Global Information Assurance Certification Paper

GCUX Practical

Version 1.9

Option 2 Track 6 Securing Unix

GIAC Enterprises Audit of an Oracle 9i/Web Server running on Solaris 2.7

By

Jeffrey Tomaszewski

December 2003

Abstract

A Security Policy is the driving dynamic that needs to be in place to help mitigate an Organizations risks. The policy not only will provide a starting point, it will also provide the empowerment the IT staff will need to help reduce its informational vulnerabilities. This paper is the result of an audit preformed on the GIAC Enterprises UNIX database server. The report and recommendations will help reduce the risks associated with this machine under its current operating environment. These recommendations along with an established Security Policy will position GIAC Enterprises in a situation to mitigate these seen and other unforeseen risks.

Table of Contents

Preface

Due to the sensitive nature of the data in this report, the dates, name(s) and IP address(s) have all been changed to protect the innocent.

Executive Summary

GIAC Enterprises, which is a fictitious e-business online fortune cookie development company, has asked an outside security consultant to conduct a security audit of one of its primary Unix server called confucious.giac-ent.com. The security consultant technical lead authoring this report was Jeffrey Tomaszewski. Jeff's work was performed during the week of July 14th-22nd 2003 in the Washington D.C. office.

This report, in essence is a detailed description of the security of GIAC Enterprises main Oracle production server. The scope of this report includes the network topology for this system, the server's operating system, the server's modus operandi, the server's application set, and the physical security of this machine. Some 3rd party vendor application specific exploits are deemed out of scope and would be deferred to the vendor's technical support center for resolution. This report should be of tremendous value to GIAC Enterprises Management, and it is advised that they follow upon its recommendations. It should be stated however, that there is never a 100% secure environment and security is a continuous job, not a mere one time audit. However, with the financial investment and policies in place to support GIAC Enterprises Information Security Team (which comprises of each and every one of GIAC Enterprises employees), they will be able to mitigate these risks. GIAC Enterprises in doing so has set an exemplary example to the industry.

The following is a brief synopsis of the most important security vulnerabilities found on this system and the appropriate fixes. The largest security concern would be to adopt a Security Policy that would not only change the corporate operational routine, it will usher the organization into a more secure computing environment. The difficulty of authoring and implementing a Security Policy is greatly understood, however this is deemed the highest priority. With the adaptation of a Risk Management process along with a Security Awareness campaign designed to educate each employee how they need to be aware of security both physical and informational as it corresponds to their daily activities. This activity of course needs to be top down approach, starting with the president who is ultimately responsible for the corporate resources on down. This should not come from the IT staff on up.

The second largest concern is with the machines network architecture. This should be addressed and a redesign should be implemented. This machine is currently using publicly available Internet Protocol (Ipv4) address space. The connectivity to this machine is open to the public, it is not protected by a firewall and as a result the machine was found to have very minimal network access controls. This machine is also running an Apache Web Server, and Oracle forms server on the same physical machine as the primary Oracle instance (database).

It is strongly recommend that the Apache Web Server and forms server be placed on a separate box located within the companies DMZ and move this machine behind a corporate firewall, and limit its connections with the appropriate firewall policy. The splitting of services off of this machine is paramount as is the introduction of a firewall architecture to the organizations corporate LAN. The topology of the current system is legacy and should be addressed.

The third largest concern is with the installation of the latest operating system patch sets. As indicated in the Appendix via the Sun Patch Report script, the necessary patches for this machine have been identified at length. It is critical that this machine is kept up with the latest operating system patch sets. Because of the staff's ability to log onto services/applications on this machine remotely and because of the network topology found at this site, exploits may be avoided and risks mitigated through the successful and continual application of patches.

The fourth largest security practice which would help to mitigate the risks of this machine is to turn off unnecessary services and to correct the AFS access control list and Unix permissions of this machine, in addition account password strength (both Unix and Oracle) and the /etc/group (group file management and account management) would all be a step in the right direction again to mitigate risks. Through password auditing with tools such as John the Ripper, and the investigation that there is no password policy at the site, it is highly recommended that password aging, dictionary checking and password re-use policies be drafted and instituted.

Description of System and Audit Methodology

The audited host contains an Oracle database version 9.0.1.3, along with a web server and Oracle forms server front end. The web server is an Apache server version 2.0.45 running on a Solaris 2.7 SUN Ultra 60 Model 1360. The machine has 768MB of RAM. The system has 5 9 gig drives, one drive containing the system disk (with the exception of /usr/local) that is a mount point to a read only AFS file system. The other 4 spindles are following Oracles disk architecture in which they contain dbf files and other Oracle software and infrastructure (archive logs etc). There are no NFS mounts being utilized on this machine. Please see the Appendix for detailed output of the sysinfo command and df –k results. This system serves as GIAC Enterprises main web presence as it pertains to its intranet functionality (not intended for use for outsiders). However, because of the topology of GIAC's LAN this machine is also accessible via the Intranet. The main usage of this machine is GIAC Enterprises corporate database, via its forms front end which is launched through the website. This system needs to be up 24 by 7 and accessible to all authorized users anywhere. Because database updates can occur at anytime there can be no downtime for backups, thus the database is running in archive log mode and Oracle backups are run hot.

Several automated auditing tools were used to conduct this investigation. All of these are freely available public software. The auditing toolsets are as follows: NMAP version 3.48, NESSUS version 2.0.9, Tara version 3.0.3 and CIS Security Benchmark Checker version 1.4.0. Operating System audit trail was done with the freely available Patch Report program, and additional freely available application specific (see Appendix Oracle) scripts were run to address Oracle user account passwords, although this is not a detailed audit report of the Oracle database and that segment would be out of scope of this investigation. There was however a basic level of audit on the Oracle Database user accounts and passwords. It is strongly recommend that GIAC Enterprises hire a database security consultant if they wish to have a more in depth understanding of Risk Mitigation as it pertains to the Oracle Database.

Detailed Analysis

Operating System Vulnerabilities

The audited host is running SunOS 5.7 (Solaris 2.7) Generic 106541-15 sun4u sparc SUNW, Ultra-60. The Appendix lists a detailed report of the number of critical security patches identified via the Patch Report program. It is in this area that brought about the third highest level of recommendations for risk mitigation as it pertains to this box. The administration of this box has been neglected as it pertains to patch management. A large number of patch sets have been identified which need to be applied to this host. These have all been identified in the Appendix and they are available via the ***sunsolve.sun.com*** site. It has been confirmed that GIAC Enterprises does have access to the patches and they are available for download for GIAC Enterprises administrators to install. Note that due care should be taken to check the validity and ramifications of these identified patches prior to their installation.

Another operating system risk includes the /etc/group file, which after consultations with GIAC Enterprise staff was found to be out of date and does not accurately reflect the current state of the IT environment. The use of the Guardrail application (Guardrail is a password deployment program which pushes out passwords on an hourly basis from a master machine via scp) complicates the manner as this application only provides accountability to the /etc/password file, not the /etc/group file, thus these files fall out of sync and need to be manually reviewed on a continual basis. It is my recommendation that the group file be audited at least on a weekly basis as the need for /etc/group changes is not regular.

The use of the Synctree application does provide an excellent safe guard to the /etc/inetd.conf and other “sync’d” files (crontab, and hostconfig etc). In essence the copying down from “gold copies” of these files from AFS adds an important security concept of knowing that if these files are tampered with they will be restored to the original condition on a nightly basis (provided everything is working correctly).

Core files are a potential treasure trove for deviants. And the management of the core files needs to be addressed through corporate policy. Currently no policy is in place to address this concern and the benefits and consequences need to be discussed and weighed accordingly. Again it should be known that core files can contain passwords, file contents, directory path info etc.[i] Some corrective steps can be introduced on a per user basis and also on a system wide basis[ii] (see Appendix).

Security Patch Installation and Management

After interviewing GIAC Enterprises, Unix Administration team it became clear that no policy is in place to ensure that the latest security operating system and application patches are being applied and addressed on a regular basis. GIAC Enterprises has the robust ability to roll out the security and application patches on a global scale through the Synctree process, however due to time limitations, reduced staffing levels and limited skill sets this has not been carried out.

A monthly review of patch sets needs to be part of the system administrator's job function. This can be setup via cron in which Patch Report could be run and the output parsed and determined what action needs to be taken (if any) on which class of machines. It is highly recommend that a policy be put in place to have this work done. Often heard are the arguments that "if it isn't broke, don't fix it". However, it is clear by the amount of patches released by the vendors that the applications are indeed broken. Also 3rd party vendors such as Oracle require the latest patch sets be applied to its application prior to the creation of an itar (Oracle Technical Support Request).

It should be noted however, that the patch installation process is tedious and requires an in-depth level of understanding. It is not merely enough to run Patch Report and apply the suggested patches because GIAC Enterprises computing environment is highly customized, not all patches that are suggested are actually applicable to the organizations needs. In addition some patches may actually cause other ramifications once applied (i.e. the machine might not boot); therefore testing should be done on a parallel system prior to any changes on this critical production machine.

The management of the machine is handled by a select group of administrators. A total number of 5 users have root access. No sudo access is granted. Both DBA's have root access and one of the two performs Unix Administration duties as well. There are in addition 16 other end user accounts that have shell access to the machine.

In addition to the user machine accounts there are 55 Oracle accounts, all with different privilege levels. Only two users have sys and system access to the Oracle database. 5 additional users have developer privileges (equating to unlimited table space). There is no password aging enforcement or password re-use policy on the Oracle accounts; this needs to be addressed through the corporate policy.

Configuration Vulnerabilities

Often services are started up that are not necessary at boot time. This is often the result of a simple configuration mishap (or even jumpstart configuration), which can be addressed by disabling these services through the RC init scripts. The following services were found not necessary and should be turned off (lockd, printd, fingerd, and lpr). In addition the application banners often reveal too much information about the applications themselves. A deviant who has a known exploit in hand for a particular application version would be delighted to know this host is running version X of… For instance the Sendmail banner, and Apache banner were two specific examples found doing so. The configuration of the applications not to display this information is rather trivial and should be addressed in the Security Policy as well.

