhost.localdomain:x11 (ESTABLISHED)
gnome-nam 787 deaves    3u  IPv4   1421       TCP localhost.localdomain:1039-
>localhost.localdomain:x11 (ESTABLISHED)
gmc       795 deaves    3u  IPv4   1526       TCP localhost.localdomain:1041-
>localhost.localdomain:x11 (ESTABLISHED)
panel     797 deaves    3u  IPv4   1512       TCP localhost.localdomain:1040-
>localhost.localdomain:x11 (ESTABLISHED)
gnome-ter 801 deaves    3u  IPv4   1554       TCP localhost.localdomain:1043-
>localhost.localdomain:x11 (ESTABLISHED)
gnome-ter 803 deaves    3u  IPv4   1559       TCP localhost.localdomain:1044-
>localhost.localdomain:x11 (ESTABLISHED)
gnome-ter 805 deaves    3u  IPv4   1562       TCP localhost.localdomain:1045-
>localhost.localdomain:x11 (ESTABLISHED)
gnome-ter 807 deaves    3u  IPv4   1566       TCP localhost.localdomain:1046-
>localhost.localdomain:x11 (ESTABLISHED)
tasklist_ 855 deaves    3u  IPv4   1862       TCP localhost.localdomain:1048-
>localhost.localdomain:x11 (ESTABLISHED)
```

Pass: The only known inet file descriptors are for the X11 service, to support the windowing activity of the Xwindows/GNOME applications.

No .rhosts or hosts.equiv anywhere on the system:

Pass: No return from either find / -name .rhosts -ls or find / -name hosts.equiv -ls

```
> which tripwire
/usr/sbin/tripwire
> tripwire -m c
### Error: File could not be opened.
### Filename: /var/lib/tripwire/hostname.domainname.twd
### No such file or directory
### Exiting...
```

Pass: If tripwire had not been initialized it would have showed something like the following:

```
### Error: File could not be opened.
### Filename: /etc/tripwire/tw.cfg
### No such file or directory
### Configuration file could not be read.
### Exiting...
```

or

Use --help to get help.

Sendmail has a secure sendmail.cf:

O PrivacyOptions=authwarnings,novrfy,noexpn,restrictqrun

and

no DAEMON except "DnMAILER-DAEMON", "DAEMON=no" inserted

Pass:

© SANS Institute 2000 - 2002, Author retains full rights.

Physical Premises:
Not pass: Only the screensaver times out: the console is not secured.

Not pass: There is no safe, the passwords are not physically secured.

Pass: The premises are locked at all times when personnel are absent.

Pass: The router is physically disconnected during prolonged absences.

Configure Xwindows to time out with inactivity of 15 minutes. Purchase a safe, put the passwords and other documents inside it.

UPS and backups are functioning

Not pass: No UPS, backups are monthly

Appropriate privileged users root, bin, daemon, gdm, and xfs are present and have passwords:

Pass: see /etc/passwd, listed above

Groups are limited to only necessary ones, and all have passwords:

```
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
tty:x:5:
disk:x:6:root
mem:x:8:
kmem:x:9:
wheel:x:10:root
nobody:x:99:
users:x:100:
utmp:x:22:
gdm:x:42:
xfs:x:43:
```

Pass: adm might be eliminated, or could be required for some system services on startup. Others can be tested for by rebooting, eliminating groups, and seeing if any required system services are impaired or prevented from startup. Other groups than this can all be safely removed without impairing normal workstation functioning.
From experience, bin and daemon are used for system daemons and services, sys, mem, and kmem are used by system internals and devices, disk, wheel, and tty are used for peripherals and devices, utmp for logging, gdm and xfs for Xwindows/GNOME, and adm for -- not sure...
/etc/gshadow indicates all groups have nontrivial passwords

IPtables is running and configured appropriately:

```
> iptables -L --line-number -n <annotated by author>
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
# Note: source routing and malformed packets logged and dropped
1    LOG        all  --  127.0.0.0            0.255.255.255      LOG flags 0 level 6
2    DROP       all  --  127.0.0.0            0.255.255.255
3    LOG        all  --  192.168.0.0          0.0.255.255        LOG flags 0 level 6
4    DROP       all  --  192.168.0.0          0.0.255.255
5    LOG        all  --  172.16.0.0           0.15.255.255       LOG flags 0 level 6
6    DROP       all  --  172.16.0.0           0.15.255.255
7    LOG        tcp  --  0.0.0.0/0            0.0.0.0/0          tcp spt:80 state
INVALID,NEW LOG flags 0 level 6
8    DROP       tcp  --  0.0.0.0/0            0.0.0.0/0          tcp spt:80 state
INVALID,NEW
9    LOG        all  --  0.0.0.0/8            0.0.0.0/0          LOG flags 0 level 6
10   DROP       all  --  0.0.0.0/8            0.0.0.0/0
```

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

```
# Note ICMP returning from pings and traceroutes accepted, all other is dropped
11   ACCEPT     icmp --  192.168.1.3          192.168.1.3        icmp type 8
12   ACCEPT     icmp --  0.0.0.0/0            192.168.1.3        icmp type 0
13   ACCEPT     icmp --  0.0.0.0/0            192.168.1.3        icmp type 3
14   ACCEPT     icmp --  0.0.0.0/0            192.168.1.3        icmp type 11
15   ACCEPT     icmp --  0.0.0.0/0            127.0.0.1          icmp type 0
16   ACCEPT     icmp --  0.0.0.0/0            127.0.0.1          icmp type 3
17   ACCEPT     icmp --  0.0.0.0/0            127.0.0.1          icmp type 11
18   LOG        icmp --  0.0.0.0/0            0.0.0.0/0          LOG flags 0 level 6
19   DROP       icmp --  0.0.0.0/0            0.0.0.0/0
# Note and the tcp, udp, and other gets split up to different rulesets
20   tcpin      tcp  --  0.0.0.0/0            0.0.0.0/0
21   udpin      udp  --  0.0.0.0/0            0.0.0.0/0
22   ip-unknown  all  --  0.0.0.0/0            0.0.0.0/0

# Note -- all forwarding is turned off
Chain FORWARD (policy DROP)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
# Note -- all invalid or other nonestablished http outbound is stopped in case
# the next HTTP worm gets by us. Done by passing all valid, logging/dropping
# the rest.
1    ACCEPT     tcp  --  192.168.1.3          0.0.0.0/0          tcp dpt:80
flags:0x021F/0x022
2    ACCEPT     tcp  --  192.168.1.3          0.0.0.0/0          tcp dpt:80 state
ESTABLISHED
3    ACCEPT     tcp  --  192.168.1.3          0.0.0.0/0          tcp dpt:80
flags:0x021F/0x0219
4    LOG        tcp  --  0.0.0.0/0            0.0.0.0/0          tcp dpt:80 LOG flags 0
level 6
5    DROP       tcp  --  0.0.0.0/0            0.0.0.0/0          tcp dpt:80

Chain ip-unknown (1 references)
num  target     prot opt source               destination
# Note don't clutter the logs with the Windows multicast noise
1    DROP       2    --  192.168.100.1        0.0.0.0/0
2    LOG        all  --  0.0.0.0/0            0.0.0.0/0          LOG flags 0 level 6
3    DROP       all  --  0.0.0.0/0            0.0.0.0/0

Chain tcpin (1 references)
num  target     prot opt source               destination
# Note -- let through sepcifically allowed IP, log and drop the rest
# All localhost Nessus, HTTP, Xwindows traffic
1    ACCEPT     tcp  --  127.0.0.1            127.0.0.1          tcp spt:1241
2    ACCEPT     tcp  --  127.0.0.1            127.0.0.1          tcp dpt:1241
3    ACCEPT     tcp  --  127.0.0.1            127.0.0.1          tcp spt:6000
4    ACCEPT     tcp  --  127.0.0.1            127.0.0.1          tcp dpt:6000
5    ACCEPT     tcp  --  127.0.0.1            127.0.0.1          tcp spt:80
6    ACCEPT     tcp  --  127.0.0.1            127.0.0.1          tcp dpt:80
# All returning HTTP, FTP, SMTP, IMAP, SSH, and NICNAME service allowed
7    ACCEPT     tcp  --  0.0.0.0/0            192.168.1.3        tcp spt:80 state
ESTABLISHED
8    ACCEPT     tcp  --  0.0.0.0/0            192.168.1.3        tcp spt:20 state
ESTABLISHED
9    ACCEPT     tcp  --  0.0.0.0/0            192.168.1.3        tcp spt:21 state
ESTABLISHED
10   ACCEPT     tcp  --  192.86.83.nnn        192.168.1.3        tcp spt:25 state
ESTABLISHED
11   ACCEPT     tcp  --  192.86.83.nnn        192.168.1.3        tcp spt:143 state
ESTABLISHED
12   ACCEPT     tcp  --  192.86.83.mmm        192.168.1.3        tcp spt:22 state
ESTABLISHED
13   ACCEPT     tcp  --  192.149.252.0/26     192.168.1.3        tcp spt:43 state
ESTABLISHED
# Don't clutter the logs with HTTP worm noise
14   DROP       tcp  --  0.0.0.0/0            192..168.1.3        tcp dpt:80
# Don't clutter the logs with network "security" surveillance
15   DROP       tcp  --  24.0.0.203           0.0.0.0/0          tcp dpt:119
16   LOG        tcp  --  0.0.0.0/0            0.0.0.0/0          LOG flags 0 level 6
```

© SANS Institute 2000 - 2002, Author retains full rights.

```
17   DROP       tcp  --  0.0.0.0/0            0.0.0.0/0

Chain udpin (1 references)
num  target     prot opt source               destination
# Note -- allow specific returning traffic, and log/drop all the rest
# DNS service returning from designated name servers
1    ACCEPT     udp  --  192.86.83.nnn        192.168.1.3        udp spt:53
2    ACCEPT     udp  --  216.148.227.68       192.168.1.3        udp spt:53
# Don't clutter the logs with SNMP, or NETBIOS/Browser broadcasts
3    DROP       udp  --  192.168.1.0/24       0.0.0.0/0          udp dpt:161
4    DROP       udp  --  192.168.1.0/24       0.0.0.0/0          udp dpt:162
5    DROP       udp  --  192.168.1.0/24       192.168.1.255      udp dpt:138
6    LOG        udp  --  0.0.0.0/0            0.0.0.0/0          LOG flags 0 level 6
7    DROP       udp  --  0.0.0.0/0            0.0.0.0/0
```

Pass: IPTables is running correctly, as rc.iptables configured it. The -n numeric-only option was used here to obscure host names.

The logging appears to be functioning correctly:

```
> ls -al /var/log/*[A-z]
-rw-------    1 root     root        43241 Dec  4 16:22 /var/log/boot.log
-rw-------    1 root     root        35488 Dec  4 19:40 /var/log/cron
-rw-r--r--    1 root     root         5113 Dec  4 16:21 /var/log/dmesg
-rw-r--r--    1 root     root       146292 Dec  4 16:22 /var/log/lastlog
-rw-------    1 root     root         1063 Dec  4 04:04 /var/log/maillog
-rw-r--r--    1 root     root      3972695 Dec  4 19:36 /var/log/messages
-rw-------    1 root     root          497 Dec  4 16:19 /var/log/secure
-rw-------    1 root     root            0 Dec  2 04:02 /var/log/spooler
-rw-r--r--    1 root     root            0 Mar  2  2001 /var/log/statistics
-rw-rw-r--    1 root     utmp       152448 Dec  4 16:22 /var/log/wtmp
-rw-r--r--    1 deaves   users       24441 Dec  4 18:48 /var/log/XFree86.0.log
```

and

```
> tail /var/log/messages
Dec  4 18:56:22 localhost kernel: IN=eth0 OUT=
MAC=00:50:ba:5a:7b:0f:00:04:5a:2a:94:e3:08:00 SRC=12.236.160.28 DST=192.168.1.3 LEN=48
TOS=0x00 PREC=0x00 TTL=123 ID=36415 DF PROTO=TCP SPT=3068 DPT=27374 WINDOW=8192 RES=0x00
SYN URGP=0
Dec  4 18:59:00 localhost kernel: IN=eth0 OUT=
MAC=ff:ff:ff:ff:ff:ff:00:e0:29:56:88:cd:08:00 SRC=192.168.1.2 DST=192.168.1.7 LEN=238
TOS=0x00 PREC=0x00 TTL=128 ID=26660 PROTO=UDP SPT=138 DPT=138 LEN=218
Dec  4 19:06:30 localhost kernel: IN=eth0 OUT= sys2
MAC=ff:ff:ff:ff:ff:ff:00:e0:29:56:88:cd:08:00 SRC=192.168.1.2 DST=192.168.1.7 LEN=261
TOS=0x00 PREC=0x00 TTL=128 ID=26916 PROTO=UDP SPT=138 DPT=138 LEN=241
Dec  4 19:06:33 localhost kernel: IN=lo OUT=
MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00 SRC=127.0.0.1 DST=127.0.0.1 LEN=84 TOS=0x00
PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=875 DPT=111 LEN=64
Dec  4 19:07:08 localhost last message repeated 7 times
Dec  4 19:07:28 localhost last message repeated 4 times
Dec  4 19:14:00 localhost kernel: IN=eth0 OUT=
MAC=ff:ff:ff:ff:ff:ff:00:e0:29:56:88:cd:08:00 SRC=192.168.1.2 DST=192.168.1.7 LEN=238
TOS=0x00 PREC=0x00 TTL=128 ID=27172 PROTO=UDP SPT=138 DPT=138 LEN=218
Dec  4 19:21:30 localhost kernel: IN=eth0 OUT=
MAC=ff:ff:ff:ff:ff:ff:00:e0:29:56:88:cd:08:00 SRC=192.168.1.2 DST=192.168.1.7 LEN=261
TOS=0x00 PREC=0x00 TTL=128 ID=27428 PROTO=UDP SPT=138 DPT=138 LEN=241
Dec  4 19:29:00 localhost kernel: IN=eth0 OUT=
MAC=ff:ff:ff:ff:ff:ff:00:e0:29:56:88:cd:08:00 SRC=192.168.1.2 DST=192.168.1.7 LEN=238
TOS=0x00 PREC=0x00 TTL=128 ID=27684 PROTO=UDP SPT=138 DPT=138 LEN=218
Dec  4 19:36:30 localhost kernel: IN=eth0 OUT=
MAC=ff:ff:ff:ff:ff:ff:00:e0:29:56:88:cd:08:00 SRC=192.168.1.2 DST=192.168.1.7 LEN=261
TOS=0x00 PREC=0x00 TTL=128 ID=27940 PROTO=UDP SPT=138 DPT=138 LEN=241
```

Pass: The logs reflect recent reboot events, and appear to show correct logging from iptables logging requirements. Iptables could have been directed to do userspace logging, or some alternative, and the eth0 interface appears to have an incorrect broadcast address, 192.168.1.7 for reasons unknown to the author at this time, probably related to the subnet mask of 248=(255-7). Impact from this is low.

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

Unusual events and known exploits logged/noted:

Pass: Personnel take enjoyment from mapping out sources of trouble, common (script-kiddie) intrusion attempts, surreptitious network surveillance such as upstairs-router compromise, sniffing, ARP or SNMP spoofing, and the like.
Filtering all requests from subnets 202-203, 210-211 (APNIC), and 68, and a few others can cut the number of serious intrusion attempts to a fractional amount, and in addition, drops requests from foreign sovereign regions that have few property or other legal conventions with the United States.

/etc/passwd, /etc/group, and /etc/shadow are root, 644, 600

```
> ls -al passwd group shadow
-rw-r--r--    1 root     root          225 Oct 23 19:16 group
-rw-r--r--    1 root     root          262 Dec  4 15:18 passwd
-rw-------    1 root     root          475 Dec  4 15:20 shadow
```

Pass: rw- is a 6, r-- is a 4, and --- is a 0.

No users or groups are uid or gid of zero

Pass: See /etc/passwd and /etc/group shown earlier

No "." in any PATH environmental variable:

/usr/kerberos/bin:/usr/java/jdk1.3.1_01/bin:/usr/bin:/bin:/usr/X11R6/bin:/usr/local/bin:/opt/bin:/home/deaves/bin:/home/deaves/jakarta-ant-1.4/bin

/usr/kerberos/bin:/bin:/usr/bin:/usr/local/bin:/usr/bin/X11:/usr/X11R6/bin

and

/usr/local/sbin:/usr/sbin:/sbin:/usr/kerberos/sbin:/usr/kerberos/bin:/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin:/usr/bin/X11:/usr/X11R6/bin:/root/bin

Pass: for the only users that support a login shell, from /etc/passwd, the PATH variables are listed above, deaves, gdm, and root. None of them has a "." entry.

No inappropriate files in /root:

```
> ls -al /root
total 7123
drwxr-x---    9 root     root         1024 Dec  4 20:08 .
drwxr-xr-x   18 root     root         1024 Dec  4 16:21 ..
-rw-------    1 root     root        20568 Dec  4 16:19 .bash_history
-rw-r--r--    1 root     root           24 Jun 10  2000 .bash_logout
-rw-r--r--    1 root     root          266 Jun 10  2000 .bash_profile
-rw-r--r--    1 root     root          176 Aug 23  1995 .bashrc
-rw-r--r--    1 root     root          210 Jun 10  2000 .cshrc
drwxr-xr-x    2 root     root         1024 Oct 24 19:06 .ethereal
drwx------    5 root     root         1024 Oct 23 17:21 .gnome
drwxr-xr-x    3 root     root         1024 Oct 23 17:10 .gnome-desktop
drwx------    2 root     root         1024 Oct 22 20:19 .gnome_private
-rw-------    1 root     root            0 Oct 23 17:21 .ICEauthority
-rw-------    1 root     root      7196900 Dec  3 11:25 mbox
drwxr-xr-x    2 root     root         1024 Oct 23 17:21 .mc
-rw-------    1 root     root          769 Oct 25 14:37 .nessus.keys
-rw-------    1 root     root        21962 Dec  3 19:18 .nessusrc
drwxr-xr-x    3 root     root         1024 Oct 23 17:10 .sawfish
-rw-r--r--    1 root     root          196 Jul 11  2000 .tcshrc
-rw-r--r--    1 root     root           32 Oct 22 19:08 .TWM-errors
-rw-r--r--    1 root     root            4 Oct 22 19:08 .wm_style
drwx------    2 root     500          1024 Oct 22 17:40 .xauth
-rw-------    1 root     users          66 Oct 23 17:47 .Xauthority
```

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

```
-rw-r--r--    1 root     root         1126 Aug 23  1995 .Xresources
```

Not pass: There are only bash, csh, ethereal, nessus, gnome, sawfish/ICE, and X related files needed here. It is not clear to the author at this time what exactly is .TWM-errors or .wm_style, best guess is that it is a prior window manager used on RedHat reinstallation on or about October 22. Impact: low
Remove these files.

User home directories and . files are all 755 or more restrictive:

```
> ls -al /home
total 37
drwxr-xr-x    7 root     root         4096 Oct 22 10:35 .
drwxr-xr-x   18 root     root         1024 Dec  4 16:21 ..
drwxr-xr-x   52 deaves   users        4096 Dec  4 19:37 deaves
drwxr-xr-x    2 deaves   users       16384 Jul 12 13:48 lost+found
drwxr-xr-x    6 deaves   users        4096 Jul 30 15:00 redhat7.1
drwxr-xr-x   24 deaves   users        4096 Aug  7 20:07 tempuser
```

Not pass: Remedial chmod -R go-w /home/deaves/* /home/tempuser/* and also chmod -R go-w /home/deaves/.* /home/tempuser/.* assures pass.

Summary of Remedies, in order of subjective estimate of cost/time, and triaged:
Done in the course of, or immediately after the audit:

1) Remove users nobody, adm, remove /home/gdm from /etc/passwd
2) Remove .TWM-errors and .wm_style from /root
3) Make user directories and all content 755 or better (go-w)
4) Disable CTRL-ALT-DEL reboot in inittab
5) Restrict users bin, daemon, gdm, and xfs in /etc/securetty
6) Purchase Linux Anti-virus software and install
7) Enforce password policy with respect to aging
8) Install RedHat packages listed above

Remedial actions to be taken:

9) Purchase a safe, put the passwords and other documents inside it.
10) Configure Xwindows to time out with inactivity of 15 minutes.
11) Investigate /usr/sbin/userhelper setuid requirement
12) Set LILO password and make /etc/lilo.conf root 600
13) Make an incident handling disk
14) Purchase a reliable UPS, change backup policy to weekly
15) Rearrange boot script for setuid, to start pump/eth0 before Xwindows

Lower priority:

16) Investigate how to restrict runlevel 1 to root user only

Final Audit for System #1 was conducted December 4, 2001, and no claim is made here for the condition of this system on any date after that.

Supporting matrixes for risk mitigation analysis follow:

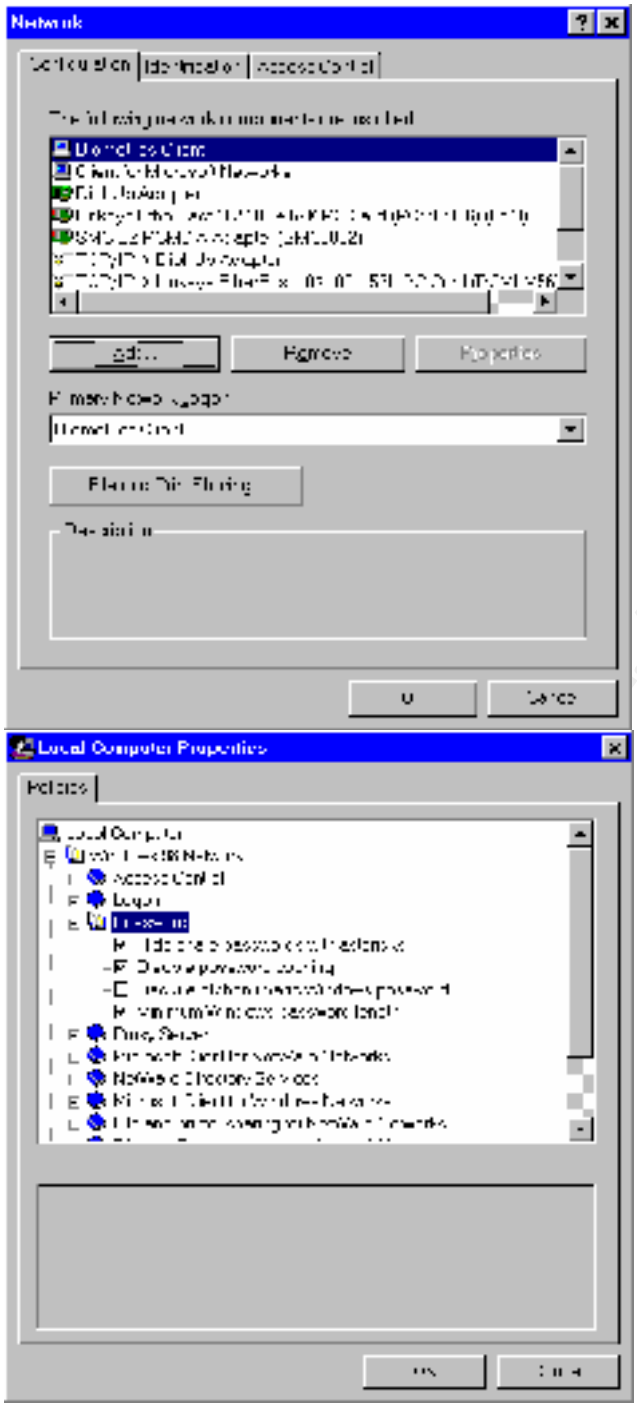
Failed checklist items represent risks of damage, times annual frequency/likelihood of a related exploit that could otherwise be prevented. These are subjective estimates provided by the management, whose assistance was invaluable in preparing this report.

	Passwords in a Safe: Premises intrusion	Xwindows times out: Premises intrusion	No setuid, setgid files: privilege escalation	LILO pw set: Premises intrusion	Incident disk: successful compromise	UPS: Power failure
System #1	0.5	0.5	0.1	0.5	0.5	0.5

Assumptions are that compromise via premises intrusion will degrade 100 percent of any exposed assets, unauthorized personnel do in fact access the premises on average once per month, with unknown technical abilities, an incident handling disk will mitigate this damage to the degree of about fifty percent of any damage done. A UPS has a fifty-fifty chance in a year of saving assets on any device attached to a faulty power source.

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

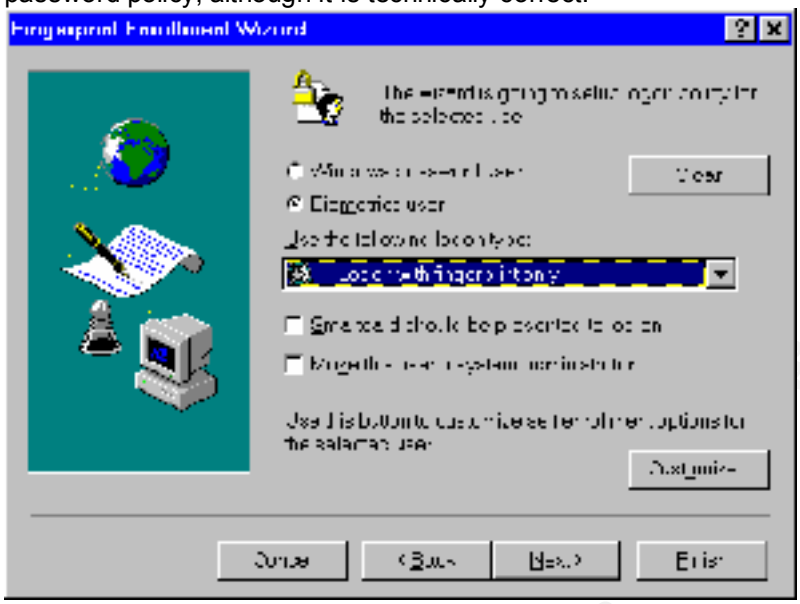
Appendix B: Benchmark and Matrixes, System #2



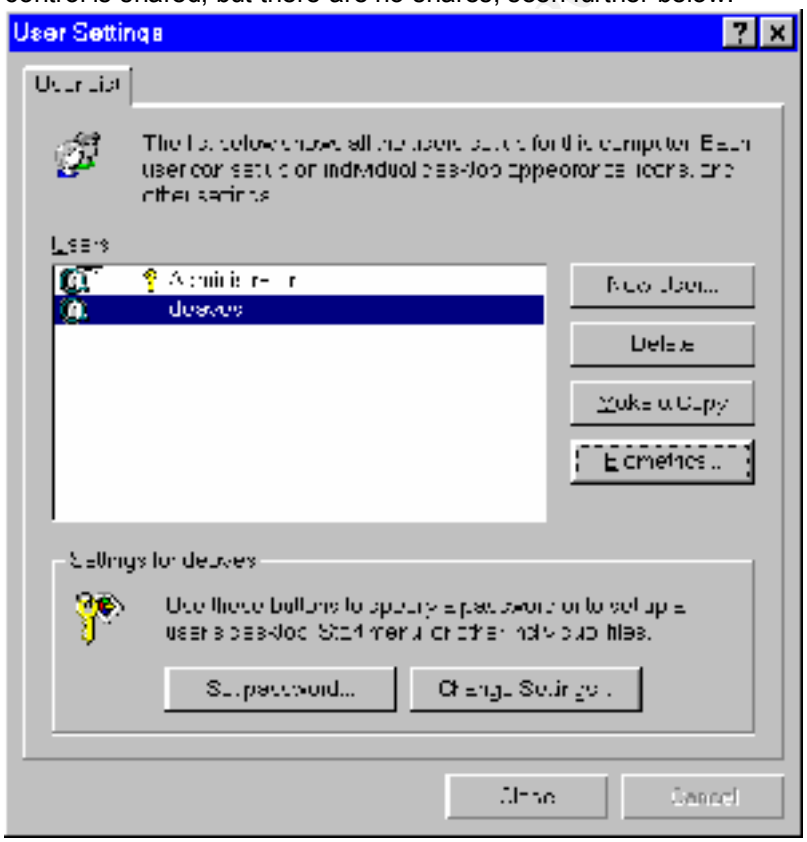
Pass: Using Settings, Network, and using poledit.exe, run from the Windows 98 install CD, from \tools\reskit\netadmin/poledit (Important – installation of this onto the machine represents a marginal security risk, however small – it is not installed here, but run from original media). The biometrics client login is specified, and using poledit.exe, select File, Open Registry, and double click Local Computer. In the properties panel, open Windows 98 Network properties, and examine the Password policy. It is correct here.

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

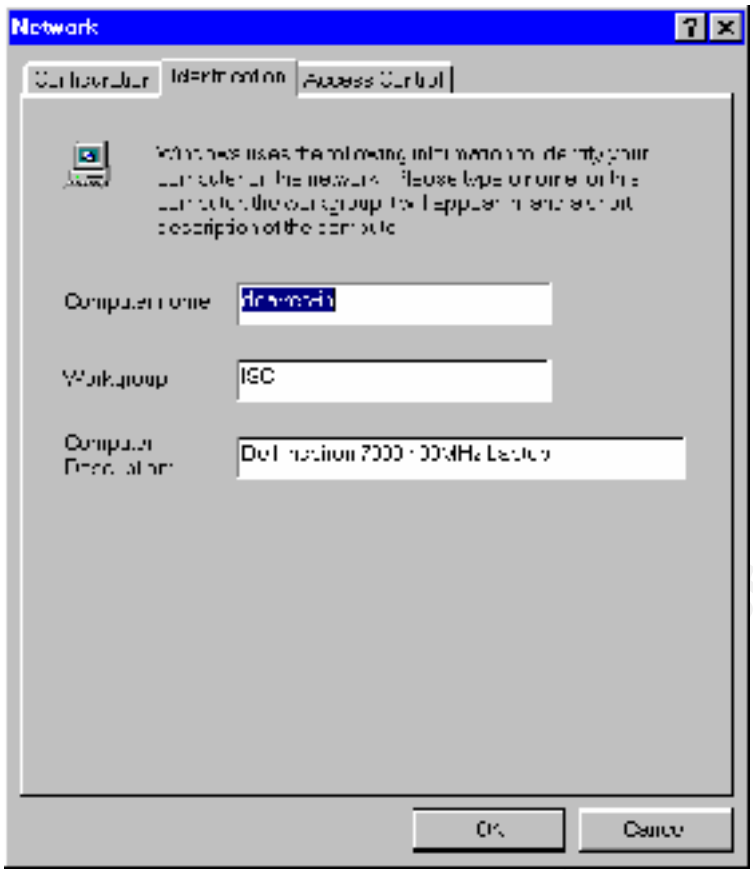
Note that the biometric logon client allows use of “fingerprint only” to log on to the system, as seen in the Control Panel, Users panel, clicking on the Biometric button inserted there as a result of the biometric client software for Windows 95/98 installed by the thumbprint reader PCMCIA card bought recently from www.identix.com and installed on this system. This actually moots the password policy, although it is technically correct.



Pass: Windows is installed multiuser and has a proper workgroup, as shown below. Access control is shared, but there are no shares, seen further below.



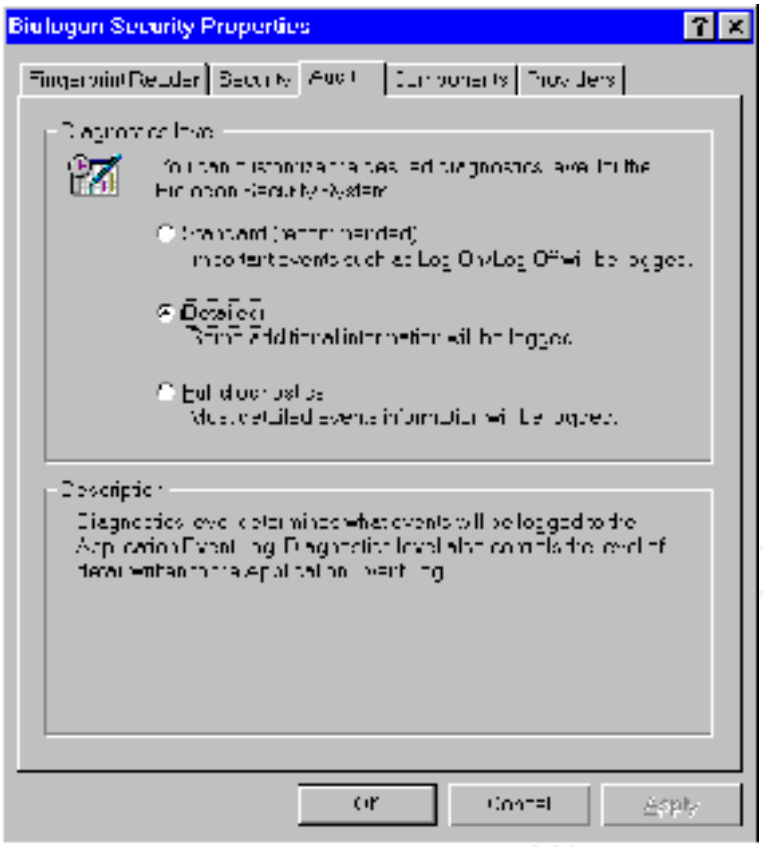
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Not pass: System events are audited: logon, and account change, but not object access, access change, boot, or policy change. The first two are only audited because of a third party product, the biometric logon client, as shown below, launched from the Control Panel. The auditing policy for system events must be investigated for Windows 95/98 in order to correct this.

Accounts are locked out after more than 20 logon attempts:
Not pass: account lockouts are not configured for more than 20 logon attempts. This may not be corrected immediately, because, 1) how to do this must be investigated for Windows 95/98, and 2) the biometric logon process is set at a high security level, sometimes requiring as many as ten or more logon attempts to successfully log on.

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



System events are logged – Not pass: viewing c:\windows\SchedLog.txt as seen in notepad below indicates that the last time a system event was logged was two days prior, when a Windows update event occurred. The EventSystem application, built into Windows 98 appears to have never been in operation since 1999, and has apparently stopped functioning correctly as of the last critical Windows 98 security update.
There is no remedial action known that can be taken at this time. Searches for the COM Services package for Windows 98 has been futile to date, it appears not to be present on the Windows 98 install media, and C:\windows/esserver.exe appears not to function because it is missing a symbolic link in the DLL estier2.dll, which bears the timestamp of a 11/27/2001 Windows security update. Many esserver.exe DLL's bear the same timestamp. The windowsupdate.microsoft.com website claims that for the IE 5.5 security patch, there is no uninstall procedure, and hence no remedial action that can be taken, pending another patch from Microsoft.

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

Schedlog.txt - Notepad

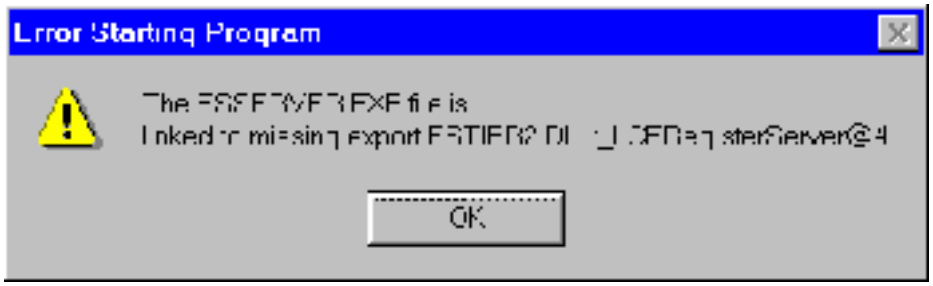
File Edit Search Help

