Global Information Assurance Certification Paper

GCUX Practical Assignment ver 1.7
Date: December 12th 2001
Original Submission: Early October 2001
Student: Jamie French, GCIA

Option 2 - Consultant's Report From Auditing UNIX
Title: UNIX Audit of GIAC Enterprises
Dragon IDS Server
running on
Redhat Linux 7.1 (revision 2)

Table of Contents

Conventions Used

Numerous conventions are used within this paper to identify different context.

Path and file names are displayed as 70% gray, 12 point Times New Roman.
Example: /etc/hosts

Commands executed with or without their output are displayed as brown, 8 point Courier New.
Example:
```
[dragon@dnids1 /etc]$ ls -las man.config
 4 -rw-r--r--    1 root     root         3646 Feb  4  2001 man.config
```

Variable user input is displayed as brown, 10 point Times New Roman, italic.
Example: `/usr/bin/chage -M 60 -W 14 -I 5 -d` *`yyyy-mm-dd username`*

Comments to aid in legibility within output are displayed as blue, 10 point Courier New.
Example:
```
02:20:38.761498 MY.DNIDS.server.8 > MY.Audit.laptop.63548: R [tcp sum ok] 0:0(0) ack 2559472883 win
0 (DF) (ttl 255, id 0, len 40)
NMAP scan, discovering that TCP port 22 was open
<<<snip>>>
```

Recommended edits to a configuration file are red, 8 point Courier New.
Example:
```
# hosts.allow
sshd:         192.168.1.
```

This page left intentionally blank

Executive Summary

Upon the request of Management, Jamie French (GCIA), an IDS Analyst within GIAC Enterprises Inc., performed a security audit of a Dragon IDS© Server known as DNIDS. The auditor recently attended the SANS GCUX track, and will present relevant issues within this audit regarding the current security status of this critical server as outlined at http://www.sans.org/giactc/GCUX_assign_17.htm#4. It is the student's belief that these requirements have been exceeded. In addition to the audit findings, solutions were provided that are not specifically required within the assignment guidelines with processes to implement these recommendations. Additionally, research into system vulnerabilities as they are implemented within the UNIX security model has been conducted and the results presented which the student finds extremely relevant to the current state of UNIX security and IT security in general. While not specifically part of the GCUX track it may be prudent to consider their inclusion in future courses. This in turn will add to the overall content of the GCUX track and bridge some of the gap between certifications such as CISSP where they are indeed covered and discussed in-depth. A discussion of their relevance in the GCUX track could pursue but this is not the venue for such discussion, suffice to say that the student has practical experience working in an environment which employs security measures directed at dealing with many of the items covered within this audit report where they were not covered in the course content.

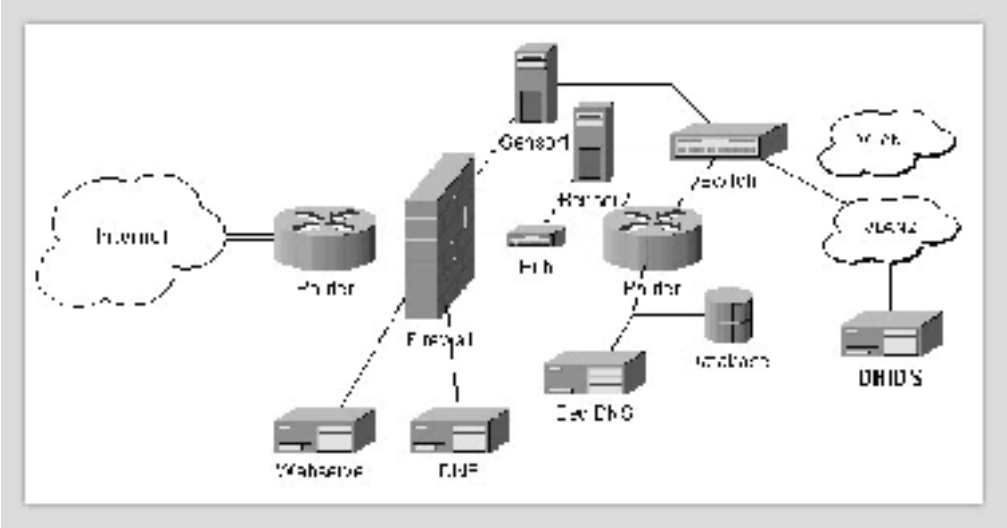
Techniques and practices taught on the GCUX track have been applied to the server in order to accomplish management's request. They highlight many inadequacies currently within the organization as they relate to UNIX security, and how the previous haphazard employment of unstructured, partial implementations needs to be addressed. These new techniques have been applied to benefit the organization, its employees, customers, and others that may have been affected by the DNIDS server. Others are presented and represented in the context of negligence, considering that improperly secured and configured servers may be grounds to sue with very real repercussions. Possible legal consequences could result should a compromised asset within the organization be used to attack another entity[1].

Many tools were employed to aid in the audit. Vulnerability scans, password crackers, port scanners, system commands, and others were used to identify inadequacies with the DNIDS server running on Redhat Linux 7.1©[2]. Key configuration files and startup scripts were reviewed, as well as physical parameter considerations. The audit was performed during the time frame of September 14th to September 20th, 2001. Specific system specifications and configuration variables are available in Appendix A.

The current network architecture was taken into consideration during the audit, with many recommendations based on how the DNIDS server fits into this environment. In particular, this server is deployed as the main data collection center for security related log files provided by network intrusion detection system (NIDS) sensors. Analysis, correlation, and report generation of security events and incidents[3] are currently being accomplished on this server. As such it has been identified as a critical resource to GIAC Enterprises and must be highly maintained. A compromise of this system would have a devastating impact on the security posture of the organization and severely limit chances for the compilation of evidence and successful prosecution of an attacker. It could also increase the workload exponentially in identifying the extent of damage caused during the attack. Post mortem analysis and cleanup required to return to business would become extremely complicated without a trusted record indicating where, when, how, why, who, and what the attacker tickled, touched, or compromised.

[1] http://www.wired.com/news/print/0,1294,37286,00.html - Nike domain Hijack
[2] List of tools available throughout
[3] Events and Incidents as identified in the GIAC Security Policy, Incident Handling subsection.

Fig 1: Simplified Network Diagram



Recommendations made within this audit are considered by the auditor to comply with Security Policy and will integrate well, requiring very little re-engineering of other assets during implementation. The application of these recommendations can be carried out while the server is online. Due to the pull method implemented by the Dragon IDS© Server, driders, the server may be rebooted without any critical service interruptions or affect on other GIAC Enterprises business resources as it is presently configured. Logs will continue to collect on the deployed sensors while the server is down (limited by disk space - currently estimated to be approximately 8.5 years[4]). Prioritized recommendations are presented within the following report.

It is important to note that this audit was performed under the assumption that the DNIDS server was not previously compromised during its tenure as a training platform and that the binaries used to perform much of the audit were trusted. A good level of confidence has been obtained through the use of remote tools, review of historical IDS logs, and testament from the previous user. The above assumption was further reinforced by the overall audit findings.

System Audit and Analysis

Operating System Vulnerabilities

Overview: It is important to understand where many of these flaws originated from in order to devise a solution whether partial or complete to mitigate the risk. The auditor of the GIAC server believes that it is important for management to understand these aspects so the dynamics of their information systems may be understood at a higher level, promoting more informed decisions to be drawn with regard to the allocation of assets and resources.

There are many vulnerabilities related to the fundamental security model implemented through the UNIX operating system (OS). The underlying basic security theorem implemented in UNIX follows aspects primarily from two security models. These security models were developed to address both corporate and

[4] 14000MB/4.5MB per day = 3111 days or approximately 8.5 years at current logging levels

military needs and how information systems could be developed into a trusted computer base. UNIX encompasses aspects originally presented by Bell and LaPadula[5], using the read down, write up security checking mechanism. It becomes a very complex issue to enforce these security models, which UNIX has addressed through the development of a central management module known as the kernel. It is the kernel that handles the majority of these security model implementations. These are centered on state and privilege based on how objects are handled. This section of the audit on GIAC Enterprises DNIDS server will attempt to address these underlying flaws in the security models as they relate to the servers OS within the scope of the directives presented by GIAC Enterprises.

Encryption: Sensitive files should be encrypted to protect them from unauthorized access, no matter how this access is achieved. With regard to OS vulnerabilities, local access is the criteria within which this vulnerability shall be qualified against. Other methods of encryption are covered later in the audit. Audit results reveal that the OS is performing encryption of integral files to a desired level. Currently, the MD5[6] algorithm (128bit) is being employed to perform one-way hashing functions on passwords (this is the default for Redhat 7.1©). Encrypted hashes are kept in the shadow password file, separate from the passwd file, with appropriate permissions. This is deemed as secure enough for the application at hand.

```
[root@dnids1 pam.d]# ls -las /etc/shadow
   4 -rw-------    1 root     root          826 Sep 17 17:51 /etc/shadow
```

Recommendations: The use of Pluggable Authentication Modules[7] would allow for the specification of other encryption methods for authentication with the passwd command. It is recommended that PAM be used for this purpose and the benefits of this flexible mechanism be realized throughout authentication procedures on the audited system. Other recommendations within this audit will return to the important topic of encryption.

Implementation: Several packages distributed with the OS, when employed correctly, enhance the security posture of the system. There were no security implementations found that subtracted from the overall security posture of the audited server based upon their initial configuration. Applications other than security features found to be running are addressed under "Configuration Vulnerabilities/Unnecessary Services" and various other areas of the audit report.

Implied Sharing: The presentation of sensitive material within an area that is readable by someone without the need to know. When an application dumps core it often includes unprotected memory addresses that contain sensitive information. These core files are usually world-readable and therefore should be protected. Audit confirms that /etc/profile was set with a line as follows:

```
ulimit -S -c 1000000 > /dev/null 2>&1
```

Recommendations: There is no requirement for development on the server and therefore it is recommended that this global setting be modified. Enhanced configuration and use of syslog will aid in capturing relevant information that might normally be accessed through core dumps. The /etc/profile should be modified to disable core dumps from being written to disk through the following change:

```
ulimit -S -c 0 > /dev/null 2>&1
```

Incomplete Parameter Checking: When state changes are made and parameters are not correctly checked, vulnerabilities are introduced that may be exploited. A common vehicle used to take advantage of this

[5] http://www.mitre.org/resources/centers/infosec/secure_computers/secure_comp.doc
[6] http://www.rsasecurity.com/rsalabs/faq/3-6-6.html - crack estimate = 24 days on a $10 million computer in 1994
[7] http://www.kernel.org/pub/linux/libs/pam/modules.html - this link gives a good idea of PAM flexibility and usefulness

fundamental vulnerability in OS' is known as a buffer overflow[8]. Generally, information on these vulnerable conditions is widely known and quickly distributed for known exploits. Patches are made available very quickly in an effort to contain compromises. There exists the possibility that a buffer overflow will be found and vulnerable systems will be targeted prior to a fix or patch being available. Audit findings identify that this risk is mitigated through effective security policy documentation and implementation by system administrators within GIAC Enterprises. Applying patches in a timely manner usually mitigates these risks. The DNIDS server however was not adequately patched. These specific patch requirements are dealt with further within the audit. In relation to the rest of GIAC Enterprises, the "default deny all but required services" with defense in-depth procedures to segregate and segment resources greatly reduces the possibility of compromise through incomplete parameter checking. This also aids in the containment of a compromise should one occur.

Recommendations: The kernel version of the Redhat 7.1© DNIDS server is 2.4.2. Various solutions are available as additional security checks, which may be compiled into a kernel to help detect and deal with buffer overflow conditions as they are attempted, either through accidental or malicious intent. Immunix System 7[9] from Immunix.org is a commercial product that may be employed on critical servers. This commercial product employs some GNU Public License (GPL) software that may be modifiable to run on the Linux 2.4.2-2smp kernel. The package this audit identifies specifically is named StackGuard[10] and it appears to have been adapted for use within the commercial product offering by Immunix.org. The version documentation covered under the GPL indicates that support for the 2.4.2 kernel will be available shortly. Another option is to continue research in this area. The use of libsafe 2.0 is an option that would help in securing the kernel as well. Yet another possible solution to this dilemma is to either write code with correct bounds checking on both HEAP and STACK buffers, as well as the proper use of arrays. Re-engineering of the source code is likely not feasible by GIAC Enterprises programmers[11], but a relative solution is feasible. Compiling source code with a bounds checker integrated into the compiler will identify possible areas of future exploit. A recent package released by Herman ten Brugger[12] supports this functionality by integrating into the GNU C Compiler (gcc) versions as recent as 3.0.1. Implementing any of these steps would enhance the security of the audited server with the following caveat: The compiler and development tools should be removed from the audited system prior to its employ in a production environment. Based upon management's objectives for this server as understood and applied to this audit, no development or compilation of code should be required after deployment. Should an attacker manage to gain unauthorized access, they will be limited in achieving their objectives, being forced to use statically linked binaries precompiled for this OS version. This is considered to be one effective deterrent to complete compromise by the auditor. Further recommendations on removing development tools are available under "Third Party Software/Development Tools".

Legality Checking: Exploits employing legality checking errors depend on input provided to a function or program that is not properly checked prior to being used as an argument by the subject function or program. A classic example of such an attack is the "Ping of Death"[13]. Improper checking of the fragmented packets size prior to reassembly in memory is essentially what enabled this attack to succeed. It is not practical for this audit to identify previously unknown legality checking errors within the OS. The audit did however check well known legality checking vulnerabilities through the use of Nessus[14]. Nessus plugins were updated from ver 1.0.9 to include those released up to and including Sept 14th 2001. This brought the total number of

[8] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci549024,00.html - definition of buffer overflow
[9] http://www.immunix.org/immunix70.html - Immunix System 7
[10] http://www.openwall.com/linux/ - StackGuard
[11] In the context of OS vulnerabilities, the OS kernel is not the primary concern for buffer overflow conditions. It is Third Party packages and the possibility that an attacker may execute arbitrary code using the kernel to obtain whatever objectives they desire, including compromise of the trusted kernel.
[12] http://web.inter.NL.net/hcc/Haj.Ten.Brugge/
[13] http://www.insecure.org/sploits/ping-o-death.html

plugins targeted against the DNIDS server to 731 during the vulnerability assessment. Generally, legality checking vulnerabilities exist in third party programs such as CGI scripts. There were plenty of CGI scripts present in the /var/www/cgi-bin/ directory on the audited server, entirely dependant on Dragon IDS. It is simply not feasible at this point in time to audit each and every CGI script within this directory (df-body.pl has 4128 lines in itself). Some good faith must be taken on behalf of the vendor, or much more resources and pay are required to complete this assignment then are currently available. An approach whereby the CGI directory is maintained outside of the web document root (/var/www/html/) with appropriately assigned privileges and having the administrator keep vigilant watch of and for security patches and vulnerabilities related to the Dragon IDS software is the most logical approach at this time. Another method of trying to identify bounds checking limits is to conduct scheduled audits. As previously stated, Nessus plugins did not detect any problems with the DNIDS server CGI scripts (due to the fact that there are no plugins written to target Dragon IDS CGI scripts). Scan reports from Nessus are available in appendix A. More information is presented on the Apache web server configuration further into the audit.

