Global Information Assurance Certification Paper

GCUX Practical Assignment Version 1.9, Option 2

Security Analysis of GIAC Enterprises Database Server

Submitted by: Rodney R. Anderson
Date: December 25, 2003

Abstract

System and network security is a continuously moving target. New vulnerabilities are found almost daily. No matter how secure an organization may feel that their servers and networks are, periodic audits are necessary to keep up with the ever-changing list of vulnerabilities. If most audits are done in-house, it is also advisable to occasionally engage an outside firm to perform an audit. This is not to imply that the in-house audits, or the people performing them, are not adequate. The outside auditor would instead augment the internal team, adding experience and a fresh perspective to pick up on things that may otherwise be overlooked. This paper discussed the results of a UNIX security audit performed by Para-noid for GIAC Enterprises. These results include specific recommendations to enhance the current level of security on the audited server.

Executive Summary

Objectives

GIAC Enterprises, an e-business supplier to fortune cookie companies, has secured the services of Para-noid, an I.T. security consulting firm, to perform an audit of their internal database server. The objectives of this audit are fourfold:

1) Assess the current security level of the database server
2) Assess the security level of policies, processes, and procedures associated with this server's management and operation
3) Provide recommendations on the necessary actions to reduce the security exposure of the audited server
4) Provide a starting point for security process and policy improvement within GIAC Enterprises' I.T. organization

Scope

This security audit specifically addresses GIAC Enterprises' internal database server, hostname fortunes. The database on this server contains much of the intellectual capital of GIAC Enterprises, and so its security is extremely business-critical. The Operating System (OS) and Database Management System (DBMS) will be assessed, as well as policies and procedures relative to the management and operation of this server.

Conclusions

The fortunes server has several steps already taken to ensure a higher-than-normal level of security, but there are several improvements that could be made, and a couple of vulnerabilities that should be addressed right away. This audit also highlighted some areas for improvement in patch and version management, as well as possible improvements in security policy. The remainder of this report covers the results in detail, but the top 5 highlights are listed below.

- Intrusion detection software (HP's IDS/9000) is installed, but not fully implemented. We recommend that this be implemented to monitor changes to the system.
- Patch management policies should be followed to ensure that the latest operating system and application patches are applied.
- Root access should be tightened.
- All unnecessary services should be removed or disabled.
- System logging should be improved.

Description of System and Audit Methodology

Description of Audited System

The primary role of the audited server, hostname fortunes, is as the production database server for GIAC Enterprises. The database housed on fortunes contains all of the intellectual property of GIAC Enterprises, namely the text of the fortunes they supply to makers of fortune cookies.

GIAC Enterprises fortunes database server is a Hewlett-Packard Unix server, model K360, with two processors and 1024 MB of memory. The Operating System is loaded on two 4 GB disks, mirrored for redundancy, and data is stored on a locally attached RAID5 disk array.

This server is running the latest version of Hewlett-Packard Company's HP-UX, version B.11.11. Both the Hardware Enablement and Required Patches patch bundles, dated June 2003, are installed. The database software in use on this server is the Hewlett-Packard supplied version of the open-source database engine MySQL, version 3.23.39.

The fortunes server is located on GIAC Enterprises' intranet, which is connected to the Internet through a firewall and router. Given the business-critical nature of this server, no assumptions should be made about the security of the network or firewall. The server should be treated as though it is vulnerable to both internal and external attack, as the viability of GIAC Enterprises depends upon the integrity and availability of this server.

Audit Methodology

A four step process was utilized to audit the fortunes database server.

Step 1 – Policy and Procedures

Interviews were conducted with both management and individual contributors with responsibility for the fortunes database server, to discuss the policies and procedures in place for managing the server. The objective of this was two-fold. First, to determine what policies and procedures are in place, gauged against industry standards. And second, to determine any discrepancies between the policies and procedures and actual implementation.

Step 2 – Use of the Center for Internet Security (CIS) Level 1 Benchmark and Scoring tool for HP-UX to assess operating system vulnerabilities

The Center for Internet Security (CIS) provides several tools for benchmarking and scoring the security levels of a system against industry standards. These

tools are available for various operating systems and software packages, with HP-UX being one of those available. Para-noid makes significant effort to use industry-standard and available tools for auditing. The purpose of the CIS scan is to determine the current security level by analyzing the results of the benchmarking tool, and make recommendations based on the vulnerabilities exposed by this tool. The raw results of this scan are available in Appendix A. The tool and supporting documentation is available from http://www.cisecurity.org.

Step 3 – Use of industry-standard scanning tool Nessus to identify network-based vulnerabilities

There are several freely available scanning tools. Nessus, combined with the port scanner nmap, is considered to be an industry-standard, or de facto, scanning tool, widely used regardless of platform or operating system. The purpose of scanning with Nessus is to identify network vulnerabilities, such as open ports or unnecessary services. Nessus is able to test for many known vulnerabilities and exploits, and exploit them if desired. Care is taken to minimize any impact the scanning tools may have on the system under investigation. The raw results of the Nessus and nmap scan are available in Appendix B. Nessus is available from http://www.nessus.org, and nmap can be obtained from http://www.insecure.org. Nessus is available for free under the GNU definition of free software, found at http://www.gnu.org/philosophy/free-sw.html, and nmap is an open-source package, also available for free.

Step 4 – Use of Hewlett-Packard Company's Security Patch Check tool

Hewlett-Packard Company provides a free tool to check the HP-UX operating system for the latest recommended security patches. This tool is referenced as product number B6834AA, and is called Security Patch Check. This is a tool to check the currency of system patches with respect to security, and to recommend patches for vulnerabilities that have not been addressed by patches already on the system. When used with the –r option, ex. security_patch_check –r, the tool will automatically download the latest security patch catalog from Hewlett-Packard, and then check your system for the existence of these recommended patches. The –r option will work provided the system has direct ftp access to Hewlett-Packard. If not, the patch catalog may be downloaded manually using ftp, placed on the system to be analyzed, and then security_patch_check run with the –c <*path to security_catalog*> option. A report is then generated, listing those patches which are missing. This report may be viewed in Appendix C. The security_patch_check tool is available for free from Hewlett-Packard at the following URL: http://www.software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B6834AA

Detailed Analysis

Operating System Vulnerabilities

The HP-UX operating system version (11.11) being used on the fortunes server is the latest available from Hewlett-Packard, with relatively recent (June 2003) patch bundles installed. However, the HP security_patch_check tool flagged 34 security-related patches that were not installed. It is recommended that these first be installed into a test environment before installing onto the production fortunes server.
These patches are:
PHCO_23492 PHCO_23909
PHCO_25918 PHCO_26061
PHCO_26561 PHCO_27019
PHCO_27037 PHCO_27345
PHCO_27694 PHCO_28259
PHCO_28481 PHCO_28719
PHCO_28848 PHCO_29010
PHCO_29495 PHKL_23335
PHKL_23423 PHKL_27179
PHKL_28990 PHNE_24512
PHNE_25644 PHNE_27703
PHNE_27765 PHNE_27796
PHNE_28444 PHNE_28983
PHNE_29774 PHNE_30068
PHSS_27858 PHSS_28470
PHSS_28677 PHSS_29371
PHSS_29964 PHSS_30011

The CIS Level 1 Benchmark and Scoring tool for HP-UX assigns a score to the system, on a scale of 1 to 10, with 10 being the most secure. The fortunes database server scored a 3.12, which means there is significant room for improvement. There were several positives which indicate that some steps have been taken to increase security over the default installation. Some of these positives are:
The system is running sshd and it's configured well.
Telnet, ftp, rsh, rcp, rlogin, tftp, and rquotad are all deactivated.
CDE-related daemons are deactivated.
Kerberos network daemons are deactivated.
DHCP Server (bootps) is not active in inetd.conf.
Serial login prompt is disabled.
Windows compatibility servers (samba) have been deactivated.
Web server is deactivated.
TCP sequence numbers are strongly random.
/var/adm/sw/save is not accessible to non-root users.

The crontabs all have good ownerships and modes
Inetd logging is enabled.
All users have passwords
There were no +: entries in passwd or group maps.
Only one UID 0 account AND it is named root.
No group or world-writable dotfiles (.profile, .cshrc, etc) in user home directories.

However, there is still significant room for improvement. Other areas of this detailed analysis will highlight specific areas to target. The Nessus scanning tool also highlighted many of the same vulnerabilities as the CIS Level 1 Benchmark and Scoring tool for HP-UX, finding 100 vulnerabilities. These were categorized with regard to risk, as high, medium, and low. The high risk vulnerabilities made up 24% of the total, medium risk covered 20%, and low risk vulnerabilities made up the balance of 56%.

Security Patch Installation and Management

Through interviews with management and I.T. staff, it was determined that GIAC Enterprises subscribes to a very conservative patch strategy. Recommended patch bundles are installed once per year, in July, during the July 4th break. Patches are installed at other times in a reactive fashion, with no testing performed. It is recommended that a policy be put in place to proactively assess and patch the fortunes database server on a regular basis, perhaps once per quarter. The HP security_patch_check tool can be utilized as part of the procedure to comply with this new policy. A process should be put in place to identify needed security patches, install them into a test environment, and then roll them onto the production server at regular intervals. Key I.T. personnel should also be subscribed to HP's Information Technology Resource Center (ITRC) Security Bulletins, which will alert them to relevant security vulnerabilities as they are identified. A policy to handle these bulletins and their required actions should also be identified and put into action. Documentation of the policies and procedures should also be created, to help ensure clear communication, accountability, and compliance.

Configuration Vulnerabilities

There were several vulnerabilities identified by the tools used, most of which can be easily taken care of. These have been split into several categories.

Files and File Systems

Several file systems could be mounted with different options to enhance security. These file systems and the recommended mount options are:
/opt should be mounted read-only.
/var should be mounted nosuid.
/home should be mounted nosuid.
/tmp should be mounted nosuid.
/stand should be mounted nosuid.