```
"Windows Critical Update Notification.job" (WUCRTUPD.EXE)
        Started 12/3/01 8:45:00 AM
"Windows Critical Update Notification.job" (WUCRTUPD.EXE)
        Finished 12/3/01 8:45:10 AM
        Result: The task completed with an exit code of (0).
"Windows Critical Update Notification.job" (WUCRTUPD.EXE)
        Started 12/3/01 8:50:00 AM
"Windows Critical Update Notification.job" (WUCRTUPD.EXE)
        Finished 12/3/01 8:50:10 AM
        Result: The task completed with an exit code of (0).
"Windows Critical Update Notification.job" (WUCRTUPD.EXE)
        Started 12/3/01 8:55:00 AM
"Windows Critical Update Notification.job" (WUCRTUPD.EXE)
        Finished 12/3/01 8:55:10 AM
        Result: The task completed with an exit code of (0).
"Windows Critical Update Notification.job" (WUCRTUPD.EXE)
        Started 12/3/01 9:00:00 AM
"Windows Critical Update Notification.job" (WUCRTUPD.EXE)
        Finished 12/3/01 9:00:10 AM
        Result: The task completed with an exit code of (0).
"Windows Critical Update Notification.job" (WUCRTUPD.EXE)
        Started 12/3/01 9:05:00 AM
"Windows Critical Update Notification.job" (WUCRTUPD.EXE)
```

C:\WINDOWS\Stuff\EventSystem.htm - Microsoft Internet Explorer

Type	Date	Time	Category	Event	Description	Data
Warning	6/24/1999	7:20:17.000	Event System	4099	The COM+ Event System could not determine the name of the current user. A call to GetUserName returned error code 1245: "The operation being requested was not performed because the user has not logged on to the network. The specified service does not exist."	
Warning	6/24/1999	7:20:18.970	Event System	4099	The COM+ Event System could not determine the name of the current user. A call to GetUserName returned error code 1245: "The operation being requested was not performed because the user has not logged on to the network. The specified service does not exist."	
Warning	6/24/1999	7:20:19.300	Event System	4099	The COM+ Event System could not determine the name of the current user. A call to GetUserName returned error code 1245: "The operation being requested was not performed because the user has not logged on to the network. The specified service does not exist."	
Warning	6/24/1999	7:20:21.550	Event System	4099	The COM+ Event System could not determine the name of the current user. A call to GetUserName returned error code 1245: "The operation being requested was not performed because the user has not logged on to the network. The specified service does not exist."	
Error	7/17/2001	8:13:35.880	Event System	4097	The COM+ Event System detected a bad return code during its internal processing. HRESULT = 800706B5 from line 39 of d:\nt\ole\ole32\ole\utsys\eventutil.idl. Please contact Microsoft Product Support Services to report this error.	

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

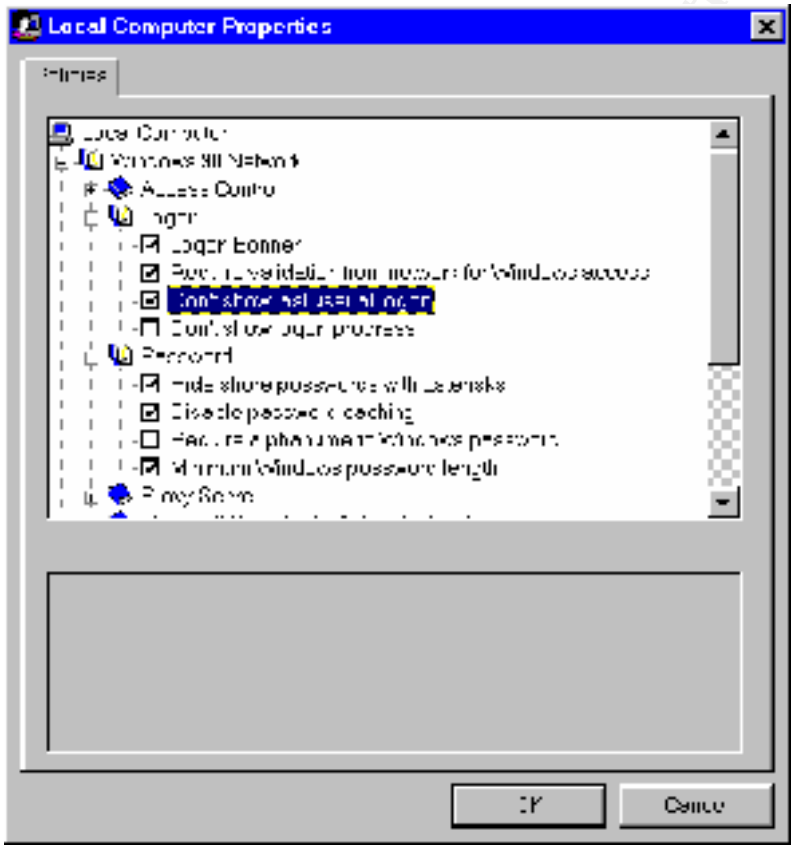


The system event logging has been broken for some time, and must be fixed somehow.

Task scheduler is only available for administrator:
Not pass: Windows 95/98 has no known way of doing this – it appears to only work for NT and Windows 2000, probably XP as well. Any user with console access can schedule any tasks, even those with administrator access.

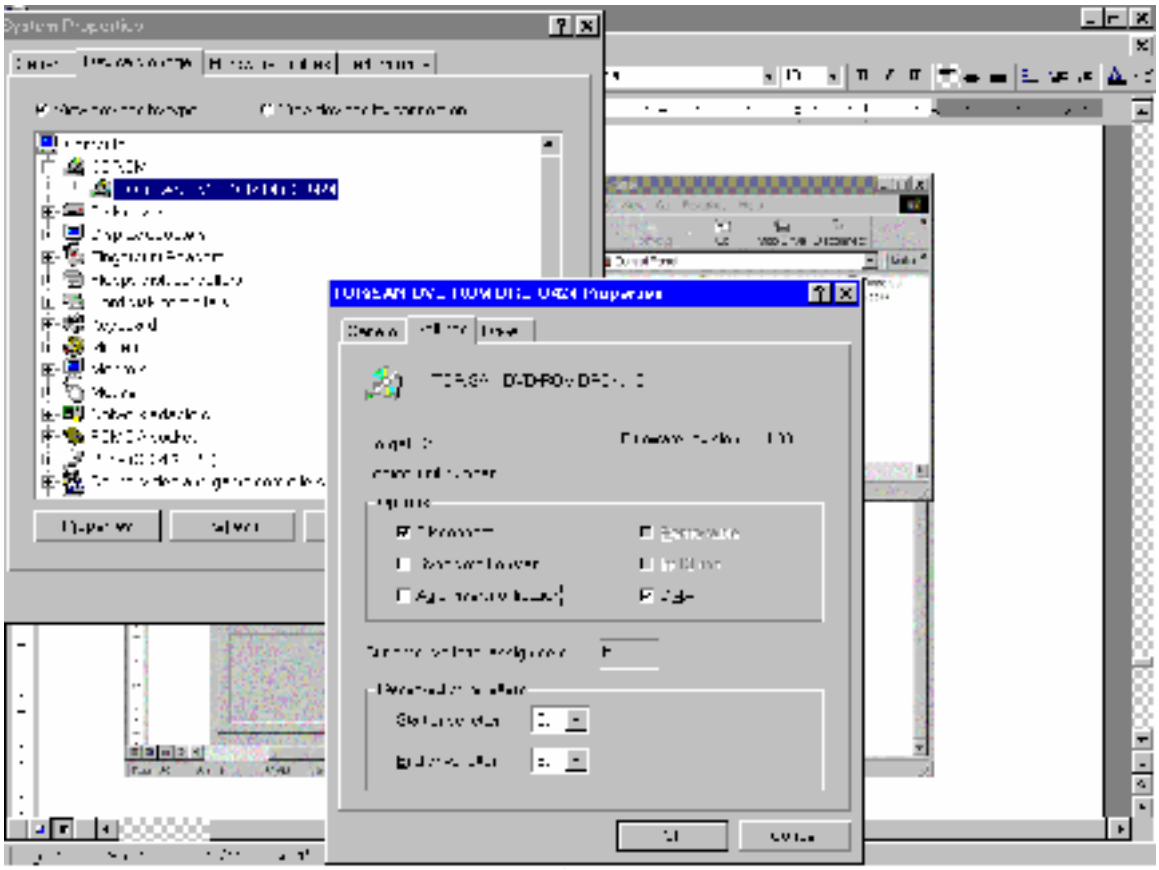
ROM-BIOS password is set: Pass, upon reboot, any attempt to change CMOS settings requires a password.

Refuse Windows access without network connection: Pass – see below.

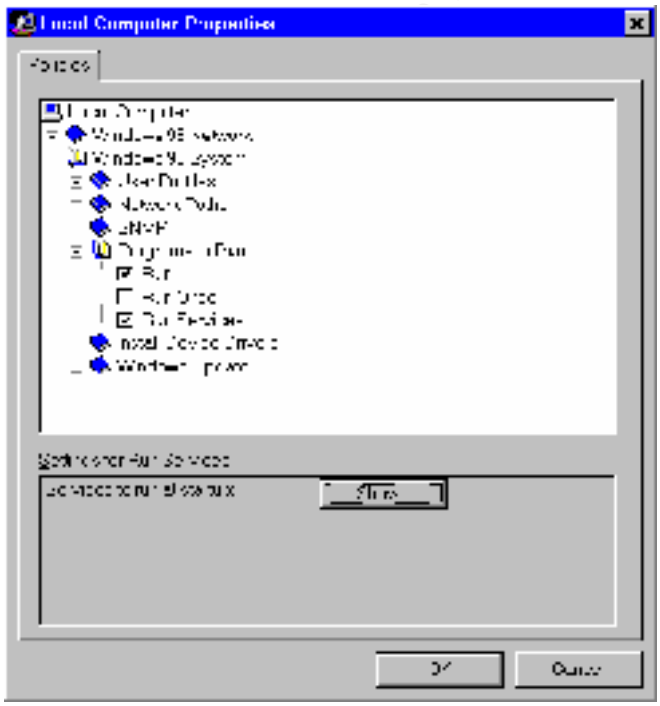


Autorun by CD player is disabled: Not pass – see below, noting that Auto-insert notification is now turned off in the Control Panel, System, Device Manager, Properties, Settings panel (There is no such setting for Floppy disks in the standard floppy controller device)

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



The inetd service is not enabled, and no other services or processes are run at startup which are not specifically desired, as shown below in the poledit.exe, Local Computer panel. Both Run and Run services should be examined by clicking the Show… button -- Pass

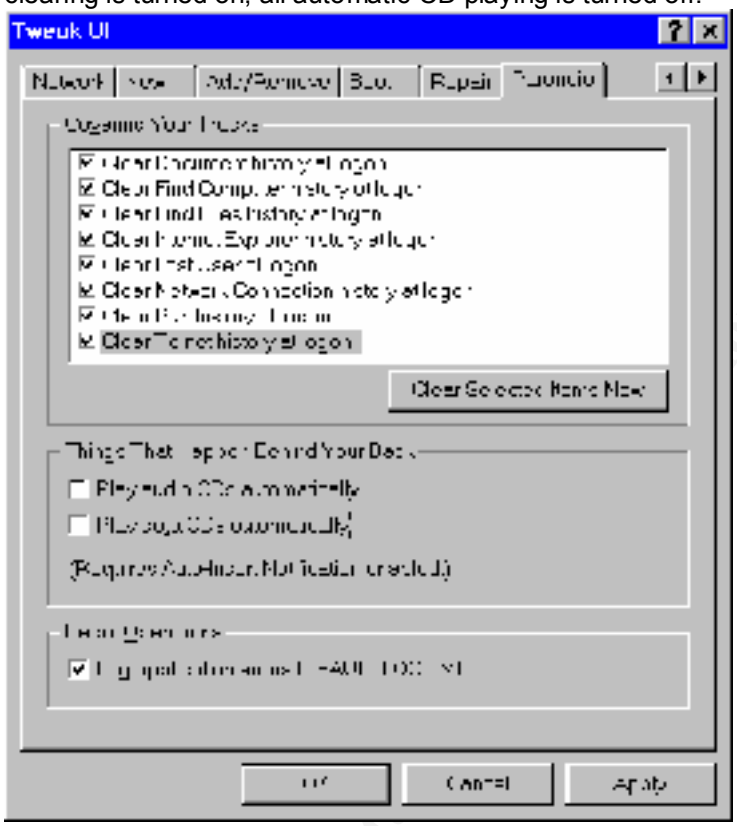


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Backups and restores are not logged, same issues as with system event logging. Not pass.

Screensaver locks console after inactivity of 10 minutes. Pass.

Virtual memory pagefile is cleared on shutdown; Not pass: Unable to figure how to do this for Windows 95/98, also, this should be done on logoff, rather than shutdown. Here is the next best thing that could be implemented for Windows 98. This is the TweakUI (http://www.annoyances.org/exec/show/tweakui) panel of the Control Panel, the Paranoia tab. All clearing is turned on, all automatic CD playing is turned off.

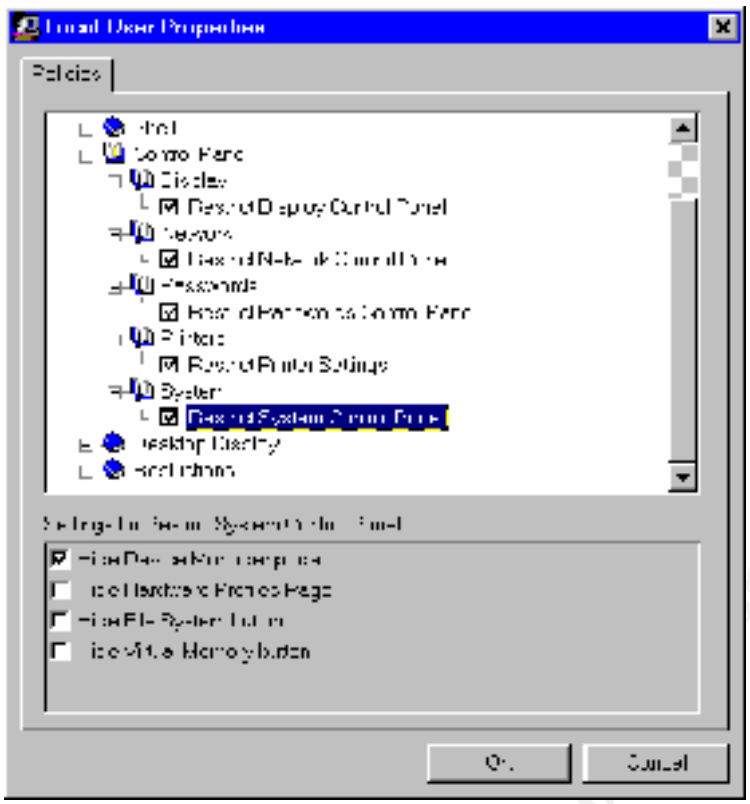


Last username is removed from the logon screen: Pass – see screenshot above (Clear Last User at logon), and three panels back poledit.exe (Don't show last user at logon).

Logon banners have legally binding warning text: Pass
Legal disclaimer and warning: Unauthorized access is prohibited. Unlawful use of any of these resources will be prosecuted to the fullest extent of California and United States law.

Driver installation is prohibited except for administrator: Not pass – No way is known for Windows 95/98 to actually restrict driver installation. It can be made more difficult by restricting the user access to the control panel items for the System Device Manager panel, Printers addition and deletion, and Network control panel items. Browser restrictions will also mitigate this risk.

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



Administrator account is renamed to delay compromise. Not pass: it is still “administrator”

No guest or other unrecognized accounts are allowed: Pass.

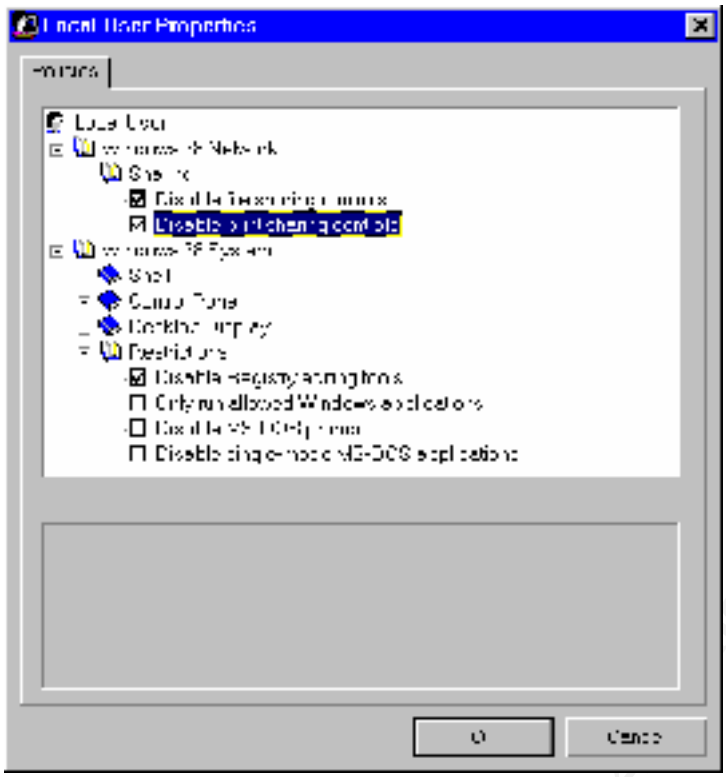
System has local firewall software installed and configured: Not pass – no such software

Biometric software declines non-matching fingerprint more than 100 times with no positives. Pass

Browser settings Refuse: all unsigned except active scripting, Prompts for signed applets/ ActiveX, Allow active scripting. Pass. All zones the same, including intranet, which scope can be spoofed from compromised outside web sites. Policy is also very restrictive in terms of downloads, except for Microsoft Corporation, which is always an exception to standard security procedures, such as signature checking.

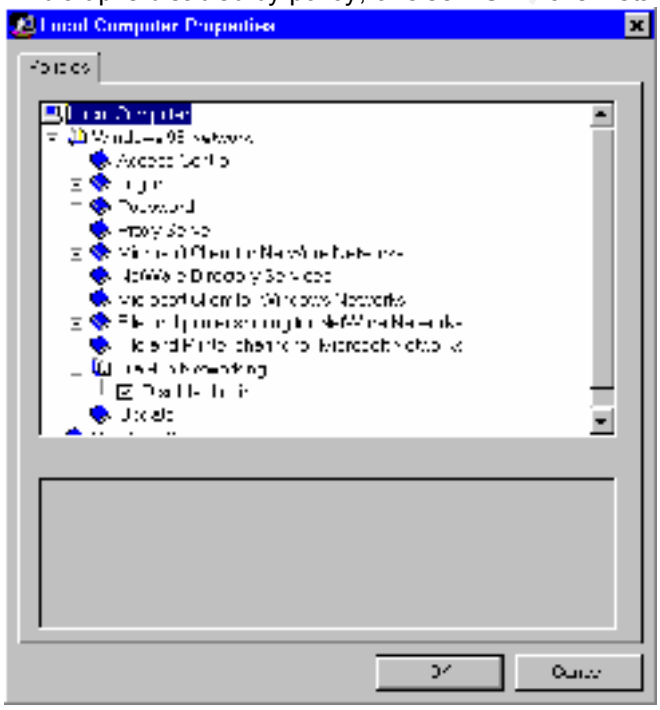
All file and print sharing is disabled by policy: Not pass – corrected, see below – in addition, registry editing should be restricted for non-privileged users (bonus)

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



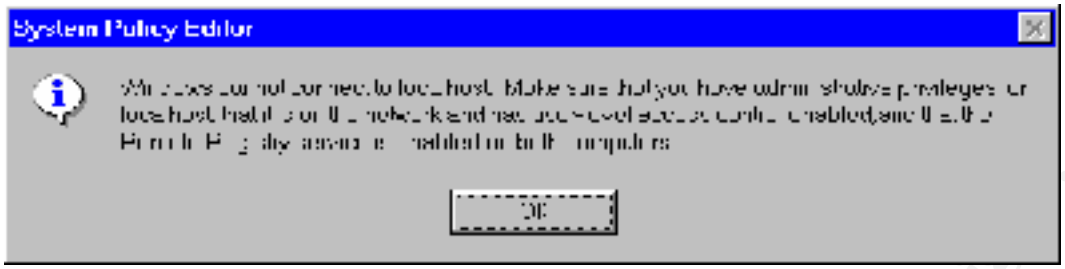
Any file sharing exceptions have names that begin with $ -- Pass, no exceptions

All dialup is disabled by policy, or else DUN 1.3 is installed: Not pass – now corrected, see below



Remote registry services are not installed/enabled: Pass – see below for response trying to File, Connect… poledit.exe to localhost

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



Reputable antivirus software is installed, enabled, and up to date. Not pass – McAfee and Symantec are both more than a year out of date. Note that no email attachments are allowed unless confirmed form a reputable source, and no web server has ever been running on this machine.

Password caching is disabled: Pass – see graphic for "Refuse Windows access without network connection" checklist item.

Vulnerability assessment: Pass, but conditional even after remedial action. Now passes, but still reveals host name and domain name as well as MAC address. ICMP and SNMP are filtered from going to this machine by the DMZ host, but IP numbering leaves all connections from this machine vulnerable to spoofing and hijacking.

Note: assume all communication from this machine can be easily sniffed.
Note: To disable remote logon, including administration with default passwords and null sessions, go to Control Panel, Network, Access Control, select User Level Access, and use the local domain name to obtain users and groups.

```
Nessus Scan Report
------------------



SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 0
 - Number of security warnings found : 4
 - Number of security notes found : 2



TESTED HOSTS

 192.168.1.2 (Security warnings found)



DETAILS

+ 192.168.1.2 :
 . List of open ports :
   o netbios-ssn (139/tcp)
   o netbios-ns (137/udp) (Security warnings found)
   o general/udp (Security notes found)
   o general/tcp (Security warnings found)
   o general/icmp (Security warnings found)

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


    . The following 8 NetBIOS names have been gathered :
     DEAVES-IN       = This is the computer name registered for workstation
     services by a WINS client.
```

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

```
    ISC             = Workgroup / Domain name
    DEAVES-IN       = Computer name that is registered for the messenger
    service on a computer that is a WINS client.
    DEAVES-IN
    ISC
    ISC
      __MSBROWSE__
    DEAVES          = Computer name that is registered for the messenger
    service on a computer that is a WINS client.
   . The remote host has the following MAC address on its adapter :
      0x00 0xe0 0x29 0x56 0x88 0xcd

   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


. Information found on port general/udp


   For your information, here is the traceroute to 192.168.1.2 :
   192.168.1.2

. 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 if the remote
   host sent a packet in reply to another request. This may be
   used for portscanning and other things.

   Solution : Contact your vendor for a patch
   Risk factor :
    Low


. Information found on port general/tcp


   QueSO has found out that the remote host OS is
   * WindowsNT, Cisco 11.2(10a), HP/3000 DTC, BayStack Switch


   CVE : CAN-1999-0454

. 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 authentifications protocols.

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

   Risk factor : Low
   CVE : CAN-1999-0524

. Warning found on port general/icmp
```

© SANS Institute 2000 - 2002, Author retains full rights.

```
The remote host answered to an ICMP_MASKREQ
query and sent us its netmask.

An attacker can use this information to
understand how your network is set up
and how the routing is done. This may
help him to bypass your filters.

Solution : reconfigure the remote host so
that it does not answer to those requests.
Set up filters that deny ICMP packets of
type 17.