The use of TARA Version 3.0.3 revealed a slew of permission problems and user challenges that need to be addressed. In addition the CIS Benchmark Tool Set independently confirmed these issues as well as other challenges. It should be noted however, many false positives were indicated by both auditing tool sets, because of the unique operating environment and AFS acl's many checks performed by these toolsets were in error and actually lowered the overall scoring values. The detailed output listed in the Appendix of these results show several directories, which need to be chown'd (group change ownership) as well.

A review of the system named.conf file indicates that this host is running Bind Version 8.2.2 (which should be updated) however the implementation of a caching name server has added security benefits.

Risks From Installed Third-Party Software

Some of the largest security risks presented to this machine are the exploits to the Oracle software and the Apache configuration. Often deviants utilize Trojan horse type attacks in which they replace the binaries of often called programs to hide their tracks and to perform other malicious activities. GIAC Enterprises utilizes a /usr/local read only file system to combat such activities, however, if the users account (path) is modified to utilize local copies such as those found in /bin this might give the organization a false sense of security. Tripwire should be utilized to check the integrity of the local file system.

In addition to the replacement of binaries, the introduction of 3rd-Party software necessitates the need/requirement for proper configuration of the application and the continual effort of patching, upgrading and maintaining (reviewing of logs etc) the software.

Administrative Practices

GIAC Enterprises operational practices incorporate the use of Synctree, which distributes on a nightly basis (gold copies) of binaries, configuration files, libraries and other operating system and application files. This process ensures the integrity of the files on the system (as long as the master copies aren't

compromised and as long as the client machines are syncing). GIAC Enterprises also uses a shell script called Guardrail which pushes out the /etc/passwd file from a master host. This process is done on an hourly basis. There are some challenges with Guardrail, especially with the fact that it does not keep in sync the /etc/group file. However this process does keep a central control for account management (as long as the master host isn't compromised).

The log rotation of the Apache log files is carried out on 3-day process due to Legal concerns. This process could potentially hamper the back tracking and investigation of security breaches. If GIAC Enterprises don't have the data to track down what happened they might not be able to recover in a quick time frame. Also GIAC Enterprises might not be able to provide evidence to law enforcement agencies in the event of a prosecution. GIAC Enterprises does utilize a central logging server which this audited hosts send /etc/syslog messages to (over the network).

Currently, no policies are in place to administer the patch sets or even to add, alter or remove accounts. It was found that often is the case that there would be support request to have an account added but rarely removed, and further more no operandi is in place to review host vulnerabilities and application. It is strongly urged to change this culture. And to have GIAC Enterprise Management and Staff make this a priority.

There is no routinely planned audit of the systems nor is there any written Security Policy or Administrative Guidelines in place to oversee the day to day operations. There is a continued 24x7 support of the machine carried out by IT staff; in addition there are self monitoring scripts on the host and remote monitoring via the Network Operations Center (NOC) which monitors the health of the machine.

Identification and Protection of sensitive Data on the Host

The Oracle Database contains the most critical information on this system. Other sensitive nature data include the server log files; Apache log hits indicate client host ip addresses and surfing habits. The triad of confidentiality, integrity and accessibility all need to be addressed.

There are currently no audits being performed to check the confidentiality of the data in the database or on the machine. Once production code is in place the code is never double-checked or even triple checked, by the developers to ensure that the valid access constraints are in place.

Currently there are no processes to check for the data integrity on the Oracle database. This current practice puts blind faith in the data that is stored and retrieved. GIAC Enterprises should invest the time and effort to ensure that the data integrity of the system is in good standing.

The system is currently monitored by pings from the NOC and the system also runs in house authored shell scripts (daemon check) that sends notification messages to the NOC for investigation, this ensures accessibility, or at lease prompt notification in the event of a failure.

Protection of sensitive Data in transit over the Network or Intranet

The use of the Oracle forms server through a secure web server, in particular the Apache Server version 2.0.45 over the network does provide minimal amount of encryption. However, the use of Amanda backups over the network is deemed a potential liability. As well is the machines dependency on /usr/local as being a remote file system (located on the AFS cell), although this points to a read-only file system, it has the potential for disaster if the AFS volume is compromised or even unavailable (not taking into consideration of replicated volumes). If the golden copies of the /usr/local software are compromised either maliciously or by administrator mistake it could potentially lead to a catastrophic outage.

The network encryption of the Oracle forms server is based on 48-bit Oracle forms security. There is also utilization of the Apache (https) secure server. Since the forms are served only through the Apache front end, it is strongly recommend to move these services off to a another machine. The utilization of sshv1 also needs to be addressed as well as several documented exploits for this protocol exist, an upgrade to sshv2 and Kerberos V would greatly mitigate the remote connection risks.

The utilization of the central logging server should be taken under advisement as well, this traffic dependent upon the LAN architecture might be available for others on the network segment to see in the clear.

Finally, a redesign of the corporate LAN should be implemented. The organization might want to consider NAT'ing its LAN's address space and certainly invest in some firewall technology, either application or appliance based, the determination can be made once the Security Policy is written.

Access Controls

After interviewing GIAC Enterprises Oracle DBA's it became clear that they are short staffed and pulling Unix Administration duties as well (it was the same person). It was hard to delineate and even tell where the change and separation of duties flowed. Due to the limited number of staff on hand and the functional duties of the staff, it is strongly urged to have GIAC Enterprise document the administrative practices of the administrators in case of staff turn over or if they get "hit by a bus". By doing so, someone else may be able to step in and know the operational functions of this system.

The physical location of the device located within a somewhat secure data center is a plus however; on the down side there are additional staff which have access to the data center. As it turns out, other staff once entering the data center have immediate physical access to this machine, which of course has its drawbacks. Therefore a recommendation to cage off this production server within the data center is suggested.

The introduction of a password policy is mandatory to help mitigate the risks associated with passwords. As shown in the Appendix the use of "John The Ripper" a password cracking application showed conclusive results, in

addition the use of an Oracle password audit script (one that simply matched the user name and password based upon the user name) brought about a significant number of hits. Because this host has both applications located on it, a password policy must be authored and endorsed. The use of Guardrail to push out the users passwords to an Oracle class machine (allowing for multiple hosts to have the same password) and even the pushing out of user accounts that have the same password on multiple hosts is a threat that can be mitigated. In addition if users use the same password in the Microsoft environment one can potentially introduce a slew of single point of failures, or single sign on, turnkey challenge set. (GIAC Enterprises is a heterogeneous computing environment) A potential mitigation towards this is the introduction of a password policy that mandates the changing of passwords on a monthly basis, and thus to have password aging and reusing enabled, also minimal strength password testing and even encouraging password audits to be conducted. Corporate education should be carried out to avoid writing down passwords, to be on the lookout for Social Engineering tricks and for "shoulder surfing". It should be mentioned that the corporate investment in Kerberos certainly has added a wealth of security features to the environment; however the migration to Kerberos V is paramount as several known published exploits to Kerberos IV are available.

Backup Policies, Disaster Preparedness

The current system is being backed up via Amanda over the network, (the client version of Amanda is 2.4.3 which should be upgraded) in addition to the operating system backups (note Amanda is backing up /, /usr, /var, and /private). The backup tapes are stored in a locked heat resistant cabinet located in another building and they are rotated every 30 days. Oracle exports and full hot backups are being performed on a daily basis. The disk layouts appear as follows (see Appendix). The Oracle exports are being stored in AFS and are being run every 12 hours. The exports contain the critical table spaces and are being imported every 12 hours on a backup machine. There is one weeks worth of exports located in the AFS space, ensuring on-line exports (backups) for immediate disaster recovery and fail over.

GIAC Enterprises has appropriated a dedicated backup server, which is a replica of this system. This backup server receives daily imports of the database by cron jobs, which import the data from AFS. In addition the use of virtual interfaces allow for quick recovery in the event of transfer of services (if the primary machine goes down). The modification of the Oracle tnsnames file which is also in AFS would be one step which is critical to activating the services however, depending on the type and time of the outage minimal disruption can occur.

Other Challenges/Vulnerabilities

Oracle account management has been identified as relaxed. Again this is a direct result of GIAC Enterprises policy, which is in absentia. No regular clean up

of Oracle accounts is scheduled. The same issue has been identified with the machine accounts, passwords and the password management; in addition /etc/group member policies are also not accounted for. The utilization of the Guardrail program which pushes out accounts and passwords is looked upon as a way to address accounts across the organization, but without a policy to address who should have access and even who should have accounts, including application accounts such as Oracle user accounts, and what users should have access to which tables etc, all need to be led by corporate policy and followed by the appropriate support staff.

As mentioned above, GIAC Enterprises should introduce a data checking (integrity check) of its corporate database on a routine basis. Many statistical formulas have been created to ensure the proper checks per database update activity. It is highly recommended that this action be carried out because currently there is no data validity checking.

Critical Issues and Recommendations

Top 10 Vulnerabilities/Challenges

1. No Policy – Because GIAC Enterprises has no Security Policy, it is obvious that the operations staff has no direction or empowerment to mitigate risks. (they spend most of their time putting out fires) It is ultimately the Presidents responsibility (on down) to protect GIAC Enterprises resources. To help the organization come to terms to help mitigate risks there must be top down approach towards security; one that receives support from the President on down. It is NOT the role of the IT staff to author policy. This is the responsibility of GIAC Enterprises management. Certainly the IT staff can recommend and work with the drafting of these policies as subject matter experts (SME's) however, it is not and should not fall on their shoulders. Even a general Security Policy could empower the IT staff with the authority it requires to do a good job at enforcing services (turning on or off), accounts (creation and deletion, and access modification), machines (building, retiring, monitoring and upgrading), access (physical and remote), backups (offline, online, retention and restoration) and the like. All of these are daily activities of the IT staff, which should be empowered by the corporate policy.

2. Network Topology – The use and consolidation of the services located on this machine make it imperative to move some of these services off onto another machine. However, this in itself will not suffice, as the entire GIAC Enterprise topology should be restructured to include a DMZ and to employ the use of a firewall to protect the corporate LAN.

a) Network topology redesign
b) Splitting of services onto protected and DMZ hosts

3. Document Operational Procedures – Currently very little documentation exists on how or what this machine does or even how it works. It would take

someone new to the organization some time to figure out what all the processes and dependencies are upon this system. A documented project plan should be drafted and maintained for the operations staff to have in the event of an emergency. In addition a Risk Assessment and Contingency Plan should be drafted and reviewed (exercised) to train for emergencies.