Here is a list of files located in the web servers CGI directory:

```
[dragon@dnids1 cgi-bin]$ pwd && dir d*
/var/www/cgi-bin
dragonweb.cfg

dfire:
df-body.pl      drcommon.pm  mkchart.hlp  mklog.hlp    mkports.hlp    mktime.hlp  sum_db.hlp     sum_ip.hlp
df-navpanel.pl  mkalarm.hlp  mkicmp.hlp   mknotes.hlp  mksession.hlp  sigdesc.pl  sum_event.hlp

drider:
cfgdesc.pl      h-dblist.pl            h-policydesc.pl       navpanel.html          pref-10.100.100.201.cache  pref-192.168.1.2.cache
cfgfile.pl      h-dbupdate.pl          h-policylist.pl       navpanel.pl            pref-10.100.100.205.cache  pref-.cache
cfglog.pl       h-groupupdate.pl       h-policysigdesc.pl    navpanel.pl.orig       pref-10.100.100.220.cache  sensordescheader.pl
cfgpush.pl      h-netdesc.pl           h-sensordescheader.pl  netdesc.pl            pref-10.100.100.230.cache  sensordesc.pl
dbdesc.pl       h-netlist.pl           h-sensordesc.pl       netlist.pl             pref-10.100.100.240.cache  sensorfile.pl
dblist.pl       h-netoptionsheader.pl  h-sensorfile.pl       netoptionsheader.pl    pref-10.100.100.242.cache  sensorlist.pl
dbupdate.pl     h-netsensors.pl        h-sensorlist.pl       netsensors.pl          pref-10.100.100.249.cache  sensorlog.pl
drcommon.pm     h-polchgdesc.pl        h-sensorlog.pl        news.pl                pref-10.100.100.250.cache  sensorupdate.pl
groupupdate.pl  h-polchgdesc.pl.save   h-sensorupdate.pl     notes                  pref-10.100.100.253.cache  sigdesc.pl
h-cfgdesc.pl    h-polchgheader.pl      h-sigdesc.pl          perfchart.pl           pref-10.100.100.254.cache  sigindex.pl
h-cfgfile.pl    h-polchgheader.pl.save h-sigfdef.pl         pref-10.100.100.10.cache   pref-10.100.100.91.cache   siglist.pl
h-cfglog.pl     h-polchgindex2.pl      h-sigindex.pl         pref-10.100.100.125.cache  pref-10.100.100.93.cache   sigupdate.pl
h-cfgpush.pl    h-polchgindex.pl       h-siglist.pl          pref-10.100.100.152.cache  pref-10.100.100.96.cache   sigupdate.pl.orig
h-dbdesc.pl     h-polchglist.pl        h-sigupdate.pl        pref-10.100.100.199.cache  pref-127.0.0.1.cache
```

Recommendations: The security administrator should be allotted time to keep up to date with new vulnerabilities through subscriptions to security related newsgroups and mailing lists. As an incentive, their personal Internet connection may be subsidized via GIAC Enterprises, thereby increasing the company's exposure to new information directly to the qualified individual(s) in a timely manner. Another recommendation would be to use a software package entitled "Saint Jude[15]". This loadable kernel module (LKM) intercepts inappropriate transitions in privilege, such as those granted through the exploit of improperly checked arguments.

Line Disconnect: The improper closure of an authorized session with a trusted system may become an entry point for malicious use and unauthorized access. An example would be when a user believes they have logged off but the connection has not been completely torn down and access is still possible with their permissions. For audit purposes, this vulnerability is considered to be a low risk and more of an artifact inherited from earlier computing hardware incompatibilities. The most recent example found dates to an advisory from l0pht in Oct 1997[16]. Audit results show tty agents being used are mingetty, which do not support the use of serial consoles. Physical access to the server is monitored, hence the installation of

[14] http://www.nessus.org - Nessus Project homepage - Nessus Vulnerability Scanner
[15] http://sourceforge.net/projects/stjude/ - should it be deemed as necessary to allow LKM's
[16] http://www.nthelp.com/40/l0phtadv.htm - interestingly, the advisory does not appear to be available on @stake (new l0pht)

additional hardware will be noticed by the security administrator, Information System Security Officer (ISSO), and captured via surveillance video. Furthermore, no line disconnect vulnerabilities are currently known to exist within the following software implementations used primarily for communication with the audited DNIDS server[17]:

SSH 2.9p2
Apache 1.3.19
OpenSSL 0.9.6-3

Recommendations: There will be no serial line or modem connections to the DNIDS server based upon server requirements. It is recommended that periodic audits be conducted against computing assets and GIAC Enterprises security posture to identify any change in the documented posture.

Maintenance Hooks: Some software developers build maintenance hooks into their products. These hooks are meant to allow easy access for maintenance of the product (usually remotely) but in essence are actually back doors into the system. Once the program is introduced to the system and trusted, these maintenance hooks can provide various levels of privilege through unauthorized access. There are no known hooks into applications presently running on DNIDS, however the possibility is not ruled out. A list of listening services and ports indicates that there are numerous networked applications listening, all of which could potentially have a remote back door. Output from the netstat command below identifies numerous services of concern on this server.

```
[dragon@dnids1 dragon]$ netstat -ln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:32768           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:515             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN
tcp        0      0 DNIDS.Server:80         0.0.0.0:*               LISTEN
tcp        0      0 DNIDS.Server:443        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:9111            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:32768           0.0.0.0:*
udp        0      0 0.0.0.0:665             0.0.0.0:*
udp        0      0 0.0.0.0:111             0.0.0.0:*
```

Recommendations: Audit the listening services for maintenance hooks. Research will also help identify any potential back doors. Services that are not required such as RPC services and Sendmail should be disabled. More is presented on this further into the audit report.

Operator Carelessness: Social engineering techniques are very likely to fail against the operators of the DNIDS server. The operators are well-trained and experienced security administrators, educated on the topic of social engineering. Security Policy requires authentication and authorization of all sources prior to changes being made, or information given regarding network architecture and enterprise computing resources. All calls are logged, and where possible, callbacks are made. Within the scope of this audit, special circumstances apply to the system as it falls into the category of "a system under audit review" within the security policy and provisions were made by the ISSO, allowing the audit to take place in a production environment. Reasoning for this is the system is on an internal segment, had prior use without any incident monitored through intrusion detection systems or otherwise reported, and would provide the opportunity to audit the previous users level of knowledge and application of security policy.

[17] This does not imply that other vulnerabilities do not apply to the identified service versions.

Recommendations: Operator error or carelessness can never be totally eliminated. Continued security awareness programs will help mitigate this risk.

Poor Passwords: Access control is still authenticated through the use of passwords on the audited system. Audit results indicate the internal segment where the DNIDS server resides relies solely upon this method of authentication. As such the strength of passwords and password policy are extremely important. This fundamental OS flaw is covered in more detail under the more relevant "Administrative Practices/Password Policy".

Repetition: This vulnerability is closely related to poor passwords. The security risk is that a brute force attempt using various random strings or educated guesses may be conducted to try and authenticate with the DNIDS server. As with the "Poor Passwords" flaw noted above, this is covered in more detail under "Administrative Practices/Password Policy".

Shielding and Electromagnetic Emissions: Auditing the DNIDS server identified that it is using category 5 shielded network cable as required by the Canadian Open Systems Application Criteria (COSAC) 6.9[18]. It is not, however running on a shielded electrical circuit, is not running in a shielded skiff[19], and none of the assets are tempest[20] approved. Thankfully, neither Infrared (IR) nor Radio Frequency (RF) hardware is being employed, greatly reducing the probability that internal communications are intercepted in these bandwidth ranges[21].

Recommendations: Due to the nature of the GIAC Enterprises Fortune Cookie business, the risk of interception via electromagnetic emissions is considered to be very low. This is a risk the auditor considers acceptable to assume. The cost and technical expertise required to successfully capture and transcribe information into a meaningful format is very high. The value of the information located on the DNIDS server is considered to be lower than that of implementing a solution to this challenge, or even the likelihood that such vulnerability might be exploited. It is recommended that no further action is required while the current circumstances apply.

TOC/TOU: Time of Check Vs Time of Use attacks. These conditions create exploitable situations where attacks are possible between the time authentication tokens and permissions are checked and the OS functions are completed. These are also known as file system race conditions. These types of exploits are often executed after an attacker has already gained access to a system, but not always. Audit results indicate that the DNIDS server is susceptible to numerous race conditions attacks identified below, and addressed on the RedHat© Errata website. These will be addressed in further detail under "Security Patches".

RHSA-2001:093-03
RHSA-2001:086-06
RHSA-2001:061-02
RHSA-2001:050-04

Recommendations: To mitigate the risk of having susceptible race conditions available on the audited server, check varying security sources and stay up to date with security bulletins and advisories. File permissions should grant the least amount of privilege required in every situation.

[18]This is a standard adopted by a government organization. Credibility is lent through the use of these standards, and in the knowledge that certification tests were passed by this wiring medium (Fast Ethernet). More links are present for further study.
[19]A room or shielded area where electromagnetic emissions are monitored and verified to be at a level below that at which external interception and use of such signals is extremely low or not believed to be technically possible.
[20]http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci522583,00.html
[21]http://www.adec.edu/tag/spectrum.html

Waste: This is a physical vulnerability that is addressed through the GIAC Enterprises security policy. Information that may be used to exploit or gain unauthorized access to information or resources on the GIAC network will be disposed of appropriately, either through a paper shredder, incineration, or appointed special waste disposal contractor. Currently, there is a paper shredder used in this room. A quick sweep of the physical access controlled area in which the server is located did not turn up any incriminating waste, however, configuration information was jotted down on paper prior to the installation of the Dragon IDS© Server software. Information such as this should be either securely filed or destroyed. Dumpster diving is still a valid method employed today to gather exploit information, which is by no means limited to computer assets.

Recommendations: A lockable filing cabinet should be installed within the access-controlled workspaces to further enhance security based on the need to know. This would augment storage room, currently provided in the safe, and further protect documents that have not been adequately protected to date.

Configuration Vulnerabilities

Banners: Audit results indicate that the message of the day (MOTD) file was blank. This file is usually read by services when a successful connection is established, and sent to the client.

Recommendations: Even though all unnecessary services will hopefully be removed as recommended by this audit, the /etc/motd banner should still be modified to convey an appropriate message to anyone logging into the server. As Secure Shell is a required service, an appropriate banner and SSH configuration is recommended. A beneficial message might bear the following, which aids in identifying further malicious intent by the client should they proceed. This may become useful in any possible legal pursuit.

```
##############################################################
##############################################################
####                                                      ####
####             This is a monitored system.              ####
####                                                      ####
####           Unauthorized access prohibited!            ####
####                                                      ####
####            Violators will be prosecuted.             ####
####                                                      ####
##############################################################
##############################################################
```

Physical Configuration: Physical security configuration vulnerabilities are considered to be minimal. More information is available under "Access Restrictions". Audit findings identified one vulnerability that could be addressed through system configuration. Currently, the server is susceptible to shutdown via the Ctl+Alt+Del keystroke combination.

Recommendations: The /etc/inittab file should be modified as indicated below to disable Ctl+Alt+Del reboots and to require a root password for single user mode. It is also recommended that a password be placed on the BIOS. This server is monitored frequently by NOC staff and a BIOS prompt would be noticed in short order. Callout of the designated security administrator would follow. Passwords must be documented and stored securely in the Network Operations Center - Security Administrators Room (NOCSA) with other critical passwords in the safe (more on password handling policies later).

```
Comment out ca::ctrlaltdel:/sbin/shutdown -t3 -r now by prepending # to the line
Append ~~:S:wait:/sbin/sulogin after si::sysinit:/etc/rc.d/rc.sysinit
```

Unnecessary Services: The threat of vulnerabilities being introduced to a system increases for every application installed. This is a logical assumption, and affirmed in an article from Windows2000 magazine[22].

Management may ask "Why is a Windows2000 magazine article relevant to this audit of a UNIX server?". This specific sample was used to highlight the fact that vulnerabilities are introduced regardless of OS as more lines of code are introduced. Simply put, the probability of error increases with every additional line of code. It is therefore also logical to conclude that by lowering the number of running applications, you will thereby lower the number of vulnerabilities presently exploitable on the system. With fewer applications running, maintenance becomes less burdensome, resources are freed up, and things generally become better for everyone concerned (except the attacker).

Recommendation: All unnecessary services should be terminated or removed from the system. It is important that the service RC scripts will not start the unneeded service at next boot. We are primarily concerned with network-enabled services even though any service, binary, or executable not required should be removed. The network-enabled services identified previously by the netstat command will be dealt with individually. After the following recommendations have been completed, the system should be rebooted into multi-user mode. For a complete listing of the processes running on the DNIDS server during the audit and the status of /etc/rc.d/init.d see appendix A. For a recap, the ports bound at the time of audit were:

```
[dragon@dnids1 dragon]$ netstat -ln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:32768           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:515             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN
tcp        0      0 DNIDS.Server:80         0.0.0.0:*               LISTEN
tcp        0      0 DNIDS.Server:443        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:9111            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:32768           0.0.0.0:*
udp        0      0 0.0.0.0:665             0.0.0.0:*
udp        0      0 0.0.0.0:111             0.0.0.0:*
```

A. A Line Printer Daemon (LPD - TCP port 515) was found to be running on DNIDS server. The current daemon version is LPRNG 3.7.4. There are no known vulnerabilities published against this version at the time of audit[23]. Management has determined that there is no requirement to offer networked printing services to other clients through the DNIDS server, however local printing is required. The current firewall policy within GIAC Enterprises is to deny all inbound Transmission Control Protocol (TCP) connections to port 515 at the border. Unfortunately, the current DNIDS server IPChains firewall policy of "inbound allow all" does not provide a layer of defense on the host. The printer used by the DNIDS server locally is connected via parallel port.