Risk factor : Low
CVE : CAN-1999-0524



-------------------------------------------------------
This file was generated by the Nessus Security Scanner
```

Registry write is disabled: Pass – see poledit.exe, Local User, Windows 98 System, Restrictions, Disable Registry Editing tools is checked. **Note: user can write to the registry from poledit.exe if they have the executable, and then can use regedit.exe to further edit.**

UPS on LAN and backups are done reliably: Not pass – No UPS, and no regular Windows 98 content backups, monthly manual backups only.

Summary of Remedies, in order of subjective estimate of cost/time, and triaged:
Items corrected in the course of the audit:

1) Dialup disabled
2) File, Print sharing disabled
3) Registry not writeable by non-privileged users – **Note, add to checklist**
4) Autorun disabled for CD player
5) Vulnerability test item: remote administration removed from network access control.

Remedial actions to be taken:

6) Local firewall software licensed, installed, configured
7) Antivirus software licensed, installed, updated
8) Task Scheduler must be restricted from non-privileged users
9) Prohibit non-privileged user driver installation (all software?)
10) System auditing and event logging must be investigated and made functional.
11) System logging for backups and restores made functional – same as above
12) System pagefile cleared on logout/shutdown
13) Purchase UPS and set network backup policy for Windows 98

Lower priority:

14) Account lockouts
15) Administrator account should be renamed

Final Audit for System #2 was conducted December 7, 2001, and no claim is made here for the condition of this system on any date after that.

Supporting matrixes for risk mitigation analysis follow:

Failed checklist items represent risks of damage, times annual frequency/likelihood of a related exploit that could otherwise be prevented. These are subjective estimates provided by the management, whose assistance was invaluable in preparing this report.

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

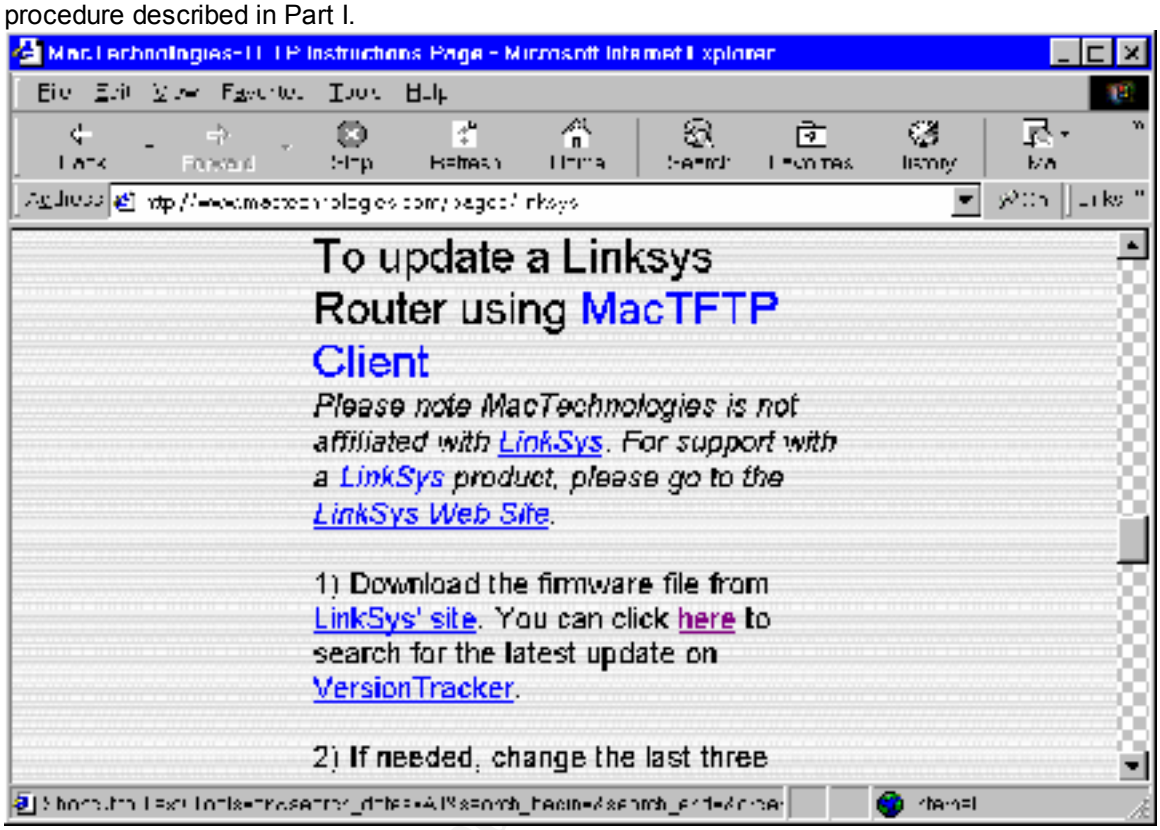
	Local Firewall: netbios exploit	Antivirus software: new virus delivery	Task scheduler: privilege escalation	Install drivers: careless users	Auditing, logging: anything at all	Clear pagefile: Premises intrusion	UPS, net backups: power outage
System #2	0.1	0.1	0.1	0.1	1.0	0.5	0.5

Assumptions are that both firewall and antivirus software represent protection from infrequent, though severe threats, due to the minimal nature of network services offered and frequency of new system level exploits for Windows 98 that are not already addressed. Similarly for privilege escalation via the task scheduler and Trojans from drivers installed by careless users, damages are large or total, but the likelihood of exposure is low.
Threats from lack of logging or auditing of any meaningful kind are total and not in any way mitigated. No attempted surveillance or exploit can be detected, and any intrusion detection will be severely impaired in case of other damage to assets.
Threats from physical intrusion onto the premises, and from power failure are described at the end of the previous section, and their proportion is duplicated here.

© SANS Institute 2000 - 2002, Author retains full rights.

Appendix C: Benchmark and Matrixes, System #3

Latest patches are installed: click here, as per reference 1 in the Linksys Router auditing procedure described in Part I.

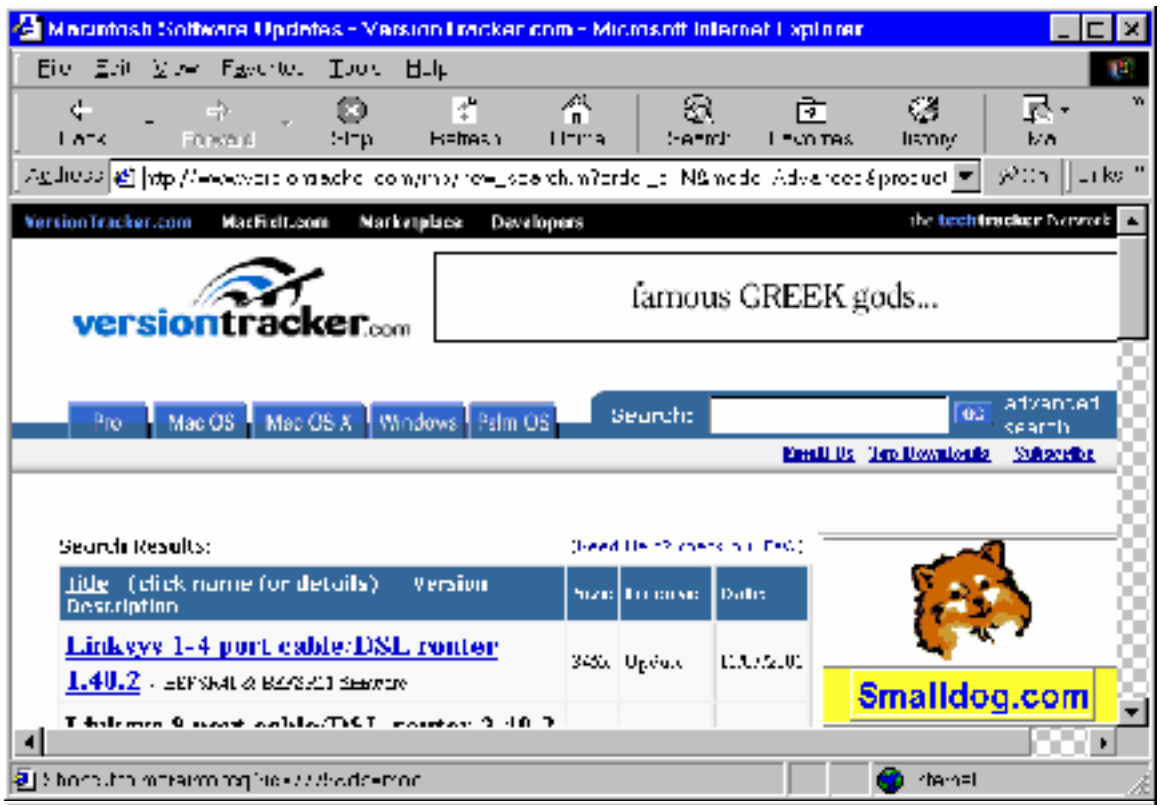


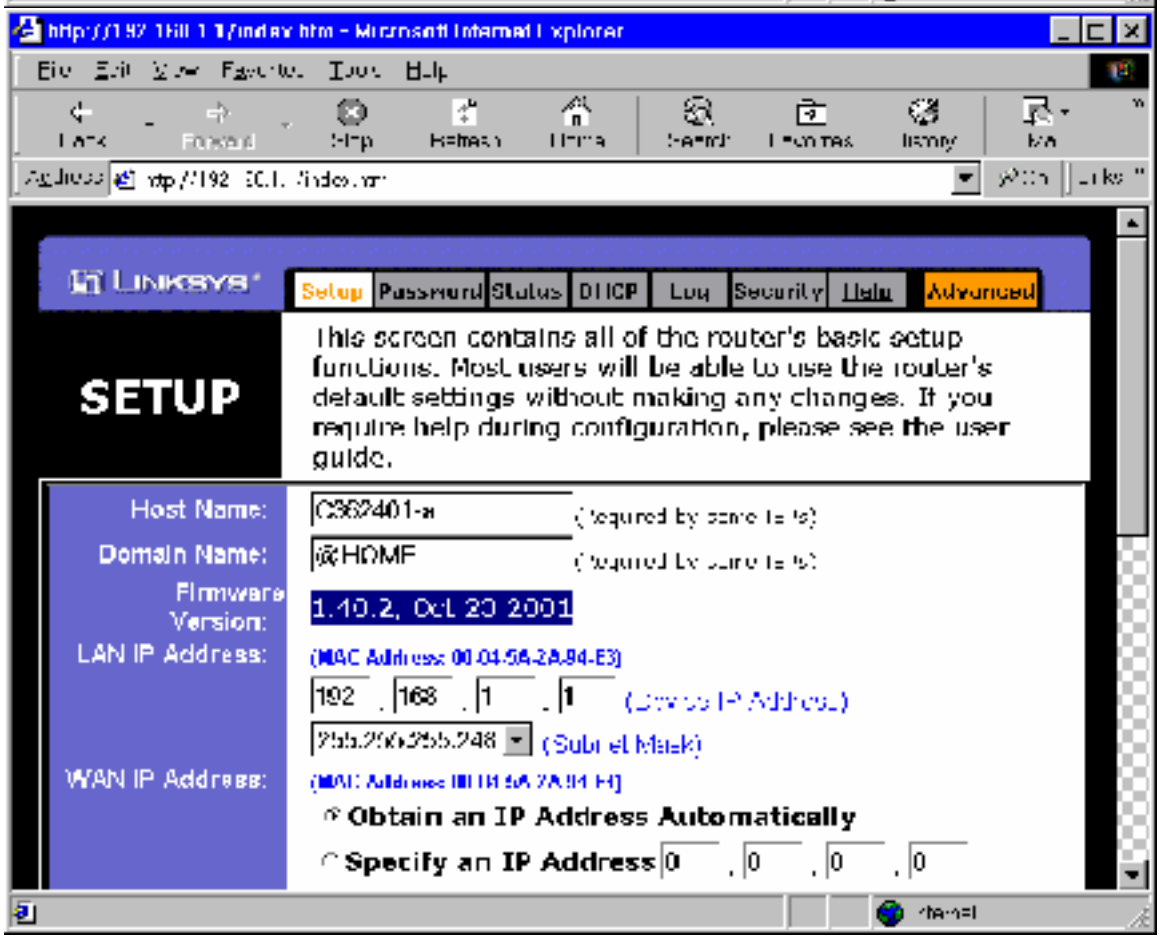
and get the following (searching at www.versiontracker.com for Linksys and MacOS – see screenshots below). The version shown here indicates that the Nov 7, 2001 release is the latest version. There are extensive version notes, which indicate that the only serious changes made have been mostly in the LAN-side web interface.

This update has been installed, as is generally indicated in the subsequent screen shot by the October 23, 2001 date. Version numbers match, and, since this is subsequent to the purchase of the router, and only one firmware update has ever been installed, it can be deduced that this update is one and the same.

It should be noted that logging is deficient, as no administrative events of any kind, or access to the administrative interface are logged, apparently. The incoming and outgoing logs appear to have timestamps, and source and destination addresses and ports only, but not any indication which protocol appears in the IP header, or traffic measurement per connection.

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





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

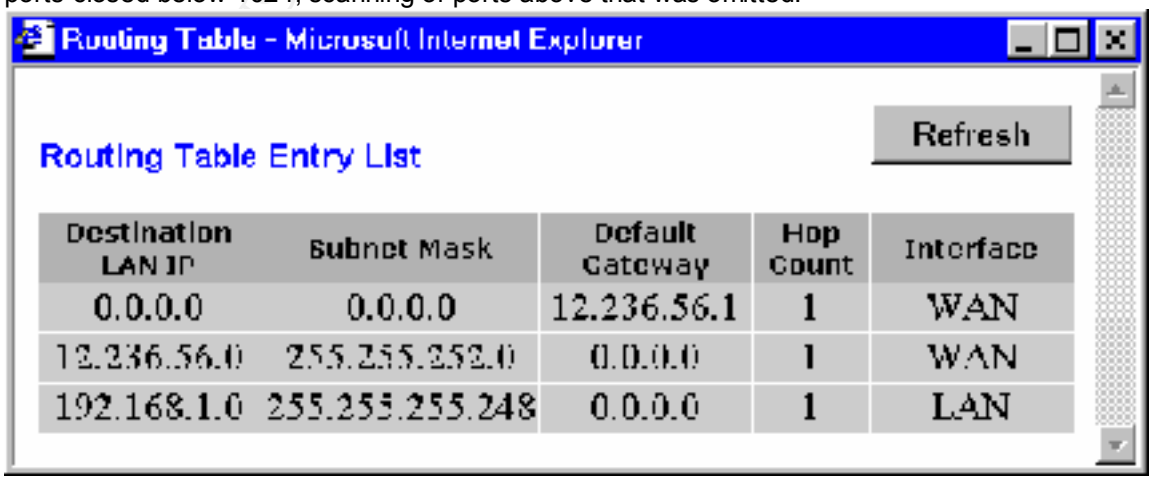
Vulnerability assessment tool shows negative database match:
LAN-side performed by nessus, running from 192.168.1.3, LAN, or clean side, onto 192.168.1.1

```
Nessus Scan Report
------------------



SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 1
 - Number of security warnings found : 2
 - Number of security notes found : 2



TESTED HOSTS

 192.168.1.1 (Security holes found)



DETAILS

+ 192.168.1.1 :
 . List of open ports :
   o http (80/tcp) (Security hole found)
   o general/udp (Security notes found)
   o general/tcp (Security warnings found)
   o domain (53/tcp) (Security warnings found)

 . Vulnerability found on port http (80/tcp) :



    The remote proxy is vulnerable to format strings attacks
    when issued a badly formed user name.

    This flaw allows an attacker to execute arbitrary code on this
    host.

    Solution : if you are using NSM, see
     http://www.solsoft.org/nsm/news/972559672/index_html
               or else contact your vendor for a patch

    Risk factor :
     High


 . Information found on port general/udp


    For your information, here is the traceroute to 192.168.1.1 :
    192.168.1.1

 . 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 if the remote
    host sent a packet in reply to another request. This may be
    used for portscanning and other things.

    Solution : Contact your vendor for a patch
    Risk factor :
```

© SANS Institute 2000 - 2002, Author retains full rights.

```
    Low

. 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.


   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 another name server, consult its documentation.

   Risk factor :
    Serious


. Information found on port domain (53/tcp)


   The remote bind version is :
    no




-------------------------------------------------------------
This file was generated by the Nessus Security Scanner
```

WAN-side, performed by nessus, making sure that the Linksys router is set temporarily to be the DMZ host, so that packets addressed to the assigned IP address are routed back to the WAN side of the Linksys router. Considering that the routing table below has no direct reference to the local IP address actually assigned by DHCP, IP packets addressed to the external ISP-assigned address 12.236.57.n must at least reference the upstream router (or at least send and receive SNMP) before returning via the WAN interface. The cable modem was observed to show activity corresponding to all requests to and responses from 12.236.57.n. Since port scanning showed all ports closed below 1024, scanning of ports above that was omitted.



Destination LAN IP	Subnet Mask	Default Gateway	Hop Count	Interface
0.0.0.0	0.0.0.0	12.236.56.1	1	WAN
12.236.56.0	255.255.252.0	0.0.0.0	1	WAN
192.168.1.0	255.255.255.248	0.0.0.0	1	LAN

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

```
Nessus Scan Report (edited by David Eaves to remove addresses)
------------------



SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 0
 - Number of security warnings found : 0
 - Number of security notes found : 1



TESTED HOSTS

 12.236.57.nnn (Security notes found)



DETAILS

+ 12.236.57.nnn :
 . List of open ports :
   o general/udp (Security notes found)

 . Information found on port general/udp


    For your information, here is the traceroute to 12.236.57.nnn :
    ?