4. Application of Operating System Patches – The application of Operating System patches needs to be completed and should be done as soon as possible. In addition an operation policy should be drafted and approved to address these:

a) Apache – configuration and version control (upgrade path)
b) OpenSSL – (upgrade path)
c) Oracle – configuration and version control (upgrade path)
d) Kerberos IV to Kerberos V. – (upgrade path)
e) Amanda – Network backups verses local backups, also (upgrade path)
f) Ssh to version 2 – Kerberos ticket handling issues with sshv2 needs to be worked out/addressed to upgrades so v2 can take place.

5. Account Cleanup – The handling of accounts especially the /etc/group file needs to be addressed. Again the drafting of policy, which would provide structure to the daily operandi for, this machine, in particular the area of account access will be addressed by this policy. A formal procedure for adding accounts and removing accounts, also for password management should be adopted.

a) Remove expired accounts
b) Verify and clean up /etc/group entries
c) Introduce password management policy (password length, and aging)
d) Introduce password changing policy

6. Service Termination – The termination of excessive services should be addressed. These daemons and programs are not required for the successful operation of the server.

a) Lockd – not required
b) printd – not required
c) fingerd was enabled on this system; it is recommend to be turned off.
d) lpr was enabled on this system; it is recommend to be turned off.

7. TCP Wrapper Review – The review and enforcement of the machines tcp wrappers should be conducted. This will make sure that machines that need remote access have remote access and those that don't require it, don't have it (via hosts. allow and hosts. deny). In addition the audit of the sqlplus logs to review the Oracle remote connections is proper.

8. Physical Access – Review who has physical access to the data center where this machine is located and if those personal have or need physical access to the machine. (Note data center access is controlled by card swiping and is under 24x7 video monitoring). However once entry is made into the data center access can be granted to all equipment within.

9. Log Monitoring – The review of system logs, both operating system to the corporate logging host and the DAILY review of Oracle and other application logs should be maintained. In addition NOC monitoring procedures should be reviewed and updated on a routine basis. (For example did the NOC respond properly to the latest alarm on the host?). The utilization of syslog parsing scripts should be taken into consideration, as it will greatly enhance the administrators' ability to cope with such a large amount of data on the syslog logging host.

10. Backdoor Access – The utilization of out of band access to the machine needs to be secure. The machine has a back door connection via console port, this needs to be secured as well as reviewed for suspicious activity. Frequently changing the console port connectivity methods (accounts/passwords and ports) should be put in policy.

Further Recommendations

The largest task laid out in this report is for the organization to grasp a Security Policy and thus impacting each and every employee's role in information security. As the organization is only as secure as its weakest link. Accordingly this machine is only secure as its weakest exploit. Often security breaches come from within the organization, and without a corporate policy or environment that raises the level of security it is as if you are Sisyphus trying to roll that rock up a hill for eternity; in other words, it is pointless.

Through the use of the freely available auditing tools several recommendations have been made in the Appendix. Of particular usefulness is Patch Report, NESSUS report, Tara report and the CIS benchmark, specifying exactly what upgrades and steps should be carried out. The UNIX administration team should follow these recommendations where applicable. Finally, a Risk Assessment is also critical for the creation of a contingency plan. The assessment will not only prepare for disaster recovery, it will help the organization understand its assets. Finally, it is highly encouraged that GIAC Enterprises to go through the exercise of writing a Risk Assessment.

Appendix

Sysinfo command output (truncated and modified, not shown sysconf information, software information)

G E N E R A L I N F O R M A T I O N

Host Name is	confucious.giac-ent.com
Host Address(es) is	xxx.xxx.xxx.xxx
Host ID is	xxxxxxxxxx
Serial Number is	xxxxxxxxxx
Manufacturer is	Sun (Sun Microsystems)
Manufacturer (Short) is	Sun
Manufacturer (Full) is	Sun Microsystems
System Model is	Ultra 60 Model 1360
Main Memory is	768 MB
Virtual Memory is	1.6 GB
ROM Version is	OBP 3.17.0 1998/10/23 11:26
Number of CPUs is	1
CPU Type is	sparcv9+vis
App Architecture is	sparc
Kernel Architecture is	sun4u
OS Name is	SunOS
OS Version is	5.7
OS Distribution is	Solaris 7 5/99 s998s_u2SunServer_09 SPARC
Kernel Version is	SunOS Release 5.7 Version Generic_106541-15
[UNIX(R) System V Release 4.0]	
Boot Time is	xxx
Current Time is	xxx

D E V I C E I N F O R M A T I O N

SUNW,Ultra-60
  cpu0 is a "Sun UltraSPARC-II" 360 MHz CPU
  kbd is a "Unknown" Keyboard

Patch Report
showrev -p | sort -n +2 | nawk ' { printf "%s ", $2 } '
106146-05 106146-17 106147-01 106148-12 106541-04 106541-14 106725-02
106733-07 106748-04 106793-02 106793-05 106812-04 106857-04 106879-01
106888-02 106917-01 106924-01 106924-06 106925-01 106925-06 106934-03
106936-01 106938-01 106938-04 106940-01 106942-01 106942-14 106944-01
106944-03 106946-01 106946-02 106948-01 106949-01 106950-03 106950-13
106952-01 106960-01 106963-01 106978-06 106978-10 106980-04 106980-15
106982-01 106985-01 106987-02 106987-03 106999-01 107001-01 107003-03

107011-01 107014-01 107018-01 107022-02 107022-06 107026-09 107031-01
107038-01 107044-01 107049-01 107058-01 107059-01 107063-01 107072-01
107074-01 107076-01 107081-03 107081-25 107094-02 107115-01 107117-03
107121-01 107127-02 107147-03 107148-03 107148-08 107171-02 107171-08
107175-01 107178-01 107180-04 107185-01 107187-01 107200-03 107219-01
107226-03 107233-01 107248-01 107250-02 107259-01 107285-01 107285-02
107293-01 107306-01 107316-01 107318-04 107330-01 107330-02 107332-02
107337-01 107359-01 107359-02 107374-01 107401-01 107403-01 107430-01
107437-02 107438-01 107441-01 107441-02 107443-03 107443-13 107445-01
107448-01 107451-01 107451-05 107453-01 107454-01 107454-05 107456-01
107458-01 107458-10 107459-01 107460-01 107460-08 107462-01 107465-02
107469-08 107475-01 107477-03 107499-02 107544-03 107546-02 107551-01
107553-01 107555-01 107584-01 107587-01 107624-01 107636-05 107650-08
107652-06 107654-08 107656-06 107658-05 107680-01 107709-07 107743-07
107744-02 107792-02 107794-01 107796-03 107834-03 107836-01 107841-02
107843-02 107853-01 107865-01 107972-01 108029-02 108068-03 108089-02
108147-01 108148-01 108158-01 108162-02 108168-01 108170-01 108219-01
108221-01 108224-01 108227-01 108244-02 108263-06 108285-01 108299-01
108301-02 108309-02 108311-01 108319-01 108327-01 108331-01 108374-04
108376-21 108378-01 108381-01 108383-01 108414-01 108451-05 108482-02
108484-01 108592-01 108610-01 108662-01 108665-01 108683-01 108721-02
108748-01 108758-01 108760-01 108762-01 108764-01 108798-01 108800-01
108838-02 108912-01 109203-02 109205-01 109253-01 109372-01 109404-01
109409-03 109439-01 109709-01 109711-01 109713-01 109744-01

106541-30	Security	Recommended	14	107544 107834	Dec/16/03	SunOS 5.7: Kernel Update Patch
☐ 106725-03	Security	Recommended	02		Nov/11/02	OpenWindows 3.6.1: mailtool va
☐ 106793-07	Security	Recommended	05		Mar/26/01	SunOS 5.7: ufsdump and ufsrest
☐ 106924-11	NA	Recommended	06		Nov/18/02	SunOS 5.7: isp driver Patch
☐ 106925-09	NA	Recommended	06		Feb/27/02	SunOS 5.7: glm Driver Patch
☐ 106934-04	Security	Recommended	03		Dec/07/01	CDE 1.3: libDtSvc Patch
☐ 106938-07	Security	Recommended	04		Feb/26/03	SunOS 5.7: libresolv, in.named, l patch
☐ 106942-	Security	Recommended	14	106541 106541	Feb/28/01	WITHDRAWN SunOS 5.7: libnsl, nis_cachemgr patch

15						
106942-28	Security	Recommended	14	106541	Aug/12/03	SunOS 5.7: libnsl, rpc.nisd and n
106949-03	Security	Recommended	01		May/01/03	SunOS 5.7: BCP (binary compati
106950-24	Security	Recommended	13		Oct/22/03	SunOS 5.7: Linker Patch
106952-03	Security	Recommended	01		Nov/05/01	SunOS 5.7: /usr/bin/uux patch
106978-12	Security	Recommended	10	107456	Jul/23/01	SunOS 5.7: sysid patch
106980-23	NA	Recommended	15	106541	Jun/24/03	SunOS 5.7: libthread patch
107022-08	Security	Recommended	06	108374	May/04/01	CDE 1.3: Calendar Manager patc
107038-02	Security	Recommended	01		Jun/28/01	SunOS 5.7: apropos/catman/mar
107058-02	Security	NA	01		Sep/03/03	SunOS 5.7: Patch for assembler
107115-13	Security	Recommended	01		Jul/17/03	SunOS 5.7: LP Patch
107148-11	NA	Recommended	08		Feb/15/02	SunOS 5.7: /kernel/fs/cachefs pa
107171-13	Security	Recommended	08	112590	Apr/07/03	SunOS 5.7: Fixes for patchadd a
107178-02	Security	NA	01		Aug/03/01	CDE 1.3: libDtHelp.so.1 patch
107180-30	Security	Recommended	04	108376	Sep/24/03	CDE 1.3: dtlogin patch
107200-16	Security	Recommended	03	108374 107887	Mar/11/03	CDE 1.3: dtmail patch
107259-04	Security	Recommended	01		Jun/28/02	SunOS 5.7: /usr/sbin/vold patch