Recommendations: The /etc/lpd.perms file should be modified to reflect the current policy with regard to (WRT) server printing requirements as indicated below[24]. Additionally a patch has been identified that is applicable to the current version of LPRNG installed. This patch should be installed. Furthermore, properly configured access restrictions should be applied to the DNIDS server to compliment the overall security posture. More info is available in the "Access Restrictions" section of this audit.

```
server localhost
job
192.168.1.2
REJECT SERVICE=X NOT SERVER
ACCEPT SERVICE=C LPC=lpd,status,printcap
ACCEPT SERVICE=C HOST=dnids1.localhost.ca PRINTER=hpjet USER=root,dragon,dnids_user2
```

[22] http://www.win2000mag.com/Articles/Index.cfm?ArticleID=4908
[23] http://icat.nist.gov/icat.cfm?cvename=CVE-2000-0917
[24] See the original configuration of lpd.perms in appendix A

```
REJECT SERVICE=R,C,M FORWARD
REJECT SERVICE=C
ACCEPT SERVICE=M SERVER USER=root
DEFAULT REJECT
```

B. Portmapper and Remote Procedure Call (RPC) enabled services were noted running on the DNIDS server. There have been many security concerns over the years with RPC services. These concerns are two fold. The first is that RPC services historically had weak authentication mechanisms. In most instances, user names and passwords were sent across the network in plain text[25]. This is considered today to be a grave security risk. Packet capture software, also known as sniffers, are commonly available and widely used, making these plain text transmissions viewable by anyone on a network segment that the packets travel on. While different authentication mechanisms are now available through the use of Pluggable Authentication Modules (PAM[26]) and other implementations (Secure RPC[27]), they still leave a margin of error for mis-configurations. The other concern in more recent years has been with the number of buffer overflows exploitable within the code. The original SUN Microsystems© code was very buggy and many exploits proliferated where remote compromise exploit scripts were created and distributed widely[28]. Cross-platform ports of these RPC services, and the popularity of the opensource distributions of Linux have multiplied the availability of vulnerable hosts.

Recommendations: Unneeded RPC services should be disabled since no requirement for these services has been identified[29]. Not only should unnecessary "R" services be removed from startup scripts, they should also be completely removed from the server as they have not been identified as being required. After the following commands have been completed successfully the server should be rebooted to confirm that the services did not load and the current state of the system does not include these services. This may be accomplished via the following commands[30]:

```
/sbin/chkconfig --del portmap && chkconfig -del rstatd && chkconfig --del netfs && chkconfig --del nfs &&
chkconfig --del nfslock

/bin/rpm -e rsh
```

C. Sendmail was found to be running during the audit. This host is not a mail server and does not require this service to be running.

Recommendations: Sendmail should be removed from the server altogether. There are a few dependencies required by Sendmail such as fetchmail. These dependencies may also be removed as they do not interfere with email services should an email account be setup to retrieve and send mail through a legitimately configured and managed mailserver within GIAC Enterprises[31].

```
/bin/rpm -e mutt
/bin/rpm -e fetchmail
/bin/rpm -e sendmail --nodeps
```

Other Software

Apache: This is one of the few software packages that are required for the DNIDS server. Hypertext Transfer

[25] http://www.sans.org/topten.htm - This could be compared with #8 on the SANS Top 10 list dealing with weak passwords.
[26] http://www.kernel.org/pub/linux/libs/pam/ - Pluggable Authentication Modules
[27] http://csrc.ncsl.nist.gov/publications/nistpubs/800-7/node184.html - Secure RPC
[28] http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=RPC - list of RPC related Common Vulnerabilities and Exposures
[29] http://www.sans.org/topten.htm - RPC services come in at #3 on the SANS Top 10 list of Critical Internet Security Threats
[30] This should effectively shut down services on tcp/udp 111, udp 665, and tcp/udp 32768.
[31] This should effectively shut down services on tcp 25.

Protocol (HTTP) is required in order to take advantage of the HTML report layouts prepared by Dragon Fire© and Dragon Rider©. It has been determined that both remote and local access to the server is required and that pages served over the network must be encrypted to protect the confidentiality of sensitive information on the internal network. The version of Apache installed on the DNIDS server is 1.3.19. The Apache 1.3.19 configuration file located at /etc/httpd/conf/httpd.conf was reviewed. The current configuration specifies the server is started with the uid of dragon and the gid of apache. This is acceptable. The server however allows access to all hosts on port 80. SSL had been configured on a virtual server and provided the specified level of encryption through a trusted privately generated certificate.

Recommendations: Firstly, the version of Apache is not the most current. A good practice to follow is to keep the most recent stable version installed and patched. Therefore it is recommended that Apache be updated to version 1.3.22[32] along with Openssl and Modssl being updated to versions openssl-0.9.6b and mod_ssl-2.8.5-1.3.22 respectively. Access to the main server should be denied to all but the localhost on TCP port 80, with remote connections only accepted to TCP port 443 through SSL/TLS. An access.conf file should be created that specifies only connections from hosts on the internal network should be allowed. Furthermore, .htaccess files with the appropriate passwd file should be employed to require a basic authentication login prior to apache serving up the required page(s). Recommended configuration files are included in appendix A that will function with the 1.3.22 version and the Dragon IDS © configuration. Aside from Apache specific configuration options, further access controls are discussed later on in the audit (such as TCPWrappers and IPChains).

Xwindows: This is deemed as an essential service on the DNIDS server. Work will be accomplished directly on the server that requires the use of graphical browsers and other graphical tools, which depend on Xwindows. TCP port range 6000 - 6255 is used by default for Xwindows. There is however no requirement to share Xwindows with other users. With this information it becomes possible to make some recommendations.

Recommendations: Providing a server devoid of any windowing system is the optimal solution (analysis compiled from a trusted client through SSL). Given direction from management and the lack of additional resources however the following recommendations have been made. The use of a host based firewall such as IPChains with a default deny all policy and then specifically no rules to open up this port range will go great lengths in limiting the possibility of access to the above identified port range and the Xwindows service. More information is available specifically on IPChains further into the audit. Other actionable options that will control access to Xwindows would be the removal of the xhost command. Auditing the various ~/.Xauthority file on the DNIDS server identifies there are magic cookies present, confirming access by other hosts was previously conducted through Xwindows. It is recommended that these entries be removed from the ~/.Xauthority files for each respective user thereby limiting access through Xwindows to localhost on the local Xserver.

Driders: The Dragon Rider© server is also required on the DNIDS server. During the interactive installation of the server software, numerous questions are asked related to the servers' settings. The driders.cfg file is read when starting up the Drider service. The answers given during the interactive setup are written into this file and are security conscious. Settings include, encrypting client/server communications using blowfish (with shared secrets), selecting the port number to bind the server socket to, specifying the number of retransmissions allowed before the server (daemonized) dies, specifying an IP address based access list of authorized sensors (similar functionality to TCPWrappers), specific logging and debugging settings, as well as the absolute path to certain trusted system binaries such as /bin/tar[33]. Packet captures were obtained between the sensors and the DNIDS server to ensure that encryption was taking place. The packets were encrypted

[32] http://httpd.apache.org/
[33] A sample configuration file is available in appendix A

and deemed as secure from intercept and unauthorized replay. Additionally, attempts to connect to the DNIDS server on TCP port 9111 (the specified service port) from IP addresses, not identified in the configuration file as trusted sensors, failed. It is interesting to note however that it was possible to gain a prompt when telneting to this port from a trusted sensor. The auditor was unable to execute commands on the DNIDS server, but it is possible that improper error handling may provide a mechanism for unauthorized access. The klog daemon wrote the following message to the console, notifying the auditor that an unauthorized access attempt was unsuccessful and provided some hints of how to format future attempts for varied results.

```
Exception: Cannot Store MD5 Info - No Sensor Name
```

Recommendations: Most security concerns have been addressed adequately through the proper configuration of this software. The /usr/driders/driders.cfg file however was stored in plaintext and contained the shared secrets between the server and client sensors. It is recommended that security concerns with both the interactive telnet prompt, and plaintext passwords located in the configuration file be raised with the product vendor.

Development Tools: This topic was briefly touched on under fundamental security model flaws/incomplete parameter checking. The DNIDS server has many development tools installed. There were 28 packages installed and listed under the Development/Languages group alone. The installation and ready availability of these tools, languages, and libraries aid an attacker should a successful compromise occur.

Recommendations: The appropriate selection of necessary packages at the time the OS was loaded would have helped eliminate many of these development tool installations. Checking the dependencies of many of these packages and removing them will help lock down the server. This will also decrease the functionality of the server. New software will not compile if the required development tools are removed. Under the assumption that the other recommendations of this audit are adhered to, it is the recommendation of the auditor to leave the development tools on the server at this time as they may be required to carry out some of the recommendations presented in this report[34]. Of course this should come under further review as circumstances change or during the next audit. Also, as previously mentioned, providing a server specifically for development would also be considered beneficial. This would make even more work but would provide a level of comfort and product support lifeline to the DNIDS server and other Redhat 7.1© boxes should the development tools be identified for removal by management. Maintaining the development server is another issue completely and is not covered in this audit report.

Administrative Practices

Incident Response and Lessons Learnt: The security policy outlines procedures to deal with disaster situations. In particular, as it applies to this audit, steps to recovering from a security incident are covered within the security policy and standard operating procedures for the security administrator[35].

These procedures were tested during the audit by playing out a scenario where the front-end webserver for GIAC Enterprises Secure Online Ordering was turned into a DDoS agent that was purportedly attacking

[34] It should be noted that the kernel source is not installed on the system, thereby limiting access to kernel modification on the DNIDS server. Should the kernel require modification, the source code will need to be installed or another machine (preferably symmetrical multiprocessor) with the source and OS need to be used. However, installing the source to review the kernel settings for security considerations and tweaking the system for optimal performance has not been ruled out and this request is currently under review by the ISSO.

[35] http://www.cert.org/tech_tips/win-UNIX-system_compromise.html - Publicly available guide, adopted for private use with minor modifications.

another victim. Preliminary reports provided by the security administrator indicated that the Network Intrusion Detection System (NIDS) captured all traffic related to the exploit. The server had not been used for any other malicious activity and no sensitive information appeared to have been transmitted over the network. The directive received was to block services via the corporate firewall related to this vulnerability. Blocking inbound access to FTP services was deemed as an acceptable business risk while the identified patches were installed on the secondary staging server. The primary web server was to be restored from backup and patched prior to being placed back into production. The active participation of administrators and management made this test a success. Conducting the test during off-hours may have produced varied results.

Recommendations: The security administrators standard operating procedures specifies that compromised machines must be disconnected from the network and shut down. It is recommended that some forensic techniques be applied to suspect compromised machines to gather state information prior to disconnecting and shutting them down and these procedures be included within the SOP's. Volatile memory and information on running processes at the time of a compromise is very valuable information. One such tool is List Open Files or lsof[36], available from Purdue University. This was installed on the machine prior to the audit and used during the audit.

Logging: The main purpose of the DNIDS server is to log files from remote sensors. The server will be used frequently in the compilation of security related event logs, correlation, and report generation. With this in mind, it makes logical sense to have critical infrastructure logs written to the DNIDS server to enhance the current security posture of GIAC Enterprises and provide a more complete picture of security related events in addition to the servers own logs. Currently there are no central syslog facilities within GIAC Enterprises. Local log rotation configuration was found to be inadequate, as handled by the package logrotate.

Recommendations: The DNIDS server should be configured to receive incoming syslog alerts from critical systems within GIAC Enterprises. Windows based systems may be supported through the use of Kiwi's Syslog Message Generator 2.0[37]. The added functionality of a central syslog server may, in the auditors opinion, be considered an interim solution to the installation of hostbased intrusion detection systems (HIDS). At the very least, it will aid in security analysis and enhance the company's security posture. The files /etc/rc.d/init.d/syslog, /etc/logrotate.d/syslog, /etc/sysconfig/syslog and /etc/logrotate.conf should be edited to conform to the provided settings in appendix A. Additionally, the topic of log files or log rotation was absent from the security and backup policies. Critical system files were addressed in the backup policy but no specific mention of log file rotation was found, nor a definition of a critical system file. This should be reviewed and addressed as appropriate. Lastly, the IPChains firewall policy must include a rule to allow UDP port 514 communications with internal logging clients. The recommended configuration of IPChains may be found under the "Access Restrictions" section.

Network Time Protocol: XNTP3-5.93 is currently in use within GIAC Enterprises however NTP was not configured to run on DNIDS, nor was the package present. Version 3-5.93 has a published security vulnerability[38]. This vulnerability allows the execution of arbitrary code through a buffer overflow.

Recommendations: It is recommended that XNTP3-5.93 be replaced with XNTP ver 4.1.0 or later, enterprise wide. External servers are the most susceptible to attack and should be updated first, preferably having time synchronization services provided through the pseudo clock with external access being temporarily blocked at the border router to UDP port 123 internally. Audit results also identify the DNIDS server as a critical security infrastructure asset. Time synchronization is extremely important for legal

[36] ftp://vic.cc.purdue.edu - lsof ftp download
[37] http://www.kiwi-enterprises.com/software_downloads.htm
[38] http://icat.nist.gov/icat.cfm?cvename=CAN-2001-0414.htm

issues, as well as internal accuracy and correlation of logs. DNIDS should have the 4.1.0 package installed and configured inline with security policy guidelines[39].