-------------------------------------------------------
This file was generated by the Nessus Security Scanner
```

Summary: Not pass – requires a patch to the web server on the LAN side administrative interface to prevent format string overflow attacks from within the network. Since this is on the LAN or clean side, rather than on the WAN or dirty side, this risk is minimal as long as physical access to the router is limited. Having investigated this, there is no such patch available. However there is no third party verification of the vulnerability, or any explanation from Nessus what the criterion was for making this determination, and the software claimed does not match the name of Mac Technologies, the third party developer for Linksys, so the actual risk is undetermined.

Router has no users other than one administrator, this has a nontrivial password:

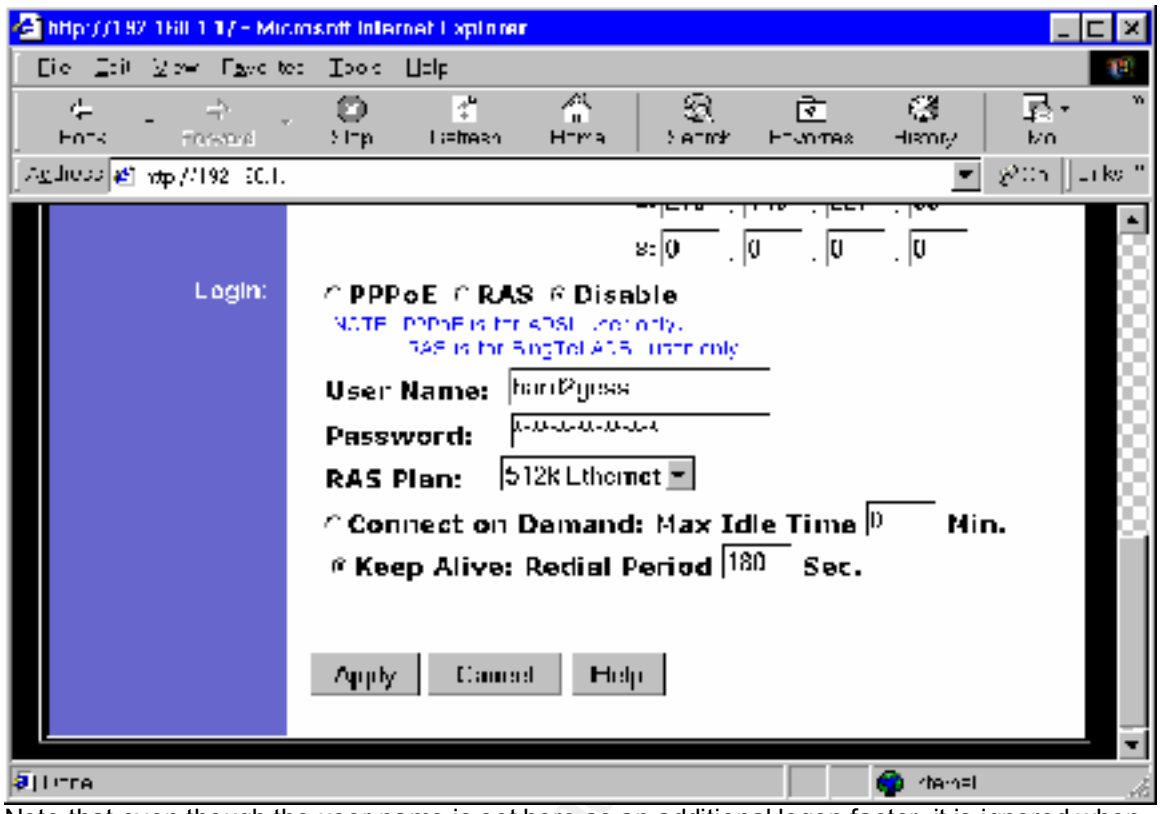
Not pass: The Linksys router appears to allow any username to log into the administrative interface. It appears to authenticate based on only password, and no other credential. The password is set and is nontrivial.

Has correct ISP-specified parameters:
As can be seen the screen shot before the previous one, DHCP is selected, and the inherited host name and domain name from prior to the Excite@home bankruptcy proceeding (which is still supported by AT&T Broadband evidently) are in force. The DNS servers are not shown, as they are temporarily set to query the remote systems (see subsequent Appendixes), and an AT&T name server. When AT&T Broadband notifies their new clients of DNS assigned servers, these will be assigned permanently. The actual IP address assigned to this private network can be seen in the Status panel (not shown here).

Pass.

Remote login is disabled – below (Main setup page, bottom)

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



Note that even though the user name is set here as an additional logon factor, it is ignored when authenticating the user logon.

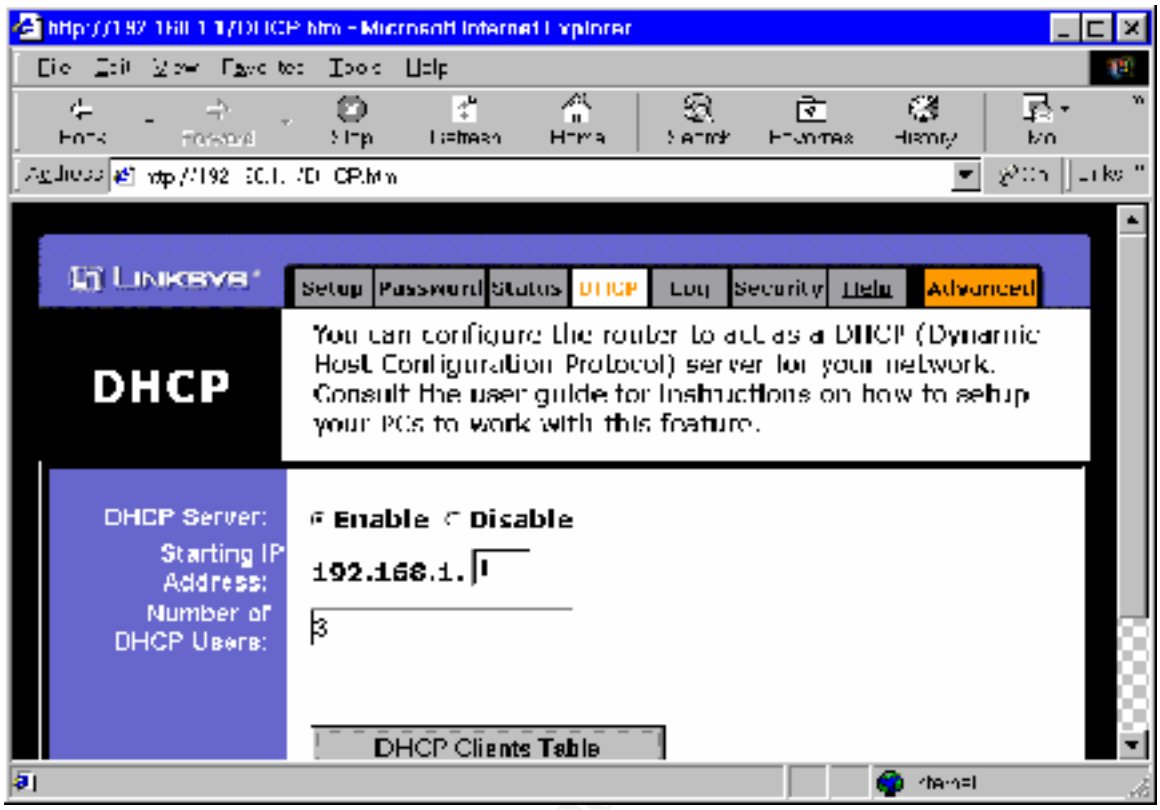
Subnet mask is minimal for the actual number of systems – preventing/discouraging spoofing of internal network addresses to get past the router: Pass – could be set to 252, allowing up to four internal addresses, low priority, considering the DMZ firewall on system #1.

Router cannot force factory configurations: 403 is returned when attempting to replay a factory settings reset HTTP request from the password panel. If the TCP session could be sniffed from inside the network, however, it could be spoofed and the basic authentication bypassed to reset the administrative password. This could be detected however, as the old password would have been lost. Pass:

Note: assert(Wireless IP + Linksys == exploit-vulnerable)

Number of DHCP users is minimal for the network (preventing some kinds of surveillance spoofing): Pass – see below

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

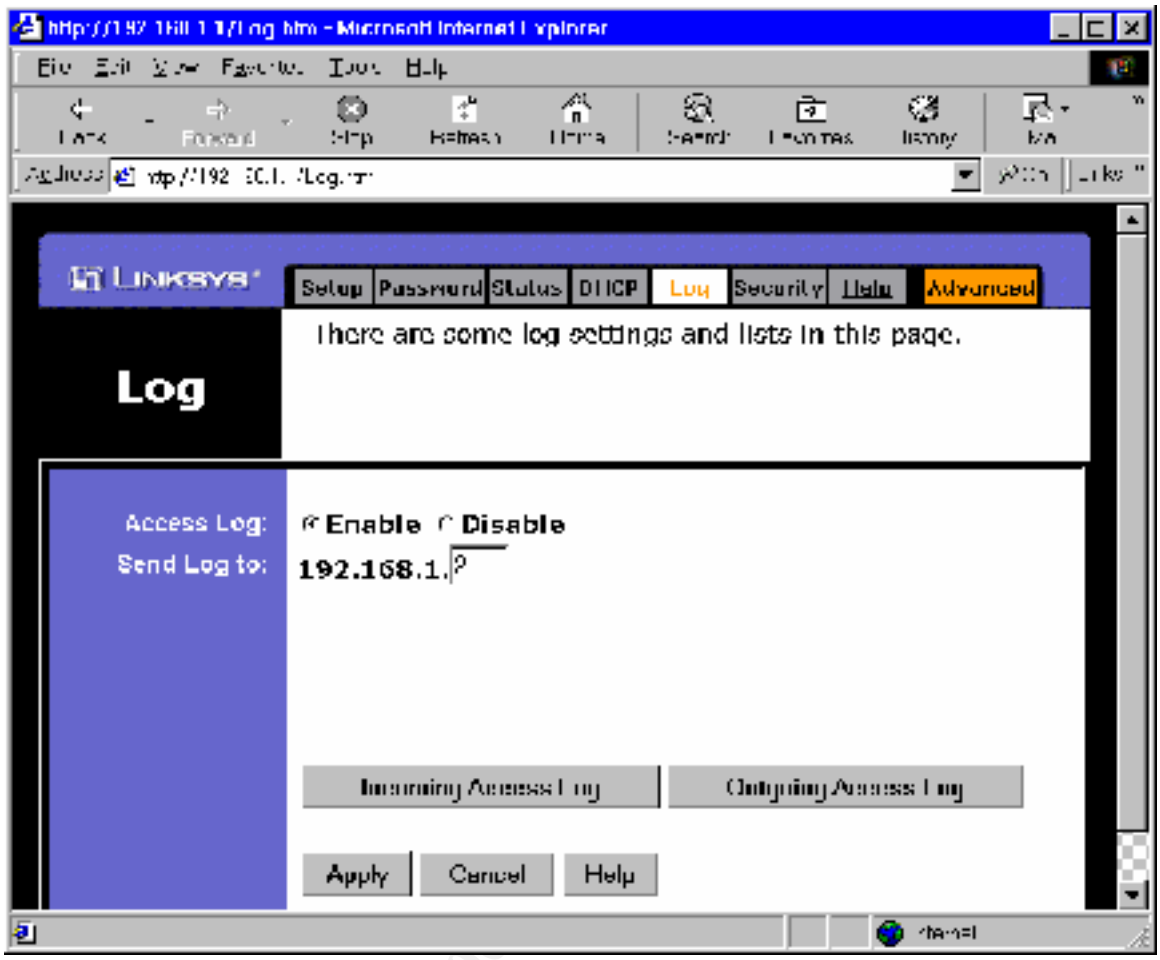


Log viewing interface views in and out access logs: Pass – note that the logs are kept on one of the network systems, not the router. For further research, where these are kept and by what process would be of interest – Find files modified more recently than the last hour has been attempted on both System #1 and System #2 with no results.

Also note that even using the LogViewer application, downloaded from the Linksys site, there is no more information logged than source and destination addresses and ports, and timestamps. This can help corroborate other, more detailed logging systems, but it is insufficient as a security device, especially considering that administrative events are not audited or logged.

There also appears to be an intermittent error having to do with logging: occasionally a malformed packet will be logged as from an unroutable address (e.g. 0.0.0.0), and whose timestamp corresponds only with one set of requests that another sniffer (ethereal) shows as having come from an address of a connection or related connection in use at the time. This could also be due to errors in the version(s) of SSH in use, or other sniffers and session-hijacking attempts in between: it only seems to occur when communicating with secure-sockets (SSL) wrapped HTTP.

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



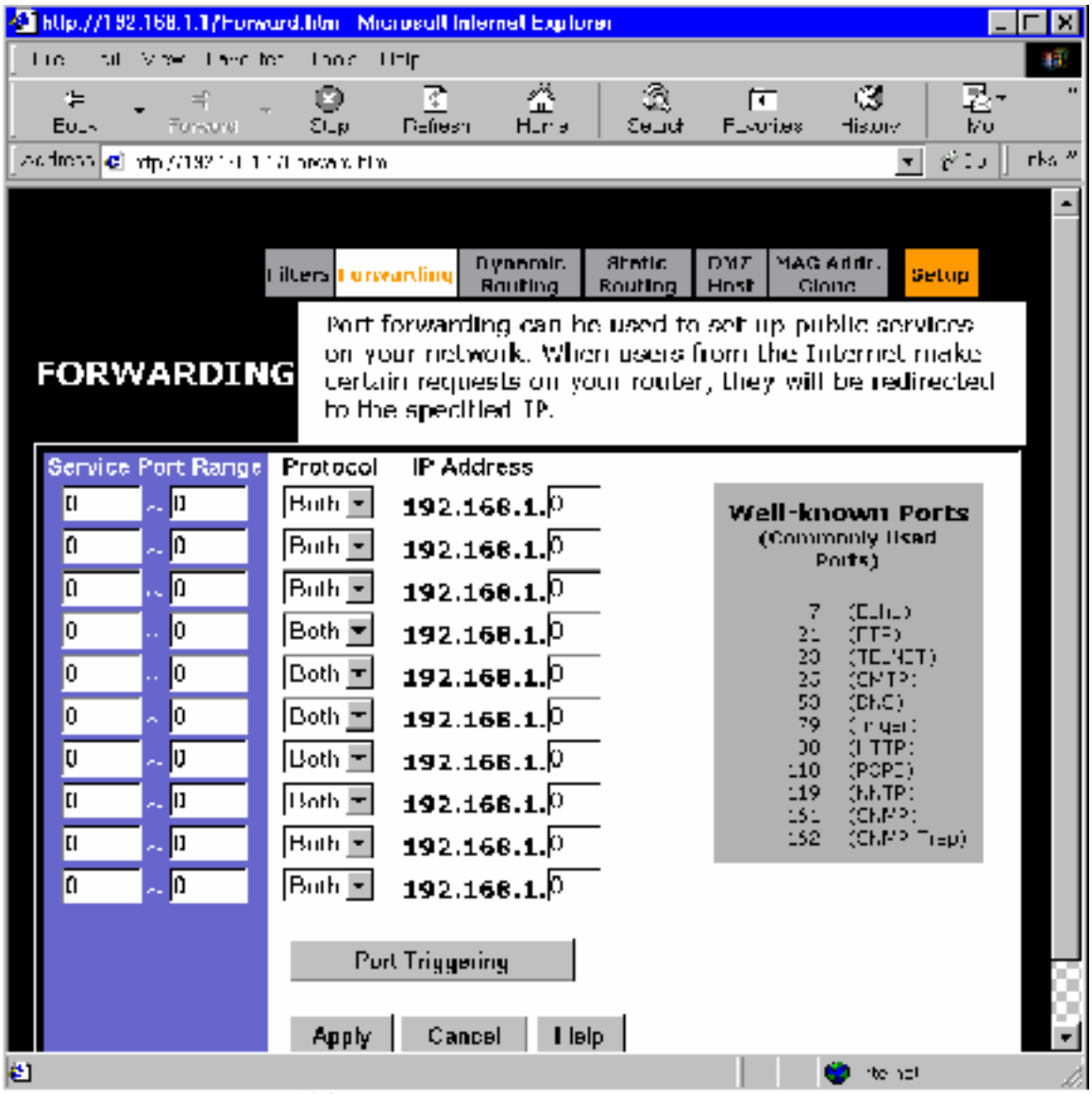
If ZoneAlarm or PC-cillin is in use from the router, then it is enforced with only the DMZ firewall exempted: Pass – not in use at this time. See firewall and antivirus failures in System #1 and System #2 audits.

Port filtering implements secure ACL's: Not pass: Not possible with this device. Access is automatic, and no other port access is filtered, except for outbound, and that is not state based, requiring that all destination port traffic be blocked. Since System #1 is used for scanning services, it must allow all ports outbound from this network.

Under other circumstances the benchmark should generally restrict outbound traffic between 1025-65535, which should not impact most networks' usability, and generally prevents certain Trojans from propagating, should they gain access. Even blocking outbound 501-65535 should have little impact on most networks that don't share print servers, but below port 500 one starts to involve key exchange (IKE), HTTPS, and more commonly used network services.

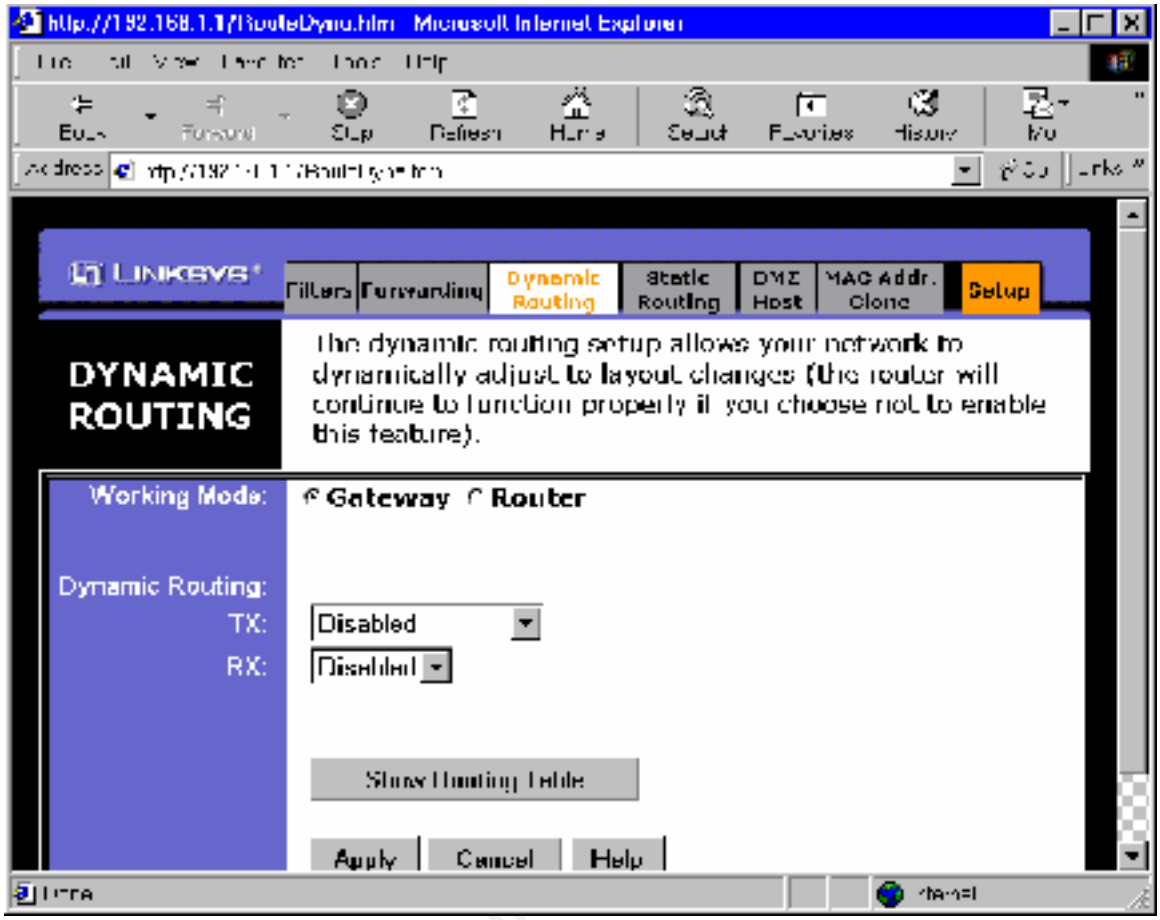
There is no port forwarding in place for this router: Pass: see screen shot below

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



All dynamic routing is disabled, gateway mode, not router mode: Pass

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



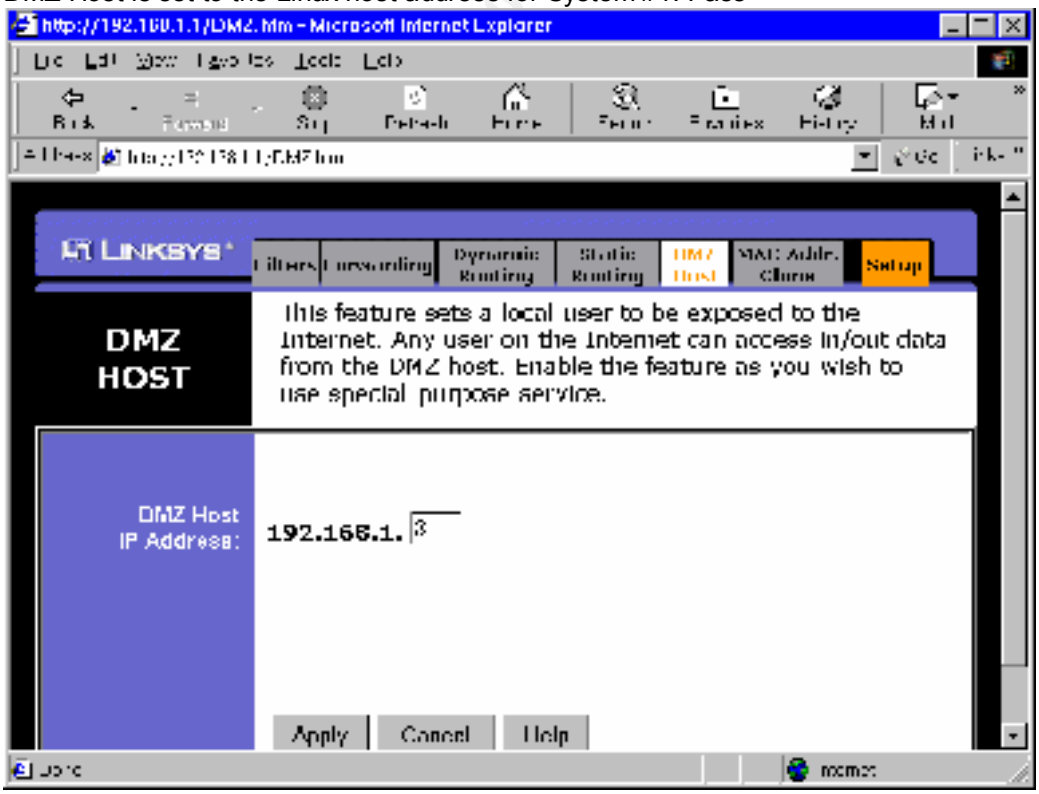
Static WAN routes exist only for ISP-designated gateways, or none if using DHCP for the WAN side: Pass – using DHCP on the WAN side.

Note in the screenshot below that the Static Routing select drop down is actively scripted. It must be tested for each static route in the list, and has been. There are no static routes defined at all. Since MAC addresses cannot be defined associated with static LAN routes in this appliance, there seems to be little security to gain from requiring only static LAN routes. Internal DHCP is therefore in use, as seen in earlier screen shots. See the routing table shown above.

Note: One can gain a marginal increase in security by using static LAN routes to set mid-range, or random internal IP addresses, away from 254 and 1, so as to frustrate some kinds of surveillance. But this would also allow other kinds of spoofing and network surveillance.

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

DMZ Host is set to the Linux host address for System #1: Pass



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

Internal LAN addresses are set away from 1 and 255, making surveillance more difficult: Not pass – using DHCP and dynamic LAN side routes.

Summary of Remedies, in order of subjective estimate of cost/time, and triaged:
Remedial actions to be taken:

1) Set ACL's for outbound port filtering while not in use for security scanning services
2) Set static LAN routes, allowing for random and mid range internal addressing to frustrate some surveillance.
3) Change the name servers to appropriate servers that are not vulnerable to recursion and cannot be poisoned (partial checklist fix)

Lower priority:

4) LAN-side web server format string overflow vulnerability requires a manufacturer patch to the web server (partial checklist fix)
5) Login to administrative interface requires a patch from the manufacturer to require a username match in addition to password

Final Audit for System #2 was conducted December 7, 2001, and no claim is made here for the condition of this system on any date after that.

Supporting matrixes for risk mitigation analysis follow:

Failed checklist items represent risks of damage, times annual frequency/likelihood of a related exploit that could otherwise be prevented. These are subjective estimates provided by the management, whose assistance was invaluable in preparing this report.

	Outbound ACL's while unused: some new exploits prevented	Static LAN routes: SNMP surveillance frustrated	Secure DNS sources: DNS cache poisoning prevented
System #3	0.05	0.1	0.1

Note that the only damage from poisoned DNS servers would be temporary, and the consequences would include responses to local DNS requests possibly being spoofed. No assets of the company are anticipated at risk in this case, other than time spent detecting and addressing the problem.

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

Appendix D: Benchmark and Matrixes, Remote System #1

The assessment of remote system #1 includes a checklist-of-checklists for the system generally, and a supplemental web application assessment. Remote system #1 hosts ssh services, and is shared with another virtual host that runs the corporate web site, – see Part I for a description of this checklist. The network diagram for the remote network, including its unusual routing details, will be kept confidential at the request of the network owner, and because they themselves are not owned by the organization being audited, only some IT assets residing upon them.

The CIS Solaris ruler measurement (internal vulnerability report):

The network owner was reticent to allow permission for such an internal procedure to be run, considering that it requires root access to be made and executed. Not pass.

The external vulnerability reports – both virtual hosts, ssh host and web host: we use insider knowledge here, that both IP addresses are served by the same actual host, and threats to the one are the same as threats to the other.

SSH/SMTP host (IP ending octets edited out):

```
Nessus Scan Report
------------------



SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 0
 - Number of security warnings found : 2
 - Number of security notes found : 4



TESTED HOSTS

 192.86.83.nnn (Security warnings found)



DETAILS

+ 192.86.83.nnn :
 . List of open ports :
   o general/udp (Security notes found)
   o ssh (22/tcp) (Security warnings found)
   o smtp (25/tcp) (Security warnings found)
   o telnet (23/tcp) (Security notes found)

 . Information found on port general/udp


    For your information, here is the traceroute to 192.86.83.nnn :
    ?

 . Warning found on port ssh (22/tcp)



    You are running a version of SSH which is
    older than (or as old as) version 1.2.27.
```

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

```
   If you compiled ssh with kerberos support,
   then an attacker may eavesdrop your users
   kerberos tickets, as sshd will set
   the environment variable KRB5CCNAME to
   'none', so kerberos tickets will be stored
   in the current working directory of the
   user, as 'none'.

   If you have nfs/smb shared disks, then an attacker
   may eavesdrop the kerberos tickets of your
   users using this flaw.

   ** If you are not using kerberos, then
   ignore this warning.

   Risk factor : Serious
   Solution : use ssh 1.2.28 or newer
   CVE : CAN-2000-0575

. Information found on port ssh (22/tcp)


   Remote SSH version : SSH-1.5-1.2.26

. Warning found on port smtp (25/tcp)


   The remote SMTP server
   answers to the EXPN and/or VRFY commands.

   The EXPN command can be used to find
   the delivery address of mail aliases, or
   even the full name of the recipients, and
   the VRFY command may be used to check the
   validity of an account.


   Your mailer should not allow remote users to
   use any of these commands, because it gives
   them too much informations.


   Solution : if you are using sendmail, add the
   option
      O PrivacyOptions=goaway
   in /etc/sendmail.cf.

   Risk factor : Low
   CVE : CAN-1999-0531

. Information found on port smtp (25/tcp)


   Remote SMTP server banner :
   220-system1.WLK.Com[192.157.31.zzz] SMTP listener readyESMTP spoken here.
   214-Commands

   214-HELO  EHLO  MAIL  RCPT  RSET  ONEX

   214 VERB  DATA  NOOP  QUIT  HELP  VERB



. Information found on port telnet (23/tcp)


   Remote telnet banner :
   ÿ¯$
```

© SANS Institute 2000 - 2002, Author retains full rights.

```
-------------------------------------------------------
This file was generated by the Nessus Security Scanner
```

SSH/HTTP host:

The scan for the virtual host assigned to manage the web site follows:

```
Nessus Scan Report
------------------



SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 1
 - Number of security warnings found : 2
 - Number of security notes found : 3



TESTED HOSTS

 www.<web_site_name>.com (Security holes found)



DETAILS

+ www.<web_site_name>.com :
 . List of open ports :
   o general/udp (Security notes found)
   o ssh (22/tcp) (Security hole found)
   o http (80/tcp) (Security notes found)
   o general/tcp (Security warnings found)

 . Information found on port general/udp


    For your information, here is the traceroute to 192.86.83.nnn :
    10.109.246.1
    12.244.98.129
    12.244.67.26
    12.244.72.194
    12.123.13.162
    12.122.11.89
    12.122.11.230
    192.205.32.126
    152.63.52.226
    152.63.53.250
    152.63.10.85
    152.63.101.154
    152.63.102.22
    152.63.103.145
    152.63.100.5
    204.177.254.203
    192.86.83.qqq
    ?

 . Vulnerability found on port ssh (22/tcp) :



    You are running a version of SSH which is
    older than version 1.2.32,
    or a version of OpenSSH which is older than
```

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

```
   2.3.0.

   This version is vulnerable to a flaw which
   allows an attacker to insert arbitrary commands
   in a ssh stream.

   Solution :
   Upgrade to version 1.2.32 of SSH which solves this problem,
   or to version 2.3.0 of OpenSSH

   More information:
   http://www.core-sdi.com/english/ssh/

   Risk factor : High
   CVE : CAN-2001-0144

. Warning found on port ssh (22/tcp)



   You are running a version of SSH which is
   older than (or as old as) version 1.2.27.

   If you compiled ssh with kerberos support,
   then an attacker may eavesdrop your users
   kerberos tickets, as sshd will set
   the environment variable KRB5CCNAME to
   'none', so kerberos tickets will be stored
   in the current working directory of the
   user, as 'none'.

   If you have nfs/smb shared disks, then an attacker
   may eavesdrop the kerberos tickets of your
   users using this flaw.

   ** If you are not using kerberos, then
   ignore this warning.

   Risk factor : Serious
   Solution : use ssh 1.2.28 or newer
   CVE : CAN-2000-0575

. Information found on port ssh (22/tcp)


   Remote SSH version : SSH-1.5-1.2.26

. Information found on port http (80/tcp)


   The remote web server type is :
   Apache/1.2.6


   We recommend that you configure your web server to return
   bogus versions, so that it makes the cracker job more difficult

. 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 if the remote
   host sent a packet in reply to another request. This may be
   used for portscanning and other things.