Several files that should not be world or group writeable were found to be so, as well as a few files whose ownerships/permissions were not set optimally. These are listed below:
Non-standard world-writable file: /var/vx/isis/tasklog/logfile0.log
Non-standard world-writable file: /var/opt/perf/status.perflbd
Non-standard world-writable file: /usr/lbin/udf_ccdc
Non-standard world-writable file: /usr/share/man/cat1m.Z/sendmail.1m
Non-standard world-writable file: /etc/hosts
Non-standard world-writable file: /usr/lbin/udf_big5
Non-standard world-writable file: /var/adm/automount.log
Non-standard world-writable file: /var/opt/perf/status.alarmgen
Non-standard world-writable file: /tmp/T1471AA_A.03.61.001_HP-UX_B.11.11_32+64.depot
Non-standard world-writable file: /var/opt/dce/svc/fatal.log
Non-standard world-writable file: /etc/resolv.conf
Non-standard world-writable file: /var/opt/perf/status.rep_server
Non-standard world-writable file: /var/vx/isis/alertlog/alert.log
Non-standard world-writable file: /var/opt/dce/svc/error.log
Non-standard world-writable file: /etc/opt/resmon/persistence/reboot_flag
Non-standard world-writable file: /var/opt/cmom/cmomd.log
Non-standard world-writable file: /usr/share/man/cat1m.Z/route.1m
Non-standard world-writable file: /.rhosts
Non-standard world-writable file: /var/vx/isis/state
Non-standard world-writable file: /usr/share/man/cat1m.Z/swlist.1m
Non-standard world-writable file: /var/opt/dce/svc/warning.log
Non-standard world-writable file: /var/sam/log/samagent.log
/etc/passwd should be owned by group sys.
/etc/group should be owned by root.
/etc/group should be owned by group sys.

/tmp should have its sticky bit set.
/var/news should have its sticky bit set.
/var/tmp should have its sticky bit set.
/var/preserve should have its sticky bit set.
/var/spool/sockets should have its sticky bit set.
/var/spool/sockets/X11 should have its sticky bit set.
/var/spool/sockets/common should have its sticky bit set.
/var/X11/Xserver/logs should have its sticky bit set.
/var/adm/automount.log should not be world-writable.
/var/opt/dce/svc/error.log should not be world-writable.
/var/opt/dce/svc/fatal.log should not be world-writable.
/var/opt/dce/svc/warning.log should not be world-writable. Negative: 8.6 Directory /usr/local/bin is world-writable.
Directory /usr/local/bin is group-writable.

Also, several files were found to be either Set-GID or Set-UID that should not be set as such. A listing of these follows:

/sbin/shutdown should not be Set-UID.
/usr/bin/bdf should not be Set-UID.
/usr/bin/df should not be Set-UID.
/usr/bin/kermit should not be Set-UID.
/usr/bin/kermit should not be Set-GID.
/usr/lbin/exrecover should not be Set-UID.
/usr/contrib/bin/X11/xconsole should not be Set-UID.
/usr/bin/elm should not be Set-GID.
/usr/sbin/wall should not be Set-GID.
/usr/dt/bin/dtaction should not be Set-UID.
/usr/dt/bin/dtaction should not be Set-GID.
/usr/dt/bin/dtappgather should not be Set-UID.
/usr/dt/bin/dtprintinfo should not be Set-UID.
/usr/dt/bin/dtsession should not be Set-UID.
Non-standard SUID program /usr/bin/X11/X
Non-standard SUID program /usr/sbin/lvmerge
Non-standard SUID program /usr/sbin/lvsplit
Non-standard SUID program /sbin/lvchange.run
Non-standard SUID program /usr/sbin/nomwcsyncd
Non-standard SUID program /sbin/vgsync
Non-standard SUID program /sbin/lvsync
Non-standard SUID program /sbin/lvmerge
Non-standard SUID program /usr/sbin/vgsync
Non-standard SUID program /sbin/lvsplit
Non-standard SUID program /usr/sbin/lvsync
Non-standard SUID program /sbin/nomwcsyncd
Non-standard SUID program /usr/sbin/lvchange.run

Network Parameters

There are several network parameters which can be configured to enhance network security. Most of these can be set by editing the file /etc/rc.config.d/nddconf. In this file, the following changes should be made:
ip_forward_directed_broadcasts should be set to 0.
tcp_syn_rcvd_max should be set to a minimum of 4096.
tcp_ip_abort_cinterval should be set to a maximum of 60,000.
ip_send_redirects should be set to 0.
arp_cleanup_interval should be set to a maximum of 60,000.
ip_forwarding should be set to 0.
ip_forward_src_routed should be set to 0.

Unnecessary Services

Several services that are not necessary for the operation of the fortunes database server are configured and running, and are recommended to be stopped. Many of these are enabled by default, but there are potential exploits for many of them. It is recommended to stop and disable all unnecessary services, to minimize exposure. Most of these services can be disabled by setting a startup variable to 0 in a file in the /etc/rc.config.d directory. Other services may be disabled by commenting them out of /etc/Inetd.conf. The correct method for each service will be detailed below.

SMTP
Sendmail is running on this server, listening and collecting mail from the network. There are many known exploits for sendmail, depending on the version in use. Since the fortunes server is a database server, and not a mail server, it is recommended to disable sendmail via the startup variable SENDMAIL_SERVER in the file /etc/rc.config.d/mailservs.

SNMP
There is a known vulnerability with SNMP, the Simple Network Management Protocol. Since SNMP is not in use for management purposes, it should not be left running on a production server. This can be disabled via the startup variable SNMP_MASTER_START in the file /etc/rc.config.d/SnmpMaster.

Printer daemon
The BSD-compatible printer daemon, rlpdaemon, is configured in /etc/Inetd.conf. Since this server is not a print server, this service should be disabled by commenting out the “printer” line in /etc/Inetd.conf. Likewise, the standard UNIX lp daemon can be stopped and disable, by setting the variable LP to 0 in the file /etc/rc.config.d/lp.

Small Services
UNIX contains several services, commonly called small services, which, while novel, are not of any functional use any longer. Several of these were found to be running, and can be disabled by commenting them out of /etc/Inetd.conf. The services which should be disabled are echo, discard, daytime, chargen, time, and ident.

Network File System (NFS)
This system's role is as a database server, and has all of its data locally. Therefore, the Network File System daemons are not essential, and should be stopped and disabled. Currently, the system is configured as both an NFS server and an NFS client. Both client and server daemons can be disabled with variables in the /etc/rc.config.d/nfsconf file. The variable for the server daemons is NFS_SERVER, and the client variable is NFS_CLIENT. Both should be set equal to 0.

Berkeley Services
UNIX also contains several services commonly called Berkeley services. These are the "r" commands, such as rcp, rlogin, rexec, and remsh. These services allow for a "user equivalency" between systems using a file called .rhosts, and they are a potential target for an attack. The famous hacking attack by Kevin Mitnick, outlined in the book "Takedown: The Pursuit and Capture of America's Most Wanted Computer Outlaw – By The Man Who Did It", by Tsutomu Shimomura and John Markoff, was possible due to the existence of these services. These services are disabled, but a .rhosts file does exist on the system, and should be linked to /dev/null.

Trusted System and System Accounting

Hewlett-Packard's HP-UX operating system provides a mode known as Trusted Mode, and if a server is configured as such, it is called a "trusted" system. This allows for detailed accounting and auditing, as well as shadow passwords and password aging. This server is not in trusted mode, and it is recommended to convert this system to a trusted system.

Console and Remote Access

It is a common practice to disallow root access from anywhere other than the physical console. This is accomplished through the existence of the file /etc/securetty. This file does not exist, so root access over the network is allowed. It is recommended to create this file, and disallow such access. It is also accepted practice to disallow remote graphical logins, as there are several known vulnerabilities within the X-windows systems such as HP's Common Desktop Environment (CDE). Although the CDE daemons are disabled, it is

recommended to create and edit the file /etc/dt/config/XAccess, which is used to disallow remote graphical login. Also, although the ftp daemon is disabled, access can be controlled using the /etc/ftpusers file. This file also does not exist, and it is recommended to create and edit this file to disallow unauthorized ftp access. It is also a good idea to explicitly state the allowed login shells. This is accomplished with the /etc/shells file, an ASCII file listing the allowed login shells. This file also does not exist, and it is recommended that it be created listing only valid login shells.

Banners

It is advisable to include banners at login with a simple message detailing that the system is a privately-owned system, and is for authorized uses only. The files /etc/issue and /etc/motd can be used to issue just such a banner. Neither file currently contains such a message, but it is recommended to edit these files to include such wording.

Access Control

The principle of least privilege is an industry-standard concept, basically meaning that a user is configured with only those privileges necessary to carry out normal job functions. There are several configuration changes which can be made under this principle to strengthen security on the fortunes server. Both cron.allow and at.allow contain non-root accounts. From interviews conducted with I.T. staff, it was determined that no non-root user on the fortunes database server should have the ability to schedule jobs, so it is recommended to edit these file to remove that privilege. Also, the /etc/passwd file contains several default "system" users, adm, daemon, bin, lp, nobody, and hpdb. All of these accounts are configured with a valid login shell. None of these users should be allowed a regular login, and the login shell changed to /bin/false. Also, the default umask is set to 022. But, umask is not specified in /etc/profile or /etc/csh.login. It is recommended to explicitly set the umask to 077 in each of these files.

Risks from Installed Third-Party Software

The fortunes database server has a standard HP-UX operating system load, with MySQL added as the database engine. There are several exploits for MySQL, and these vulnerabilities have been flagged by the Nessus scan. The version of MySQL currently in use on fortunes is 3.23.39. It is recommended that MySQL be upgraded to at least version 3.23.56 to remove these vulnerabilities.
Also, it is recommended that no other third-party software be installed on this system unless it is directly related to the primary role of the server. Shareware or

free software can contain exploits or vulnerabilities. A stringent change control process would mitigate risks from additional third-party software.

Administrative Practices

GIAC Enterprises has several policies in place to provide structure to the I.T. environment. But, through interviews and observation we found that these policies are not enforced, and in fact are often not followed. It is recommended that GIAC Enterprises management clearly define the role of systems administrator, and set up procedures for ensuring that policies are adhered to. Current practices are to perform tasks reactively, with no set procedures being followed. Strong change control and change management policies, and enforcement of those policies, will make a significant difference in the security, integrity, and availability of the fortunes database server, and improve the I.T. environment as a whole.