Password Policy: This issue is addressed in the GIAC Enterprises security policy and administered throughout the network amongst the companies' users. The policy states that user passwords must be changed every 60 days, accounts with an unchanged password older than 65 days will be locked, a 14 day warning period will be given, and they must be a minimum of 6 characters in length. The accounts on DNIDS were audited by comparing the /etc/passwd file with the passwd structure[40]. Another command used to produce more reader friendly output is /usr/bin/chage. The file /etc/login.defs was also audited. The results did not match the password policy.

The password policy also covered acceptable methods of storing passwords. All server and critical system passwords were stored and available in a non-electronic format. Passwords were written legibly in ink, on a sheet of paper, which is stored in a fireproof safe within the NOCSA. The combination to the safe is only known by those with a need to know the most sensitive information contained within the safe. No passwords were found stored in rolodexes or under keyboards during audit of the physical area.

A password-cracking program was employed to test the strength of current passwords on DNIDS. The current passwords are considered as strong. Approximately 49 million MD5 one-way hashes were generated and compared against the current shadow password file and user accounts. Only the test account setup for audit purposes was cracked (proving the password cracker was operating properly). The test account was removed afterwards[41].

Recommendation: The current security policy, password policy subsection should be reviewed to consider specifying a minimum age between password changes. This would strengthen the current policy and force users to actually use new passwords instead of changing them back to a well-known password immediately. A password cracker should be employed on a regular basis to check password strength. Passwords identified as poor should be changed immediately, upon direction from the system administrator. The /etc/login.defs file should be edited to reflect the appropriate password policy, then the three user accounts must be modified to comply with the security policy. The following commands will change current accounts to comply with company password policy. Each user must change their password to comply with the above-described policy.

```
/usr/bin/chage -M 60 -W 14 -I 5 -d yyyy-mm-dd username
/usr/bin/passwd username
```

Security Training: There is a user security educational awareness program in place at GIAC Enterprises. This program promotes the use of secure passwords, enforces the need for security, educates users about social engineering techniques used by malicious individuals, communicates the key aspects of the security policy, and identifies ways in which the security posture of the company may be better served. An award of recognition is given out quarterly to an employee that has brought forth suggestions or security concerns of significant impact to their fellow employees and the company as a whole.

Recommendations: Continue with this program, keeping the content relevant to the security needs of the company, while making the training enjoyable by the attendees.

System Integrity: In the event of a system compromise, evidence collection and following the steps required

[39] http://www.eecis.udel.edu/~mills/ntp/
[40] Password structure available in appendix A
[41] Test results are available in appendix A

to retrace an attackers footsteps can become extremely labor and time intensive. The use of a file integrity checker can greatly reduce the amount of work required. This may be compared simply to having a good "before" picture to compare with the "after" picture of the system. It also provides piece of mind and may be checked regularly against the current system to confirm integrity. Current security policy does not stipulate that integrity checkers need to be employed. There were no integrity checkers installed on the DNIDS server.

Recommendations: Install Tripwire Open Source Edition©[42]. This is considered one of the best integrity checkers in the security industry for Linux systems. This free application allows for the creation of checksum and signed lists of files on the Linux system. Since everything in Linux is in essence a file, the entire system may be catalogued and checksums provided. This would not be practical since numerous files change regularly and their checksums would be constantly changing, creating false positive events, but files and directory structures considered to be essential to system integrity should be included in the tw.conf file.

Security Patches

As previously mentioned, the operating system being audited is Redhat© 7.1 (seawolf).

Most OS producers are very susceptible to bad publicity related to flaws within their product or to flaws within other products distributed with or designed to run on the specified OS. The OS vendor presented in this analysis is motivated to provide solutions to security issues identified in their product. This is evident by the long history of security updates provided by the OS producer and can be correlated by viewing the security releases going back as far as October of 1996 with Redhat ver 4.0©. It is with this in mind that the OS producers website has been used as the primary source for identifying OS related vulnerabilities[43].

As of September 14th 2001, there were a total of 27 vulnerabilities listed for Redhat 7.1©[44]. No patches had been installed since the system was put into production on May 23rd 2001. Prior to the boxes identification as the new DNIDS server, the previous system owner had used the system internally for personal development and training (This indicated that the subject box might make a good candidate for a security audit!).

After a review of the patches available, it was determined that the following patches should be applied to this server:

Date	Reason	URL	Status
2001-04-16	Netscape Patch	http://www.redhat.com/support/errata/RHSA-2001-046.html	
2001-04-18	Up2Date Patch	http://www.redhat.com/support/errata/RHBA-2001-048.html	
2001-05-02	Mount Patch (swap)	http://www.redhat.com/support/errata/RHSA-2001-058.html	
2001-05-09	Minicom Patch	http://www.redhat.com/support/errata/RHSA-2001-067.html	
2001-06-07	GPG Patch	http://www.redhat.com/support/errata/RHSA-2001-073.html	
2001-06-11	LPRng Patch	http://www.redhat.com/support/errata/RHSA-2001-077.html	
2001-06-21	Kernel IPTables Patch	http://www.redhat.com/support/errata/RHSA-2001-084.html	
2001-06-22	Xfree86 Updates	http://www.redhat.com/support/errata/RHSA-2001-071.html	
2001-07-06	Xinetd Patch	http://www.redhat.com/support/errata/RHSA-2001-092.html	
2001-07-13	Procmail Patch	http://www.redhat.com/support/errata/RHSA-2001-093.html	
2001-07-16	Util Linux Patch	http://www.redhat.com/support/errata/RHSA-2001-095.html	
2001-07-18	OpenSSL Patch	http://www.redhat.com/support/errata/RHSA-2001-051.html	Already Updated

[42] http://www.tripwire.com/products/linux/

[43] Keep in mind that with the release of opensource OS distributions, such as Redhat© Linux distributions, there are many, many Third Party contributions within the OS as well as distributed packages. Many people fail to realize that it is often not the OS producers fault directly when a security vulnerability is found, but merely that a third party software package was distributed with the OS, which introduced a vulnerability that people associate primarily with the OS producer.

[44] http://www.redhat.com/support/errata/rh71-errata.html

2001-08-09	Telnet Patch	http://www.redhat.com/support/errata/RHSA-2001-099.html	
2001-08-09	Kerberos 5 Patch	http://www.redhat.com/support/errata/RHSA-2001-100.html	

One of the patches available is for the up2date agent. The version installed on the audited system is 2.5.2. According to RedHat©, additional functionality is offered through the applicable patch to version 2.5.4 as well as a fix that corrects a bug related to the use of proxies for obtaining updates. Currently, the DNIDS server is not registered with RedHat© for the use of up2date.

> Recommendations: Manually apply the up2date patch, then run `/usr/sbin/rhn_register`. Configure the up2date agent using `/usr/sbin/up2date --configure`. Then apply the appropriate patches identified above. Keep current on security issues affecting programs running on the DNIDS server, as well as the OS. The application of patches and maintenance of software is covered in the Security Policy, but was not applied to this host previously. It would be beneficial to create a rotating checklist that covers in the very least, the critical servers within GIAC Enterprises to ensure that each machine receives the appropriate service, as well as creating a chain of responsibility and recourse should duties be neglected.

Other sources consulted for potential OS vulnerabilities on a regular basis include but are not limited to (in alphabetical order):

NIPC Cybernotes - http://www.nipc.gov/cybernotes/cyber2001.htm
Redhat Bugzilla - http://bugzilla.redhat.com/bugzilla
Sans Newsletters - http://server2.sans.org/sansnews/
Security Focus Bugtraq - http://www.securityfocus.com/templates/archive.pike?list=1

Sensitive Data Stored Encrypted

Access to the audited server through remote and physical means is tightly controlled. This has been a largely beneficial factor in protecting data accessed, greatly reducing the requirement to encrypt it, but not eliminating the threat. Raw log files could be encrypted on the disks, but this does not seem practical given the amount of access, and frequency with which the data is required, and the server load at peak times. In rating the DNIDS servers criticality, it has been determined that should an attacker be able to gain unauthorized access to the server, other very severe security infractions in this defense in-depth environment must also have happened. It is important to note that system authentication mechanisms and passwords are stored encrypted as discussed under the password policy section above.

> Recommendations: Weighing the cost vs gain of encrypting local data on the server results in the auditor recommending that this risk be accepted by management. An interesting point to consider is obfuscation through the use of technology. One of the identified desires for the audited server is to log all data into a database. Doing so will remove the data from direct access, making it more difficult for a potential attacker to gain access or accidentally find the data. Should a database server be integrated into the environment in the future, this may help hide the data making it appear to be encrypted on the disk, or at least more technical expertise will be required to retrieve the data. Future audits and review should circumstances change is recommended as well. It is important to note that a database may also be installed and configured locally on the DNIDS server.

Data Sent Encrypted Over Internet

It is necessary to weigh the use of this server in respect to the need for external communications and determine whether or not these communication channels are appropriate. The DNIDS client programs in use

are currently configured to use a proxy through the firewall and DNS traffic is directed at the secondary DNS server, located within the corporate intranet. While this is not encrypted, consideration must be made to the type of data sent over the Internet. This is currently not limited and controls are not in place to do so. During the audit, many services previously enabled have been identified for removal. Assuming these recommendations will be actioned, there are very few communication channels or ports left open. Firewall policies recommended for the host based firewall coupled with other access restrictions implemented resultant from the audit findings along with corporate remote access controls (such as the corporate firewall and border routers) should greatly aid in limiting communications from this server. The server previously was not being used to convey any sensitive clear text information over the Internet for any critical applications. Telnetd was disabled and the telnet client was not used by the previous system owner, FTP client was in use for anonymous connections, HTTP was being used to retrieve web pages from non-critical systems that are not business partners of GIAC Enterprises, and there were no mail clients even configured on the system. Any requirement to communicate or login to other external or internal hosts was accomplished through the use of the SSH client.

Recommendations: The results of this audit highly recommend against any of the servers communications going directly to the Internet! This would be considered sensitive information based on the function of the server and the types of traffic that may be sniffed off the wire. The employ of other recommendations within this audit will greatly limit the possibility of traffic passing over the Internet from the DNIDS server in the clear. The Security Administrator's job description and standard operating procedures (SOP's) should also address this issue with relation to the DNIDS server. The use of secure shell (SSH) is discussed in further depth under "Access Restrictions". This method of communication employs encryption and is the primary method of communications between the audited server and other internal hosts. The requirement for this server to access the Internet directly is very low. With SSH already employed, any required communications over the Internet should be carried out using SSH. Other communications should be carried out from a separate workstation. One exception to this recommendation (due to the lack of a development server) would be the use of Up2Date. Settings should be modified on a scheduled basis specifically for the purpose of updating the DNIDS server as outlined on the Redhat website[45]. This provides the settings necessary to open up access and it could be done on a manual schedule or automated through cron. Remember that the network employs Network Address Translation that obfuscates the actual host URL on the Internet, adding a very limited, timed window of opportunity for attack against the DNIDS server during Up2Date functions[46].

Anti-virus Software

During the audit it was determined that this server does not have any anti-virus protection installed locally. The server is protected via anti-virus scanning at the mail gateway through the use of McAfee WebShield Solaris©[47].

Recommendations: As this is a dedicated server that will not be used to generate email, or otherwise execute newly introduced binaries or programs it is recommended that the support of the WebShield server will suffice for anti-virus protection. The criteria for having anti-virus software installed on a server is flexible within GIAC Enterprises and assessed on a per server basis, defined by the servers purpose. This varies greatly from workstations, where strict policy is regimented and enforced through scanning schedules, training, on demand and on access scanning with weekly signature updates and a baseline

[45] http://www.redhat.com/docs/manuals/RHNetwork/ref-guide/up2date-config-text.html - Up2Date
[46] http://archives.neohapsis.com/archives/sf/linux/2001-q2/0074.html - as an example of a rule insertion vulnerability that corresponds to the attack described as a potential vulnerability in this scenario.
[47] http://www.mcafeeb2b.com/products/webshield-solaris/default.asp

configuration of most desktop workstations. The risk is considered extremely low that the DNIDS server will become infected by a virus as a result of the execution of this policy, and simply stated, the number of viruses[48] that target the servers OS platform add credibility to this conclusion. The current configuration is acceptable.

Access Restrictions

Remote Access: Audit findings show host based remote access is controlled through the use of IPChains ver 1.3.10, Secure Shell ver 2.9p2[49] and TCPWrappers.

A. IPChains was enabled at boot, unfortunately the default policy was set as "input accept". There were no rules enabled either. Basically, the firewall was doing nothing except waste resources. For the servers intended role with a single homed interface, it has been determined that IPChains is an acceptable, stateless firewall to use. The enterprise border firewall is stateful and well maintained, adding to the internal protection of this server dramatically. The employ of ACL's on infrastructure routers also enhances access restrictions to the DNIDS host.