☐ 107285-09	Security	Recommended	02			Nov/26/02	SunOS 5.7: passwd & pam Libra
☐ 107337-02	Security	Recommended	01			Jun/15/01	SunOS 5.7: KCMS configure tool vulnerability
☐ 107374-02	Security	Recommended	01			Jul/23/01	Openwindows 3.6.1: Xview Patch
☐ 107403-03	Security	Recommended	01	106541		Apr/15/03	SunOS 5.7: rlmod & telmod patch
☐ 107441-03	Security	Recommended	02			Nov/09/01	SunOS 5.7: /usr/bin/mailx patch
☐ 107443-17	Security	Recommended	13	107332 106938		Jan/07/03	SunOS 5.7: packaging utilities pa
☐ 107451-07	Security	Recommended	05	106541		Apr/03/02	SunOS 5.7: /usr/sbin/cron Patch
☐ 107454-06	Security	Recommended	05			Feb/21/03	SunOS 5.7: /usr/bin/ftp patch
☐ 107460-13	NA	Recommended	08			Sep/18/02	SunOS 5.7: st driver Patch
☐ 107469-09	NA	Recommended	08			Sep/13/02	SunOS 5.7: sf & socal drivers pa
☐ 107475-05	Security	Recommended	01			Apr/08/03	SunOS 5.7: /usr/sbin/in.telnetd P
☐ 107477-04	Security	Recommended	03			Nov/30/01	SunOS 5.7: /usr/lib/nfs/mountd P
☐ 107589-13	Security	NA		106541		Jul/31/03	SunOS 5.7: se, zs, kbd and kbio.
☐ 107636-10	Security	Recommended	05	107081		Apr/25/03	SunOS 5.7: X Input & Output Me
☐ 107654-10	Security	Recommended	08	108376		May/09/02	OpenWindows 3.6.1: X11R6.4 L Extensions Patch
☐ 107656-11	NA	Recommended	06	108376		Dec/09/02	OpenWindows 3.6.1 libXt Patch

107684-10	Security	Recommended			Sep/29/03	SunOS 5.7: sendmail patch
107702-12	Security	Recommended		108376	Apr/14/03	CDE 1.3: dtsession patch
107709-21	Security	Recommended	07		Apr/29/03	SunOS 5.7: libssasnmp/libssagent/snmpdx/sr Patches
107716-22	Security	NA			Dec/09/02	WITHDRAWN PATCH SunOS 5. Patch
107716-26	Security	Recommended			Oct/28/03	SunOS 5.7: PGX32 Graphics Pa
107743-14	NA	Recommended	07		Apr/25/03	SunOS 5.7: Sun Quad FastEther
107792-05	Security	Recommended	02		Jan/30/03	SunOS 5.7: /usr/bin/pax patch
107834-04	NA	Recommended	03		Sep/18/02	SunOS 5.7: dkio.h & commands.
107841-03	NA	Recommended	02		May/03/01	SunOS 5.7: rpcsec patch
107885-09	Security	Recommended		106934	Dec/03/03	CDE 1.3: dtprintinfo Patch
107887-10	Security	Recommended			Oct/31/00	CDE 1.3: Actions Patch
107893-21	Security	Recommended		106942	Sep/24/03	OpenWindows 3.6.1: Tooltalk pa
107972-02	Security	Recommended	01		Mar/26/01	SunOS 5.7: /usr/sbin/static/rcp pa
108029-03	NA	Recommended	02		Aug/28/01	SunOS 5.7: S899 u3 prodreg fix Java 1.2 VM
108117-06	Security	Recommended			Dec/18/02	OpenWindows 3.6.1: Font Serve
108162-08	Security	Recommended	02		Feb/26/03	SunOS 5.7: jsh, rsh, ksh, rksh, sh

☐ 108221-02	Security	Recommended	01			Aug/15/03	CDE 1.3: dtspcd Patch
☐ 108263-10	Security	Recommended	06	106541		Apr/15/03	SunOS 5.7: hme driver Patch
☐ 108317-04	Security	NA		106541		Apr/15/03	SunOS 5.7: idn driver patch
☐ 108319-03	Security	Recommended	01			Jan/27/03	SunOS 5.7: /usr/bin/at patch
☐ 108327-02	Security	Recommended	01			Apr/06/01	SunOS 5.7: /usr/bin/cu patch
☐ 108343-04	NA	Recommended		108374		Aug/29/00	CDE 1.3: sdtperfmeter patch
☐ 108374-07	NA	Recommended	04	107702		Jun/26/02	CDE 1.3: libDtWidget Patch
☐ 108376-44	Security	Recommended	21			Oct/03/03	OpenWindows 3.6.1: Xsun Patch
☐ 108381-02	Security	NA	01	106541		Apr/15/03	SunOS 5.7: ptsl driver patch
☐ 108451-07	Security	Recommended	05			Apr/09/03	SunOS 5.7: rpcmod patch
☐ 108551-03	Security	Recommended				Dec/15/00	SunOS 5.7: /usr/sbin/rpc.nispass
☐ 108574-04	Security	Recommended				Jan/23/02	SunOS 5.7: /usr/bin/csh Patch
☐ 108585-04	Security	NA		106541		Apr/15/03	SunOS 5.7: llc2 driver patch
☐ 108721-05	Security	Recommended	02			Feb/18/03	SunOS 5.7: admintool patch
☐ 108748-02	Security	Recommended	01			Oct/03/01	SunOS 5.7: /usr/lib/nfs/statd patc
☐ 108750-02	Security	Recommended				Jun/19/01	SunOS 5.7: /usr/lib/netsvc/yp/ypb

108756-01	Security	Recommended			Dec/19/00	SunOS 5.7: /usr/lib/netsvc/yp/rpc
108760-02	Security	Recommended	01	106942	Sep/18/02	SunOS 5.7: /usr/sbin/rpcbind pat
108798-02	Security	Recommended	01		Jun/28/01	SunOS 5.7: /usr/bin/tip patch
108800-03	Security	Recommended	01		Jul/31/03	SunOS 5.7: /usr/lib/fs/cachefs pa
108815-02	NA	Recommended			Jul/11/00	OpenWindows 3.6.1: Calendar M
108838-03	Security	Recommended	02		Nov/13/01	SunOS 5.7: allocate/mkdevmaps
109203-03	Security	Recommended	02		Aug/27/01	SunOS 5.7: edit & vi patch
109253-07	Security	Recommended	01		Jan/23/03	SunOS 5.7: /usr/bin/mail Patch
109372-02	Security	NA	01	106541	Apr/15/03	SunOS 5.7: /kernel/strmod/ldterm
109409-04	Security	Recommended	03	106541	Oct/15/01	SunOS 5.7: xntpd and ntpdate P
109744-02	Security	Recommended	01		Sep/19/02	SunOS 5.7: nfsd and lockd Patch
109797-03	Security	NA		106541	Apr/15/03	SunOS 5.7: kernel/drv/stc Patch
109949-01	Security	Recommended			Aug/17/00	SunOS 5.7: jserver buffer overflo
110070-01	Security	Recommended			Mar/09/01	SunOS 5.7: security: libcurses:se overflow
110072-01	NA	Recommended			Oct/30/00	SunOS 5.7: Sol7 11/99, can't mo a udfs filesyst
110281-02	NA	Recommended			Apr/18/01	SunOS 5.7: patch /usr/bin/find

110646-05	Security	Recommended			Jun/25/03	SunOS 5.7: /usr/sbin/in.ftpd Patc
110869-01	Security	Recommended			Mar/21/01	SunOS 5.7: useradd, usermod d expiration dates
110881-01	NA	Recommended			Apr/12/01	SunOS 5.7: semop() hangs due t
111093-01	Security	Recommended			May/03/01	SunOS 5.7: /etc/security/bsmunc
111113-02	NA	Recommended			Feb/19/02	SunOS 5.7: nawk Patch
111238-01	Security	Recommended			May/11/01	SunOS 5.7: Patch to /usr/sbin/in.
111242-01	Security	Recommended			May/11/01	SunOS 5.7: Patch to /usr/bin/fing
111350-02	Security	Recommended			Jun/13/02	SunOS 5.7: Patch for ttymon pro
111578-02	NA	Recommended			Oct/22/01	SunOS 5.7: arp Patch
111590-03	Security	Recommended		107285	Feb/28/03	SunOS 5.7: rpc.yppasswdd Patch
111600-01	Security	Recommended			Aug/15/01	SunOS 5.7: /usr/sbin/whodo Patc
111646-01	Security	NA			Aug/06/01	SunOS 5.7: BCP libmle buffer ov
111666-01	NA	Recommended			Jun/29/01	SunOS 5.7: bzip patch
111931-02	Security	NA		106541	Apr/15/03	SunOS 5.7: /kernel/strmod/timod
111980-02	Security	Recommended			Mar/19/02	SunOS 5.7: ipcs Patch
112106-01	NA	Recommended			Nov/05/01	SunOS 5.7: mkfs Patch

112300-01	Security	Recommended			Dec/13/01	SunOS 5.7: usr/bin/login Patch
112448-01	Security	NA			Mar/07/02	SunOS 5.7: pt_chmod Patch
112590-01	NA	Recommended			Apr/01/02	SunOS 5.7: fgrep Patch
112604-02	Security	Recommended			Sep/24/03	SunOS 5.7: le patch
112672-01	Security	NA			Apr/19/02	SunOS 5.7: vipw Patch
112820-01	Security	Recommended			May/27/02	SunOS 5.7: in.talkd Patch
112899-01	Security	Recommended			Jun/17/02	SunOS 5.7: rwall Patch
113752-02	Security	Recommended			May/28/03	SunOS 5.7: utmp_update patch
114151-01	NA	Recommended			Dec/18/02	SunOS 5.7: Japanese SunOS 4.x Compatibility(BCP) patch
114891-01	Security	Recommended			Apr/17/03	SunOS 5.7: /usr/sbin/wall patch
114944-01	Security	Recommended			Jul/09/03	SunOS 5.7: namefs patch
115565-01	Security	Recommended			Nov/25/03	SunOS 5.7: ed creates tempfiles manner

Total Patches	Security Patches	Recommended Patches
116	93	103

http://cgi.cs.duke.edu/~wjs/patchreport/patchreport.html

3. NMAP Version 3.48

Comman output enabled with the following syntax –sT for TCP scan and –P0 to disable ICMP ping. (nmap -sT -P0 host)

Starting nmap 3.48 (http://www.insecure.org/nmap/) at 2003-8-13 21:34 EST

Interesting ports on (xxx.xxx.xxx.xxx):
(The 1640 ports scanned but not shown below are in state: closed)

PORT	STATE	SERVICE
22/tcp	open	ssh
53/tcp	open	domain
80/tcp	open	http
111/tcp	open	rpcbind
135/tcp	filtered	msrpc
137/tcp	filtered	netbios-ns
138/tcp	filtered	netbios-dgm
139/tcp	filtered	netbios-ssn
443/tcp	open	https
445/tcp	filtered	microsoft-ds
515/tcp	open	printer
4045/tcp	open	lockd
8080/tcp	open	http-proxy
9090/tcp	open	zeus-admin
32771/tcp	open	sometimes-rpc5

4. TARA Version 3.0.3 NOTE THIS REPORT HAS BEEN ALTERED AND EDITED.

Security scripts *** 3.0.2 ARC, 2002.0513.2100 ***
Mon Dec 15 20:24:30 PST 2003
20:24> Beginning security report for xxx.xxx.xxx.xxx (sun4u SunOS 5.7).