Identification and Protection of Business-Critical Data

File Integrity

Para-noid has noticed that HP's IDS/9000 software is installed on the fortunes database server. However, this software is not configured and therefore is not being used. HP's IDS/9000, among other uses, has the ability to track the integrity of files, much like the de facto standard Tripwire. It is recommended that GIAC Enterprises configure and actively use IDS/9000. Not only will file integrity be monitored, but the other intrusion detection features of IDS/9000 can also be taken advantage of.

System Logging

There are a few concerns around the system logging on the fortunes database server. HP-UX logs its system logs to /var/adm/syslog/syslog.log, but these logs are not being rotated, and are not being monitored on a regular basis. They are only consulted in the event of an outage or other such event. It is advisable to not only check these logs on a regular basis, but also to log their data to a central log server, so that an attacker can not modify the logs to cover traces of an exploit. The HP-UX version of syslogd does contain this feature, and it is configured through /etc/syslog.conf.

Protection of Sensitive Data in Transit over the Network

Remote access to the fortunes database server is only allowed through ssh, which is a secure and encrypted method of access. Telnet, ftp, and the "r" commands have been disable, which protects passwords and account data from being transmitted over the network in unencrypted form. The database is only accessed locally, and not through applications over the network. This is a positive development, and the I.T. staff of GIAC Enterprises should be praised for implementing this secure measure.

Access Controls

Certain aspects of access control, and the principle of least privilege, were discussed earlier in the Configuration Vulnerabilities section. There are a few points yet to be brought up, however, which can increase the security of the fortunes server.

Administrator Access and root Password Control

The root password to the fortunes database server is known by all of the I.T. staff, even those who have no direct responsibility for the server. It is recommended that the root password immediately be changed, and that it then be given only to those who absolutely need root access. It should also be standard policy that Administrators do not log into the system as root, but instead use their own personal user name, and then use a facility such as su, or a third party product such as sudo, to obtain root access. In our opinion at Para-noid, sudo should be implemented and used for all root access needs, both for the tighter access control it affords, and the increased logging it provides.

Password Policy

As noted before, this system is not in trusted mode. With the later versions of HP-UX, HP included a mechanism for enforcing stronger passwords through the file /etc/defaults/security. It is recommended that the /etc/defaults/security file be utilized to enforce minimum password lengths, password history, and the number of logins per user.

Backup Policy and Disaster Recovery

Backup Policy

GIAC Enterprises has a very well-developed backup policy in place, and it has been followed on a consistent basis. An incremental backup is performed on a daily basis, with a full backup each weekend. Backups are checked on a random basis to ensure that data is being backed up, and tapes are rotated to ensure that there is always at least one known good full backup tape on hand. However, all tape storage is onsite, with no off-site location for tape storage. It is recommended to implement an off-site storage location into the tape rotation scheme, to ensure that critical data is available in the event of a disaster which affects the onsite tape storage.

Disaster Recovery

While a strong backup policy is in place, disaster recovery plans have not been developed. It is recommended that a disaster recovery plan be developed and, once it is written, tested on a bi-annual basis. Several vendors offer disaster recovery services, including off-site system hosting. Without the data stored on the fortunes database server, and without availability of that data, the GIAC Enterprises business may very well cease to be a viable concern. With that in mind, it is vital to create a disaster recovery plan that ensures the integrity and availability of that data in the event of a disaster affecting the existing server hardware or location.

Top Ten Issues and Recommendations

Although there are many recommendations scattered throughout the detailed analysis, the top ten issues are outlined in this section. They are not in any particular order of importance, as each one will strengthen the security level of the fortunes database server, and quite possibly the overall security level of the GIAC Enterprises I.T. department.

Disable Non-essential Services

The fortunes server has only one role, and that is as a database server. There are many services running on the fortunes server that are not essential to its main role. These services not only utilize resources which could be freed up to aid performance of the server's primary role, they open the server to several vulnerabilities which can be easily mitigated by just disabling these services. None of those mentioned in the detailed analysis will have a detrimental effect on the server's primary role as a database server, so there is no good reason not to disable them. Two services are of primary concern, SMTP and SNMP, as there are well-known vulnerabilities for each.

Patch Management Policy

As outlined earlier, GIAC Enterprises lacks a defined patch policy. It is strongly recommended to design and implement a policy to stay up to date on security related patches. HP's security_patch_check can be used as part of the procedures to comply with the patch policy, and has been installed as part of this audit process. A sound security patch management policy should include the following:

Identification
There should be a method of identifying needed security patches. HP's security_patch_check tool will suffice to check the current state of the system versus the recommended list of security patches. And I also recommend subscribing all responsible systems administrators to HP's ITRC Security Bulletins, which will alert them to possible vulnerabilities, and the vendor fixes for these, as they are identified. With the use of these two tools, it should be relatively easy to identify which security patches are needed to bring the system up to date at any given time.

Testing
GIAC Enterprises has a test server for the fortunes database, but it is seldom used except by application developers. It is recommended to integrate this test server into a patch management process that includes installing the patches onto

the test server before implementing them into production. This will enable the I.T. Department to identify any potential problems before they have an effect on the business.

Documentation
Records should be kept of patches that are identified, tested, and installed. These lists may not be identical, as some patches may be identified, but then fail to pass the test environment, and are therefore never installed on the fortunes database server. This should be documented, so that when the same patch is identified at the next scheduled patch interval, the reason that it was never installed is readily apparent.

Tighten Root Access

As mentioned in the detailed analysis, there are several administrators with knowledge of the root password to the fortunes server. Many of these administrators do not have any direct responsibility for the fortunes server, and therefore do not need root access. It is recommended to tighten root access by taking the following steps:

1. Immediately change the root password, and only allow a small number of administrators to have the new password. It is also important, though, that more than one person know this password, in case of emergency or disaster.
2. Implement sudo, or a similar tool, to allow administrators to perform functions requiring root access while logged in as their own personal account. This will enhance logging of root access, as well as minimize the chances of error due to administrators always being logged in as root.

Implement File Integrity Checks

As noted earlier, IDS/9000 is installed on the fortunes server. This is a free intrusion detection package from Hewlett-Packard. Although it is installed, it is not currently configured. It is recommended to configure this package, and begin to use it as a host-based intrusion detection system and file integrity monitor. IDS/9000 will allow you to monitor critical files for changes, similar to the de facto integrity checker Tripwire. Alternatively, Tripwire version 2.3.47 is available under the GNU Public License, from http://www.tripwire.org/downloads/index.php. As noted on http://www.tripwire.org, Tripwire was originally an intrusion detection tool. Tripwire monitors key attributes of files that should not change. Either Tripwire or the file integrity features of IDS/9000 should be taken advantage of, to provide protection for the integrity of critical files.

Implement Password Controls

Without converting to a trusted system, HP-UX provides the /etc/defaults/security file. This file can be used to set controls on password history, minimum password length, number of logins per user, and several other controls on root access. It is recommended that this be implemented, regardless of plans to convert to a trusted system. Also, to augment this step, it is recommended that GIAC Enterprises also put in place a password aging policy, whereby each user must change their password at a maximum frequency of every 90 days, and a minimum frequency of every 30 days.

Update MySQL

The fortunes server's primary role is as a database server. The database engine used is the HP-supplied version of MySQL, version 3.23.39. This version is susceptible to several known exploits, and it is recommended to upgrade to a minimum of version 3.23.56. According to http://www.mysql.org, the latest production release is now 4.0.17, and this version resolves all valid bugs identified by Reasoning, Inc and reported in a press release titled, "Reasoning Study Reveals Code Quality of MySQL Open Source Database Ranks Higher than Commercial Equivalents." This press release is available from http://www.reasoning.com/newsevents/pr/12_15_03.html. It is recommended to upgrade to 4.0.17, in order to resolve as many known bugs and vulnerabilities as possible.

Improve System Logging

HP-UX contains a syslogd daemon, syslogd, which by default logs system messages to /var/adm/syslogd/syslog.log. It was determined through interviews with I.T. staff that the system logs on fortunes were only consulted reactively, in the event of a hardware failure, application outage, or other such event. These logs are also allowed to grow unchecked until the next system reboot, and are only stored on the local host. There are several recommendations with respect to system logging. First and foremost, a policy should be put in place requiring the system logs to be monitored on a regular basis, to track and confirm normal activity on the fortunes server. Second, a central logging server should be set up, and the fortunes server's syslogd configured to log data to this server. Logging to a remote server decreases the chances that a malicious user or attacker could alter the log data to hide evidence of an attack. And third, some sort of mechanism to rotate the logs should be implemented. A common, and free, solution is logrotate. Logrotate is available from the HP-UX Porting and Archive Center, at http://hpux.cs.utah.edu/hppd/hpux/Sysadmin/logrotate-2.5/. Logrotate is a log management tool for system administrators of UNIX systems. It is allows for automatic rotation, compression, removal, and mailing of log files. By implementing logrotate, GIAC Enterprises can avoid availability issues and

possible loss of log data if the log files were to grow too large for the file system they are currently stored in. Logrotate would provide a means to manage the log data, preventing file system full messages and issues.

Convert to Trusted System

According to the Hewlett-Packard manual "Administering Your HP-UX Trusted System", a trusted system is one that can be relied upon to perform correctly in two important ways:
The system's operational features work correctly and satisfy the needs of the computing users, and the system's security features provide the mechanisms necessary to enforce the site's security policy and provide protection from threats. As mentioned earlier, converting to trusted mode is recommended, but should not be entered into lightly. Planning is essential to a successful conversion to a trusted system.
In trusted mode, HP-UX complies with, and in some respects exceeds, the Department of Defense's C2 class of security. Features of C2 security include Discretionary Access Control, Object Reuse, Identification and Authentication, Auditing, System Architecture, and System Integrity.
Trusted mode adds Access Control Lists to the standard UNIX permissions to comply with C2 level security requirements, and enables auditing to hold users accountable for their activity. Converting to a trusted system will create a new, protected password database, move all encrypted passwords from /etc/passwd to the new database, force all users to use passwords, and enable auditing for all users.
Once the decision is made to convert to a trusted system, and the planning has all been completed, the actual conversion is relatively easy. You can use HP-UX's System Administration Manager, or SAM, to perform the conversion for you. In SAM, first select "Auditing and Security", and then select "Audited Events". You will be asked if you want to convert to a trusted system. Select "Yes" and SAM will perform the conversion for you. For more information, and for help in planning a trusted system, you may consult the HP manual "Administering Your HP-UX Trusted System", available at http://docs.hp.com/hpux/onlinedocs/B2355-90121/B2355-90121.html.