Recommendations: The IPChains firewall should be modified to reflect an "input deny all" policy. All inbound communications via UDP and TCP must be explicitly permitted. No forwarding is required, nor is Network Address Translation (NAT). ICMP may be managed and filtered in an additional chain, with specific types such as 0, 3, 8, and 11[50] being allowed. Only a very limited number of UDP and TCP ports are required to be accessible to inbound connections. The following is a basic, suggested, firewall configuration that should be reviewed and modified according to server requirements and network architecture. Once accepted and applied, it should be reviewed regularly during routine audits. The rules presented in purple may be removed dependent on the implementation of future policy WRT accessing the Internet from the DNIDS server. The use of SSH port forwarding also affects the configuration of the firewall and what is required to run through it should SSH port forwarding be implemented. Of note also is the rule to allow traffic outbound to TCP 8080. This is used for Up2Date as it is configured.

```
:input DENY
:forward DENY
:output ACCEPT
:icmp -
-A input -s 0.0.0.0/0.0.0.0 -d 0.0.0.0/0.0.0.0 -p 1 -j icmp
-A input -s MY Internal Net/255.255.255.0 -d DNIDS server/255.255.255.255 443:443 -p 6 -j ACCEPT
-A input -s firewall/255.255.255.255 80:80 -d DNIDS server/255.255.255.255 -p 6 -j ACCEPT
-A input -s secondary dns/255.255.255.255 53:53 -d DNIDS server/255.255.255.255 -p 17 -j ACCEPT
-A input -s MY Internal Net/255.255.255.0 22:22 -d MY Internal Net/255.255.255.0 -p 6 -j ACCEPT
-A input -s MY Internal Net/255.255.255.0 -d DNIDS server/255.255.255.255 22:22 -p 6 -j ACCEPT
-A input -s dragon sensor1/255.255.255.255 -d DNIDS server/255.255.255.255 9111:9111 -p 6 -j ACCEPT
-A input -s dragon sensor2/255.255.255.255 -d DNIDS server/255.255.255.255 9111:9111 -p 6 -j ACCEPT
-A input -s dragon sensor3/255.255.255.255 -d DNIDS server/255.255.255.255 9111:9111 -p 6 -j ACCEPT
-A input -s firewall/255.255.255.255 8080:8080 -d DNIDS server/255.255.255.255 -p 6 -j ACCEPT
-A input -s firewall/255.255.255.255 21:21 -d DNIDS server/255.255.255.255 -p 6 -j ACCEPT
-A input -s firewall/255.255.255.255 20:20 -d DNIDS server/255.255.255.255 -p 6 -j ACCEPT
-A input -s MY Internal Net/255.255.255.0 514:514 -d DNIDS server/255.255.255.255 514:514 -p 17 -j ACCEPT
-A input -s time server1/255.255.255.255 123:123 -d DNIDS server/255.255.255.255 -p 17 -j ACCEPT
-A input -s time server2/255.255.255.255 123:123 -d DNIDS server/255.255.255.255 -p 17 -j ACCEPT
-A input -s time server3/255.255.255.255 123:123 -d DNIDS server/255.255.255.255 -p 17 -j ACCEPT
-A icmp -s 0.0.0.0/0.0.0.0 3:3 -d 0.0.0.0/0.0.0.0 -p 1 -j ACCEPT
-A icmp -s 0.0.0.0/0.0.0.0 11:11 -d 0.0.0.0/0.0.0.0 -p 1 -j ACCEPT
-A icmp -s 0.0.0.0/0.0.0.0 8:8 -d 0.0.0.0/0.0.0.0 -p 1 -j ACCEPT
-A icmp -s 0.0.0.0/0.0.0.0 0:0 -d 0.0.0.0/0.0.0.0 -p 1 -j ACCEPT
-A icmp -s 0.0.0.0/0.0.0.0 -d 0.0.0.0/0.0.0.0 -j DENY
```

[48] http://www.whitehats.ca/main/members/Slyfox/slyfox_virus_faq/slyfox_virus_faq.html - Difference between Virus and Worm

[49] Recent findings identify a CRC vulnerability in this version. It is recommended at this time to replace this version with 3.0.2 released 3rd December 2001.

[50] http://www.iana.org/assignments/icmp-parameters - ICMP Parameters

B. Secure Shell is essentially an application and protocol used to securely log into another computer[51]. Configuration files audited were /etc/ssh/sshd_config, /etc/ssh/ssh_config, /etc/rc.d/init.d/sshd and /root/.ssh/known_hosts2. SSH was compiled with TCPWrappers support. Daemon configuration options enabled include root logins, X11 forwarding, MOTD banner, strict modes, syslog AUTH info logging, and RSA authentication. Client configuration options enabled include X11 forwarding, RSA authentication, password authentication, identify file ~/.ssh/id_dsa, port 22, protocol 2,1. There were no abnormalities found in the startup script. The known_hosts2 file had appropriate RSA public keys from known workstations used by the security administrators. An X11 forwarded connection through SSH was attempted and it succeeded. TCPDump log files of this activity are located in appendix A. It has been determined that X11 forwarding is not a requirement, nor are root logins. Root access to the DNIDS server requires console or physical access. Furthermore, non-root access to the DNIDS server shall be either through command line SSH or via encrypted SSL sessions through HTTPS.

Recommendations: Secure Shell was already implemented and working towards a secured environment. Periodic key changes should be carried out, preferably during scheduled system audits. Security mail lists should also be monitored for future exploit and patch releases against SSH ver 2.9p2. Analysts requiring services supported within GIAC Enterprises, where supported, should use secure shell port forwarding. Specific changes to the configuration listed in appendix A should include changing the following to conform to the above specified recommendations:

```
/etc/ssh/sshd.config
PermitRootLogin no
X11Forwarding no
```

C. TCPWrappers was not configured. Not one entry was present in either the /etc/hosts.allow or /etc/hosts.deny configuration files. Based on the fact that all services offered on DNIDS should be private, and given that the hosts with which DNIDS requires regular private communications are static, it is possible to employ TCPwrappers very effectively.

Recommendations: Ensure SSHD and HTTPD are wrapped to allow connections only from specified hosts as required. Wrapping the Dragon Rider© service is achieved through the Dragon Riders configuration file previously discussed.

```
# hosts.allow
sshd:    My.Internal.NET. <<in IP format>>
httpd:   Authorized.Internal.Host <<in IP format>>

# hosts.deny
ALL:     ALL
```

Root Privilege: Login to the DNIDS server is currently accomplished through the use of 2 user accounts. Should root access be required for elevated privilege in order to execute a binary or perform a specific administrative task, it is currently accomplished via the `/bin/su` command. Sudo[52] version 1.6.3p6 is installed on the server, however it does not appear to have been configured for use. The /etc/sudoers configuration file was found with the default configuration allowing root (All)=All. The current version of sudo was found to be 1.6.3 patch level 7. There are specific commands that are quite often required during daily use on the DNIDS server. The two users with access to the server both know the root password and often su back and forth between root. This is a dangerous practice that will likely catch up with the users through accidental misuse.

Recommendations: Upgrade sudo to the latest patch level and configure it for use. This will add a great

[51] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214091,00.html - definition of Secure Shell
[52] http://www.courtesan.com/sudo - Toby Miller's Sudo

degree of safety, ensuring that accidental commands are not executed as root. Identification of binaries will occur as they are needed, and the /etc/sudoers file may be modified at that time using the /usr/sbin/visudo program. An example configuration line for the user dragon might be the following:

```
Dragon   ALL=NOPASSWD: /bin/kill, /bin/ls, /bin/cat, /bin/more, /root/, PASSWD: /sbin/ifconfig
```

Set UID and GID Files: Securing the UNIX[53] file system is extremely important in the overall scheme of ensuring a systems current and continued integrity. During the audit, many files owned by root, or with a group of root were found that had the SUID or SGID bits on. This allows others to execute the command as the user or group assigned to the file. Review of these files indicates that most are required and properly handled. The exceptions to this rule would be some games that appear to be installed on the server set group ID equal to root. While these files do not pose a grave security risk, there has been no requirement identified for games on the DNIDS server. The other file of notice is the SCSI device emulator employed by the CDRW software (part of XCDRoast). This has been determined as normal by the XCDRoast documentation and configuration settings.

Recommendations: The unnecessary files should be removed from the server. While current exploits against these binaries are not known, the possibility exists that privilege may be elevated through them, or that the server may realize other undesired effects. If the binaries are not required as is the case with the games, they should be removed with the command:

```
/bin/rpm -e gnome-games
```

Unowned Files: The audit turned up some unowned files on the DNIDS server. These appear to be related to the test account that was created, then deleted during the password strength-testing phase of the audit. A login to the Xserver using the account was performed, which created these files. When the account was removed, the home directory was not.

Recommendations: The test home directory should be removed as it is no longer required and there is no longer a test user.

```
rm -rf /home/test
```

User Accounts: On servers where possibly hundreds of accounts exist, it can become a complicated task to manage users. This is especially true in an environment where contractors come and go on a regular basis. GIAC Enterprises does not fit into this category thankfully, and has a fairly stable staff. The dynamics of the company make it a stable place of employment with median employment tenure of 7 years. This bodes well in identifying user requirements. The DNIDS server only had three active user accounts. All three accounts were determined as necessary. This is acceptable to the auditor.

World Writable Files: A search for world writable files also turned up some results. All of the files require these permissions for use by the OS with the exception of four. The four files in question are dictionary files with no requirement to be world writable. It would appear that poor permissions were applied to the files during installation and modification.

Recommendations: Remove the world permissions completely from these four files. There is no need for these files to be modifiable by world. It would be prudent to also remove the user permissions too as these files should only be accessed by root when running password crackers. Periodic checks for world writable files should be carried out.

[53] http://www.linuxdoc.org/HOWTO/Security-HOWTO-5.html - File System Security HowTO

Backup Policies and Disaster Preparedness

GIAC Enterprises as an organization has a detailed backup policy in place, and all critical infrastructure servers are incrementally backed up nightly, into a rotating float of tapes. Full backups are performed bi-weekly. The rotation policy specifies that two months of previous data be available for restoration. Furthermore, a bonded offsite storage facility is used to store the off rotation backups. Policy specifies that the tapes must be available to GIAC Enterprises within 1 hour of the request. This was tested during the audit and the offsite storage facility was contacted for a request to pickup off rotation backup tapes. Upon presenting proper corporate credentials, the tapes were released to the auditor, within the specified hour. Future policy may need to be adjusted for specific systems. Currently the DNIDS server employs a stripped and mirrored internal raid configuration. Swappable spares are kept on the premises in case of a disk failure. The DNIDS server also has critical files backed up to tape on a rotating schedule, inline with the backup policy.

Recommendations: File integrity checkers such as Tripwire Open Source Edition©[54] help reduce the workload required in identifying a compromise in integrity. As noted above, it is recommended that Tripwire be installed on the DNIDS server. This would greatly aid in identifying which backups should be used in the event of a compromise. Also, due to the nature of the data stored on the DNIDS server, and its increasing volume due to higher bandwidth applications and network communications, it is determined that the FIFO policy of log storage may someday become inadequate and another method of maintaining this large collection of logs may have to be devised. It is the auditor's recommendation that management start considering the costs of implementing a SAN or other large data warehousing solution.

Prioritized List of Security Vulnerabilities

Audit findings clearly show many areas in which security does not meet the recommended standard on the DNIDS server. Some of these concerns are small, while others, if exploited would have a critical impact on the whole GIAC Enterprises security structure. Requirements as directed by management state "1. A prioritized list of security vulnerabilities or issues uncovered by your audit." and "2. A prioritized list of recommended fixes (as a bonus you may include estimated costs for hardware/software/personnel to implement the recommendation)." should be addressed.

Throughout the audit report, recommendations have been made surrounding the reported items. This was aimed at keeping relevant information together with the findings for ease of understanding by all concerned. This presentation format however does not put everything into perspective. Questions such as "What should be done first?", "How will this impact the organization?", or "How much will it cost to implement this recommendation?" were not rated in a scalar fashion. The following weighted chart addresses these questions, modeled after Dr. Peter Tippett's, Quantifying Risk Formula[55]. The base formula is [Risk = Threat x Vulnerability x Cost]. Other formulas exist like Stephen Northcutt's severity equation[56] and Julie Ryan's risk formula[57] but Tippett's was chosen as it performed well when modified to present an action priority that was proportional to the audited server.

Basically, the formula was modified to include the cost of fixing the problem by providing a factor under

[54] http://www.tripwire.com/products/linux/ - Tripwire
[55] http://www.networkmagazine.com/article/NMG20010119S0002 - Quantifying Risk
[56] http://www.sans.org/giactc/ID_assignment_guidelines.htm - Severity = (Criticality + Lethality) - (System Countermeasures + Network Countermeasures)
[57] http://www.julieryan.com/riskmgt.htm - Risk = Threat x Vulnerability x Impact / Countermeasures

which the organization generally accepts risk. This provides a weighted point score that identifies and prioritizes security items identified during the audit as well as establishing an order of cost that, evaluates in a scalar fashion, items such as man-hours, asset acquisition costs with maintenance, and the potential value of lost data should a loss occur. The results are sorted into an order where the highest payoffs with the least price are at the top of the list. I believe this covers both the items requested by management adequately. The modified equation for GIAC Enterprises follows:

$$\text{Action Priority} = \frac{[\text{Solution Modifier}=1000 \times \%\text{Risk Tolerance} \times \%\text{Solution Ease}]}{[\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Cost}]}$$

Key

action priority = lowest point value should be actioned first (higher point = lower priority)
risk tolerance = constant for the organization (higher points = acceptance of more risk)
solution ease = cost to implement solution (higher points = more manhours, money etc.)
cost = cost to recover from situation (higher points = higher cost)
threat = odds of someone targeting this (higher points = greater threat)
vulnerability = how dire is the vulnerability (higher points = bigger problems resultant in vulnerability)

Vulnerability	Solution Modifier	Risk	Action Priority
Remove RPC's	1000*.3*.05=15	7*7.5*8=420	0.0357
Remove unnecessary init Svc	1000*.3*.08=24	7*7.5*8=420	0.0571
Edit LPD perms	1000*.3*.01=3	3*2*8=48	0.0625
Change Core Values	1000*.3*.01=3	2*4*6=48	0.0625
Subscribe to Newslists and Monitor	1000*.3*.15=45	9*9*7=567	0.0790
Remove Sendmail	1000*.3*.02=6	4*2*7=56	0.1071
IPChains modifications	1000*.3*.15=45	6*9*7.5=405	0.1111
Modify MOTD	1000*.3*.01=3	3.5*1*7=24.5	0.1224
Setup central syslog server	1000*.3*.2=60	7*8*8.5=476	0.1261
TCPWrappers config.	1000*.3*.01=3	3*1.5*5=22.5	0.1333
Install Patches	1000*.3*.3=90	8*8*8=512	0.1758
Remove unowned files	1000*.3*.01=3	2*2*4=16	0.1875
Modify inittab	1000*.3*.01=3	1*2*8=16	0.1875
Remove world writable files	1000*.3*.02=6	2*3.25*4=26	0.2308
Setup and use SUDO	1000*.3*.15=45	8*4.5*4=144	0.3125
Replace NTP enterprise wide	1000*.3*.75=225	8*9.5*8.5=646	0.3483
Remove Set UID & GID files	1000*.3*.02=6	2*2*4=16	0.3750
Stack and Bounds Protection	1000*.3*.3=90	6*6*6=216	0.4166
Address Driders issues	1000*.3*.4=120	2*3*7.5=270	0.4444
Continued Sec. Awareness Prog.	1000*.3*.5=150	7*4.5*8=252	0.5952
Make modifications to Security Policy	1000*.3*.35=105	5*3.5*9=157.5	0.6667
Capture volatile info prior to powering down compromised boxes	1000*.3*.1=30	4*3*3.5=42	0.7142
Update and configure Apache	1000*.3*.2=60	3*7*3=63	0.9523
Install Integrity Checker	1000*.3*.2=60	3.5*8*7=56	1.0714
Install Locked Filing Cabinet	1000*.3*.1=30	1.5*1.5*8=18	1.6660
Enforce password policy changes	1000*.3*.38=114	3*3*7=63	1.8100
Periodic Audits	1000*.3*.35=105	6*5*1.5=45	2.3330
Use PAM	1000*.3*.25=75	1*5*6=30	2.5000
Research for Maint. Hooks	1000*.3*.7=210	2*7*6=84	2.5000

Remove Development Tools	1000*.3*.6=180	5*1*7=35	5.1420
Shielding and EME	1000*.3*.9=270	0.25*6*6=9	30.0000
Plan to buy a SAN	1000*.3*.4=120	1*1.25*3=3.75	32.0000

The scores presented in this table are subjective and may vary depending on the values chosen. The auditor chose high values for the RISK quotient where the compromise and threat to the internal structure of GIAC Enterprises appeared high; conversely a lower value was awarded when the level of exploit lowered such as a reconnaissance type of exploit where assets were only moderately affected. Other items that affected points selected for hosts were things like how likely is this type of exploit to be carried out against the DNIDS server? Some of these exploits are critical, but mitigated at the companies border through defense in-depth techniques presently in place. This greatly reduces the possibility of an attacker knowing where the DNIDS server is, and affects whether it could be effectively targeted even if the attacker new it existed. Mileage may vary, but the basic goal was to prioritize the recommendations, including some measure of cost while doing so.