Performing check of passwd files...
--WARN-- [pass002w] UID x exists multiple times in /etc/passwd or username appears twice in /etc/shadow.

Performing check of group files...
--WARN-- [grp001w] Groupname `xxx' exists multiple times in /etc/group.
--WARN-- [grp002w] GID xxx exists multiple times in /etc/group.

Performing check of user accounts...
Checking accounts from /etc/passwd.
--WARN-- [acc012w] Login ID xxx has uid == 0.
--WARN-- [acc005w] Login ID xx is disabled, but has a 'cron' file or cron entries.
--WARN-- [acc001w] Login ID xxx is disabled, but still has a valid shell.
--WARN-- [acc006w] Login ID xxx's home directory (/xxx) has group `xxx' and world write access.
--WARN-- [acc008w] Login ID xxx's .cshrc config file has group `xxx' write access.
--WARN-- [acc006w] Login ID xxx's home directory (/xxx) has group `xxx' and world write access.

Performing check of /etc/hosts.equiv and .rhosts files...

Checking accounts from /etc/passwd...
--WARN-- [rcmd006w] User xxx's .rhosts file has group `xxx' and world read access.
--WARN-- [rcmd006w] User xxx's .rhosts file has group `xxx' and world read access.

Performing check of .netrc files...

Checking accounts from /etc/passwd...

Performing check of /etc/default/login, /securetty, and /etc/ttytab...

--WARN-- [xxx001w] Remote xxx login allowed in /etc/sshd_config

Performing check of PATH components...
Only checking user 'xxx'
--WARN-- [path002w] /bin/disable in xxx's PATH from .profile is not owned by xxx (owned by xxx).
--WARN-- [path002w] /bin/enable in xxx's PATH from .profile is not owned by xxx (owned by xxx).
--WARN-- [path002w] /usr/bin/disable in xxx's PATH from .profile is not owned by xxx (owned by xxx).
--WARN-- [path002w] /usr/bin/enable in xxx's PATH from .profile is not owned by xxx (owned by xxx).
--WARN-- [path002w] /usr/ucb/lptest in xxx's PATH from .profile is not owned by xxx (owned by xxx).
--WARN-- [path001w] /etc/acct in xxx's PATH from .profile is group `xxx' writable.
--WARN-- [path002w] /etc/acct in xxx's PATH from .profile is not owned by xxx (owned by xxx).

Performing check of anonymous FTP...

Performing checks of mail aliases...
Checking aliases from /etc/mail/aliases.

Performing check of `cron' entries...
--WARN-- [cron002] cron entry for xxx uses `/etc/cron.d/logchecker' which is not owned by xxx (owned by xxx).

--WARN-- [cron002] cron entry for xxx uses `/usr/lib/gss/gsscred_clean' which contains `/usr/lib/gss' which is not owned by xxx (owned by xxx).

--WARN-- [cron002] cron entry for xxx uses `/usr/lib/gss/gsscred_clean' which contains `/usr/lib/gss' which is not owned by xxx (owned by xxx).

--WARN-- [cron002] cron entry for xxx
`/usr/private/admin/synctree/bin/run_synctasks' which contains `/afs/xxx/system'
which is not owned by xxx (owned by xxx).

--FAIL-- [cron003] cron entry for xxx uses
`/usr/private/admin/synctree/bin/run_synctasks' which contains `/afs/xxx/admin'
which is group `xxx' and world writable.

CUT

Performing check of 'services' and 'inetd'...
Checking services from /etc/services.
Checking inetd entries from /etc/inetd.conf
--WARN-- [inet099w] 'ident' is not protected by tcp wrappers.
--WARN-- [inet005w] Service talk is using /usr/sbin/tcpd instead of
        /usr/sbin/in.talkd.
Checking inetd entries from /etc/inet/inetd.conf
--WARN-- [inet099w] 'ident' is not protected by tcp wrappers.
--WARN-- [inet005w] Service talk is using /usr/sbin/tcpd instead of
        /usr/sbin/in.talkd.

Performing NFS exports check...

Performing check of system file permissions...
--WARN-- [perm001w] /export should not have group write.
--WARN-- [perm001w] /usr/4lib should not have group write.
--WARN-- [perm001w] /usr/demo should not have group write.
--WARN-- [perm001w] /usr/games should not have group write.
--WARN-- [perm001w] /dev should not have group write.
--ALERT-- [perm001w] /etc/shadow should not have owner write.
--WARN-- [perm001w] The owner of /etc/uucp/Permissions should be xxx
(owned by xxx).
--WARN-- [perm001w] The owner of /usr/bin/uulog should be xxx (owned by xxx).
--WARN-- [perm001w] The owner of /usr/bin/uuto should be xxx (owned by xxx).
--WARN-- [perm001w] The owner of /usr/bin/uupick should be xxx (owned by
xxx).
--WARN-- [perm001w] /usr/bin/tip should not have owner write.
--WARN-- [perm021w] Disk device /dev/dsk/c0t0d0s0 has read access for group
sys.

CUT

Performing signature check of system binaries...
--WARN-- [sig004w] None of the following versions of /sbin/sh (-r-xr-xr-x)
        matched the /sbin/sh on this machine.
        >>>>>> SunOS 5.7

```
--WARN-- [sig004w] None of the following versions of /usr/bin/lpstat
        (lrwxrwxrwx) matched the /usr/bin/lpstat on this machine.
        >>>>>> SunOS 5.7

--WARN-- [sig004w] None of the following versions of /usr/bin/passwd
        (-r-sr-sr-x) matched the /usr/bin/passwd on this machine.
        >>>>>> SunOS 5.7

--WARN-- [sig004w] None of the following versions of /usr/bin/rdist
        (-r-xr-xr-x) matched the /usr/bin/rdist on this machine.
        >>>>>> SunOS 5.7

--WARN-- [sig004w] None of the following versions of /usr/bin/sh (-r-xr-xr-x)
        matched the /usr/bin/sh on this machine.
        >>>>>> SunOS 5.7

--WARN-- [sig004w] None of the following versions of
        /usr/lib/netsvc/yp//ypserv (-r-xr-xr-x) matched the
        /usr/lib/netsvc/yp//ypserv on this machine.
        >>>>>> SunOS 5.7

--WARN-- [sig004w] None of the following versions of /usr/lib/rsh (-r-xr-xr-x)
        matched the /usr/lib/rsh on this machine.
        >>>>>> SunOS 5.7

--WARN-- [sig004w] None of the following versions of /usr/sbin/in.ftpd
        (-r-xr-xr-x) matched the /usr/sbin/in.ftpd on this machine.
        >>>>>> SunOS 5.7

--WARN-- [sig004w] None of the following versions of /usr/sbin/in.telnetd
        (-r-xr-xr-x) matched the /usr/sbin/in.telnetd on this machine.
        >>>>>> SunOS 5.7

--WARN-- [sig004w] None of the following versions of /usr/sbin/in.tftpd
        (-r-xr-xr-x) matched the /usr/sbin/in.tftpd on this machine.
        >>>>>> SunOS 5.7

# Checking for known intrusion signs...
# Testing for promiscuous interfaces
# Testing for backdoors in inetd.conf
--WARN-- [kis004w] /xxx/lost+found is not empty:
        Files:

# Performing check of files in system mail spool...
```

```
# Performing system specific checks...
# Performing checks for SunOS/5...
--WARN-- [no-id] The PROM monitor is not in secure mode.
--WARN-- [misc008w] NFS port checking disabled in kernel.
# Running './scripts/check_sendmail'...

# Checking sendmail...
```

5. John the Ripper version 1.6

John the Ripper was run against the /etc/shadow file and it immediately cracked 1 out of the 22 passwords trying 21 different salts standard DES [24/32 4k]. Without much effort or customizable dictionary plug –ins. The old adage of it only takes one account, well these results makes that point clear.

6. NTP version 3.4y

```
ntpq> version
ntpq version=3.4y (beta multicast); Fri Aug 23 19:55:23 PDT 1996 (2)e
ntpq> peers
     remote           refid      st t when poll reach   delay   offset    disp
==============================================================================
*xxx.xxx.xxx     nist1-dc.glasse  2 b   27   64  376     0.49   -0.032    1.04
```

The results of the NTP peers command indicates that this host is only syncing against one other host, this configuration should be altered to include at lease two other syncing hosts.

7. Apache Version 2.0.43

The apache configuration file had several issues that need to be addressed. Turning off the ServerSignature parameter is a good start. This configuration was set to YES which displayed the server version. Setting this variable to know disabled this “feature”. Another modification is to add ServerTokens Prod to the httpd.conf file[iii]. The utilization of IncludesNOEXEC was found positive throughout the configuration file.