Implement Network Parameters to Tighten Security

There are several network parameters which can be adjusted to enhance security. These were outlined in the detailed analysis section of this document, but are one of the top ten recommendations. These parameters can be set using the /etc/rc.config.d/nddconf file to set them permanently, or through the ndd command to set until the next reboot. Each parameter is set with three variables in nddconf, TRANSPORT_NAME, NDD_NAME, and NDD_VALUE. The TRANSPORT_NAME is either tcp, udp, ip, or arp. NDD_NAME will be the name of the network parameter to be set, such as ip_forward_src_routed. And

NDD_VALUE is the value you'd like to set the parameter equal to. Para-noid recommends the following parameters be set:
ip_forward_directed_broadcasts should be set to 0, to disable IP directed broadcasts.
tcp_syn_rcvd_max should be set to a minimum of 4096, to mitigate TCP syn floods and denial of service attacks.
tcp_ip_abort_cinterval should be set to a maximum of 60,000. This is the amount of time a connection is allowed to stay in a half-open state, and will server to help mitigate denial of service attacks.
ip_send_redirects should be set to 0, to avoid sending icmp redirect messages.
arp_cleanup_interval should be set to a maximum of 60,000, to minimize chances of arp cache poisoning.
ip_forwarding should be set to 0 to disallow forwarding of IP packets.
ip_forward_src_routed should be set to 0, to disallow packets which contain their own routing information. This will serve to mitigate effects of address spoofing.

Implement Banners

In today's legal climate, it has been noted that if you don't specifically state that your system is not to be used for unauthorized purposes, then you may have no legal basis for prosecution or damage claims due to unauthorized or malicious use. It is recommended to edit /etc/issue to include a simple message such as "Unauthorized Use Prohibited". This will greet anyone who gets a login prompt from the fortunes server, and serves as a simple warning before login is attempted. The /etc/motd (Message of the Day) file can also be edited to include a more detailed message, which will be displayed following a successful login. Each is recommended for implementation, as they complement on another. Any other services that are utilized in the future, such as ftp or sendmail, should also have banners added before allowing the services to run on the fortunes server.

Change Control

Through interviews with I.T. staff, it was determined that much of the activity surrounding the management of the fortunes database server was reactive rather than proactive. And most of those activities were undocumented, and did not follow set procedures. Due to the extremely critical nature of the fortunes database server, it is recommended that GIAC Enterprises institute a formal change control process for all changes to this server, and extend this process throughout the I.T. environment. In order for a change control process to be effective, it must be supported by upper management. A change control board should be established, with representatives from each business unit with responsibility or a dependency on the fortunes database server. For any change, a request form should be submitted to the change control board. The change request should include a detailed description of the change, why it is necessary and a contingency plan in case the change has undesired effects. The control

board would then review the change, and either authorize or deny it. If the change is authorized, it could then be implemented. Once the change has been implemented, a verification process should be performed by an independent group to ensure that only the approved changes were made. This independent group should then sign off on the change request as having been implemented and verified. This should then be reported back to the change control board, and the issue closed. A simple process which can reap significant benefits in not only availability, but also in shortening troubleshooting or investigation time in the event of an outage or incident.

References

"Takedown: The Pursuit and Capture of America's Most Wanted Computer Outlaw – By The Man Who Did It", by Tsutomu Shimomura and John Markoff

http://www.tripwire.org

"Reasoning Study Reveals Code Quality of MySQL Open Source Database Ranks Higher than Commercial Equivalents."
http://www.reasoning.com/newsevents/pr/12_15_03.html

http://www.mysql.org

http://hpux.cs.utah.edu/hppd/cgi-bin/wwwtar?/hpux/Sysadmin/logrotate-2.5/logrotate-2.5-ss-11.00.tar.gz+logrotate-2.5/HPUX.Install+text

"Administering Your HP-UX Trusted System"
http://docs.hp.com/hpux/onlinedocs/B2355-90121/B2355-90121.html

Appendix A – Output of Center for Internet Security (CIS) Level 1 Benchmark and Scoring tool for HP-UX

*** CIS Ruler Run ***
Starting at time 20031224-11:14:30

Negative: 1.1 /opt/sec_mgmt/spc/bin/security_patch_check cannot be run to check patch status.
Negative: 1.2 tcp-protocol service ident in inetd.conf is not wrapped.
Negative: 1.2 tcp-protocol service printer in inetd.conf is not wrapped.
Negative: 1.2 tcp-protocol service daytime in inetd.conf is not wrapped.
Negative: 1.2 udp-protocol service daytime in inetd.conf is not wrapped.
Negative: 1.2 tcp-protocol service time in inetd.conf is not wrapped.
Negative: 1.2 tcp-protocol service echo in inetd.conf is not wrapped.
Negative: 1.2 udp-protocol service echo in inetd.conf is not wrapped.
Negative: 1.2 tcp-protocol service discard in inetd.conf is not wrapped.
Negative: 1.2 udp-protocol service discard in inetd.conf is not wrapped.
Negative: 1.2 tcp-protocol service chargen in inetd.conf is not wrapped.
Negative: 1.2 udp-protocol service chargen in inetd.conf is not wrapped.
Positive: 1.3 System is running sshd and it's configured well.
Negative: 2.1 inetd service echo requires full deactivation -- comment out or delete its line in inetd.conf.
Negative: 2.1 inetd service discard requires full deactivation -- comment out or delete its line in inetd.conf.
Negative: 2.1 inetd service daytime requires full deactivation -- comment out or delete its line in inetd.conf.
Negative: 2.1 inetd service chargen requires full deactivation -- comment out or delete its line in inetd.conf.
Negative: 2.1 inetd service ident requires full deactivation -- comment out or delete its line in inetd.conf.
Positive: 2.2 telnet is deactivated.
Positive: 2.3 ftp is deactivated.
Positive: 2.4 rsh, rcp and rlogin are deactivated.
Positive: 2.5 tftp is deactivated.
Negative: 2.6 BSD-compatible print server should be deactivated.
Positive: 2.7 rquotad is deactivated.
Positive: 2.8 CDE-related daemons are deactivated.
Positive: 2.9 kerberos network daemons are deactivated.
Positive: 2.10 DHCP Server (bootps) is not active in inetd.conf.
Positive: 3.1 Serial login prompt is disabled.
Negative: 3.2 inetd is still active.
Negative: 3.3 NIS-related script pwgr not deactivated.
Negative: 3.4 printer daemon script lp not deactivated.
Negative: 3.5 Graphical login not deactivated.
Negative: 3.5 /usr/dt/bin/dtaction should not be Set-UID.

Negative: 3.5 /usr/dt/bin/dtaction should not be Set-GID.
Negative: 3.5 /usr/dt/bin/dtappgather should not be Set-UID.
Negative: 3.5 /usr/dt/bin/dtprintinfo should not be Set-UID.
Negative: 3.5 /usr/dt/bin/dtsession should not be Set-UID.
Negative: 3.6 Mail daemon is on and collecting mail from the network.
Negative: 3.7 SNMP daemon should be deactivated.
Negative: 3.8 script ptydaemon is not deactivated.
Negative: 3.8 script vt is not deactivated.
Positive: 3.9 Windows compatibility servers (samba) have been deactivated.
Negative: 3.10 NFS Server script nfs.server not deactivated.
Negative: 3.11 NFS script nfs.client not deactivated.
Negative: 3.12 RPC rc-script (nfs.core) has not been deactivated.
Positive: 3.13 Web server is deactivated.
Negative: 4.1 Non-executable stack is not activated -- this system may only need a reboot to score positively.
Negative: 4.2 Network parameter ip.ip_forward_src_routed needs to be 0.
Negative: 4.2 Network parameter ip.ip_forward_directed_broadcasts needs to be 0 in /etc/rc.config.d/nddconf
Negative: 4.2 Network parameter tcp.tcp_syn_rcvd_max needs to be at least 4096 in /etc/rc.config.d/nddconf
Negative: 4.2 Network parameter tcp.tcp_ip_abort_cinterval needs to be at most 60,000 in /etc/rc.config.d/nddconf
Negative: 4.2 Network parameter ip.ip_send_redirects needs to be 0 in /etc/rc.config.d/nddconf
Negative: 4.2 Network parameter arp.arp_cleanup_interval needs to be at most 60,000 in /etc/rc.config.d/nddconf
Positive: 4.3 TCP sequence numbers are strongly random.
Negative: 4.4 Network parameter ip.ip_forwarding is not set to 0 in /etc/rc.config.d/nddconf
Negative: 5.1 /opt is not mounted read-only.
Negative: 5.1 /var is not mounted nosuid.
Negative: 5.1 /home is not mounted nosuid.
Negative: 5.1 /tmp is not mounted nosuid.
Negative: 5.1 /stand is not mounted nosuid.
Negative: 5.2 /etc/passwd is not owned by group sys!
Negative: 5.2 /etc/group is not owned by root!
Negative: 5.2 /etc/group is not owned by group sys!
Negative: 5.3 /tmp should have its sticky bit set.
Negative: 5.3 /var/news should have its sticky bit set.
Negative: 5.3 /var/tmp should have its sticky bit set.
Negative: 5.3 /var/preserve should have its sticky bit set.
Negative: 5.3 /var/spool/sockets should have its sticky bit set.
Negative: 5.3 /var/spool/sockets/X11 should have its sticky bit set.
Negative: 5.3 /var/spool/sockets/common should have its sticky bit set.
Negative: 5.3 /var/X11/Xserver/logs should have its sticky bit set.
Negative: 5.5 File /sbin/shutdown shouldn't be Set-UID.