References

1. ftp://vic.cc.purdue.edu
2. http://bugzilla.redhat.com/bugzilla
3. http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=RPC
4. http://httpd.apache.org/
5. http://icat.nist.gov/icat.cfm?cvename=CAN-2001-0414.htm
6. http://icat.nist.gov/icat.cfm?cvename=CVE-2000-0917
7. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214091,00.html
8. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci522583,00.html
9. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci549024,00.html
10. http://server2.sans.org/sansnews/
11. http://sourceforge.net/projects/stjude/
12. http://web.inter.NL.net/hcc/Haj.Ten.Brugge/
13. http://www.cert.org/tech_tips/win-UNIX-system_compromise.html
14. http://www.courtesan.com/sudo
15. http://www.eecis.udel.edu/~mills/ntp/
16. http://www.iana.org/assignments/icmp-parameters
17. http://www.immunix.org/immunix70.html
18. http://www.insecure.org/sploits/ping-o-death.html
19. http://www.julieryan.com/riskmgt.htm
20. http://www.kernel.org/pub/linux/libs/pam/modules.html
21. http://www.kiwi-enterprises.com/software_downloads.htm
22. http://www.mcafeeb2b.com/products/webshield-solaris/default.asp
23. http://www.mitre.org/resources/centers/infosec/secure_computers/secure_comp.doc
24. http://www.nessus.org
25. http://www.networkmagazine.com/article/NMG20010119S0002
26. http://www.nipc.gov/cybernotes/cyber2001.htm
27. http://www.nthelp.com/40/l0phtadv.htm
28. http://www.openwall.com/linux/
29. http://www.redhat.com/apps/support/updates.html
30. http://www.redhat.com/support/errata/rh71-errata.html
31. http://www.redhat.com/support/manuals/RHNetwork/ref-guide/up2date.html
32. http://www.rsasecurity.com/rsalabs/faq/3-6-6.html

33. http://www.sans.org/giactc/ID_assignment_guidelines.htm
34. http://www.sans.org/topten.htm
35. http://www.sans.org/y2k/practical/Paul_Parzen_GCUX.doc
36. http://www.securityfocus.com/templates/archive.pike?list=1
37. http://www.tripwire.com/products/linux/
38. http://www.whitehats.ca/main/members/Slyfox/slyfox_virus_faq/slyfox_virus_faq.html
39. http://www.win2000mag.com/Articles/Index.cfm?ArticleID=4908
40. http://www.wired.com/news/print/0,1294,37286,00.html
41. Information Security Management Handbook 4th Edition, Harold F. Tipton, Micki Krause, Auerback Publications, 2000

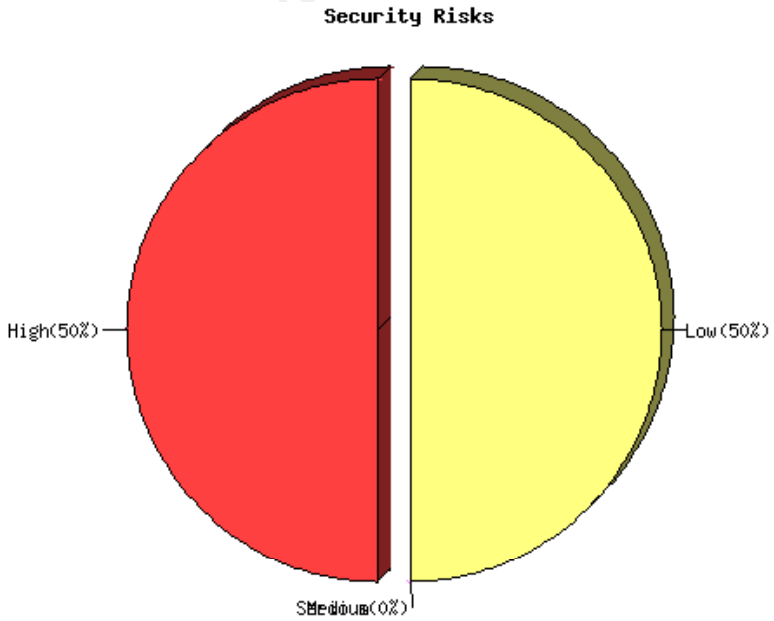
Appendix A

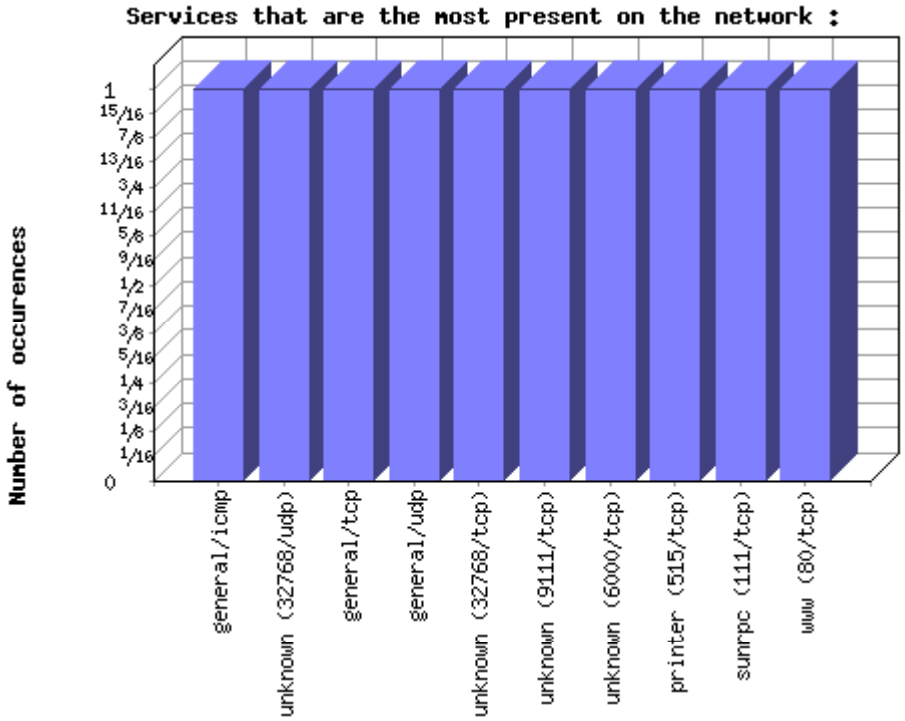
Nessus Report

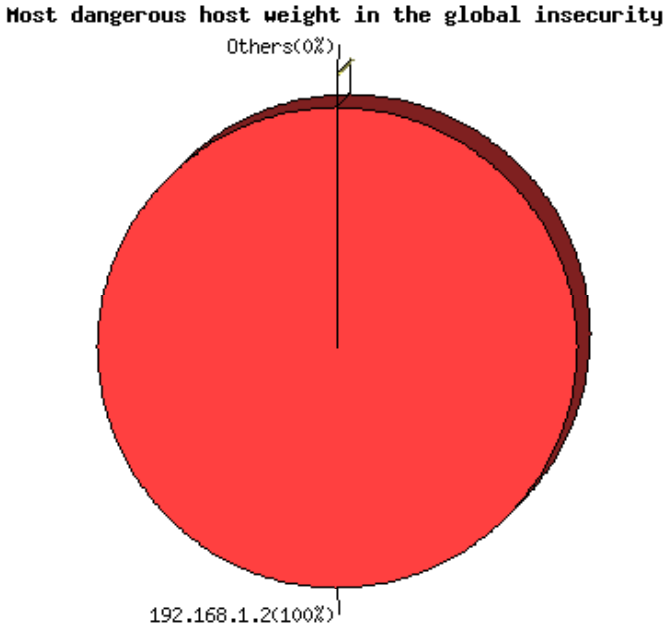
The Nessus Security Scanner was used to assess the security of 1 host

- 2 security warnings have been found
- 4 security notes have been found

Part I : Graphical Summary :





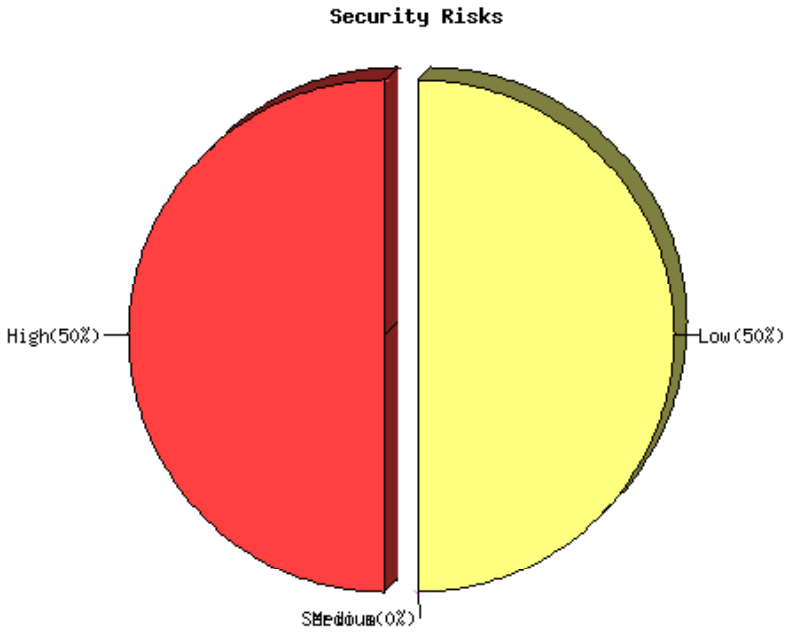


Part II. Results, by host :

192.168.1.2 **(found 2 security warnings)**

This file was generated by Nessus, *the open-sourced security scanner.*
192.168.1.2

Repartition of the level of the security problems :



[Back to the index]

List of open ports :

- *ssh (22/tcp) (Security notes found)*
- *www (80/tcp) (Security notes found)*
- *sunrpc (111/tcp)*
- *printer (515/tcp)*
- *unknown (6000/tcp)*
- *unknown (9111/tcp)*
- *unknown (32768/tcp)*
- *general/udp (Security notes found)*
- *general/tcp (Security notes found)*
- *unknown (32768/udp) (Security warnings found)*
- *general/icmp (Security warnings found)*

[back to the list of ports]

Information found on port ssh (22/tcp)

Remote SSH version : ssh-1.99-openssh_2.9p2

[back to the list of ports]

Information found on port www (80/tcp)

The remote web server type is :
Apache/1.3.19 (Unix) (Red-Hat/Linux)

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

[back to the list of ports]

Information found on port general/udp

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

[back to the list of ports]

Information found on port general/tcp

QueSO has found out that the remote host OS is
* Standard: Solaris 2.x, Linux 2.1.???, Linux 2.2, MacOS

CVE : CAN-1999-0454

[back to the list of ports]

Warning found on port unknown (32768/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 *

We suggest you to disable this
service.