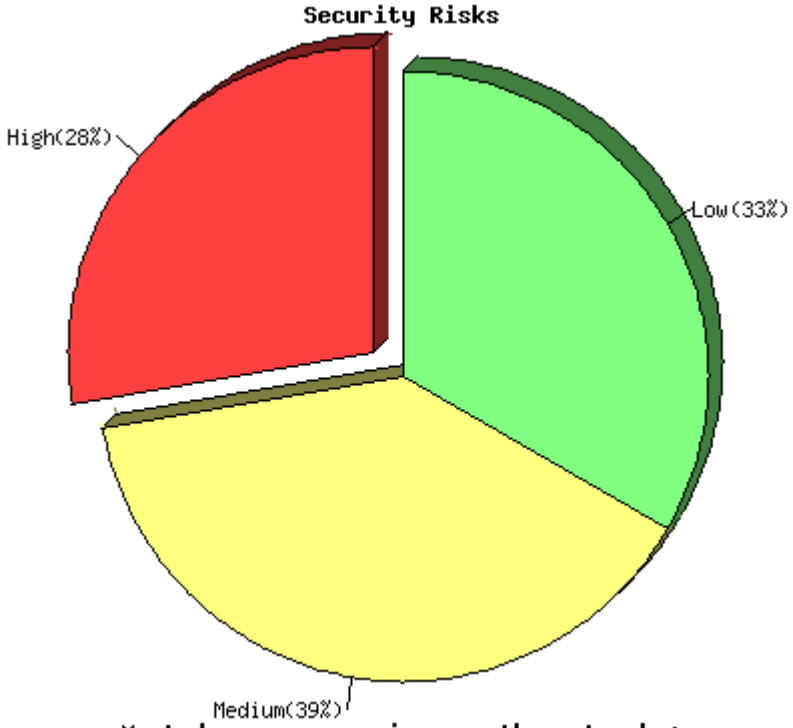
The use of CGI’s were configured appropriately allowing Options none and AllowOverride None. And containing the directories to a limited few.

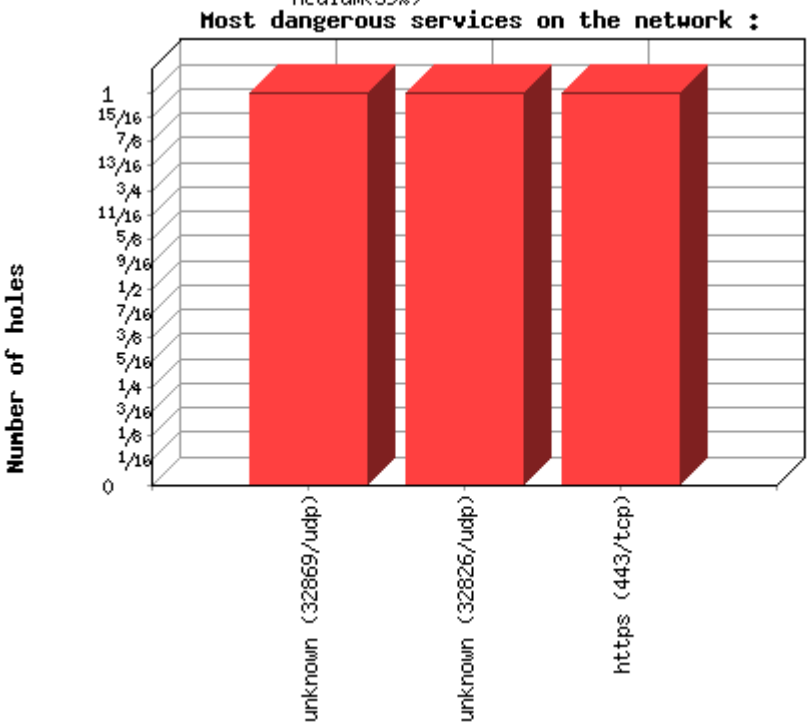
8. NESSUS

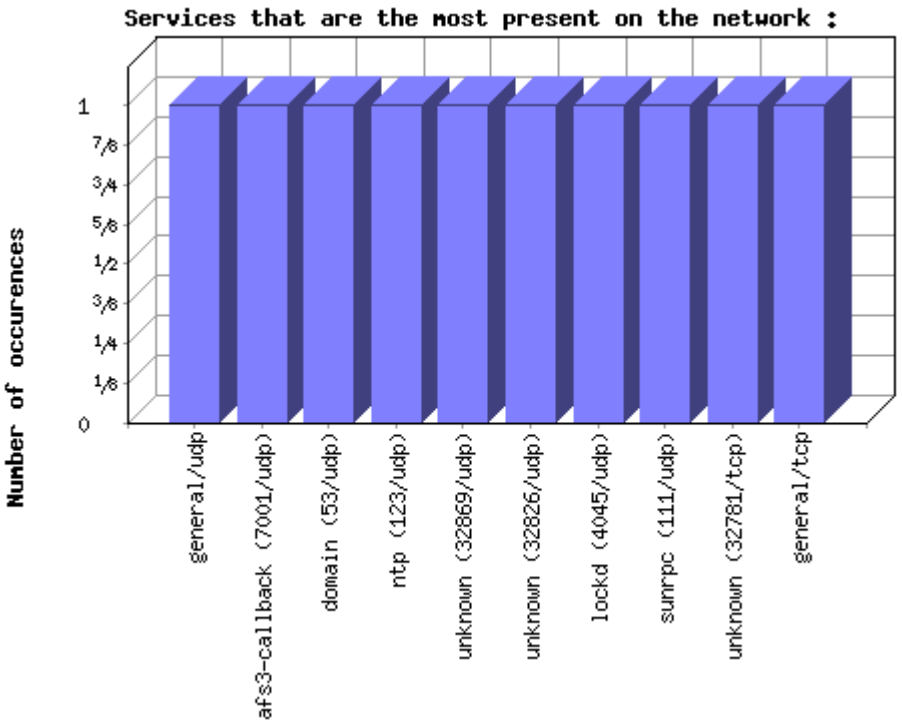
The Nessus Security Scanner was used to assess the security of 1 host

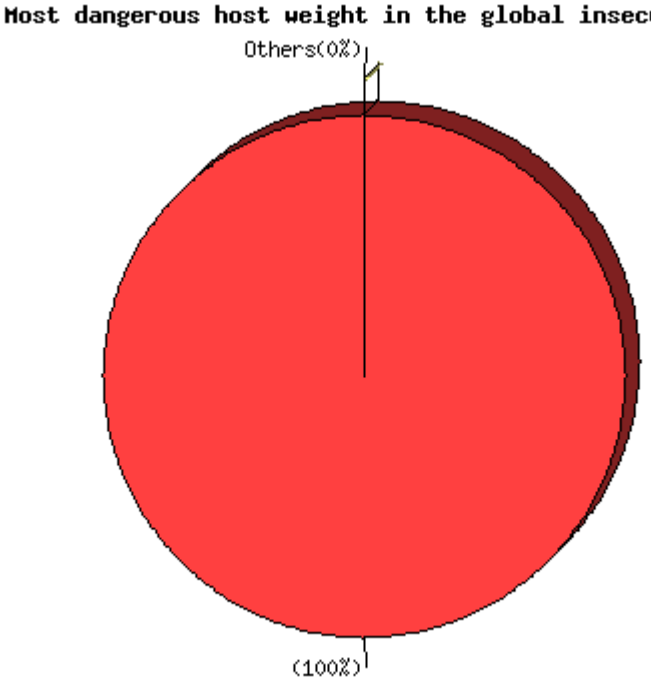
- **3 security holes have been found**
- **11 security warnings have been found**
- **22 security notes have been found**

Part I : Graphical Summary :









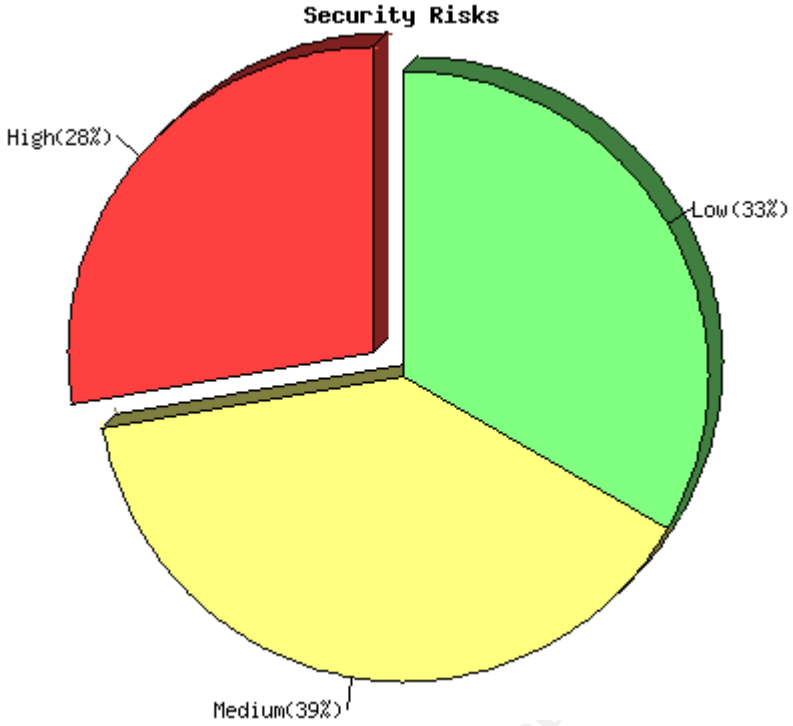
Part II.

Results, by host :

xxx.xxx.xxx **(found 3 security holes)**

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

Repartition of the level of the security problems :



[Back to the index]

List of open ports :

- *ssh (22/tcp)* *(Security notes found)*
- *domain (53/tcp)* *(Security notes found)*
- *http (80/tcp)* *(Security warnings found)*
- *sunrpc (111/tcp)* *(Security notes found)*
- *https (443/tcp)* *(Security hole found)*
- *printer (515/tcp)* *(Security notes found)*
- *ncube-lm (1521/tcp)*
- *oracle-em2 (1754/tcp)*
- *oracle-em1 (1748/tcp)* *(Security notes found)*
- *oracle-vp1 (1809/tcp)*
- *oracle-vp2 (1808/tcp)*
- *giop-ssl (2482/tcp)*
- *giop (2481/tcp)*
- *lockd (4045/tcp)* *(Security notes found)*
- *http-alt (8080/tcp)*
- *cslistener (9000/tcp)*
- *websm (9090/tcp)*
- *dynamid (9002/tcp)* *(Security notes found)*
- *etlservicemgr (9001/tcp)* *(Security notes found)*
- *filenet-rmi (32771/tcp)* *(Security notes found)*
- *general/tcp* *(Security warnings found)*
- *unknown (32781/tcp)* *(Security notes found)*

- *sunrpc (111/udp) (Security notes found)*
- *lockd (4045/udp) (Security warnings found)*
- *unknown (32826/udp) (Security hole found)*
- *unknown (32869/udp) (Security hole found)*
- *ntp (123/udp) (Security warnings found)*
- *domain (53/udp) (Security notes found)*
- *AFS3-callback (7001/udp) (Security notes found)*
- *general/udp (Security notes found)*

[back to the list of ports]

Information found on port ssh (22/tcp)

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

[back to the list of ports]

Information found on port domain (53/tcp)

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

Risk factor : Low
Nessus ID : 11002

[back to the list of ports]

Warning found on port http (80/tcp)

The remote host appears to be running a version of Apache 2.x which is older
than 2.0.48.