Negative: 5.5 File /usr/bin/bdf shouldn't be Set-UID.
Negative: 5.5 File /usr/bin/df shouldn't be Set-UID.
Negative: 5.5 File /usr/bin/elm shouldn't be Set-GID.
Negative: 5.5 File /usr/bin/kermit shouldn't be Set-UID.
Negative: 5.5 File /usr/bin/kermit shouldn't be Set-GID.
Negative: 5.5 File /usr/lbin/exrecover shouldn't be Set-UID.
Negative: 5.5 File /usr/sbin/wall shouldn't be Set-GID.
Negative: 5.5 File /usr/contrib/bin/X11/xconsole shouldn't be Set-UID.
Negative: 5.7 /var/dt/Xerrors should not be group-writable.
Negative: 5.7 /var/sam/log/samagent.log should not be world-writable.
Negative: 5.7 /var/sam/log/samagent.log should not be group-writable.
Positive: 5.8 /var/adm/sw/save is not accessible to non-root users.
Negative: 5.9 checkperms has not been run on this system.
Negative: 6.1 Trusted mode not enabled.
Negative: 6.2 File //.rhosts exists, is non-zero size, isn't linked to /dev/null, and doesn't contain only the - character.
Warning: 6.3 On HP-UX 11.x, but didn't find an /etc/ftpd/ftpusers file. Assuming file is /etc/ftpusers.
Negative: 6.4 /etc/shells does not exist.
Negative: 6.5 /etc/dt/config/Xaccess doesn't exist, thus permits remote X-terminal login.
Negative: 6.6 /etc/dt/config/C/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/C.iso885915/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/C.utf8/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/de_DE.iso88591/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/de_DE.iso885915/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/de_DE.utf8/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/es_ES.iso88591/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/es_ES.iso885915/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/es_ES.utf8/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/fr_CA.iso88591/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/fr_CA.utf8/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/fr_FR.iso88591/sys.resources doesn't exist, so screenlocker can't be set.

Negative: 6.6 /etc/dt/config/fr_FR.iso885915/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/fr_FR.utf8/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/it_IT.iso88591/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/it_IT.iso885915/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/it_IT.utf8/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/ja_JP.SJIS/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/ja_JP.eucJP/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/ja_JP.utf8/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/ko_KR.eucKR/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/ko_KR.utf8/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/sv_SE.iso88591/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/sv_SE.iso885915/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/sv_SE.utf8/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/zh_CN.hp15CN/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/zh_CN.utf8/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/zh_HK.big5/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/zh_HK.utf8/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/zh_TW.big5/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/zh_TW.eucTW/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.6 /etc/dt/config/zh_TW.utf8/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 6.7 Non-root accounts are in cron.allow.
Negative: 6.7 Non-root accounts are in at.allow.
Positive: 6.8 crontabs all have good ownerships and modes
Negative: 6.9 /etc/dt/config/C/Xresources doesn't exist, so alternate GUI welcome message can't be set.

Negative: 6.9 /etc/dt/config/C.iso885915/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/C.utf8/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/de_DE.iso88591/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/de_DE.iso885915/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/de_DE.utf8/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/es_ES.iso88591/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/es_ES.iso885915/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/es_ES.utf8/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/fr_CA.iso88591/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/fr_CA.utf8/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/fr_FR.iso88591/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/fr_FR.iso885915/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/fr_FR.utf8/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/it_IT.iso88591/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/it_IT.iso885915/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/it_IT.utf8/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/ja_JP.SJIS/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/ja_JP.eucJP/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/ja_JP.utf8/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/ko_KR.eucKR/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/ko_KR.utf8/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/sv_SE.iso88591/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/sv_SE.iso885915/Xresources doesn't exist, so alternate GUI welcome message can't be set.

Negative: 6.9 /etc/dt/config/sv_SE.utf8/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/zh_CN.hp15CN/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/zh_CN.utf8/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/zh_HK.big5/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/zh_HK.utf8/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/zh_TW.big5/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/zh_TW.eucTW/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 /etc/dt/config/zh_TW.utf8/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 6.9 No Authorized Only message in /etc/motd.
Negative: 6.9 No Authorized Only message in /etc/issue.
Negative: 6.9 Couldn't open /etc/ftpd/ftpaccess to check for a banner.
Negative: 6.10 Couldn't open /etc/securetty.
Negative: 7.1 System accounting not enabled.
Negative: 7.2 Kernel-level auditing not enabled, according to the audsys command.
Positive: 7.3 Inetd-logging enabled.
Negative: 7.4 /var/adm/automount.log should not be world-writable.
Negative: 7.4 /var/opt/dce/svc/error.log should not be world-writable.
Negative: 7.4 /var/opt/dce/svc/fatal.log should not be world-writable.
Negative: 7.4 /var/opt/dce/svc/warning.log should not be world-writable.
Negative: 8.1 adm has a valid shell of /sbin/sh.
Negative: 8.1 daemon has a valid shell of /sbin/sh.
Negative: 8.1 bin has a valid shell of /sbin/sh.
Negative: 8.1 lp has a valid shell of /sbin/sh.
Negative: 8.1 nobody has a valid shell of /usr/bin/sh.
Negative: 8.1 hpdb has a valid shell of /sbin/sh.
Positive: 8.2 All users have passwords
Negative: 8.3 User smbnull should have a minimum password life of at least 7 days.
Negative: 8.3 User smbnull should have a maximum password life of between 1 and 90 days.
Negative: 8.3 User smbnull should have a password expiration warning of at least 7 days.
Negative: 8.3 User mysql should have a minimum password life of at least 7 days.
Negative: 8.3 User mysql should have a maximum password life of between 1 and 90 days.

Negative: 8.3 User mysql should have a password expiration warning of at least 7 days.
Negative: 8.3 User sshd should have a minimum password life of at least 7 days.
Negative: 8.3 User sshd should have a maximum password life of between 1 and 90 days.
Negative: 8.3 User sshd should have a password expiration warning of at least 7 days.
Negative: 8.3 Couldn't get minimum password life from getprdef utility - parsing error.
Negative: 8.3 Couldn't get maximum password life from getprdef utility - parsing error.
Negative: 8.3 Couldn't get password expiration warning time from getprdef utility - parsing error.
Positive: 8.4 There were no +: entries in passwd or group maps.
Positive: 8.5 Only one UID 0 account AND it is named root.
Negative: 8.6 Directory /usr/local/bin is in root's PATH and is world-writable.
Negative: 8.6 Directory /usr/local/bin is in root's PATH and is group-writable.
Negative: 8.6 Current-directory link . is in root's PATH!
Negative: 8.7 User sshd has a world-executable homedir!
Negative: 8.7 User sshd has a world-readable homedir!
Positive: 8.8 No group or world-writable dotfiles in user home directories!
Negative: 8.9 User root has an .rhosts file.
Negative: 8.9 User daemon has an .rhosts file.
Negative: 8.9 User sys has an .rhosts file.
Negative: 8.9 User hpdb has an .rhosts file.
Negative: 8.9 User nobody has an .rhosts file.
Negative: 8.9 User www has an .rhosts file.
Negative: 8.10 Default umask for sh may not block world-write/read/execute.
Checks file(s) /etc/profile
Negative: 8.10 Default umask for sh may not block group-write/read/execute.
Checks file(s) /etc/profile
Negative: 8.10 Default umask for ksh may not block world-write/read/execute.
Checks file(s) /etc/profile
Negative: 8.10 Default umask for ksh may not block group-write/read/execute.
Checks file(s) /etc/profile
Negative: 8.10 Default umask for csh may not block world-write/read/execute.
Checks file(s) /etc/csh.login
Negative: 8.10 Default umask for csh may not block group-write/read/execute.
Checks file(s) /etc/csh.login
Negative: 8.11 /etc/profile should set mesg n to block talk/write commands and strengthen permissions on user tty.
Negative: 8.11 /etc/csh.login should set mesg n to block talk/write commands and strengthen permissions on user tty.
Negative: 8.11 /etc/d.profile should set mesg n to block talk/write commands and strengthen permissions on user tty.

Negative: 8.11 /etc/d.login should set mesg n to block talk/write commands and strengthen permissions on user tty.
Preliminary rating given at time: Wed Dec 24 11:14:40 2003