   Solution : Contact your vendor for a patch
   Risk factor : Low
```

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

```
-------------------------------------------------------
This file was generated by the Nessus Security Scanner
```

Pass: SSH is relatively safe, since no nfs/smb, or kerberos is in use, while the SMTP information giveaway is according to that system's policy.

The web server (HTTP port) is subject to the web application checklist, following:

Web server product cannot be easily identified – Not pass: Apache/1.2.6. There is no good reason to run such an old version of a free product. Replacement cost about two days out of production and employee time. Possible risks to custom CGI in other virtual hosts run by the same server. Assuming backward compatibility with the Apache C API this should require a simple rebuild of the custom modules with the new Apache header files.

No default install materials available: for address=http:// <web_site_name>.com, try address/default.html, address/index.html, address/., address/.., address/\/. All show Not found or main page except "..", which shows parent directory. Pass – no default materials.

Available web map is correct. No web map, simple design – pass.

No well-known executables are installed in or linked to document root: examination shows only non-executable html files and one directory, for graphic content, which contains only non-executable gif files. Only directories and vi-content are executable. Latter has only commands to vi all html files. Pass – see internal listing, below

```
> ls -al
total 360
drwxr-xr-x   3 deaves   www         1536 Oct 15 17:18 .
drwxr-xr-x  12 deaves   root         512 Dec 11 13:46 ..
-rw-r--r--   1 deaves   www         4368 Jul 25 18:08 NonDisC.txt
-rw-r--r--   1 deaves   www         5822 Oct 15 21:39 about-iscorp.html
-rw-r--r--   1 deaves   www         4658 Oct 15 19:15 auth.html
-rw-r--r--   1 deaves   www         1721 Jul  2 16:54 bill_bio.html
-rw-r--r--   1 deaves   www          433 Jul  2 17:03 bob_bio.html
-rw-r--r--   1 deaves   www          538 Jul  2 10:25 ccard.html
-rw-r--r--   1 deaves   www        10596 Oct 15 17:27 cert-work.html
-rw-rw-rw-   1 deaves   www         7605 Oct 15 18:42 certification.html
-rw-rw-rw-   1 deaves   www          415 Oct 15 14:57 content-list
-rw-rw-rw-   1 deaves   www         4753 Oct 15 19:13 custom-soft.html
-rw-rw-rw-   1 deaves   www         6583 Oct 15 19:19 custom-vpns.html
-rw-r--r--   1 deaves   www         1620 Aug 27 17:53 dave_bio.html
-rw-r--r--   1 deaves   www         1412 Jul  2 16:34 earl_bio.html
-rw-r--r--   1 deaves   www         5689 Oct 15 17:27 firewall-how-to.html
-rw-rw-rw-   1 deaves   www          186 Jul 23 20:04 footer.html
-rw-r--r--   1 deaves   www         3208 Oct 15 19:11 frus-answer.html
lrwxrwxrwx   1 deaves   www            7 Oct 15 17:18 gifs -> ../gifs
-rw-rw-rw-   1 deaves   www          775 Aug 27 18:42 header.html
-rw-r--r--   1 deaves   www         4254 Oct 15 17:27 index.html
-rw-rw-rw-   1 deaves   www         5903 Oct 15 16:39 intrusion-detect.html
-rw-rw-rw-   1 deaves   www         5507 Oct 15 16:42 ironhand.html
-rw-rw-rw-   1 deaves   www          253 Jul 23 19:07 isc-style.css
-rw-rw-rw-   1 deaves   www         1128 Aug 23 15:13 left-navbar.html
-rw-r--r--   1 deaves   www         5640 Oct 15 16:49 library.html
-rw-r--r--   1 deaves   www         1297 Jul  2 10:25 mark_bio.html
-rw-r--r--   1 deaves   www         8360 Aug 27 18:42 nondisclosure.html
-rw-rw-rw-   1 deaves   www         3630 Oct 15 18:58 partners.html
-rw-r--r--   1 deaves   www         3774 Aug 27 18:43 quick-response.html
-rw-r--r--   1 deaves   www         3718 Aug 27 17:56 reach-us.html
-rw-rw-rw-   1 deaves   www           97 Jul 23 19:10 sample-table.html
-rw-rw-rw-   1 deaves   www         6519 Oct 15 16:59 sec-policy.html
```

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

```
-rw-r--r--   1 deaves   www         5632 Oct 15 19:00 server.html
-rw-r--r--   1 deaves   www         5872 Oct 15 17:10 service-offerings.html
-rw-rw-rw-   1 deaves   www         2859 Aug 27 18:43 surround.html
-rw-rw-rw-   1 deaves   www         5182 Aug 27 18:43 systems-int.html
-rw-r--r--   1 deaves   www          480 Jul 26 19:05 teacher.html
-rw-rw-rw-   1 deaves   www         2859 Aug 27 18:44 template.html
-rw-r--r--   1 deaves   www         4203 Aug 27 18:44 tokens.html
-rw-rw-rw-   1 deaves   www         4113 Oct 15 19:36 toolkit.html
drwxr-xr-x   2 deaves   www          512 Aug 23 15:48 unused
-rwxrwxrwx   1 deaves   www          418 Oct 15 14:59 vi-content
-rw-r--r--   1 deaves   www         7474 Aug 27 18:44 waiver.html
-rw-r--r--   1 deaves   www         5683 Aug 27 18:44 why-router-bastion.html

> ls -al ../gifs
total 488
drwxr-xr-x   2 deaves   www         1536 Jul 23 17:01 .
drwxr-xr-x  12 deaves   root         512 Dec 11 13:46 ..
-rw-rw-r--   1 deaves   www         1876 Sep  4  1997 announce.gif
-rw-rw-r--   1 deaves   www         2229 Sep  3  1997 baghead.gif
-rw-r--r--   1 deaves   www         3018 Sep  3  1997 baghead.jpg
-rw-rw-r--   1 deaves   www         2880 Sep  4  1997 books.gif
-rw-rw-r--   1 deaves   www           50 Sep  2  1997 bullet1.gif
-rw-rw-r--   1 deaves   www         8794 Sep  2  1997 button-cauce.gif
-rw-rw-r--   1 deaves   www           92 Sep  3  1997 comp_doc.gif
-rw-r--r--   1 deaves   www          771 Apr 14  1998 compaq.gif
-rw-r--r--   1 deaves   www         3811 Jan 29  1997 congrats.gif
-rw-r--r--   1 deaves   www         3634 Jan 25  2000 construction.gif
-rw-rw-r--   1 deaves   www         2011 Sep  9  1997 curbstone.gif
-rw-rw-r--   1 deaves   www         3013 Sep  3  1997 detective.gif
-rw-rw-r--   1 deaves   www           43 Sep  4  1997 dot_clear.gif
-rw-rw-r--   1 deaves   www         3506 Aug 12  1998 email6.gif
-rw-rw-r--   1 deaves   www         2221 Sep  9  1997 evalic.gif
-rw-rw-r--   1 deaves   www          102 Sep  3  1997 file_cab.gif
-rw-r--r--   1 deaves   www          341 Jan  8  1996 frus_logo.gif
-rw-r--r--   1 deaves   www          117 Jan  8  1996 frus_logo_sml.gif
-rw-rw-r--   1 deaves   www           96 Sep  3  1997 ftp.gif
-rw-rw-r--   1 deaves   www         1048 Sep  4  1997 handout.gif
-rw-rw-rw-   1 deaves   www        19338 Jul 23 12:51 hex-services.GIF
-rw-rw-r--   1 deaves   www           85 Sep  3  1997 home.gif
-rw-rw-rw-   1 deaves   www         3676 Jul 23 12:51 isc-name-blue.GIF
-rw-rw-rw-   1 deaves   www         1091 Jul 23 12:51 keyhole-logo4-sml.gif
-rw-rw-r--   1 deaves   www         1391 Sep  8  1997 keylock.gif
-rw-rw-r--   1 deaves   www         1938 Sep  5  1997 launcher.gif
-rw-rw-r--   1 deaves   www         1483 Sep  4  1997 license.gif
-rw-r--r--   1 deaves   www          232 Jan  9  1996 line.eyes.gif
-rw-r--r--   1 deaves   www         2334 Jan  8  1996 line.sun.gif
-rw-rw-r--   1 deaves   www          680 Sep  4  1997 log.gif
-rw-rw-r--   1 deaves   www         3354 Sep  3  1997 maduser.gif
-rw-r--r--   1 deaves   www         5383 Sep  3  1997 maduser.jpg
-rw-rw-r--   1 deaves   www           82 Sep  3  1997 mail.gif
-rw-rw-r--   1 deaves   www           95 Sep  3  1997 mail_in.gif
-rw-rw-r--   1 deaves   www           96 Sep  3  1997 mail_out.gif
-rw-rw-r--   1 deaves   www         2318 Sep  3  1997 mailbag.gif
-rw-r--r--   1 deaves   www         3156 Sep  3  1997 mailbag.jpg
-rw-r--r--   1 deaves   www         2065 Jul 19  1998 mailbox.jpg
-rw-rw-r--   1 deaves   www         1947 Sep  3  1997 masked.gif
-rw-rw-r--   1 deaves   www         1042 Sep  4  1997 mbox.gif
-rw-rw-r--   1 deaves   www         1661 Sep  4  1997 microscope.gif
-rw-r--r--   1 deaves   www         5259 Jan 29  1997 noenter.gif
-rw-rw-r--   1 deaves   www         2642 Sep  4  1997 nursemed.gif
-rw-rw-r--   1 deaves   www         1537 Sep  4  1997 passport.gif
-rw-r--r--   1 deaves   www         3275 Jul 19  1998 passport.jpg
-rw-rw-r--   1 deaves   www         2522 Sep  4  1997 pinchdollar.gif
-rw-rw-r--   1 deaves   www         1558 Sep  3  1997 police.gif
-rw-rw-r--   1 deaves   www          105 Sep  3  1997 postscrp.gif
-rw-rw-r--   1 deaves   www          766 Sep  4  1997 potofgold.gif
-rw-rw-r--   1 deaves   www         2166 Sep  3  1997 prisoner.gif
-rw-rw-r--   1 deaves   www         1854 Sep  3  1997 redlight.gif
-rw-rw-rw-   1 deaves   www         1929 Jul 23 17:01 rib_bar_eeeee4.gif
-rw-rw-r--   1 deaves   www          193 Sep  2  1997 rule01.gif
-rw-rw-r--   1 deaves   www         1407 Sep  9  1997 srclic.gif
```

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

```
-rw-rw-r--   1 deaves   www         1705 Sep  2  1997 stamp-out-spam.gif
-rw-rw-r--   1 deaves   www          661 Sep  4  1997 suggest.gif
-rw-rw-r--   1 deaves   www          661 Sep  4  1997 suggestbox.gif
-rw-r--r--   1 deaves   www         1164 Sep  3  1997 surrender.gif
-rw-r--r--   1 deaves   www         5053 Sep  3  1997 surrender.jpg

>  ls -al unused
total 594
drwxr-xr-x   2 deaves   www          512 Aug 23 15:48 .
drwxr-xr-x   3 deaves   www         1536 Oct 15 17:18 ..
-rw-r--r--   1 deaves   www         6110 Jul  2 10:25 activ.jpg
-rw-r--r--   1 deaves   www         9627 Jul  2 10:25 ak2.jpg
-rw-r--r--   1 deaves   www         3180 Jul  2 10:25 bastion-product.html
-rw-r--r--   1 deaves   www         4392 Jul  2 11:42 cert-inner.html
-rw-r--r--   1 deaves   www        48897 Jul  2 10:25 cert-work.ps
-rw-r--r--   1 deaves   www          937 Jul  2 10:25 frus_ad.html
-rw-r--r--   1 deaves   www         5468 Jul  2 10:25 nondisc.asc
-rw-r--r--   1 deaves   www        30498 Jul  2 10:25 nondisc.pcl
-rw-r--r--   1 deaves   www        32342 Jul  2 10:25 nondisc.ps
-rw-r--r--   1 deaves   www        10895 Jul  2 10:25 nondisc.wpd
-rw-r--r--   1 deaves   www        86462 Jul  2 10:25 policy.ps
-rw-r--r--   1 deaves   www         3649 Jul  2 10:25 product-sheet.html
-rw-r--r--   1 deaves   www         3279 Jul  2 10:25 rb1.gif
-rw-r--r--   1 deaves   www         6841 Jul  2 10:25 scat-t.jpg
-rw-r--r--   1 deaves   www         3649 Jul  2 10:25 secure-router-product.html
-rw-r--r--   1 deaves   www        32736 Jul  2 10:25 waiver.ps
-rw-r--r--   1 deaves   www         4003 Jul  2 10:25 waiver.txt
-rw-r--r--   1 deaves   www          543 Jul  2 10:25 weather.txt
```

Site server is set to resist mirroring applications: Pass – While conducting the audit, a traffic based DoS application cut off responses several times. The three sites were successfully mirrored with fewer threads, and therefore lower request frequency.

Robots.txt is set properly in each document root. Not pass – no robots.txt file is set

HTML contains no unintended name tags or comments: Not pass – minor problem in that all pages contain commented out left navigation bar item for quick-response-form.html, which submits to a URL for frus-answer.html. This latter returns a 405, resource not allowed. Other than that, and some obsolete and unused content, the revealed information looks clean.

HTML and Javascript are obfuscated or compressed: Not pass – not compressed, actually quite clearly written and easy to read.

If HTTPS, 128 encryption or better: Not applicable, no authentication for www.<web_site_name>.com

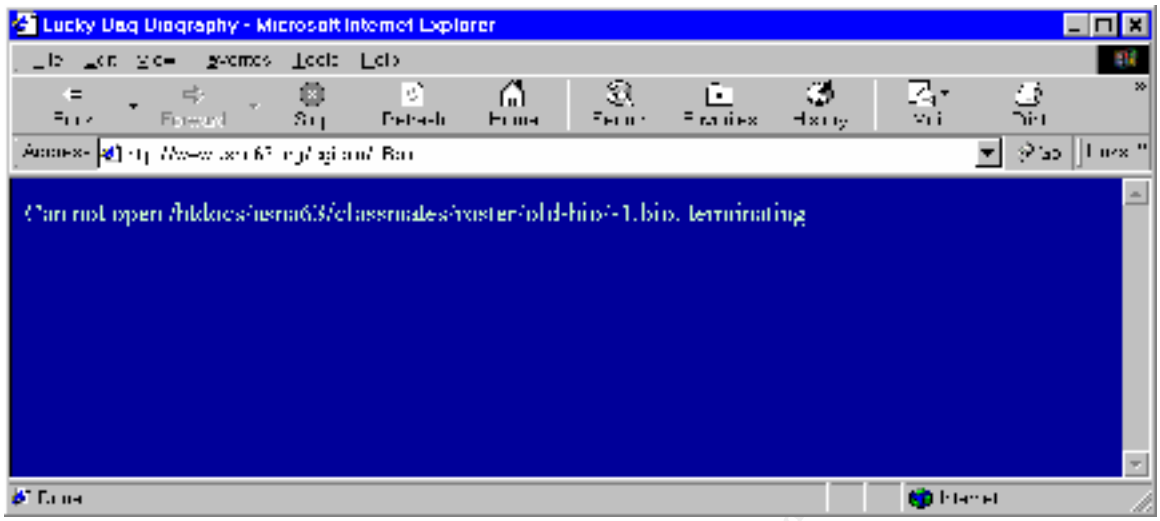
Application testing results:

www.<web_site_name>.com -- Pass, a simple site with only information and not even any forms logic, only links and static HTML. There is one form, quick-response.html that returns a 405, and has no links to it: this should be removed, and comments referring to it as well.

www.<private1>.com -- Pass, a simple site with only information, no forms, only links and static HTML, except for links to the site below, and one link to a CGI page that displays local weather readings.

www.<private2>.org -- Pass – See below
Forms have variables “Cur”, “Page”, “fini”, contact information such as addresses, data for HTTP MIME responses such as Have-sound and Have-RA. Cur and Page appear to be master identity indices, possibly used for session tracking (Cur), and user record indexing (Page). Responses to some boundary values indicate a mid-range database driven web application, but otherwise disclose little or no information. This database could probably be reverse engineered by examining a USNA Annapolis 1963 yearbook.

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



The variable Cur denotes the .bio file name used. The HTML from a yearbook bio was edited as text, and the value of Cur replaced with 0, -1, a 5000+ character string, and 999999999. One may be able to cause a stack overflow if the value can be spoofed with a large number of characters: attempting this shows that this input is truncated at 8 characters. Similar attempts with numbers and other variables show that good programming practices generally prevail within this site. No attempt at full path coverage was attempted since this site is not the property of Generic Services Corporation, and only represents a possible security exposure to the firm's own web site. Administrative functions have their own interface, which allows HTML editing, feedback approval, and email disposition. This uses basic authentication, and appears to be subject to brute force attack, but the system where these are hosted is at a separate virtual address, and appears to be firewalled off from all but a number of allowed addresses.

Browser cache does not cache private information: Pass. The related sites, www.<private1>.com and www.<privte2>.org do show biographic and similar private information, intentionally, but do not compromise any known client or customer information associated with www.<web_site_name>.com.

Certification Authority agency is trustworthy, only one session concurrently allowed: Not applicable, no authentication for www.<web_site_name>.com.

Method of certificate authentication is itself secure: Not applicable, no authentication for www.<web_site_name>.com.

If form based authentication, this submission is secure: Not applicable, no authentication for www.<web_site_name>.com.

If form based and secure, additional factor is used: Not applicable, no authentication for www.<web_site_name>.com.

If HTTP Basic authentication, then initially HTTPS: Not applicable, no authentication for www.<web_site_name>.com.

No mixed-scope authentication schemes: Not applicable, no authentication for www.<web_site_name>.com.

No concurrent authentication from different sources: Not applicable, no authentication for www.<web_site_name>.com.

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

Authentication error message does not allow for brute force attacks: Not applicable, no authentication for www.<web_site_name>.com.

Lockout of users upon too many failed authentication attempts: Not applicable, no authentication for www.<web_site_name>.com.

For heavy traffic sites, load balancing, sign-on timeouts work properly: Pass, prepared well for mid range traffic, even though low traffic currently – see below

Used webstripper to download 14.5 megs of data in about 25 minutes, with only two threads in use. Four or more threads caused a DoS lockout from the web server after more than about five minutes.

If auth used, then sign off does actually sign the user off. Not applicable, no authentication for www.<web_site_name>.com.

Application variables are encrypted or obfuscated: Not pass – any location or other tags are visible in the HTML, for the other two shared sites as well. Session tracking only exists for www.<private2>.org.

Any cookies with sensitive information are encrypted: Not applicable, no cookies used by www.<web_site_name>.com.

If there is authentication, and if session tracking can be predicted, different IP concurrency is not allowed: Pass, administrative interface on shared web application filters IP sources.

Session inactivity timeouts are short: Not applicable, no session authentication for www.<web_site_name>.com.

Form submissions are POST, not GET: Pass, no forms on www.<web_site_name>.com, but all shared web application forms are POST.

Web site allowing user input filters for harmful or malicious HTML: Pass – no user material is posted at www.<web_site_name>.com, but it is at www.<private2>.org, and an operator filters this for appropriate content.

Product specific vulnerabilities are specifically scanned for: Not pass: These would be buffer overflows in the Apache C API CGI modules, or Apache 1.2.6 vulnerabilities. We await a specialty checklist for that old a product, a server update, or a general CIS ruler for Apache.

Sniffing the SSH connection reveals no inappropriate information (in the case of ssh, that should be no information at all) is revealed in plaintext. Pass – see below

How to use hunt (http://lin.fsid.cvut.cz/~kra/) from command-line:

```
> ./hunt eth0
/*
 *      hunt 1.5
 *      multipurpose connection intruder / sniffer for Linux
 *      (c) 1998-2000 by kra
 */
starting hunt
--- Main Menu --- rcvpkt 0, free/alloc 63/64 ------
l/w/r) list/watch/reset connections
u)     host up tests
a)     arp/simple hijack (avoids ack storm if arp used)
s)     simple hijack
d)     daemons rst/arp/sniff/mac
```

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

```
o)     options
x)     exit
-> d
--- daemons --- rcvpkt 70, free/alloc 63/64 ------
r) reset daemon
a) arp spoof + arp relayer daemon
s) sniff daemon
m) mac discovery daemon
x) return
-dm> r
--- reset daemon --- rcvpkt 148, free/alloc 63/64 ------
s/k)   start/stop daemon
l)     list reset database
a/m/d) add/mod/del entry
x)     return
-rstd> s
rst daemon started
--- reset daemon --- rcvpkt 218, free/alloc 63/64 ---R---
s/k)   start/stop daemon
l)     list reset database
a/m/d) add/mod/del entry
x)     return
-rstd> x
--- daemons --- rcvpkt 277, free/alloc 63/64 ---R---
r) reset daemon
a) arp spoof + arp relayer daemon
s) sniff daemon
m) mac discovery daemon
x) return
-dm> s
--- sniff daemon --- rcvpkt 557, free/alloc 63/64 ---R---
s/k)   start/stop sniff daemon
l)     list sniff database   c) list sniff connection
a/m/d) add/mod/del sniff item
o)     options
x)     return
-sniff> l
--- sniff daemon --- rcvpkt 609, free/alloc 63/64 ---R---
s/k)   start/stop sniff daemon
l)     list sniff database   c) list sniff connection
a/m/d) add/mod/del sniff item
o)     options
x)     return
-sniff> a
src ip addr/mask ports [0.0.0.0/0]> 192.168.1.3
dst ip addr/mask ports [0.0.0.0/0]> 192.86.83.0/24
want to search for y/n [n]> n
log mode [s]rc/[d]st/[b]oth [b]> b
log bytes [64]>
log file name [by conn]> ssh-sniff.txt
insert at [0]>
--- sniff daemon --- rcvpkt 5245, free/alloc 63/64 ---R---
s/k)   start/stop sniff daemon
l)     list sniff database   c) list sniff connection
a/m/d) add/mod/del sniff item
o)     options
x)     return
-sniff> s
sniffer started
--- sniff daemon --- rcvpkt 5469, free/alloc 63/64 ---RS---
s/k)   start/stop sniff daemon
l)     list sniff database   c) list sniff connection
a/m/d) add/mod/del sniff item
o)     options
x)     return
```

The only actions done were as follows:

```
> ssh system1.wlk.com
deaves@system1.wlk.com's password:*******
```

© SANS Institute 2000 - 2002, Author retains full rights.

```
Last login Tue Dec 11 17:37:30 2001 from 12.236.57.nnn
No mail
Sun Microsystems Inc.  SunOS 5.5.1     Generic May 1996
hostname% hello
hello: Command not found
hostname% world
world: Command not found
hostname% exit
hostname% logout
Connection to system1.wlk.com closed
```

And the sniffed result is as follows. Note that even the initial prompts are encrypted using Diffie-Hellman, even before key exchange (after, in boldface).