This version is vulnerable to a bug which may allow a rogue CGI to disable
the httpd service by issuing over 4K of data to stderr.

To exploit this flaw, an attacker would need the ability to upload a rogue CGI script to this server and to have it executed by the Apache daemon (httpd).

Solution : Upgrade to version 2.0.48 when it is available
See also : http://nagoya.apache.org/bugzilla/show_bug.cgi?id=22030

Risk factor : Low
CVE : CVE-2002-0061, CAN-2003-0789, CAN-2003-0542
BID : 8926
Nessus ID : 11853

[back to the list of ports]

Warning found on port http (80/tcp)

Your webserver supports the TRACE and/or TRACK methods. TRACE and TRACK
are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject
to cross-site-scripting attacks, dubbed XST for
"Cross-Site-Tracing", when used in conjunction with
various weaknesses in browsers.

An attacker may use this flaw to trick your
legitimate web users to give him their
credentials.

Solution: Disable these methods.

If you are using Apache, add the following lines for each virtual
host in your configuration file :

RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]

If you are using Microsoft IIS, use the URLScan tool to deny HTTP
TRACE
requests or to permit only the methods needed to meet site requirements
and policy.

If you are using Sun ONE Web Server releases 6.0 SP2 and later, add the
following to the default object section in obj.conf:
<Client method="TRACE">
AuthTrans fn="set-variable"
remove-headers="transfer-encoding"
set-headers="content-length: -1"
error="501"
</Client>

If you are using Sun ONE Web Server releases 6.0 SP2 or below, compile the NSAPI plugin located at:
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603

See http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf
http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603
http://www.kb.cert.org/vuls/id/867593

Risk factor : Medium
Nessus ID : 11213

[back to the list of ports]

Warning found on port http (80/tcp)

The remote host is using a version of OpenSSL which is older than 0.9.6j or 0.9.7b

This version is vulnerable to a timing based attack which may allow an attacker to guess the content of fixed data blocks and may eventually be able to guess the value of the private RSA key of the server.

An attacker may use this implementation flaw to sniff the data going to this host and decrypt some parts of it, as well as impersonate your server and perform man in the middle attacks.

*** Nessus solely relied on the banner of the remote host
*** to issue this warning

See also : http://www.openssl.org/news/secadv_20030219.txt
http://lasecwww.epfl.ch/memo_ssl.shtml
http://eprint.iacr.org/2003/052/

Solution : Upgrade to version 0.9.6j (0.9.7b) or newer
Risk factor : Medium
CVE : CAN-2003-0078, CAN-2003-0131, CVE-1999-0428
BID : 6884, 7148
Nessus ID : 11267

[back to the list of ports]

Warning found on port http (80/tcp)

The remote host appears to be running a version of
Apache 2.x which is older than 2.0.47

This version is vulnerable to various flaws which may allow
an attacker to disable this service remotely and/or locally.

Solution : Upgrade to version 2.0.47
See also : http://www.apache.org/dist/httpd/CHANGES_2.0
Risk factor : Medium
CVE : CAN-2003-0192, CAN-2003-0253, CAN-2003-0254
BID : 8134, 8135, 8137, 8138
Nessus ID : 11788

[back to the list of ports]

Warning found on port http (80/tcp)

The remote host appears to be running a version of
Apache 2.x which is older than 2.0.45

This version is vulnerable to various flaws :

- There is a denial of service attack which may allow
an attacker to disable this server remotely

- The httpd process leaks file descriptors to child processes,
such as CGI scripts. An attacker who has the ability to execute
arbitrary CGI scripts on this server (including PHP code) would
be able to write arbitrary data in the file pointed to (in particular,
the log files)

Solution : Upgrade to version 2.0.45
See also : http://www.apache.org/dist/httpd/CHANGES_2.0
Risk factor : Medium
CVE : CAN-2003-0132
BID : 7254, 7255
Nessus ID : 11507

[back to the list of ports]

Warning found on port http (80/tcp)

The remote host appears to be running a version of
Apache 2.x which is older than 2.0.46

This version is vulnerable to various flaws :

- There is a denial of service vulnerability which may allow
an attacker to disable basic authentication on this host

- There is a denial of service vulnerability in the mod_dav module
which may allow an attacker to crash this service remotely

Solution : Upgrade to version 2.0.46
See also : http://www.apache.org/dist/httpd/CHANGES_2.0
Risk factor : Medium
CVE : CAN-2003-0245, CAN-2003-0189
BID : 7723, 7725
Nessus ID : 11665

[back to the list of ports]

Information found on port http (80/tcp)

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

[back to the list of ports]

Information found on port http (80/tcp)

The remote web server type is :

Apache/2.0.43 (Unix) mod_perl/1.99_07-dev Perl/v5.6.1 mod_ssl/2.0.43
OpenSSL/0.9.6

Solution : You can set the directive 'ServerTokens Prod' to limit
the information emanating from the server in its response headers.
Nessus ID : 10107

[back to the list of ports]

Information found on port sunrpc (111/tcp)

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
Nessus ID : 10223

[back to the list of ports]

Information found on port sunrpc (111/tcp)

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

Nessus ID : 11111

[back to the list of ports]

Vulnerability found on port https (443/tcp)

The remote host seem to be running a version of OpenSSL which is older than 0.9.6k or 0.9.7c.

There is a heap corruption bug in this version which might be exploited by an
attacker to gain a shell on this host.

Solution : If you are running OpenSSL, Upgrade to version 0.9.6k or 0.9.7c or newer
Risk factor : High
CVE : CAN-2003-0543, CAN-2003-0544, CAN-2003-0545
BID : 8732
Nessus ID : 11875

[back to the list of ports]

Warning found on port https (443/tcp)

The remote host is using a version of OpenSSL which is

older than 0.9.6j or 0.9.7b

This version is vulnerable to a timing based attack which may allow an attacker to guess the content of fixed data blocks and may eventually be able to guess the value of the private RSA key of the server.

An attacker may use this implementation flaw to sniff the data going to this host and decrypt some parts of it, as well as impersonate your server and perform man in the middle attacks.

*** Nessus solely relied on the banner of the remote host
*** to issue this warning

See also : http://www.openssl.org/news/secadv_20030219.txt
http://lasecwww.epfl.ch/memo_ssl.shtml
http://eprint.iacr.org/2003/052/

Solution : Upgrade to version 0.9.6j (0.9.7b) or newer
Risk factor : Medium
CVE : CAN-2003-0078, CAN-2003-0131, CVE-1999-0428
BID : 6884, 7148
Nessus ID : 11267

[back to the list of ports]

Information found on port https (443/tcp)

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

[back to the list of ports]

Information found on port printer (515/tcp)

A LPD server seems to be running on this port
Nessus ID : 10330

[back to the list of ports]

Information found on port oracle-em1 (1748/tcp)

The service closed the connection after 1 seconds without sending any data
It might be protected by some TCP wrapper

Nessus ID : 10330

[back to the list of ports]

Information found on port lockd (4045/tcp)

RPC program #100021 version 1 'nlockmgr' is running on this port
RPC program #100021 version 2 'nlockmgr' is running on this port
RPC program #100021 version 3 'nlockmgr' is running on this port
RPC program #100021 version 4 'nlockmgr' is running on this port

Nessus ID : 11111

[back to the list of ports]

Information found on port dynamid (9002/tcp)

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

Nessus ID : 10330

[back to the list of ports]

Information found on port etlservicemgr (9001/tcp)

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

Nessus ID : 10330

[back to the list of ports]

Information found on port filenet-rmi (32771/tcp)

RPC program #100024 version 1 'status' is running on this port
RPC program #100133 version 1 is running on this port

Nessus ID : 11111

[back to the list of ports]

Warning found on port general/tcp

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

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

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

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

[back to the list of ports]

Information found on port unknown (32781/tcp)

RPC program #300598 version 1 is running on this port
RPC program #805306368 version 1 is running on this port

Nessus ID : 11111

[back to the list of ports]

Information found on port sunrpc (111/udp)

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

Nessus ID : 11111

[back to the list of ports]

Warning found on port lockd (4045/udp)

The nlockmgr RPC service is running.
If you do not use this service, then disable it as it may become a security

threat in the future, if a vulnerability
is discovered.

Risk factor : Low
CVE : CVE-2000-0508
BID : 1372
Nessus ID : 10220

[back to the list of ports]

Information found on port lockd (4045/udp)

RPC program #100021 version 1 'nlockmgr' is running on this port
RPC program #100021 version 2 'nlockmgr' is running on this port
RPC program #100021 version 3 'nlockmgr' is running on this port
RPC program #100021 version 4 'nlockmgr' is running on this port

Nessus ID : 11111

[back to the list of ports]

Vulnerability found on port unknown (32826/udp)

The remote statd service may be vulnerable to a format string attack.

This means that an attacker may execute arbitrary code thanks to a bug in this daemon.

*** Nessus reports this vulnerability using only information that was gathered.
*** Use caution when testing without safe checks enabled.

Solution : upgrade to the latest version of rpc.statd
Risk factor : High
CVE : CVE-2000-0666, CAN-2000-0800
BID : 1480
Nessus ID : 10544

[back to the list of ports]

Warning found on port unknown (32826/udp)

The statd RPC service is running. This service has a long history of security holes, so you should really know what you are doing if you decide to let it run.

*** No security hole regarding this program have been tested, so
*** this might be a false positive.

Solution : We suggest that you disable this service.
Risk factor : High
CVE : CVE-1999-0018, CVE-1999-0019, CVE-1999-0493
BID : 127, 450
Nessus ID : 10235

[back to the list of ports]

Information found on port unknown (32826/udp)

RPC program #100024 version 1 'status' is running on this port
RPC program #100133 version 1 is running on this port

Nessus ID : 11111

[back to the list of ports]

Vulnerability found on port unknown (32869/udp)

The dmisd RPC service is running.