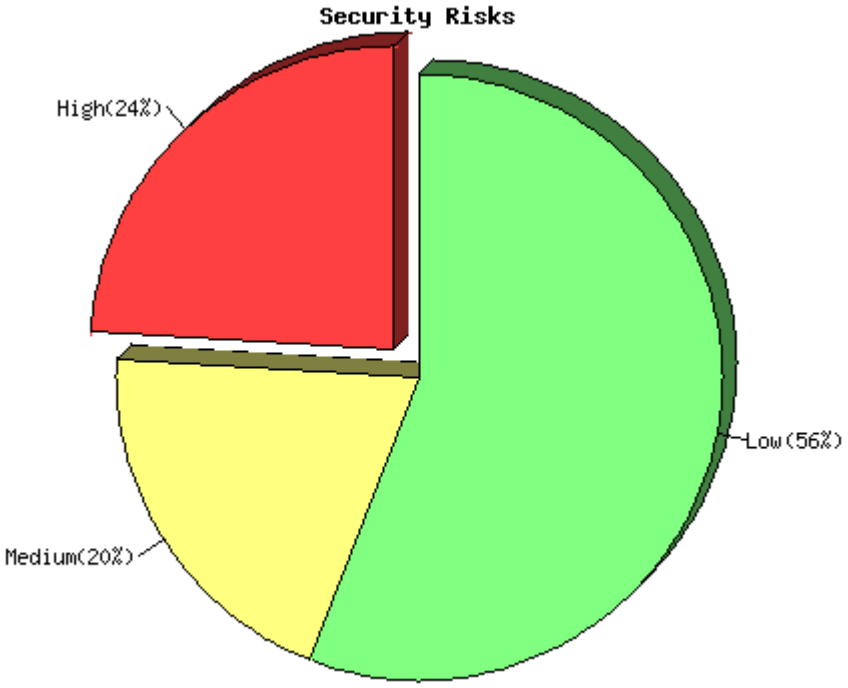
Preliminary rating = 3.12 / 10.00

Negative: 5.4 Non-standard world-writable file: /var/vx/isis/tasklog/logfile0.log
Negative: 5.4 Non-standard world-writable file: /var/opt/perf/status.perflbd
Negative: 5.4 Non-standard world-writable file: /usr/lbin/udf_ccdc
Negative: 5.4 Non-standard world-writable file: /usr/share/man/cat1m.Z/sendmail.1m
Negative: 5.4 Non-standard world-writable file: /etc/hosts
Negative: 5.4 Non-standard world-writable file: /usr/lbin/udf_big5
Negative: 5.4 Non-standard world-writable file: /var/adm/automount.log
Negative: 5.4 Non-standard world-writable file: /var/opt/perf/status.alarmgen
Negative: 5.4 Non-standard world-writable file: /tmp/T1471AA_A.03.61.001_HP-UX_B.11.11_32+64.depot
Negative: 5.4 Non-standard world-writable file: /var/opt/dce/svc/fatal.log
Negative: 5.4 Non-standard world-writable file: /etc/resolv.conf
Negative: 5.4 Non-standard world-writable file: /var/opt/perf/status.rep_server
Negative: 5.4 Non-standard world-writable file: /var/vx/isis/alertlog/alert.log
Negative: 5.4 Non-standard world-writable file: /var/opt/dce/svc/error.log
Negative: 5.4 Non-standard world-writable file: /etc/opt/resmon/persistence/reboot_flag
Negative: 5.4 Non-standard world-writable file: /var/opt/cmom/cmomd.log
Negative: 5.4 Non-standard world-writable file: /usr/share/man/cat1m.Z/route.1m
Negative: 5.4 Non-standard world-writable file: /.rhosts
Negative: 5.4 Non-standard world-writable file: /var/opt/mysql/fortunes.err
Negative: 5.4 Non-standard world-writable file: /var/vx/isis/state
Negative: 5.4 Non-standard world-writable file: /usr/share/man/cat1m.Z/swlist.1m
Negative: 5.4 Non-standard world-writable file: /var/opt/dce/svc/warning.log
Negative: 5.4 Non-standard world-writable file: /var/sam/log/samagent.log
Negative: 5.6 Non-standard SUID program /usr/bin/X11/X
Negative: 5.6 Non-standard SUID program /usr/sbin/lvmerge
Negative: 5.6 Non-standard SUID program /usr/sbin/lvsplit
Negative: 5.6 Non-standard SUID program /sbin/lvchange.run
Negative: 5.6 Non-standard SUID program /usr/sbin/nomwcsyncd
Negative: 5.6 Non-standard SUID program /sbin/vgsync
Negative: 5.6 Non-standard SUID program /sbin/lvsync
Negative: 5.6 Non-standard SUID program /sbin/lvmerge
Negative: 5.6 Non-standard SUID program /usr/sbin/vgsync
Negative: 5.6 Non-standard SUID program /sbin/lvsplit
Negative: 5.6 Non-standard SUID program /usr/sbin/lvsync
Negative: 5.6 Non-standard SUID program /sbin/nomwcsyncd
Negative: 5.6 Non-standard SUID program /usr/sbin/lvchange.run
Negative: 5.6 Non-standard SGID program /var/opt/wlm/.wlmd.LCK

Negative: 5.6 Non-standard SGID program /var/opt/wlm/.vpar.LCK
Ending run at time: Wed Dec 24 11:15:08 2003

Final rating = 3.12 / 10.00

Appendix B – Output from Nessus/nmap



Total security holes found: 100

Host: fortunes

Open ports:

login (513/tcp)
ftp (21/tcp)
chargen (19/tcp)
daytime (13/tcp)
discard (9/tcp)
echo (7/tcp)
time (37/tcp)
smtp (25/tcp)
auth (113/tcp)
sunrpc (111/tcp)
hp-managed-node (382/tcp)
shell (514/tcp)
telnet (23/tcp)
exec (512/tcp)

printer (515/tcp)
klogin (543/tcp)
kshell (544/tcp)
diagmond (1508/tcp)
nfs (2049/tcp)
lockd (4045/tcp)
hacl-probe (5303/tcp)
hacl-cfg (5302/tcp)
dtspc (6112/tcp)
loc-srv (135/tcp)

Service: general/icmp
Severity: High

The remote host is vulnerable to an 'Etherleak' -
the remote ethernet driver seems to leak bits of the
content of the memory of the remote operating system.

Note that an attacker may take advantage of this flaw
only when its target is on the same physical subnet.

See also : http://www.atstake.com/research/advisories/2003/a010603-1.txt
Solution : Contact your vendor for a fix
Risk factor : Serious
CVE : CAN-2003-0001
BID : 6535

Service: smtp (25/tcp)
Severity: High

mail.local in the remote sendmail server, according to its
version number, does not properly identify the .\n string
which identifies the end of message text, which allows a
remote attacker to cause a denial of service or corrupt
mailboxes via a message line that is 2047 characters
long and ends in .\n.

Solution : Install sendmail version 8.10.0 and higher, or install a vendor supplied patch.

Risk factor : High
CVE : CVE-2000-0319
BID : 1146

Service: smtp (25/tcp)
Severity: High

The remote sendmail server, according to its version number, may be vulnerable to a remote buffer overflow allowing remote users to gain root privileges.

Sendmail versions from 5.79 to 8.12.8 are vulnerable.
Solution : Upgrade to Sendmail ver 8.12.9 or greater or if you cannot upgrade, apply patches for 8.10-12 here: http://www.sendmail.org/patchps.html

NOTE: manual patches do not change the version numbers. Vendors who have released patched versions of sendmail may still falsely show vulnerabilty.

*** Nessus reports this vulnerability using only
*** the banner of the remote SMTP server. Therefore,
*** this might be a false positive.

Risk factor : High
CVE : CAN-2003-0161
BID : 7230

Service: smtp (25/tcp)
Severity: High

The remote sendmail server, according to its version number, allows remote attackers to cause a denial of service by sending a series of ETRN commands then disconnecting from the server, while Sendmail continues to process the commands after the connection has been terminated.

Solution : Install sendmail version 8.10.1 and higher, or install a vendor supplied patch.

Risk factor : Medium
CVE : CVE-1999-1109

Service: smtp (25/tcp)
Severity: High

The remote sendmail server, according to its version number, may be vulnerable to the -bt overflow attack which allows any local user to execute arbitrary commands as root.

Solution : upgrade to the latest version of Sendmail
Risk factor : High
Note : This vulnerability is _local_ only

Service: ftp (21/tcp)
Severity: High

You seem to be running an FTP server which is vulnerable to the
'glob heap corruption' flaw.
An attacker may use this problem to execute arbitrary commands on this host.

*** Nessus relied solely on the banner of the server to issue this warning,
*** so this alert might be a false positive
*** NOTE: must have a valid username/password to fully check this vulnerability

Solution : Upgrade your ftp server software to the latest version.
Risk factor : High

CVE : CAN-2001-0249, CVE-2001-0550
BID : 2550, 3581

Service: smtp (25/tcp)
Severity: High

smrsh (supplied by Sendmail) is designed to prevent the execution of
commands outside of the restricted environment. However, when commands
are entered using either double pipes (||) or a mixture of dot
and slash characters, a user may be able to bypass the checks
performed by smrsh. This can lead to the execution of commands
outside of the restricted environment.

Solution : upgrade to the latest version of Sendmail (or at least 8.12.8).
Risk factor : Medium
CVE : CAN-2002-1165
BID : 5845

Service: smtp (25/tcp)
Severity: High

The remote sendmail server, according to its version number,
may be vulnerable to a buffer overflow its DNS handling code.

The owner of a malicious name server could use this flaw
to execute arbitrary code on this host.

Solution : Upgrade to Sendmail 8.12.5
Risk factor : High
CVE : CVE-2002-0906
BID : 5122

Service: smtp (25/tcp)
Severity: High

The remote sendmail server, according to its version number,
may be vulnerable to a remote buffer overflow allowing remote
users to gain root privileges.

Sendmail versions from 5.79 to 8.12.7 are vulnerable.
Solution : Upgrade to Sendmail ver 8.12.8 or greater or
if you cannot upgrade, apply patches for 8.10-12 here:
http://www.sendmail.org/patchcr.html

NOTE: manual patches do not change the version numbers.
Vendors who have released patched versions of sendmail
may still falsely show vulnerabilty.

*** Nessus reports this vulnerability using only
*** the banner of the remote SMTP server. Therefore,
*** this might be a false positive.

see http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21950
http://www.cert.org/advisories/CA-2003-07.html
http://www.kb.cert.org/vuls/id/398025

Risk factor : High
CVE : CAN-2002-1337
BID : 6991

Service: snmp (161/udp)
Severity: High

SNMP Agent responded as expected with community name: public
SNMP Agent responded as expected with community name: snmpd
CVE : CAN-1999-0517, CAN-1999-0186, CAN-1999-0254
BID : 177, 7081, 7212, 7317

Service: general/tcp
Severity: Low

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

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

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

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

Service: snmp (161/udp)
Severity: Low
It was possible to obtain the list of processes of the
remote host via SNMP :

. swapper
. init
. vhand
. statdaemon
. unhashdaemon
. supsched
. strmem
. strweld
. strfreebd
. ttisr
. ioconfigd
. lvmkd
. lvmkd
. lvmkd
. lvmkd
. lvmkd
. lvmkd
. lvmschedd
. smpsched
. smpsched
. sblksched
. sblksched
. vxfsd
. /usr/sbin/syncer
. /usr/sbin/syslogd -D
. /usr/sbin/ptydaemon
. /usr/lbin/nktl_daemon 0 0 0 0 0 1 -2
. /usr/lbin/ntl_reader 0 1 1 1 1000 2 /var/adm/nettl /var/adm/con
. /usr/sbin/netfmt -C -F -f /var/adm/nettl.LOG000 -c /var/adm/con
. /usr/sbin/rpcbind