```
192.168.1.3 [3443] <-- 192.86.83.nnn [22]
SSH-1.5-1.2.26[0xA]<ACTION bytes_logged=15>

192.168.1.3 [3443] --> 192.86.83.nnn [22]
SSH-1.5-OpenSSH_2.5.2p2[0xA]<ACTION bytes_logged=24>

192.168.1.3 [3443] <-- 192.86.83.nnn [22]
[0x0][0x0][0x1][0xB][0x0][0x0][0x0][0x0][0x0][0x2]n[0xD1]:v[0xBC][0x91][0xB8][0x81][0x0][
0x0][0x3][0x0][0x0][0x6]%[0x3][0x0][0xBF][0xB3]1[0x8F]E"[0x9D][0xBF][0xA1][0xE6][0x8E][0x
EA][0xCB]=|v[0x17][0xE1]\[0x90][0x14][0x93]l[0x0][0x9F][0x89][0x95][0xD5]l$>[0xB6][0xC5][
0x9E][0xB1][0x10]F[0xBF])[0x9E][0x89]=|[0xF4]0[0xC2]([0xCB]h[0x8C][0xA1][0xA6]M[0x15][0x9
3]C[0xCA][0x12]=WJY[0xD6][0xF9][0x7F][0x91][0x9A][0x97]$[0xFF][0xE9][0x98][0xE5][0xEC][0x
A1][0xBE][0x8B][0xB3][0xBC][0xB0][0x9D][0x9C][0xA0][0xE8][0xD8][0xCC][0x83][0xC1])[0x94][
0xB6][0xC0][0x19][0xE1]Q[0x8D][0x0][0x0][0x4][0x0][0x0][0x6]%[0x4][0x0][0xA8][0xF8][0x98]
[0xE6][0x8F]3[0x87][0xE4][[0xEC][0xB7][0xCA][0xC3][0xE0][0x8]u[0x2][0xC2][0xA2]Q[0x8A][0x
AE]{7[[0xB5]y6[0xA9][0x89][0x1E][0x4]Q[0x8D]y;[0xA9]I!j[0xE4][0xDA][0x8A][0xDF][0xF0]$RX[
0xF8]b-
[0x86]x[0xCB]tM[0xDF][0xF5][0xA1]o[0xE]]`[0x1F][0xA8][0x19][0xCD]R[0x14][0xB][0x1E][0x89]
[0x7F]-
[0xF0]2[0xAE]*CZK|[0xE0]CS.[0x9A][0xDB][0xEC]A[0x7F][0x15][0x2]d[0xEE]l[0xFF][0xF][0x9D][
0xB8]W[0xB1]b[0x1E]n[0x14][0xD2]a[0xCA][0xB7][0xE9]y[0xF3][0xEC][0xA0][0x1]p[0xDD]v[0xE0]
*[0x94][0xAA]_[0xF7][0xAB][0xAA][[0x0][0x0][0x0][0x2][0x0][0x0][0x0]N[0x0][0x0][0x0][0x1C
][0xB6][0xBC][0x14][0xF3]<ACTION bytes_logged=276>

192.168.1.3 [3443] --> 192.86.83.nnn [22]
[0x0][0x0][0x0][0x94][0x0][0x0][0x0][0x0][0x3][0x3]n[0xD1]:v[0xBC][0x91][0xB8][0x81][0x3]
[0xFE]8[0xD2][0x89]e[0x17][0xEC]7[0xC5][0xB8][0xD7]3[0xBA][0xD5][0x83][0x8B]k[0x1E][0xF][
0x1][0x92][0x9E][0xCB]1[0xD6][0x0]tfD[0xDE][0x93][0x83]xT[0x2][0xAC][0xA][0xD6]u[0xD8][0x
EE][0xB7][0xD9][0xE][0xAE][0xF7]_[0xB3][0xD]f[0xC0][0x0]KP'[0x18][0x0][0xE7][0xDF][0xCA][
0xF8][0xF][0xCE][0x9D][0xDC][0xA1]i[0xF][0xEB]W[0xF7]lBi{]&=[0xF7][0xDD]X[0x1E][0xC1][0xB
]M<[0x9D]C[0xE6]cRN[0xA0][0x9B]gW[0xA1][0x1A]d8[0x6][0x8][0x10][0xD3][0xF0]cLX[0xB5][0x9]
[0xDE][0xBD]/[0x14][0xDE][0xA6]v
[0xC6]s)v[0x96])[0xEE][0x8A][0xD9]@[0xD3][0x0][0x0][0x0][0x3][0xC4]][0x81][0x11]<ACTION
bytes_logged=156>

192.168.1.3 [3443] <-- 192.86.83.nnn [22]
[0x0][0x0][0x0][0x5][0x83]Cx[0xC9][0xC6]A[0xA5][0xAD]<ACTION bytes_logged=12>

192.168.1.3 [3443] --> 192.86.83.nnn [22]
[0x0][0x0][0x0][0xF][0xE7][0xD7][0xCA][0xA1][0x1D][0xF5]%[0x7F]8V[0xC4][0xE3][/[0xF3][0xC
E]<ACTION bytes_logged=20>

192.168.1.3 [3443] <-- 192.86.83.nnn [22]
[0x0][0x0][0x0][0x5]E[0x7]$[0x12][0xCC][0xCD]tm<ACTION bytes_logged=12>

192.168.1.3 [3443] --> 192.86.83.nnn [22]
[0x0][0x0][0x0])[0xC8][0xDF][0x1A][0xF9][0xC1]r[0x8A][0x8A][0x93][0xEF][0xB8][0x9A][0x0]Z
8[0xC3][0xB5]]][0x13][0xA3][0xAF]/[0xB7]k[0xA0]srV[0xFD][0xD7][0xB9]hP[0xD]2[0xC]M[0x9][0x
9A][0x98][0xE4][0x9][0x93][0xE0][0x1][0x85][0x8A][0x8]<ACTION bytes_logged=52>

192.168.1.3 [3443] <-- 192.86.83.nnn [22]
[0x0][0x0][0x0][0x5][0x14][0x81][0xC5][0xB1][0x17][0x0]c9<ACTION bytes_logged=12>

192.168.1.3 [3443] --> 192.86.83.nnn [22]
[0x0][0x0][0x0][0x8B]57[0x7][0x8A][0x19]ON#[0x9E][0xF1][0x1C]#[0xF7][0x1F]voh[0xEF]B[0xA9
]Y[0x10]'[0xAD][0xAF][0xCB]^[0xD7]D[0xA][0x14]Mf[0xE8]'[0x17]q[0x89][0x7][0x84][0x83]>[0x
```

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

```
F2][0xB6]K[0x15][0x93]P{[0xB4]kH[0xF2][0x11]p[0xDC]Ml[0xEE][0xBF]+jQ[0x9][0xB9][0xA0]`[0x
B9][0xEA][0xD0][0xD3][0xD1]f[0x83][0xED][0x5][0xD2][0xF7][0x1F]0[0x9B][0xB0][0xF1]sP[0xA8
][0xC4][0xD][0xF][0xAA][0xC7]%>[0xF2]}%n[0x17]9[0x86]![0xAB][0xA7]Q[0x13][0x88][0xA6]v[0x
8B][0xA7][0x9][0xA2][0xE0][0x9]scu[0xE3]N[0x95][0x9D]CD`FS[0xEE]{.[0xDD][0xA][0xD1][0xC5]
BYBz[0xFA]'[0x1F][0xDC]q[0xBC][0xDD]<ACTION bytes_logged=148>

192.168.1.3 [3443] <-- 192.86.83.nnn [22]
[0x0][0x0][0x0][0x5]m[0xC9][0xAE]0[0x97][0x99]>[0x86]<ACTION bytes_logged=12>

192.168.1.3 [3443] --> 192.86.83.nnn [22]
[0x0][0x0][0x0]Cjx[0xDE][0x1D]G[0xDC][0xED][0x9B]n[0xBA][0xA2][0xD1]C[0xF9][0xA6]F[0xF8][
0xE7][0xD4][0x9][0xA5]J[0xE0][0xFA]%[0x18][0x6]_[0x83]g[0x6][0x93][0x2][0x8E]![0xC2][0xC8
]|[0x1D]|[0xA5]e[0x15][0xF2]_[0xAB]0[0x86][0xF2][0xBD]([0x90][0x8A][0xC1]U6[0xF4][0x16][0
xA0]$m8o[0x97][0x85][0xAC][0xF7]h/[0x85]o[0x9D]<ACTION bytes_logged=76>

192.168.1.3 [3443] <-- 192.86.83.nnn [22]
[0x0][0x0][0x0][0x5]\[0x7]_[0xD7][0x10][0xFD][0x7][0x10]<ACTION bytes_logged=12>

192.168.1.3 [3443] --> 192.86.83.nnn [22]
[0x0][0x0][0x0][0x5][0xCB][0xE4][0xE3][0xEF][0x1D][0xC7][0xB4]~<ACTION bytes_logged=12>

192.168.1.3 [3443] <-- 192.86.83.nnn [22]
[0x0][0x0][0x0]C%[0xDB]uU[0x14][0x8E][0x89][0xE0]([0x9F]?[0x91][0x4][0x81]o[0x19][0xCB][0
xC2]Rw[0xFB][0xA4][0xB5][0xD][0x8E]2R[0xAC][0xB3][0x14][0xDB]zo1[0x9E]X[0xF0][0xFC][0xEB]
[0x93]3[0x8B].[0xBE]]pH[0xE2]%[0xF]R9[0x95][0x11][0xBD][0xFD][0x3][0x0]_[0x8][0xF9]{[0x16
][0x8E],[0x1C][0x17][0xBA]=[0x85][0xE7][0xB7]<ACTION bytes_logged=76>

192.168.1.3 [3443] <-- 192.86.83.nnn [22]
[0x0][0x0][0x0][0x13][0xD6][0xBE]F[0x9F]A[0xA][0x8D][0xC]U[0x2][0xBE]O[0xF0]f1[0xD9][0xD5
][0xE3]M[0x94][0xC1]P[0x1D][0xCB][0x0][0x0][0x0]C[0x92]J[0xB4][0xAB][0x1F][0xDB][0x2]{[0x
7F]L[0xB2]8[0xB8][0xAE]z:[0xB][0x88]E/[0x88][0xAA]h[0xE1]!p0z[0xF4][0x88]Q[0x12][0xC7][0x
D6][0xAC]_[0xC3][0xF4][0xDD][0x95][0xC4][0xFB][0xF7]c[0xC7][0x7F][0x10]O6-
[0x7]U[0x1F]Y[0x96][0x18][0xE6][0xCA][0xB1][0xC2]44"[0xE3][0xF4].0[0xC2][0xB4][0x86]'[0xF
6]<ACTION bytes_logged=104>

192.168.1.3 [3443] <-- 192.86.83.nnn [22]
[0x0][0x0][0x0][0x13][0xC2]Hj|[0x1C][0xD2][0x11]y;kF[0xFF]|3[0xF][0xAE]K.J&[0xFA][0x1A]n[
0x1B]<ACTION bytes_logged=28>

192.168.1.3 [3443] --> 192.86.83.nnn [22]
[0x0][0x0][0x0][0xA][0x6][0xB0][0xA]k[0xA0][0xD5]HP[0xA2][0xC3]D![0xB][0xB9]Y[0xDD][0x0][
0x0][0x0][0xA]u[0x91][0xD5][0x9][0xA3];[0x7][0xB1]K[0x96][0x17][0xEC][0x12]1[0x1][0xC]<AC
TION bytes_logged=40>

192.168.1.3 [3443] <-- 192.86.83.nnn [22]
[0x0][0x0][0x0][0xA][0xEA]c[0xC7][0x8E][0x15][0xD5]2[0xFE]{[0xF6][0xF1]3[0xB7][0xA3][0x8A
]l[0x0][0x0][0x0][0xA]im[0x16][0xFF][0x90][0xD9][0xED][0xC3][0x8F]G[0xDF][0x12][0xF6]F[0x
D5]+<ACTION bytes_logged=40>

192.168.1.3 [3443] --> 192.86.83.nnn [22]
[0x0][0x0][0x0][0xA][0x1E][0x5][0xCE][0x6][0x9D]RJLJ=4[0x8B]B[0xD]/[0xD5]<ACTION
bytes_logged=20>

192.168.1.3 [3443] <-- 192.86.83.nnn [22]
[0x0][0x0][0x0][0xA][0xC4]M[0xE8]'[0xA2][0x8B]5N[0xB3]4[0xC6]^[0x94]h[0xED]V<ACTION
bytes_logged=20>

192.168.1.3 [3443] --> 192.86.83.nnn [22]
[0x0][0x0][0x0][0xA][0xC2]VB[0xB3]fs[0xCF]I[0xEB][0xE2][0xF8]L$[0xB9][0xA3][0x9A]<ACTION
bytes_logged=20>

192.168.1.3 [3443] <-- 192.86.83.nnn [22]
[0x0][0x0][0x0][0xA][0xE6][0x97][0xB7][0xC7]J[0x0][0x14]G[0x15][0x84][0xE][0x9F][0x9D][0x
9][0xB7][0x96]<ACTION bytes_logged=20>

192.168.1.3 [3443] --> 192.86.83.nnn [22]
[0x0][0x0][0x0][0xA][0x8E]<[0xF7][0xA]C[0x7][0xF7][0xB]t[0xF9][0xF2]G[0xD7]D[0xA9]d<ACTIO
N bytes_logged=20>

192.168.1.3 [3443] <-- 192.86.83.nnn [22]
```

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

```
[0x0][0x0][0x0][0xA][0xB][0x6][0xD]u=[0xEB]]]X"O,p[0x8][0x19][0x80]<ACTION
bytes_logged=20>

192.168.1.3 [3443] --> 192.86.83.nnn [22]
[0x0][0x0][0x0][0xA][0xD7][0xCB][0xF1]7[0xF][0xC0][0xC8][0xE0][0x0]yq#@#&[0xFD]<ACTION
bytes_logged=20>

192.168.1.3 [3443] <-- 192.86.83.nnn [22]
[0x0][0x0][0x0]/[0x8A][0xA2]i[0x7F]FW[0xB8]o[0xB7][0xAA]|[0xA4]l2[0xE3]A([0xF][0x8F][0xE4
][0xA1][0xDC][0xB8][0x9F]f[0xC8]G
[0xF1]?[0x16]#[0x83][0xCD][0x9C][0xB1][0xC8][0xF][0xB8][0xE6][0xCE]fsA[0xDB][0xCB]I'<ACTI
ON bytes_logged=52>

192.168.1.3 [3443] --> 192.86.83.nnn [22]
[0x0][0x0][0x0][0xA][0xB5]&[0xDE]a [0x17]z[0x91][0xE]-
}[0xAF][0x6][0x96]2[0xEF][0x0][0x0][0x0][0xA]??[0xC][0x9C][0xCC][0x8A]I[0x2]f[0x9E]/[0xE2
][0xA4][0xE2][0xB6][0xD1]<ACTION bytes_logged=40>

192.168.1.3 [3443] <-- 192.86.83.nnn [22]
[0x0][0x0][0x0][0xA][0xE6][0xC3]}zk[0xCC][0xD2][0xAB][0xA3]Z[0xBB]}[0xA1]P[0xE5][0xA8][0x
0][0x0][0x0][0xA][0xE1]X[0xE5][0x85]([0xAE][0x7F]G[0x98]q[0x4][0xCB][0xB2][0xE7]\U<ACTION
bytes_logged=40>

192.168.1.3 [3443] --> 192.86.83.nnn [22]
[0x0][0x0][0x0][0xA]w[0xF7]y[0xA6][0xC9][0xEF][0x6][0xD2][0xC0][0xE1][0xC5][0xC5][0xB6]*[
0xC]&[0x0][0x0][0x0][0xA]\[0xD9][0xB5][0x15][0xC7]7[0x1B][0x8E][0x1A][0xBE]8b[0xC0]5[0x1B
][0xD9]<ACTION bytes_logged=40>

192.168.1.3 [3443] <-- 192.86.83.nnn [22]
[0x0][0x0][0x0][0xA]-
[0xCA][0xA9][0xAB][0xDF]f[0xCF][0x86][0x9F]w[0x81]~9[0xB1]H[0x93][0x0][0x0][0x0][0xA][0x9
C]6[0xA4]U>F@}n[0xF8][0x8C]C[0xCD]0[0x15][0xB]<ACTION bytes_logged=40>

192.168.1.3 [3443] --> 192.86.83.nnn [22]
[0x0][0x0][0x0][0xA]BdQ[0x98][0xF4]`[0x97]V-[0x1F]b[0x94][0x97]"G[0xAA]<ACTION
bytes_logged=20>

192.168.1.3 [3443] <-- 192.86.83.nnn [22]
[0x0][0x0][0x0]/K[0xCF]
,[0xDD][0x1C][0x1D][0x1E][0xB6]1[0xF0][0xE5][0x85]&Q[0xC0][0x9A];[0xB]:D[0x11]5[0x1D][0xB
0][0xC8][0xEF][0xBD]\[0x83][0x8B][0xA4][0x94][0xAD].[0xED][0xA2][0xD8]{[0xF6][0xD8]u[0xB6
][0xA1]f[0x12][0xDC][0xF5]<ACTION bytes_logged=52>

192.168.1.3 [3443] --> 192.86.83.nnn [22]
[0x0][0x0][0x0][0xA]w[0xEE][0xAB][0xB4][0x6]+[0x9F]e[0xE9]@[0xD7]5[0x4][AR[0x0][0x0][0x0]
[0xA].[0xC5]{[0xD][0xB7]M}[0x15][0xC0]9[0x88][0xEB]-
D|[0x1F][0x0][0x0][0x0][0xA]w[0xEE][0xAB][0xB4][0x6]+[0x9F]e[0xE9]@[0xD7]5[0x4][AR[0x0][0
x0][0x0][0xA].[0xC5]{[0xD][0xB7]M}[0x15][0xC0]9[0x88][0xEB]-D|[0x1F]<ACTION
bytes_logged=80>

192.168.1.3 [3443] <-- 192.86.83.nnn [22]
[0x0][0x0][0x0][0xA][0xDB][0xD7][0xFA][0x9B][0xE]R[0xAE][0xEB]lt[0xD1][0xD1]m[0xE0]A[0x12
][0x0][0x0][0x0][0xA][0x93]j[0xB2][0xF9]'7R[0xCC][0xF2][0xC2]|[0xE9][0x94][0x97][0xA5]2<A
CTION bytes_logged=40>

192.168.1.3 [3443] --> 192.86.83.nnn [22]
[0x0][0x0][0x0][0xA]p[0xD3]([0xA][0xAA][0x94][0x88][0xA6][0xCB][0xFC][0x7F][0xB0]_[0xFD][
0x98][0xA8]<ACTION bytes_logged=20>

192.168.1.3 [3443] <-- 192.86.83.nnn [22]
[0x0][0x0][0x0][0xA]M|[0x6][0x7]S4[0xC3]%w}[0xE1][0x86][0xCF],[0x8D][0xF9]<ACTION
bytes_logged=20>

192.168.1.3 [3443] --> 192.86.83.nnn [22]
[0x0][0x0][0x0][0xA][0xAD]k[0xA8][0xB9]@[0x6]1[0xFA]Cy[0xB8][0xD4]e_[0xC4]5<ACTION
bytes_logged=20>

192.168.1.3 [3443] <-- 192.86.83.nnn [22]
[0x0][0x0][0x0][0xA][0xF6][0xC6]s+[0x2][0xC6][0xAD]w3[0xDA]sS[0x5][0x83][0xBD][0xE]<ACTIO
N bytes_logged=20>
```

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

```
192.168.1.3 [3443] <-- 192.86.83.nnn [22]
[0x0][0x0][0x0][0x1D][0x4][0xCD]J[0xA0][0xEA])![0x3]j[0x87][0xB6][0x87]0[0xD9][0xB0][0x82
][0x99][0x84][0x15]4T[0xDC][0xB6](*W[0xA1]a[0x3][0xD2]G'[0x0][0x0][0x0][0x9][0xFC]f-
Q[0xAD][0x82][0xF1][0xCF]7u[0x80]g[0x88][0x9D]@[0xB2]<ACTION bytes_logged=56>

192.168.1.3 [3443] --> 192.86.83.nnn [22]
[0x0][0x0][0x0][0x5][0xD8]y[0xCF]KG[0xBF][0xB]G<ACTION bytes_logged=12>
```

Pass: SSH appears to be actually secure, mostly unprintable characters.

Server request logs are monitored and responded to: Pass – web access logs are distributed daily to clients. Traffic is relatively low, less than twenty independent hits per day, which allows informal usage adaptation, and DoS and surveillance detection. The automated traffic based DoS prevention system seems likely to protect against any but a widely distributed DoS attack.

Scoring note: Since there are no secure features, checklist items involving HTTPS, authentication, and cookies should not be counted in the scoring denominator.

Summary of Remedies, in order of subjective estimate of cost/time, and triaged:

Actions taken during the course of the audit:

1) Directory viewing turned off for www.<web_site_name>.com

Remedial actions to be taken:

2) Scan Apache for Apache 1.2.6 specific vulnerabilities
3) Update Apache and/or obscure its banner
4) Correctly place the robots.txt file
5) Remove quick-response-form.html comments
6) Compress/obfuscate HTML and form variables

Lower priority:

7) Run Solaris CIS ruler for added internal security assurance
8) Update SSH

Final Audit for Remote system #1 was conducted December 12, 2001, and no claim is made here for the condition of this system on any date after that.

Supporting matrixes for risk mitigation analysis follow:

Failed checklist items represent risks of damage, times annual frequency/likelihood of a related exploit that could otherwise be prevented. These are subjective estimates provided by the management, whose assistance was invaluable in preparing this report.

	Scan Apache: Apache exploits	Update/obscure Apache: Apache exploits	Robots.txt: Crawlers, DoS, surveillance	Remove comments: Surveillance	Compress HTML: Surveillance
Remote system #1	1.0	1.0	0.1	0.1	0.1

Assumptions are that use of known Apache exploits is common and frequent, and when used that they can give root access, with possibility of root kit and system compromise if successful. Surveillance involves relatively minimal harm/disclosure, although it could occur frequently. Crawlers can also increase legitimate site traffic, which mitigates the risks from surveillance. It is unknown here whether there are any known Apache 1.2.6 exploits that were only fixed in subsequent Apache versions and never patched in 1.2.6. This represents a research project outside the scope of this IT audit. Alternatively the Apache version could simply be updated.

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

Appendix E: Benchmark and Matrixes, Remote system #2

The assessment of remote system #2 includes a checklist-of-checklists for the system generally. The system hosts email services here for Generic Services Corporation, and runs both IMAP and SMTP services. There should be, as described in Part I, an internal vulnerability scan using the CIS Solaris ruler, an external vulnerability scan conducted using nessus from the local system, and a sniff of the actual IMAP sessions to make sure they do not disclose anything inappropriate in plaintext.

The CIS Solaris ruler measurement (internal vulnerability report):

The network owner was reticent to allow permission for such an internal procedure to be run, considering that it requires root access to be made and executed. Not pass.

SSH/IMAP/SMTP host (IP ending octets edited out):

```
Nessus Scan Report
------------------



SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 0
 - Number of security warnings found : 3
 - Number of security notes found : 3



TESTED HOSTS

 192.86.83.nnn (Security warnings found)



DETAILS

+ 192.86.83.nnn :
 . List of open ports :
   o general/udp (Security notes found)
   o ssh (22/tcp) (Security warnings found)
   o telnet (23/tcp) (Security notes found)
   o smtp (25/tcp) (Security warnings found)
   o general/tcp (Security warnings found)

 . Information found on port general/udp


    For your information, here is the traceroute to 192.86.83.nnn :
    ?