This service uses the function xdr_array() of the RPC library.
It turns out that some older versions of the RPC library
are vulnerable to an integer overflow in this function,
which could allow an attacker to gain xxx privileges on
this host.

*** No security hole regarding this program has been tested, so
*** this might be a false positive.

Solution : We suggest that you disable this service.
See also : http://www.cert.org/advisories/CA-2002-25.html
Risk factor : High
CVE : CVE-2002-0391
BID : 5356
Nessus ID : 11405

[back to the list of ports]

Information found on port unknown (32869/udp)

RPC program #300598 version 1 is running on this port
RPC program #805306368 version 1 is running on this port

Nessus ID : 11111

[back to the list of ports]

Warning found on port ntp (123/udp)

An NTP server is running on the remote host. Make sure that
you are running the latest version of your NTP server,
as some versions have been found out to be vulnerable to
buffer overflows.

*** Nessus reports this vulnerability using only
*** information that was gathered. Use caution
*** when testing without safe checks enabled.

If you happen to be vulnerable : upgrade
Solution : Upgrade
Risk factor : High
CVE : CVE-2001-0414
BID : 2540
Nessus ID : 10647

[back to the list of ports]

Information found on port ntp (123/udp)

It is possible to determine a lot of information about the remote host
by querying the NTP variables - these include OS descriptor, and
time settings.

It was possible to gather the following information from the remote NTP
host :

system='UNIX/Solaris 2.x', leap=0, stratum=3, xxxdelay=19.24,
xxxdispersion=4.26, peer=32532, refid=198.108.1.42,
reftime=0xc38657de.fbfcc000, poll=10, clock=0xc3865803.0722f000,
phase=-0.042, freq=-2664.31, error=1.08

Quickfix: Set NTP to restrict default access to ignore all info packets:
restrict default ignore

Risk factor : Low
Nessus ID : 10884

[back to the list of ports]

Information found on port domain (53/udp)

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

Risk factor : Low
Nessus ID : 11002

[back to the list of ports]

Information found on port AFS3-callback (7001/udp)

AFS version: Base configuration AFS3.6 2.5
Nessus ID : 10441

[back to the list of ports]

Information found on port general/udp

For your information, here is the traceroute to xxx.xxx.xxx.xxx :
192.168.0.4
192.168.0.1
xxx.xxx.xxx.xxx

Nessus ID : 10287

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

9. CIS Security Benchmark Checker Version 1.4.0
Note: Due to the sensitive nature of the information in this report, only the "Positive" results are published, it should be noted that the final score indicated below reflects that there is a lot of work to be done here. In addition there were many false positives found in this audit, many dealing with permissions on files found in AFS which does not utilize standard UNIX file permissions. AFS utilizes ACL's in which supersedes the UNIX permissions, thus lowering the end result of this machines score.

***** CIS Ruler Run *****
Positive: 1.3 System is running sshd and it's configured well.

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.
Positive: 2.6 BSD-compatible printer server is deactivated.
Positive: 2.7 rquotad is deactivated.
Positive: 2.8 CDE-related daemons are deactivated.
Positive: 3.5 Mail daemon is not listening on TCP 25.
Positive: 3.19 SNMP daemon is deactivated.
Positive: 5.1 syslog captures auth messages.
Positive: 5.4 cron usage is being logged.
Positive: 6.3 /etc/rmmount.conf mounts all file systems nosuid.
Positive: 6.4 /etc/dfs/dfstab doesn't have any non-fully qualified pathname share commands.
Positive: 6.6 all temporary directories have sticky bits set.
Positive: 7.2 /etc/hosts.equiv and root's .rhosts/.shosts files either don't exist or are links to /dev/null.
Positive: 7.4 /etc/shells exists and has good permissions.
Positive: 7.11 Root is only allowed to login on console
Positive: 8.2 All users have passwords
Positive: 8.4 There were no +: entries in passwd, shadow or group maps.
Positive: 8.6 root's PATH is clean of group/world writable directories or the current-directory link.
Positive: 8.9 No user has a .netrc file.

Final rating = 3.24 / 10.00

10. Oracle Audit Scripts source: metalink.oracle.com

```
create or replace procedure sys.find_joes as
-- Find users that have their password equal to their username
  hexpw varchar2(30);
  modpw varchar2(30);
  un varchar2(30);
  cursor c1 is select username,password from dba_users;
begin
  for i in c1 loop
    hexpw := i.password;
    un := i.username;
    execute immediate 'alter user '||un||' identified by '||un;
    select password into modpw from dba_users where username = un;
    if modpw = hexpw then
       dbms_output.put_line(un);
    else
--     change password back to what it was
       execute immediate
```

```
        'alter user '||un||' identified by values '''||hexpw||''';
    end if;
  end loop;
end;
/
```

tfsprivs.sql

```
SET ECHO off
REM NAME:   TFSPRIVS.SQL
REM USAGE:"@path/tfsprivs grantee_name"
REM ------------------------------------------------------------------------
REM REQUIREMENTS:
REM    SELECT on DBA_ROLE_PRIVS, DBA_SYS_PRIVS, DBA_TAB_PRIVS,
DBA_COL_PRIVS
REM ------------------------------------------------------------------------
REM PURPOSE:
REM    The following script shows privileges granted to a user,
REM    as well as the level, object, and object owner.
REM ------------------------------------------------------------------------
REM EXAMPLE:
REM    LVL      PRIVILEGE  GRA OWNER              Name
REM    -------- ---------- --- ------------------------------
REM    Column   UPDATE      NO  SYSTEM             TOOL_DEPENDENT
REM    Program  DELETE      NO                  FRM45__BUFFER
REM    Program  DELETE      NO                  FRM45__GRP
REM    Program  INSERT      NO  SYSTEM             MENU_B_OBJ_TEXT
REM    Program  INSERT      NO                  MENU_B_PARAM
REM    Program  SELECT      NO                  MENU_B_APPL_GRP
REM    Program  UPDATE      NO                  MENU_B_OBJ_TEXT
REM    Program  UPDATE      NO                  MENU_B_PARAM
REM    table    INSERT      NO                 MENU_V_GRP_PRIV
REM    table    SELECT      NO                 MENU_B_APPL_GRP
REM    table    UPDATE      NO                 MENU_B_OBJ_TEXT
REM
REM ------------------------------------------------------------------------
REM DISCLAIMER:
REM    This script is provided for educational purposes only. It is NOT
REM    supported by Oracle World Wide Technical Support.
REM    The script has been tested and appears to work as intended.
REM    You should always run new scripts on a test instance initially.
REM ------------------------------------------------------------------------
REM Main text of script follows:

set pause on
set pause Continues...
```

```
set verify off
set pages 20
set lines 132

select 'Column' lvl,c.privilege,c.grantable,c.owner,c.table_name,c.column_name
from dba_col_privs c
where grantee = upper('&&grantee')
union
select 'Role' GrType,r.granted_role obj,r.admin_option a, null,null,null
from dba_role_privs r
where r.grantee = upper('&grantee')
union
select 'Sys Priv',s.privilege,s.admin_option,null,null,null
from dba_sys_privs s
where s.grantee = upper('&grantee')
union
select 'table',t.privilege,t.grantable,t.owner,t.table_name,null
from dba_tab_privs t
where t.grantee = upper('&grantee')
and t.privilege !='EXECUTE'
union
select 'Program', e.privilege,e.grantable,e.owner,e.table_name,null
from dba_tab_privs e
where e.grantee = upper('&grantee')
and e.privilege !='EXECUTE'
order by 1,2,4,5,6
/
undefine grantee
```

11. Disk Layout: df -k

```
Filesystem            kbytes    used   avail capacity  Mounted on
/proc                      0       0       0     0%    /proc
/dev/dsk/c0t0d0s0     124330   65776   46121    59%    /
/dev/dsk/c0t0d0s6     963869  660227  245810    73%    /usr
fd                         0       0       0     0%    /dev/fd
/dev/dsk/c0t0d0s3     246881  115886  106307    53%    /var
/dev/dsk/c0t0d0s7    5492798 3083851 2354020    57%    /private
/dev/dsk/c0t0d0s5     246881  174435   47758    79%    /usr/vice/cache
/dev/dsk/c0t0d0s4     493688     254  444066     1%    /var/tmp
/dev/dsk/c1t14d0s0   3096309 1836758 1197625    61%    /ora
/dev/dsk/c1t14d0s7   5649354  365733 5227128     7%    /ora1
/dev/dsk/c1t15d0s7   8746424 3004354 5654606    35%    /ora2
/dev/dsk/c2t3d0s7    8746424 1380432 7278528    16%    /ora3
/dev/dsk/c2t4d0s0    6678155  295029 6316345     5%    /ora4
/dev/dsk/c2t4d0s7    2056708  468920 1526087    24%    /ora5
AFS                  9000000       0 9000000     0%    /afs
```

References

2600 The Hacker Quarterly, Volume Twenty, Number Three Fall 2003

Allen, Julia H. The CERT Guide to System and Network Security Practices Boston: Addison-Wesley, 2001

Anonymous Maximum Security 2nd Edition Indianapolis: SAMS, August 1998.

Cole, Eric Hackers Beware Defending Your Network From The Wiley Hacker Indianapolis: New Riders, August 2001.

Garfinkel, Spafford and Schwartz Practical Unix & Internet Security 3rd Edition Sebastopol: O'Reilly, February 2003.

Nichols, Ryan & Ryan Defending Your Digital Assets Against Hackers, Crackers, Spies & Thieves New York: McGraw-Hill RSA Press, 2000.

Pomeranz, Hal The SANS Institute Solaris Security Step By Step Version 2.0, 2001.

Pomerans, Hal The SANS Institute Track 6 – Securing Unix, July 2003

URL's

Sun http://sunsolve.sun.com

Oracle http://metalink.oracle.com

Patch Report http://cgi.cs.duke.edu/~wjs/patchreport/patchreport.html

---

Endnotes

[i] Pomeranz, Hal Ths SANS Institute Solaris Security Step By Step Version 2.0 2001
[ii] Pomeranz, Hal The SANS Institute Solaris Security Step By Step Version 2.0 2001
[iii] Pomeranz, Hal The SANS Institute Solaris Security Step By Step Version 2.0 2001