Risk factor : High
CVE : CVE-1999-0018

[back to the list of ports]

Warning found on port general/icmp

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

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

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

Risk factor : Low
CVE : CAN-1999-0524

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

Core Settings at time of audit

```
[dragon@dnids1 dragon]$ ulimit -a
core file size (blocks)     1000000
data seg size (kbytes)      unlimited
file size (blocks)          unlimited
max locked memory (kbytes)  unlimited
max memory size (kbytes)    unlimited
open files                  1024
pipe size (512 bytes)       8
stack size (kbytes)         8192
cpu time (seconds)          unlimited
max user processes          20478
virtual memory (kbytes)     unlimited
```

Xauthority Sample

```
[dragon@dnids1 dragon]$ strings .Xauthority
MIT-MAGIC-COOKIE-1
]L&X
dnids1
MIT-MAGIC-COOKIE-1
MIT-MAGIC-COOKIE-1
```

Configuration File for Dragon Rider© Server /usr/drider/driders.cfg

```
#====================================================================
# Configuration File for driders
#
# Copyright 1999-2000 - Network Security Wizards.
#====================================================================

#--------------------------------------------------------------------
# FILE LOCATIONS
#
# DRAGON_DB_DIR: Parent directory to be used for creating centralized
#                dragon.db files.  If LOG_TO_DRAGON_DB is set to 1,
#                All events forwarded to the driders daemon will
#                be logged into a dragon.db file in a subdirectory
#                created for each date of activity (e.g., 99Oct26).
#
# DISTRIBUTE_CONFIG_DIR: Parent directory that contains the directory
#                structure used for configuration file/binary
#                distribution to the sensors.  This directory is
#                meaningful, if the DISTRIBUTE_CONFIG_FILES is set to 1.
#
# DRIDERS_DIR:   Directory where driders executable and configuration
#                files reside.  The daemon will chdir() to the directory
#                at startup.
# SIGNATURE_DIR: Directory that contains the master set of signature
#                files.  The files contained in this directory (e.g., *.sigs)
#                are used by the web GUI for signature management.
#--------------------------------------------------------------------
DRAGON_DB_DIR=/usr/drider/DB
DISTRIBUTE_CONFIG_DIR=/usr/drider/distribute
DRIDERS_DIR=/usr/drider
SIGNATURE_DIR=/usr/drider/signatures
```

```
#-----------------------------------------------------------------
# ENCRYPTION SETTINGS
#
# ENCRYPT=BLOWFISH: This line should be uncommented to enable Blowfish
#                encryption.  If the line is commented, data transfer
#                will occur in cleartext.  Please ensure that the
#                encryption settings in effect in this file match
#                the settings in the 'drider.cfg' file on the client.
#                Otherwise, communication from the client will be
#                rejected.
#
# SHARED_SECRET: Enter a shared secret to be used for the Blowfish
#                encryption.  The shared secret cannot exceed 56 bytes
#                and must match the setting used in the client's
#                'drider.cfg' file.
#
# [CLIENT_SHARED_SECRETS]: Shared secrets can be defined so
#                that they are unique to a client.  This is
#                done by adding a [CLIENT_SHARED_SECRETS]
#                section (similar to the [ALLOWED_CLIENTS])
#                and specify the shared secret for each remote
#                IP Address.  As the client connects, the
#                config file will be searched for a
#                client-specific shared secret.  If one is
#                found, it will be used.  Otherwise, the
#                server will default to using SHARED_SECRET
#-----------------------------------------------------------------
ENCRYPT=BLOWFISH
SHARED_SECRET=myserversecret

#[CLIENT_SHARED_SECRETS]
#Sensor 1 IP=mysensorsecret1
#Sensor 2 IP=mysensorsecret2
#Sensor 3 IP=mysensorsecret3
#[END_CLIENT_SHARED_SECRETS]

#-----------------------------------------------------------------
# SOCKET SETTINGS
#
# SERVER_PORT:   Port number used by driders to listen for client
#                connections from driderc.  This port number should
#                match the corresponding entry of the 'driderc.cfg' file.
#
# BACKLOG_CONNECTIONS: Number of client connections to allow to queue
#                when the server is too busy to accept() the connection.
#                Traditionally, this number is set to 5.
#
# SOCKET_RETRY_TIME_1: Amount of time to delay after an error has
#                occurred reading/writing or connecting to SERVER_PORT
#                at SERVER_ADDRESS.  After SOCKET_RETRY_TIME_1 seconds
#                expire, a reconnect is attempted.
#
# SOCKET_RETRY_TIME_2: If an error is encountered trying to reconnect
#                after SOCKET_RETRY_TIME_1 seconds, the daemon will
#                pause SOCKET_RETRY_TIME_2 seconds and try again.
#
# SOCKET_RETRY_TIME_3: If an error is encountered trying to reconnect
#                after SOCKET_RETRY_TIME_2 seconds, the daemon will
#                pause SOCKET_RETRY_TIME_3 seconds and try one last time.
#                If an error is still encountered, the daemon will
#                terminate.
#
# NAK_RETRIES:   Number of times to attempt to send a packet as NAKS
#                are returned from the server.  If this number is
#                exceeded, the client daemon terminates.  The daemon
#                does not continue processing until the packet is
#                ACKnowledged.
#-----------------------------------------------------------------
SERVER_PORT=9111
BACKLOG_CONNECTIONS=5
SOCKET_RETRY_TIME_1=60
SOCKET_RETRY_TIME_2=300
SOCKET_RETRY_TIME_3=900
```

```
NAK_RETRIES=3

#--------------------------------------------------------------------------
# LIST OF ALLOWED CLIENTS
#
# Enter a list of IP Addresses that are allowed to establish a
# connection to the DragRDBMS process.  All other IP
# addresses will be rejected.  Update the NUMBER_ALLOWED_IPS to
# reflect the number in the list.
#
# NUMBER_ALLOWED_IPS: Specify the number of entries that have been
#                entered under the ALLOWED_CLIENTS section.
#
# [ALLOWED_CLIENTS]: This section should contain one line per
#                client IP Address that is allowed to talk to the
#                server. Any lines that begin with a '#' or ' '
#                be ignored when this configuration file is read.
#--------------------------------------------------------------------------
NUMBER_ALLOWED_IPS=3

[ALLOWED_CLIENTS]
Sensor 1 IP
Sensor 2 IP
Sensor 3 IP
[END_ALLOWED_CLIENTS]

#--------------------------------------------------------------------------
#  DAEMON BEHAVIOR
#
#  LOG_TO_RDBMS: Indicates whether or not events should be inserted into
#                the RDBMS.
#
#  LOG_TO_DRAGON_DB: Whether or not to write events to a centralized
#                dragon.db file located in the DRAGON_DB_DIR
#
#  DISTRIBUTE_CONFIG_FILES:  Whether or not to push files located in
#                DISTRIBUTE_CONFIG_DIR to the corresponding
#                sensors as needed.
#
#  DAEMONIZE:    Specifies whether or not the code will daemonize itself
#                versus running in foreground mode.
#
#  DEBUG:        Specifies whether or not debug code will be displayed
#                to stderr.  Caution: this flag causes a large quantities
#                of output to be displayed to the screen and will
#                negatively impact driders performance.
#--------------------------------------------------------------------------
LOG_TO_RDBMS=0
LOG_TO_DRAGON_DB=1
DISTRIBUTE_CONFIG_FILES=1
DAEMONIZE=1
DEBUG=0

#--------------------------------------------------------------------------
# O/S SPECIFIC COMMANDS
#
#
# TAR_COMMAND:   Fully qualified name of the tar command.  This command
#                is used to package configuration files prior to
#                distributing them to remote sensors.  No flags should
#                be included on the TAR_COMMAND.  The driders daemon
#                assumes that the tar command can support the '-cvpf'
#                options.
#
# COMPRESS_COMMAND: Fully qualified name of the command to be used to
#                compress the distribution file prior to sending it
#                to the remote sensor.  No options should be included
#                on the COMPRESS_COMMAND.
#
# UNCOMPRESS_COMMAND: Fully qualified name of the command to be used to
#                uncompress the package files that are distributed to the
#                remote sensors.  No options should be included on the
#                UNCOMPRESS_COMMAND.
#
# COMPRESS_FILE_EXTENSION: File extension added to original file name
```

```
#                upon successful compression.  If the command compresses
#                to the original file name, set 'COMPRESS_FILE_EXTENSION='.
#-----------------------------------------------------------------------
TAR_COMMAND=/bin/tar

COMPRESS_COMMAND=/usr/bin/gzip
UNCOMPRESS_COMMAND=/usr/bin/gunzip
COMPRESS_FILE_EXTENSION=.gz
#-----------------------------------------------------------------------
# EXPORT LOGGING COMMANDS
#
#
# LOG_TO_EXPORTLOG: Turn this flag on (1) to cause driders to create one
#           log file containing all events for all sensors.  This
#           option is helpful if the customer will be 'tail'ing the file
#           and forwarding the events to a custom SQL database.  The log
#           file created will be DRAGON_DB_DIR/dragon.log.999.  999 is
#           a sequence number that is incremented by 1 each time
#           EXPORTLOG_ROTATION days pass.  This will allow older logs to be
#           removed by the customer without impacting the active log.
#
#           A filler field %F is available and can be used to force the
#           record layouts to match the number of fields in the target
#           database.  This is in an attempt to allow a customer to load
#           the data file directly using SQL tools (e.g., mysqlimport,
#           dbload, etc).
#
#           Fields can be used multiple times within the same format.
#
# EXPORTLOG_FORMAT:  Format of the SWATCH Output.  Specifies which fields to
#           include in the log file. Valid options are:
#
#           %S - Source IP
#           %s - Source IP (integer representation)
#           %D - Destination IP
#           %d - Destination IP (integer representation)
#           %G - Source Port (if Available)
#           %H - Destination Port (if Available)
#           %T - Date/Time of Event (YYYY-MM-DD HH:MM:SS)
#           %t - Date of Event (YYYY-MM-DD)
#           %h - Time of Event (HH:MM:SS)
#           %N - Name of Sensor
#           %E - Event Name
#           %A - Alarm Data
#           %P - Protocol (1 = ICMP, 6 = TCP, 17 = UDP)
#           %B - Direction (I = Internal, X = External, F = From , T = To)
#           %C - TCP Flags (e.g., ---A-R--)
#           %F - Filler Field
#
#           Example: %T%F%F%F%E%N%S%s%D%F%d%P%A
#           NSW MYSQL Format =%T%N%E%S%D%G%H%B%C%P%A
#
# EXPORTLOG_FS: 1 byte Character to be used as a field Seperator. Do not use
#               a comma (',') if you include the Alarm Data field.  The Alarm
#               data field includes it's own commas and will conflict.
#
# EXPORTLOG_FILLER_VALUE: Value to be used for each %F position. Comment
#           this field to create blank filler fields.
#
# EXPORTLOG_ROTATION: Number of days between log rotations.  For example,
#           1 would cause the logs to rotated daily.  Files are rotated
#           by closing the existing log and logging to a dragon.log.999
#           incremented by 1.  Hint:  Set EXPORTLOG_ROTATION to a very high
#           number if you do not want to rotate between logs.
#
#-----------------------------------------------------------------------
LOG_TO_EXPORTLOG=0
EXPORTLOG_FORMAT=%T%N%E%S%D%G%H%B%C%P%A
EXPORTLOG_FS=|
EXPORTLOG_FILLER_VALUE=0
EXPORTLOG_ROTATION=1
```

TCPDump 3.6.1 log files of driders traffic

```
[root@dnids1 /tmp]# tcpdump -Xvns 0 -r /tmp/driders.log
16:44:38.205801 dragon.sensor.1.32778 > MY.DNIDS.server.9111: S [tcp sum ok] 2078435672:2078435672(0) win
5840 <mss 1460,sackOK,timestamp 8403857 0,nop,wscale 0> (DF) (ttl 64, id 21193, len 60)
0x0000       4500 003c 52c9 4000 4006 649a xxxx xxxx       E..<R.@.@.d.....
0x0010       xxxx xxxx 800a 2397 7be2 6958 0000 0000       ......#.{.iX....
0x0020       a002 16d0 e8f0 0000 0204 05b4 0402 080a       ................
0x0030       0080 3b91 0000 0000 0103 0300                 ..;.........
16:44:38.205801 MY.DNIDS.server.9111 > dragon.sensor.1.32778: S [tcp sum ok] 1328234358:1328234358(0) ack
2078435673 win 5792 <mss 1460,sackOK,timestamp 969310 8403857,nop,wscale 0> (DF) (ttl 64, id 0, len 60)
0x0000       4500 003c 0000 4000 4006 b763 xxxx xxxx       E..<..@.@..c....
0x0010       xxxx xxxx 2397 800a 4f2b 3f76 7be2 6959       ....#...O+?v{.iY
0x0020       a012 16a0 9001 0000 0204 05b4 0402 080a       ................
0x0030       000e ca5e 0080 3b91 0103 0300                 ...^..;.....
16:44:38.205801 dragon.sensor.1.32778 > MY.DNIDS.server.9111: . [tcp sum ok] ack 1 win 5840
<nop,nop,timestamp 8403857 969310> (DF) (ttl 64, id 21194, len 52)
0x0000       4500 0034 52ca 4000 4006 64a1 xxxx xxxx       E..4R.@.@.d.....
0x0010       xxxx xxxx 800a 2397 7be2 6959 4f2b 3f77       ......#.{.iYO+?w
0x0020       8010 16d0 be96 0000 0101 080a 0080 3b91       ..............;.
0x0030       000e ca5e                                     ...^
16:44:38.205801 dragon.sensor.1.32778 > MY.DNIDS.server.9111: P [tcp sum ok] 1:83(82) ack 1 win 5840
<nop,nop,timestamp 8403857 969310> (DF) (ttl 64, id 21195, len 134)
0x0000       4500 0086 52cb 4000 4006 644e xxxx xxxx       E...R.@.@.dN....
0x0010       xxxx xxxx 800a 2397 7be2 6959 4f2b 3f77       ......#.{.iYO+?w
0x0020       8018 16d0 83b0 0000 0101 080a 0080 3b91       ..............;.
0x0030       000e ca5e 0052 7430 7223 7124 7662 1457       ...^.Rt0r#q$vb.W
0x0040       4007 0f72 aec3 91c5 46bd e4c4 3c86 cb40       @..r....F...<..@
0x0050       2b04 6e0b 1d2b 0919 cffa 9665 4501 2fb9       +.n..+.....eE./.
0x0060       d9bb 5b95 6577 4ba2 0851 5916 3207 69e4       ..[.ewK..QY.2.i.
0x0070       6519 9aca 59d0 dbe6 7d8c 91e5 6fe7 a8bc       e...Y...}...o...
0x0080       5e2a 5c8e fe25                                ^*\..%
16:44:38.205801 MY.DNIDS.server.9111 > dragon.sensor.1.32778: . [tcp sum ok] ack 83 win 5792
<nop,nop,timestamp 969310 8403857> (DF) (ttl 64, id 62761, len 52)
0x0000       4500 0034 f529 4000 4006 c241 xxxx xxxx       E..4.)@.@..A....
0x0010       xxxx xxxx 2397 800a 4f2b 3f77 7be2 69ab       ....#...O+?w{.i.
0x0020       8010 16a0 be74 0000 0101 080a 000e ca5e       .....t.........^
0x0030       0080 3b91                                     ..;.
16:44:38.205801 MY.DNIDS.server.9111 > dragon.sensor.1.32778: P [tcp sum ok] 1:11(10) ack 83 win 5792
<nop,nop,timestamp 969310 8403857> (DF) (ttl 64, id 62762, len 62)
0x0000       4500 003e f52a 4000 4006 c236 xxxx xxxx       E..>.*@.@..6....
0x0010       xxxx xxxx 2397 800a 4f2b 3f77 7be2 69ab       ....#...O+?w{.i.
0x0020       8018 16a0 a982 0000 0101 080a 000e ca5e       ...............^
0x0030       0080 3b91 000a da40 6854 efbb e284             ..;....@hT....
16:44:38.205801 dragon.sensor.1.32778 > MY.DNIDS.server.9111: . [tcp sum ok] ack 11 win 5840
<nop,nop,timestamp 8403857 969310> (DF) (ttl 64, id 21196, len 52)
0x0000       4500 0034 52cc 4000 4006 649f xxxx xxxx       E..4R.@.@.d.....
0x0010       xxxx xxxx 800a 2397 7be2 69ab 4f2b 3f81       ......#.{.i.O+?.
0x0020       8010 16d0 be3a 0000 0101 080a 0080 3b91       .....:........;.
0x0030       000e ca5e                                     ...^
```