 . Warning found on port ssh (22/tcp)



    You are running a version of SSH which is
    older than (or as old as) version 1.2.27.

    If you compiled ssh with kerberos support,
    then an attacker may eavesdrop your users
    kerberos tickets, as sshd will set
    the environment variable KRB5CCNAME to
    'none', so kerberos tickets will be stored
```

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

```
   in the current working directory of the
   user, as 'none'.

   If you have nfs/smb shared disks, then an attacker
   may eavesdrop the kerberos tickets of your
   users using this flaw.

   ** If you are not using kerberos, then
   ignore this warning.

   Risk factor : Serious
   Solution : use ssh 1.2.28 or newer
   CVE : CAN-2000-0575

. Information found on port telnet (23/tcp)


   Remote telnet banner :
   ÿ¯$


. Warning found on port smtp (25/tcp)



   The remote SMTP server is vulnerable to a redirection
   attack. That is, if a mail is sent to :

              user@hostname1@victim

   Then the remote SMTP server (victim) will happily send the
   mail to :
              user@hostname1

   Using this flaw, an attacker may route a message
   through your firewall, in order to exploit other
   SMTP servers that can not be reached from the
   outside.

   *** THIS WARNING MAY BE A FALSE POSITIVE, SINCE
       SOME SMTP SERVERS LIKE POSTFIX WILL NOT
       COMPLAIN BUT DROP THIS MESSAGE ***


   Solution : if you are using sendmail, then at the top
   of ruleset 98, in /etc/sendmail.cf, insert :
   R$*@$*@$*       $#error $@ 5.7.1 $: '551 Sorry, no redirections.'

   Risk factor :
    Low


. Information found on port smtp (25/tcp)


   Remote SMTP server banner :
   0
   220-system2.WLK.Com[192.86.83.nnn] SPAM is not welcome220 ESMTP spoken here.

   214-Commands

   214-HELO  EHLO  MAIL  RCPT  RSET  ONEX

   214 VERB  DATA  NOOP  QUIT  HELP  VERB


. Warning found on port general/tcp



   The remote host uses non-random IP IDs, that is, it is
```

© SANS Institute 2000 - 2002, Author retains full rights.

```
    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 if the remote
    host sent a packet in reply to another request. This may be
    used for portscanning and other things.

    Solution : Contact your vendor for a patch
    Risk factor :
     Low




-------------------------------------------------------
This file was generated by the Nessus Security Scanner
```

Pass: Unexpectedly, SSH was found operating on this machine as well as the designated SSH host on remote system #1. However, it appears to be the same version of SSH as remote system #1 and passes on the same criteria. A sniffed SSH session is shown in the last checklist, to compare to the sniffed IMAP session originally called for.

And the sniffed result is as follows. Note that the password exchange (boldface) appears to be at least hashed, if not strongly encrypted, although the contents are not encrypted using IMAP only for authentication. This is a simple email authentication and download:

```
192.168.1.3 [3604] <-- 192.86.83.250 [143]
* OK news IMAP4rev1 v12.264 server ready[0xD][0xA]<ACTION bytes_logged=22>

192.168.1.3 [3604] --> 192.86.83.250 [143]
00000000 CAPABILITY[0xD][0xA]<ACTION bytes_logged=21>

192.168.1.3 [3604] <-- 192.86.83.250 [143]
* CAPABILITY IMAP4 IMAP4REV1 NAMESPACE IDLE SCAN SORT MAILBOX-REFERRALS LOGIN-REFERRALS
AUTH=LOGIN THREAD=ORDEREDSUBJECT[0xD][0xA]00000000 OK CAPABILITY
completed[0xD][0xA]<ACTION bytes_logged=156>

192.168.1.3 [3604] --> 192.86.83.250 [143]
00000001 AUTHENTICATE LOGIN[0xD][0xA]<ACTION bytes_logged=29>

192.168.1.3 [3604] <-- 192.86.83.250 [143]
+ VXNlciBOYWllAA==[0xD][0xA]<ACTION bytes_logged=20>

192.168.1.3 [3604] --> 192.86.83.250 [143]
ZGVidmVz[0xD][0xA]<ACTION bytes_logged=10>

192.168.1.3 [3604] <-- 192.86.83.250 [143]
+ UBZzc3dvcmQA[0xD][0xA]<ACTION bytes_logged=16>

192.168.1.3 [3604] --> 192.86.83.250 [143]
TGFCc2BSQjg7Lg==[0xD][0xA]<ACTION bytes_logged=18>

192.168.1.3 [3604] <-- 192.86.83.250 [143]
00000001 OK AUTHENTICATE completed[0xD][0xA]<ACTION bytes_logged=36>

192.168.1.3 [3604] --> 192.86.83.250 [143]
00000002 CAPABILITY[0xD][0xA]<ACTION bytes_logged=21>

192.168.1.3 [3604] <-- 192.86.83.250 [143]
* CAPABILITY IMAP4 IMAP4REV1 NAMESPACE IDLE SCAN SORT MAILBOX-REFERRALS LOGIN-REFERRALS
AUTH=LOGIN THREAD=ORDEREDSUBJECT[0xD][0xA]00000002 OK CAPABILITY
completed[0xD][0xA]<ACTION bytes_logged=156>

192.168.1.3 [3604] --> 192.86.83.250 [143]
00000003 SELECT INBOX[0xD][0xA]<ACTION bytes_logged=23>

192.168.1.3 [3604] <-- 192.86.83.250 [143]
```

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

```
* 36 EXISTS[0xD][0xA]* 0 RECENT[0xD][0xA]* OK [UIDVALIDITY 995566850] UID validity
status[0xD][0xA]* OK [UIDNEXT 379] Predicted next UID[0xD][0xA]* FLAGS (\Answered
\Flagged \Deleted \Draft \Seen)[0xD][0xA]* OK [PERMANENTFLAGS (\* \Answered \Flagged
\Deleted \Draft \Seen)] Permanent flags[0xD][0xA]00000003 OK [READ-WRITE] SELECT
completed[0xD][0xA]<ACTION bytes_logged=294>

192.168.1.3 [3604] --> 192.86.83.250 [143]
00000004 FETCH 1:36 (UID INTERNALDATE RFC822.SIZE FLAGS)[0xD][0xA]<ACTION
bytes_logged=58>

192.168.1.3 [3604] <-- 192.86.83.250 [143]
* 1 FETCH (UID 253 INTERNALDATE " 1-Nov-2001 09:09:00 -0600" RFC822.SIZE 5554 FLAGS
(\Seen))[0xD][0xA]* 2 FETCH (UID 258 INTERNALDATE " 2-Nov-2001 19:30:20 -0600"
RFC822.SIZE 5499 FLAGS (\Seen))[0xD][0xA]* 3 FETCH (UID 259 INTERNALDATE " 2-Nov-2001
19:42:07 -0600" RFC822.SIZE 2471 FLAGS (\Seen \Answered))[0xD][0xA]* 4 FETCH (UID 266
INTERNALDATE " 5-Nov-2001 16:22:12 -0600" RFC822.SIZE 17881 FLAGS (\Seen))[0xD][0xA]* 5
FETCH (UID 269 INTERNALDATE " 6-Nov-2001 15:49:32 -0600" RFC822.SIZE 3630 FLAGS
(\Seen))[0xD][0xA]* 6 FETCH (UID 272 INTERNALDATE " 7-Nov-2001 13:38:10 -0600"
RFC822.SIZE 32752 FLAGS (\Seen))[0xD][0xA]* 7 FETCH (UID 273 INTERNALDATE " 7-Nov-2001
16:15:16 -0600" RFC822.SIZE 14828 FLAGS (\Seen))[0xD][0xA]* 8 FETCH (UID 276 INTERNALDATE
" 8-Nov-2001 15:15:25 -0600" RFC822.SIZE 19811 FLAGS (\Seen))[0xD][0xA]* 9 FETCH (UID 280
INTERNALDATE " 9-Nov-2001 09:32:16 -0600" RFC822.SIZE 3073 FLAGS (\Seen))[0xD][0xA]* 10
FETCH (UID 281 INTERNALDATE " 9-Nov-2001 19:36:36 -0600" RFC822.SIZE 7011 FLAGS (\Seen
\Answered))[0xD][0xA]* 11 FETCH (UID 282 INTERNALDATE " 9-Nov-2001 21:19:52 -0600"
RFC822.SIZE 25116 FLAGS (\Seen))[0xD][0xA]* 12 FETCH (UID 285 INTERNALDATE "10-Nov-2001
13:04:48 -0600" RFC822.SIZE 3203 FLAGS (\Seen))[0xD][0xA]* 13 FETCH (UID 290 INTERNALDATE
"12-Nov-2001 16:09:08 -0600" RFC822.SIZE 5422 FLAGS (\Seen))[0xD][0xA]* 14 FETCH (UID 291
INTERNALDATE "12-Nov-2001 19:48:22 -0600" RFC822.SIZE 14231 FLAGS (\Seen))[0xD][0xA]* 15
FETCH (UID 294 INTERNALDATE "13-Nov-2001 09:55:12 -0600" RFC822.SIZE 5399 FLAGS
(\Seen))[0xD][0xA]* 16 FETCH (UID 29<ACTION bytes_logged=1460>

192.168.1.3 [3604] <-- 192.86.83.250 [143]
7 INTERNALDATE "14-Nov-2001 11:20:00 -0600" RFC822.SIZE 19729 FLAGS (\Seen))[0xD][0xA]*
17 FETCH (UID 298 INTERNALDATE "14-Nov-2001 14:54:49 -0600" RFC822.SIZE 2903 FLAGS (\Seen
\Answered))[0xD][0xA]* 18 FETCH (UID 299 INTERNALDATE "14-Nov-2001 19:19:24 -0600"
RFC822.SIZE 4181 FLAGS (\Seen \Answered))[0xD][0xA]* 19 FETCH (UID 302 INTERNALDATE "15-
Nov-2001 12:49:42 -0600" RFC822.SIZE 2062 FLAGS (\Seen))[0xD][0xA]* 20 FETCH (UID 305
INTERNALDATE "15-Nov-2001 15:21:42 -0600" RFC822.SIZE 15767 FLAGS (\Seen))[0xD][0xA]* 21
FETCH (UID 318 INTERNALDATE "20-Nov-2001 14:46:52 -0600" RFC822.SIZE 10423 FLAGS
(\Seen))[0xD][0xA]* 22 FETCH (UID 321 INTERNALDATE "21-Nov-2001 16:31:45 -0600"
RFC822.SIZE 7712 FLAGS (\Seen))[0xD][0xA]* 23 FETCH (UID 322 INTERNALDATE "21-Nov-2001
16:52:52 -0600" RFC822.SIZE 17877 FLAGS (\Seen))[0xD][0xA]* 24 FETCH (UID 327
INTERNALDATE "23-Nov-2001 08:46:45 -0600" RFC822.SIZE 12220 FLAGS (\Seen))[0xD][0xA]* 25
FETCH (UID 332 INTERNALDATE "25-Nov-2001 16:42:41 -0600" RFC822.SIZE 3113 FLAGS (\Seen
\Answered))[0xD][0xA]* 26 FETCH (UID 337 INTERNALDATE "27-Nov-2001 19:37:35 -0600"
RFC822.SIZE 7342 FLAGS (\Seen))[0xD][0xA]* 27 FETCH (UID 340 INTERNALDATE "28-Nov-2001
15:30:51 -0600" RFC822.SIZE 16336 FLAGS (\Seen))[0xD][0xA]* 28 FETCH (UID 341
INTERNALDATE "28-Nov-2001 17:19:39 -0600" RFC822.SIZE 3614 FLAGS (\Seen
\Answered))[0xD][0xA]* 29 FETCH (UID 344 INTERNALDATE "29-Nov-2001 19:16:39 -0600"
RFC822.SIZE 15217 FLAGS (\Seen))[0xD][0xA]* 30 FETCH (UID 345 INTERNALDATE "29-Nov-2001
19:53:50 -0600" RFC822.SIZE 19528 FLAGS (\Seen))[0xD][0xA]* 31 <ACTION bytes_logged=1460>

192.168.1.3 [3604] <-- 192.86.83.250 [143]
FETCH (UID 348 INTERNALDATE "30-Nov-2001 17:02:33 -0600" RFC822.SIZE 39043 FLAGS
(\Seen))[0xD][0xA]* 32 FETCH (UID 359 INTERNALDATE " 5-Dec-2001 09:53:59 -0600"
RFC822.SIZE 15598 FLAGS (\Seen))[0xD][0xA]* 33 FETCH (UID 362 INTERNALDATE " 6-Dec-2001
15:38:44 -0600" RFC822.SIZE 20999 FLAGS (\Seen))[0xD][0xA]* 34 FETCH (UID 373
INTERNALDATE "11-Dec-2001 08:36:22 -0600" RFC822.SIZE 3059 FLAGS (\Seen))[0xD][0xA]* 35
FETCH (UID 375 INTERNALDATE "11-Dec-2001 18:02:58 -0600" RFC822.SIZE 6586 FLAGS
(\Seen))[0xD][0xA]* 36 FETCH (UID 378 INTERNALDATE "12-Dec-2001 12:55:15 -0600"
RFC822.SIZE 12339 FLAGS (\Seen))[0xD][0xA]00000004 OK FETCH completed[0xD][0xA]<ACTION
bytes_logged=598>

192.168.1.3 [3604] --> 192.86.83.250 [143]
00000005 FETCH 1,2:21 (ENVELOPE BODY.PEEK[HEADER.FIELDS (Path Message-ID Content-Type
Newsgroups Followup-To References)] FLAGS)[0xD][0xA]<ACTION bytes_logged=130>

192.168.1.3 [3604] <-- 192.86.83.250 [143]
* 1 FETCH (ENVELOPE ("1 Nov 2001 10:07:14 -0500" "48 hours left to SAVE for LinuxWorld
Conference & Expo!" (("LinuxWorld" NIL "J24049-R19414" "iqmailer.net")) (("LinuxWorld"
NIL "J24049-R19414" "iqmailer.net")) ((NIL NIL "J24049-R19414" "iqmailer.net")) ((NIL NIL
```

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

```
"deaves" "internet-security-corp.com")) NIL NIL NIL
"<CRISMTP4E2FGwQ21ju200005df3@mail4.iqmailer.net>") BODY[HEADER.FIELDS ("PATH" "MESSAGE-
ID" "CONTENT-TYPE" "NEWSGROUPS" "FOLLOWUP-TO" "REFERENCES")] {112}[0xD][0xA]Content-Type:
text/plain; charset="iso-8859-1"[0xD][0xA]Message-ID:
<CRISMTP4E2FGwQ21ju200005df3@mail4.iqmailer.net>[0xD][0xA][0xD][0xA] FLAGS
(\Seen))[0xD][0xA]* 2 FETCH (ENVELOPE ("Fri, 2 Nov 2001 20:27:36 -0500 (EST)" "Re:
Surveillance from VNCyber -- no permission -- illegal (B-TSI-004021748)" (("UUNET
Internet Abuse Investigations" NIL "nobody" "UU.NET")) (("UUNET Internet Abuse
Investigations" NIL "nobody" "UU.NET")) ((NIL NIL "nobody" "UU.NET")) (("David M Eaves"
NIL "deaves" "internet-security-corp.com")) NIL NIL {96}[0xD][0xA]Your message of "Fri, 2
Nov 2001 11:48:38 -0800 (PST)" <<20011102194847.04B5925ED@news.wlk.com>>
"<QQlnmb15779.200111030127@iaremedy.corp.us.uu.net>") BODY[HEADER.FIELDS ("PATH"
"MESSAGE-ID" "CONTENT-TYPE" "NEWSGROUPS" "FOLLOWUP-TO" "REFERENCES")]
{66}[0xD][0xA]Message-Id:
<QQlnmb15779.200111030127@iaremedy.corp.us.uu.net>[0xD][0xA][0xD][0xA] FLAGS
(\Seen))[0xD][0xA]* 3 FETCH (ENVELOPE ("Fri, 2 Nov 2001 19:41:52 -0600 (CST)" "Re: Can I
pick your brain a sec?" (("Bob_Tracy" NIL "rct" "yowza.bogus1.wlk.com")) (("Bob_T<ACTION
bytes_logged=1460>

etc…
```

Pass: IMAP by itself, without SSH, does not encrypt email, only authenticates securely.

Summary of Remedies, in order of subjective estimate of cost/time, and triaged:

Remedial actions to be taken:

1. Update IMAP to more secure version

Lower priority:

2. Run Solaris CIS ruler for added internal security assurance
3. Update SSH

Final Audit for Remote system #2 was conducted December 13, 2001, and no claim is made here for the condition of this system on any date after that.

Supporting matrixes for risk mitigation analysis follow:

Failed checklist items represent risks of damage, times annual frequency/likelihood of a related exploit that could otherwise be prevented. These are subjective estimates provided by the management, whose assistance was invaluable in preparing this report.

	Update IMAP: IMAP exploits
Remote system #2	0.05

Assumptions are that this single source of vulnerability involves compromising one or more upstream routers to perform a man-in-the-middle attack, spoofing the source IP address to be able to pass through the firewall, provisioned per POPn/IMAP client IP address. This is unlikely, although if it were possible, a simple IMAP overflow exploit could gain access; further root or privileged access is unknown and would likely be protected. Updating imapd would not significantly mitigate risks to email information, given that it can be sniffed anyway if not additionally encrypted.

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

Appendix F: Overall Value-at-Risk Mitigation Matrix

The assets are from Part II, The Audit, section C, the list of IT assets. The assets by systems matrix is shown here, ***O***. (Matrix math done in Excel)

		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	0	0
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	0	[illegible]
[illegible]	[illegible]	0	[illegible]	[illegible]	[illegible]	0
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	0	0
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	50	[illegible]	[illegible]	0	0
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	0	[illegible]	[illegible]	0	0
[illegible]	[illegible]	0	[illegible]	[illegible]	0	0
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	0	[illegible]	[illegible]	0	0

Since there are many remedial measures, some of which apply to multiple systems (a UPS for example), but most of which apply to individual systems, the systems by risks, or "damage done" matrix, ***D***, and risks by remedies matrix, ***F***, will be quite large. In this simple case, no effort is made to separate risks from remedies, and the analysis is checklist-driven. When the analysis is checklist-driven, each item not passed represents its own risk, and correction is its remedy. In this case, the risks by remedies matrix, ***F***, is the identity matrix, and ***D*** x ***F*** = ***D***. This matrix, ***D***, is shown following, compiled from Appendixes A through F:

This matrix, (***D*** x ***F***), must be multiplied on the left by the assets matrix shown before, ***O***, to see the value at risk mitigation matrix, ***V***, described in the first part. The Value-at-Risk Mitigation is also shown on the next page. The sum row at the bottom (on the right) is a rough measure of the value at risk mitigated by each corrective measure, in thousands of dollars annually.

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

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

As can be seen above, Email records, Passwords, and Web site assets face the most risk in dollar-value terms that can be mitigated, while the premises protection, UPS, compromise recovery, and Windows 98 system logging remedies appear to be of the largest value in protecting IT assets. The setuid/setgid issues and pagefile clearing appear to be probably worthwhile, while the other measures are less valuable.

The large value mitigated by the UPS may be partly due to double counting independent benefits accruing to both systems #1 and #2. Even if this were adjusted for by dividing by two, it would still be one of the more beneficial corrective measures in gross terms.

The sum-row at the bottom is a rough indication of the dollar value of risk (in thousands of dollars) that any given measure will tend to mitigate during the course of a year. When the assumption that risks and remedies are independent of each other is relaxed it should be understood that some corrective measures will duplicate each other's efforts, and value at risk avoided will be less than the sum of the columns. (In plain language, the columns can tend to double-count the risk reductions, especially when the assets would be saved from total or near total losses from different risks).

© SANS Institute 2000 - 2002, Author retains full rights.

Last Updated: April 28th, 2017

Upcoming Training

SANS Secure Europe 2017	**Amsterdam, Netherlands**	**Jun 12, 2017 - Jun 20, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**