. nfskd
. /usr/sbin/biod 16
. /usr/sbin/biod 16
. /usr/sbin/biod 16
. /usr/sbin/biod 16
. /usr/sbin/biod 16
. /usr/sbin/biod 16
. /usr/sbin/biod 16
. /usr/sbin/biod 16
. /usr/sbin/biod 16
. /usr/sbin/biod 16
. /usr/sbin/biod 16
. /usr/sbin/biod 16
. /usr/sbin/biod 16
. /usr/sbin/biod 16
. /usr/sbin/biod 16
. /usr/sbin/biod 16
. /usr/sbin/rpc.statd
. /usr/sbin/rpc.lockd
. /usr/lib/netsvc/fs/automount/automount -f /etc/auto_master
. /usr/sbin/inetd
. sendmail: accepting connections on port 25
. /usr/sbin/snmpdm
. /usr/sbin/hp_unixagt
. /usr/sbin/mib2agt
. /usr/sbin/trapdestagt
. /usr/lbin/cmsnmpd
. /usr/sbin/fddi4subagt
. /opt/dce/sbin/rpcd
. /usr/dmi/bin/dmisp
. /var/dmi/bin/hpuxci
. /var/dmi/bin/swci
. scrdaemon
. /usr/sbin/pwgrd
. /usr/sbin/cron
. /usr/sbin/stm/uut/bin/sys/diagmond
. /usr/sbin/envd
. /opt/perf/bin/ttd
. /opt/perf/bin/midaemon
. /opt/perf/bin/perflbd
. /opt/perf/bin/scopeux
. /opt/prm/bin/prm3d
. /usr/sbin/swagentd -r
. diaglogd
. memlogd
. psmctd

. /etc/opt/resmon/lbin/registrar
. /etc/opt/resmon/lbin/emsagent
. /opt/VRTSob/bin/vxsvc -r /etc/vx/isis/Registry
. /usr/sbin/rpc.mountd
. /usr/sbin/nfsd 16
. /usr/sbin/nfsd 16
. /usr/sbin/nfsd 16
. /usr/sbin/nfsd 16
. /usr/sbin/nfsd 16
. /usr/sbin/nfsd 16
. /usr/sbin/nfsd 16
. /usr/sbin/nfsd 16
. /usr/sbin/nfsd 16
. /usr/sbin/nfsd 16
. /usr/sbin/nfsd 16
. /usr/sbin/nfsd 16
. /usr/sbin/nfsd 16
. /usr/sbin/nfsd 16
. /usr/sbin/nfsd 16
. /usr/sbin/nfsd 16
. /usr/sbin/nfsd 16
. /sbin/sh /usr/dt/bin/dtrc
. /usr/sbin/getty console console
. /sbin/krsd -i
. /sbin/sfd
. /usr/sam/lbin/samd
. /etc/opt/resmon/lbin/p_client
. /usr/dt/bin/dtlogin
. /usr/sbin/stm/uut/bin/tools/monitor/disk_em
. /usr/sbin/stm/uut/bin/tools/monitor/dm_core_hw
. /usr/sbin/stm/uut/bin/tools/monitor/dm_memory
. /usr/sbin/stm/uut/bin/tools/monitor/dm_stape
. /usr/sbin/stm/uut/bin/tools/monitor/scsi123_em
. /usr/sbin/stm/uut/bin/tools/monitor/sysstat_em
. /opt/perf/bin/rep_server -t SCOPE /var/opt/perf/datafiles/loggl
. /opt/perf/bin/agdbserver -t alarmgen /var/opt/perf/datafiles/
. /opt/perf/bin/alarmgen -svr 3140 -t alarmgen /var/opt/perf/data
. nfsktcpd
. ntalkd

An attacker may use this information to gain more knowledge about the target host.

Solution : disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port

Risk factor : Low

Service: smtp (25/tcp)

Severity: Low

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 information.

Solution : if you are using Sendmail, add the option :

O PrivacyOptions=goaway

in /etc/sendmail.cf.

Risk factor : Low
CVE : CAN-1999-0531

Service: unknown (901/tcp)
Severity: Low

SWAT (Samba Web Administration Tool) is running on this port.

SWAT allows Samba users to change their passwords, and offers to the sysadmin
an easy-to-use GUI to configure Samba.
However, it is not recommended to let SWAT be accessed by the world, as it allows an intruder to attempt to brute force some accounts passwords.
In addition to this, the traffic between SWAT and web clients is not ciphered, so an eavesdropper can gain clear text passwords easily.

Solution: Disable SWAT access from the outside network by making your firewall filter this port.
If you do not need SWAT, disable it by commenting the relevant /etc/inetd.conf line.

Risk factor : Medium
CVE : CVE-2000-0935
BID : 1872

Service: chargen (19/tcp)
Severity: Low
The chargen service is running.
The 'chargen' service should only be enabled when testing the machine.

When contacted, chargen responds with some random characters (something like all the characters in the alphabet in a row). When contacted via UDP, it will respond with a single UDP packet. When contacted via TCP, it will continue spewing characters until the client closes the connection.

An easy attack is 'pingpong' in which an attacker spoofs a packet between two machines running chargen. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

Solution : disable this service in /etc/inetd.conf.

Risk factor : Low
CVE : CVE-1999-0103

Service: xdmcp (177/udp)
Severity: Low

The remote host is running XDMCP.

This protocol is used to provide X display connections for
X terminals. XDMCP is completely insecure, since the traffic and
passwords are not encrypted.

An attacker may use this flaw to capture all the keystrokes of
the users using this host through their X terminal, including
passwords.

Risk factor : Medium
Solution : Disable XDMCP

Risk factor : Low
CVE : CAN-1999-0651

Service: daytime (13/udp)
Severity: Low
The daytime service is running.
The date format issued by this service
may sometimes help an attacker to guess
the operating system type.

In addition to that, when the UDP version of
daytime is running, an attacker may link it
to the echo port using spoofing, thus creating
a possible denial of service.

Solution : disable this service in /etc/inetd.conf.

Risk factor : Low
CVE : CVE-1999-0103

Service: loc-srv (135/tcp)
Severity: Low

DCE services running on the remote can be enumerated
by connecting on port 135 and doing the appropriate
queries.

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

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

Service: echo (7/udp)
Severity: Low

The 'echo' port is open. This port is
not of any use nowadays, and may be a source of problems,
since it can be used along with other ports to perform a denial
of service. You should really disable this service.

Risk factor : Low

Solution : disable this service
CVE : CVE-1999-0103

Service: echo (7/tcp)
Severity: Low
The 'echo' port is open. This port is
not of any use nowadays, and may be a source of problems,
since it can be used along with other ports to perform a denial
of service. You should really disable this service.

Risk factor : Low

Solution : disable this service
CVE : CVE-1999-0103

Service: auth (113/tcp)

Severity: Low

The 'ident' service provides sensitive information
to potential attackers. It mainly says which accounts are running which services. This helps attackers to focus on valuable services [those owned by root]. If you don't use this service, disable it.

Risk factor : Low

Solution : comment out the 'auth' or 'ident' line in /etc/inetd.conf
CVE : CAN-1999-0629

Service: snmp (161/udp)
Severity: Low
It was possible to obtain the list of network interfaces of the
remote host via SNMP :

. lan1 Hewlett-Packard 10/100Base-TX Half-Duplex Hw Rev 0
. lan1 Hewlett-Packard LAN Interface Hw Rev 0

An attacker may use this information to gain more knowledge about the target host.
Solution : disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port
Risk factor : Low

Service: general/tcp
Severity: Low

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

Service: daytime (13/tcp)
Severity: Low

The daytime service is running.

The date format issued by this service
may sometimes help an attacker to guess
the operating system type.

In addition to that, when the UDP version of
daytime is running, an attacker may link it
to the echo port using spoofing, thus creating
a possible denial of service.

Solution : disable this service in /etc/inetd.conf.

Risk factor : Low
CVE : CAN-1999-0651

Service: discard (9/tcp)
Severity: Low

The 'discard' port is open. This port is
not of any use nowadays, and may be a source of problems,

Solution : comment out 'discard' in /etc/inetd.conf

Risk factor : Low
CVE : CAN-1999-0636

Service: smtp (25/tcp)
Severity: Low

According to the version number of the remote mail server,
a local user may be able to obtain the complete mail configuration
and other interesting information about the mail queue even if
he is not allowed to access those information directly, by running
sendmail -q -d0-nnnn.xxx
where nnnn & xxx are debugging levels.

If users are not allowed to process the queue (which is the default)
then you are not vulnerable.

Solution : upgrade to the latest version of Sendmail or
do not allow users to process the queue (RestrictQRun option)
Risk factor : Very low / none
Note : This vulnerability is _local_ only
CVE : CAN-2001-0715
BID : 3898

Service: snmp (161/udp)
Severity: Info

Using SNMP, we could determine that the remote operating system is :
HP-UX fortunes B.11.11 U 9000/800 157460511

Service: unknown (49159/udp)
Severity: Info

RPC program #100068 version 2 is running on this port
RPC program #100068 version 3 is running on this port
RPC program #100068 version 4 is running on this port
RPC program #100068 version 5 is running on this port

Service: unknown (49153/tcp)
Severity: Info

RPC program #100021 version 1 'nlockmgr' is running on this port

Service: auth (113/tcp)
Severity: Info

An identd server is running on this port

Service: unknown (49154/tcp)
Severity: Info

RPC program #100021 version 3 'nlockmgr' is running on this port

Service: unknown (49169/udp)
Severity: Info

RPC program #100005 version 1 'mountd' (mount showmount) is running on this port
RPC program #100005 version 3 'mountd' (mount showmount) is running on this port

Service: unknown (49156/udp)
Severity: Info

RPC program #100021 version 4 'nlockmgr' is running on this port

Service: unknown (49157/tcp)
Severity: Info

RPC program #100083 version 1 is running on this port

Service: unknown (49207/tcp)
Severity: Info

RPC program #100005 version 1 'mountd' (mount showmount) is running on this port
RPC program #100005 version 3 'mountd' (mount showmount) is running on this port

Service: unknown (49156/tcp)
Severity: Info

RPC program #100021 version 2 'nlockmgr' is running on this port

Service: unknown (49155/udp)
Severity: Info

RPC program #100021 version 3 'nlockmgr' is running on this port

Service: unknown (49154/udp)
Severity: Info

RPC program #100021 version 1 'nlockmgr' is running on this port

Service: time (37/tcp)
Severity: Info

A time server seems to be running on this port

Service: echo (7/tcp)
Severity: Info

An echo server is running on this port

Service: unknown (49153/udp)
Severity: Info

RPC program #100024 version 1 'status' is running on this port

Service: loc-srv (135/tcp)
Severity: Info

Here is the list of DCE services running on this port:
UUID: e1af8308-5d1f-11c9-91a4-08002b14a0fa, version 3
Endpoint: ncacn_ip_tcp:192.168.1.90[135]
Annotation: Endpoint Resolution

UUID: 333b33c3-0000-0000-0d00-008784000000, version 4
Endpoint: ncacn_ip_tcp:192.168.1.90[135]
Annotation: NCS1.5 Local Location Broker

Service: unknown (49159/tcp)
Severity: Info

Here is the list of DCE services running on this port:
UUID: 892b2b90-1532-11cf-9a39-00aa0034b922, version 2
Endpoint: ncacn_ip_tcp:192.168.1.90[49159]
Service: unknown (49279/tcp)
Severity: Info

Here is the list of DCE services running on this port:
UUID: 6a7914bf-d421-0000-020f-0898df000000, version 2
Endpoint: ncacn_ip_tcp:192.168.1.90[49279]
Annotation: Repository Interface - Version 2

Service: unknown (49281/tcp)
Severity: Info

Here is the list of DCE services running on this port:
UUID: 6e714df1-b3d2-0000-020f-08984b000000, version 2
Endpoint: ncacn_ip_tcp:192.168.1.90[49281]
Annotation: Alarm Generator Interface

Service: loc-srv (135/udp)
Severity: Info

Here is the list of DCE services running on this port:
UUID: e1af8308-5d1f-11c9-91a4-08002b14a0fa, version 3
Endpoint: ncadg_ip_udp:192.168.1.90[135]
Annotation: Endpoint Resolution

UUID: 333b33c3-0000-0000-0d00-008784000000, version 4
Endpoint: ncadg_ip_udp:192.168.1.90[135]
Annotation: NCS1.5 Local Location Broker

Service: unknown (49162/udp)
Severity: Info

Here is the list of DCE services running on this port:
    UUID: 892b2b90-1532-11cf-9a39-00aa0034b922, version 2
    Endpoint: ncadg_ip_udp:192.168.1.90[49162]

Service: unknown (49175/udp)
Severity: Info

Here is the list of DCE services running on this port:
    UUID: 6a7914bf-d421-0000-020f-0898df000000, version 2
    Endpoint: ncadg_ip_udp:192.168.1.90[49175]
    Annotation: Repository Interface - Version 2

Service: unknown (49178/udp)
Severity: Info

Here is the list of DCE services running on this port:
    UUID: 6e714df1-b3d2-0000-020f-08984b000000, version 2
    Endpoint: ncadg_ip_udp:192.168.1.90[49178]
    Annotation: Alarm Generator Interface

Service: lockd (4045/udp)
Severity: Info

RPC program #100020 version 1 'llockmgr' is running on this port

Service: nfs (2049/udp)
Severity: Info

RPC program #100003 version 2 'nfs' (nfsprog) is running on this port
RPC program #100003 version 3 'nfs' (nfsprog) is running on this port

Service: unknown (49152/tcp)
Severity: Info

RPC program #100024 version 1 'status' is running on this port

Service: smtp (25/tcp)
Severity: Info

This server could be fingerprinted as being Sendmail 8.9.3

Service: sunrpc (111/udp)
Severity: Info

RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is running on this port
RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is running on this port
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port

Service: smtp (25/tcp)
Severity: Info

An SMTP server is running on this port
Here is its banner :
220 fortunes ESMTP Sendmail 8.9.3/8.9.3; Tue, 26 Aug 2003 15:25:34 -0400 (EDT)r

Service: smtp (25/tcp)
Severity: Info

Remote SMTP server banner :
220 fortunes ESMTP Sendmail 8.9.3/8.9.3; Tue, 26 Aug 2003 15:26:21 -0400 (EDT)r

This is probably: Sendmail

Service: lockd (4045/tcp)
Severity: Info

RPC program #100020 version 1 'llockmgr' is running on this port

Service: nfs (2049/tcp)
Severity: Info

RPC program #100003 version 2 'nfs' (nfsprog) is running on this port
RPC program #100003 version 3 'nfs' (nfsprog) is running on this port

Service: unknown (910/tcp)
Severity: Info

RPC program #805306352 version 1 is running on this port

Service: unknown (49155/tcp)
Severity: Info

RPC program #100021 version 4 'nlockmgr' is running on this port

Service: sunrpc (111/tcp)
Severity: Info
RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is running on this port
RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is running on this port
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port

Service: sunrpc (111/tcp)
Severity: Info
The RPC portmapper is running on this port.

An attacker may use it to enumerate your list
of RPC services. We recommend you filter traffic
going to this port.

Risk factor : Low
CVE : CAN-1999-0632, CVE-1999-0189
BID : 205

Service: general/tcp
Severity: Info
Remote OS guess : Apple Mac OS 9.04 or HP-UX B.11.00
CVE : CAN-1999-0454

Service: dtspc (6112/tcp)
Severity: Info
The service closed the connection after 0 seconds without sending any data
It might be protected by some TCP wrapper

Service: chargen (19/tcp)
Severity: Info
Chargen is running on this port

Service: smtp (25/tcp)
Severity: Info

Nessus sent several emails containing the EICAR test strings in them to the postmaster of the remote SMTP server.
The EICAR test string is a fake virus which triggers anti-viruses, in order to make sure they run.

Nessus attempted to e-mail this string five times, with different codings each time, in order to attempt to fool the remote anti-virus (if any).

If there is an antivirus filter, these messages should all be blocked.

*** To determine if the remote host is vulnerable, see if any mail arrived to the postmaster of this host

Solution: Install an antivirus / upgrade it

Reference : http://online.securityfocus.com/archive/1/256619
Reference : http://online.securityfocus.com/archive/1/44301
Reference : http://online.securityfocus.com/links/188

Risk factor : Low

Service: general/udp
Severity: Info

Service: daytime (13/tcp)
Severity: Info

An unknown server is running on this port.
If you know what it is, please send this banner to the Nessus team:
00: 54 75 65 20 41 75 67 20 32 36 20 31 35 3a 32 35 Tue Aug 26 15:25
10: 3a 33 31 20 45 44 54 20 32 30 30 33 0d 0a :31 EDT 2003..

Appendix C – Security_Patch_Check output

/opt/sec_mgmt/spc/bin/security_patch_check –c ./security_catalog

WARNING: HP has issued Critical warnings for the active patch PHCO_27408 on the target system. Its record, including the Warn field, is available from ./security_catalog, through the Patch Database area of the ITRC or by using the -m flag (security_patch_check -m ...).

WARNING: HP has issued Critical warnings for the active patch PHKL_27156 on the target system. Its record, including the Warn field, is available from ../security_catalog, through the Patch Database area of the ITRC or by using the -m flag (security_patch_check -m ...).

*** BEGINNING OF SECURITY PATCH CHECK REPORT ***
Report generated by: /opt/sec_mgmt/spc/bin/security_patch_check.pl, run as root
Analyzed localhost (HP-UX 11.11) from fortunes
Security catalog: ./security_catalog
Security catalog created on: Tue Dec 23 21:13:16 2003
Time of analysis: Wed Dec 24 13:37:10 2003

List of recommended patches for most secure system:

#	Recommended	Bull(s)	Spec?	Reboot?	PDep?	Description
1	PHCO_23492	159	No	Yes	No	Kernsymtab
2	PHCO_23909	167	No	No	No	cu(1)
3	PHCO_25918	237	No	No	No	sort(1) cumulative
4	PHCO_26061	153	No	No	No	Kernel configuration commands
5	PHCO_26561	275	No	No	No	csh(1) cumulative
6	PHCO_27019	275	No	No	No	ksh(1)
7	PHCO_27037	191	No	No	Yes	libpam_unix cumulative
8	PHCO_27345	275	No	No	Yes	cumulative sh-posix(1)
9	PHCO_27694	160	No	No	No	login(1) cumulative
10	PHCO_28259	213	Yes	No	No	lpspool subsystem cumulative
11	PHCO_28481	252	Yes	No	Yes	cumulative 10.20 libc compatibility support
12	PHCO_28719	258	No	No	No	wall(1M)
13	PHCO_28848	293	No	No	No	Software Distributor Cumulative
14	PHCO_29010	304	No	No	No	shar(1)
15	PHCO_29495	294	Yes	No	Yes	libc cumulative
16	PHKL_23335	178	No	Yes	No	solve inode deadlock with mmap and pagefault

17 PHKL_23423 156 No Yes No improper core dump msg
18 PHKL_27179 206 No Yes No Corrected reference to thread register state
19 PHKL_28990 183 No Yes No Cumulative VM
20 PHNE_24512 232 Yes No No NTP timeservices upgrade plus utilities
21 PHNE_25644 192 205 No Yes Yes See WARNINGS in patch database, itrc.hp.com, cumulative ARPA Transport
22 PHNE_27703 271 No Yes Yes Cumulative STREAMS
23 PHNE_27765 162 No No No ftpd(1M)
24 PHNE_27796 209 Yes No Yes libnss_dns DNS backend
25 PHNE_28444 270 No Yes No nettl(1M), netfmt(1M) and nettladm(1M)
26 PHNE_28983 252 Yes Yes Yes ONC/NFS General Release/Performance
27 PHNE_29774 281 Yes No No sendmail(1m) 8.9.3
28 PHNE_30068 303 No No No Bind 8.1.2
29 PHSS_27858 208 Yes No No OV EMANATE14.2 Agent Consolidated
30 PHSS_28470 228 No No No X Font Server
31 PHSS_28677 263 Yes No Yes CDE Applications Periodic
32 PHSS_29371 289 No No No X/Motif Runtime Periodic
33 PHSS_29964 276 299 Yes No Yes HP DCE/9000 1.8 DCE Client IPv6
34 PHSS_30011 297 Yes No No CDE Base

*** END OF REPORT ***

NOTE: Security bulletins can be found ordered by number at
http://itrc.hp.com/cki/bin/doc.pl/screen=ckiSecurityBulletin