Line Printer Daemon Configuration at time of audit

```
server
job
130.191.X.X
REJECT SERVICE=X NOT REMOTEIP=192.168.1.1/255.255.255.0
ACCEPT SERVICE=C SERVER REMOTEUSER=root
ACCEPT SERVICE=C LPC=lpd,status,printcap
REJECT SERVICE=C
ACCEPT SERVICE=M SAMEHOST SAMEUSER
ACCEPT SERVICE=M SERVER REMOTEUSER=root
REJECT SERVICE=M
DEFAULT ACCEPT
```

Recommended Apache Configuration

access.conf

```
[dragon@dnids1 conf]$ pwd && more access.conf
/usr/local/apache/conf
##
## access.conf -- Apache HTTP server configuration file
##
```

```
#
# This is the default file for the AccessConfig directive in httpd.conf.
# It is processed after httpd.conf and srm.conf.
#
<Directory /usr/local/apache/htdocs>
Options None
AllowOverride All
order deny,allow
deny from all
allow from 192.168.1.
</Directory>
```

.htaccess

```
[dragon@dnids1 htdocs]$ pwd && more .htaccess
/usr/local/apache/htdocs
AuthUserFile /usr/local/apache/.passwd
AuthGroupFile /dev/null
AuthName "Protected Area"
AuthType Basic
<Limit GET POST>
require user dragon
</Limit>
```

.passwd

```
[dragon@dnids1 apache]$ more .passwd
dragon:iG01UwloIBPwA
```

httpd.conf

```
### Section 1: Global Environment

ServerType standalone
ServerRoot "/usr/local/apache"
PidFile /usr/local/apache/logs/httpd.pid
ScoreBoardFile /usr/local/apache/logs/httpd.scoreboard
AccessConfig conf/access.conf
Timeout 300
KeepAlive On
MaxKeepAliveRequests 100
KeepAliveTimeout 60
MinSpareServers 5
MaxSpareServers 10
StartServers 5
MaxClients 150
MaxRequestsPerChild 0
<IfDefine SSL>
LoadModule ssl_module         libexec/libssl.so
</IfDefine>
ClearModuleList
AddModule mod_env.c
AddModule mod_log_config.c
AddModule mod_mime.c
AddModule mod_negotiation.c
AddModule mod_status.c
AddModule mod_include.c
AddModule mod_autoindex.c
AddModule mod_dir.c
AddModule mod_cgi.c
AddModule mod_asis.c
AddModule mod_imap.c
AddModule mod_actions.c
AddModule mod_userdir.c
AddModule mod_alias.c
AddModule mod_access.c
AddModule mod_auth.c
AddModule mod_so.c
AddModule mod_setenvif.c
<IfDefine SSL>
AddModule mod_ssl.c
</IfDefine>
Port 443
```

```
<IfDefine SSL>
Listen 443
</IfDefine>
User dragon
Group "#-501"
ServerAdmin root@dnids1.localhost.ca
ServerName dnids1.localhost.ca
DocumentRoot "/var/www/html"
<Directory />
    Options FollowSymLinks
    AllowOverride None
</Directory>
<Directory "/usr/local/apache/htdocs">
    Options Indexes FollowSymLinks MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
<IfModule mod_userdir.c>
    UserDir public_html
</IfModule>
<IfModule mod_dir.c>
    DirectoryIndex index.html
</IfModule>
AccessFileName .htaccess
<Files ~ "^\.ht">
    Order allow,deny
    Deny from all
    Satisfy All
</Files>
UseCanonicalName On
<IfModule mod_mime.c>
    TypesConfig /usr/local/apache/conf/mime.types
</IfModule>
DefaultType text/plain
<IfModule mod_mime_magic.c>
    MIMEMagicFile /usr/local/apache/conf/magic
</IfModule>
HostnameLookups Off
ErrorLog /var/logs/httpd/error_log
LogLevel warn
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent
CustomLog /var/logs/httpd/access_log common
ServerSignature On
<IfModule mod_alias.c>
    Alias /icons/ "/usr/local/apache/icons/"
    <Directory "/usr/local/apache/icons">
        Options Indexes MultiViews
        AllowOverride None
        Order allow,deny
        Allow from all
    </Directory>
    Alias /manual/ "/usr/local/apache/htdocs/manual/"
    <Directory "/usr/local/apache/htdocs/manual">
        Options Indexes FollowSymlinks MultiViews
        AllowOverride None
        Order allow,deny
        Allow from all
    </Directory>
    ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
    <Directory "/var/www/cgi-bin">
        AllowOverride None
        Options None
        Order allow,deny
        Allow from all
    </Directory>
</IfModule>
<IfModule mod_autoindex.c>
    IndexOptions FancyIndexing
    AddIconByEncoding (CMP,/icons/compressed.gif) x-compress x-gzip
    AddIconByType (TXT,/icons/text.gif) text/*
    AddIconByType (IMG,/icons/image2.gif) image/*
```

```
    AddIconByType (SND,/icons/sound2.gif) audio/*
    AddIconByType (VID,/icons/movie.gif) video/*
    AddIcon /icons/binary.gif .bin .exe
    AddIcon /icons/binhex.gif .hqx
    AddIcon /icons/tar.gif .tar
    AddIcon /icons/world2.gif .wrl .wrl.gz .vrml .vrm .iv
    AddIcon /icons/compressed.gif .Z .z .tgz .gz .zip
    AddIcon /icons/a.gif .ps .ai .eps
    AddIcon /icons/layout.gif .html .shtml .htm .pdf
    AddIcon /icons/text.gif .txt
    AddIcon /icons/c.gif .c
    AddIcon /icons/p.gif .pl .py
    AddIcon /icons/f.gif .for
    AddIcon /icons/dvi.gif .dvi
    AddIcon /icons/uuencoded.gif .uu
    AddIcon /icons/script.gif .conf .sh .shar .csh .ksh .tcl
    AddIcon /icons/tex.gif .tex
    AddIcon /icons/bomb.gif core
    AddIcon /icons/back.gif ..
    AddIcon /icons/hand.right.gif README
    AddIcon /icons/folder.gif ^^DIRECTORY^^
    AddIcon /icons/blank.gif ^^BLANKICON^^
    DefaultIcon /icons/unknown.gif
    ReadmeName README
    HeaderName HEADER
    IndexIgnore .?? *~ *# HEADER* README* RCS CVS *,v *,t
</IfModule>
<IfModule mod_mime.c>
    AddEncoding x-compress Z
    AddEncoding x-gzip gz tgz
    AddLanguage da .dk
    AddLanguage nl .nl
    AddLanguage en .en
    AddLanguage et .ee
    AddLanguage fr .fr
    AddLanguage de .de
    AddLanguage el .el
    AddLanguage he .he
    AddCharset ISO-8859-8 .iso8859-8
    AddLanguage it .it
    AddLanguage ja .ja
    AddCharset ISO-2022-JP .jis
    AddLanguage kr .kr
    AddCharset ISO-2022-KR .iso-kr
    AddLanguage nn .nn
    AddLanguage no .no
    AddLanguage pl .po
    AddCharset ISO-8859-2 .iso-pl
    AddLanguage pt .pt
    AddLanguage pt-br .pt-br
    AddLanguage ltz .lu
    AddLanguage ca .ca
    AddLanguage es .es
    AddLanguage sv .se
    AddLanguage cz .cz
    AddLanguage ru .ru
    AddLanguage zh-tw .tw
    AddLanguage tw .tw
    AddCharset Big5        .Big5    .big5
    AddCharset WINDOWS-1251 .cp-1251
    AddCharset CP866       .cp866
    AddCharset ISO-8859-5   .iso-ru
    AddCharset KOI8-R      .koi8-r
    AddCharset UCS-2       .ucs2
    AddCharset UCS-4       .ucs4
    AddCharset UTF-8       .utf8
    <IfModule mod_negotiation.c>
        LanguagePriority en da nl et fr de el it ja kr no pl pt pt-br ru ltz ca es sv tw
    </IfModule>
    AddType application/x-httpd-php3 .php3
    AddType application/x-httpd-php .php
    AddType application/x-tar .tgz
</IfModule>
<IfModule mod_setenvif.c>
    BrowserMatch "Mozilla/2" nokeepalive
```

```
    BrowserMatch "MSIE 4\.0b2;" nokeepalive downgrade-1.0 force-response-1.0
    BrowserMatch "RealPlayer 4\.0" force-response-1.0
    BrowserMatch "Java/1\.0" force-response-1.0
    BrowserMatch "JDK/1\.0" force-response-1.0
</IfModule>
<IfDefine SSL>
AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-crl    .crl
</IfDefine>
<IfModule mod_ssl.c>
SSLPassPhraseDialog  builtin
SSLSessionCache         dbm:/usr/local/apache/logs/ssl_scache
SSLSessionCacheTimeout  300
SSLMutex  file:/usr/local/apache/logs/ssl_mutex

SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
SSLLog      /usr/local/apache/logs/ssl_engine_log
SSLLogLevel info
</IfModule>
<IfDefine SSL>
<VirtualHost _default_:443>
DocumentRoot "/var/www/html"
ServerName dnids1.localhost.localdomain
ServerAdmin root@dnids1.localhost.localdomain
ErrorLog /var/logs/httpd/error_log
TransferLog /var/logs/httpd/access_log
SSLEngine on
SSLCipherSuite ALL:!ADH:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MEDIUM:+SSLv2:+EXP:+eNULL
SSLCertificateFile /usr/local/apache/conf/ssl.crt/server.crt
SSLCertificateKeyFile /usr/local/apache/conf/ssl.key/server.key
<Files ~ "\.(cgi|shtml|phtml|php3?)$">
    SSLOptions +StdEnvVars
</Files>
<Directory "/var/www/cgi-bin">
    SSLOptions +StdEnvVars
</Directory>
SetEnvIf User-Agent ".*MSIE.*" \
        nokeepalive ssl-unclean-shutdown \
        downgrade-1.0 force-response-1.0
CustomLog /var/logs/httpd/ssl_request_log \
        "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>
</IfDefine>
```

Shadow Password Field Format

```
[root@dnids1 dict]# more /etc/shadow | grep root
root:encryptedpasswordhere:11465:0:99999:7:::

struct spwd {
                char *sp_namp; /* user login name */
                char *sp_pwdp; /* encrypted password */
                long sp_lstchg; /* last password change */
                int  sp_min; /* days until change allowed. */
                int  sp_max; /* days before change required */
                int  sp_warn; /* days warning for expiration */
                int  sp_inact; /* days before account inactive */
                int  sp_expire; /* date when account expires */
                int  sp_flag; /* reserved for future use */
```

John The Ripper v1.6 results on a SMP933 Intel box with default john.ini. Roughly 49,166,832 password combinations hashed in 5:58:09.

```
[root@dnids1 run]# wc -l password2.lst
 396701 password2.lst

[root@dnids1 run]# ./john -wordfile:password2.lst -rules mylist
Loaded 4 passwords with 4 different salts (FreeBSD MD5 [32/32])
abc123           (test)
guesses: 1  time: 0:05:58:09 100%  c/s: 2285  trying: Zoundsing

[root@dnids1 run]# userdel test && grep test /etc/passwd
```

```
[root@dnids1 run]#
```

Process Status

```
[dragon@dnids1 dragon]$ ps -aux > ps.txt

USER       PID %CPU %MEM   VSZ  RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0  1368  544 ?        S    18:43   0:05 init [5]
root         2  0.0  0.0     0    0 ?        SW   18:43   0:00 [keventd]
root         3  0.0  0.0     0    0 ?        SW   18:43   0:00 [kswapd]
root         4  0.0  0.0     0    0 ?        SW   18:43   0:00 [kreclaimd]
root         5  0.0  0.0     0    0 ?        SW   18:43   0:00 [bdflush]
root         6  0.0  0.0     0    0 ?        SW   18:43   0:00 [kupdated]
root         7  0.0  0.0     0    0 ?        SW<  18:43   0:00 [mdrecoveryd]
root        72  0.0  0.0     0    0 ?        SW   18:43   0:00 [khubd]
root       411  0.0  0.0     0    0 ?        SW   18:43   0:00 [eth0]
root       460  0.0  0.1  1948 1116 ?        S    17:00   0:00 klogd -2
rpc        474  0.0  0.0  1512  596 ?        S    17:00   0:00 portmap
rpcuser    489  0.0  0.1  1560  776 ?        S    17:00   0:00 rpc.statd
root       610  0.0  0.1  1480  648 ?        S    17:00   0:00 /usr/sbin/automou
daemon     622  0.0  0.0  1400  584 ?        S    17:00   0:00 /usr/sbin/atd
root       636  0.0  0.1  2604 1208 ?        S    17:00   0:00 sshd
root       657  0.0  0.1  2240  964 ?        S    17:00   0:00 xinetd -stayalive
lp         675  0.0  0.1  2540  968 ?        S    17:00   0:00 lpd Waiting
root       709  0.0  0.3  5004 1936 ?        S    17:00   0:00 sendmail: accepti
root       722  0.0  0.0  1396  500 ?        S    17:00   0:00 gpm -t ps/2 -m /d
root       734  0.0  0.1  1552  700 ?        S    17:00   0:00 crond
xfs        778  0.0  0.7  6240 5096 ?        S    17:00   0:01 xfs -droppriv -da
root       784  0.0  0.0  1340  436 tty1     S    18:43   0:00 /sbin/mingetty tt
root       785  0.0  0.0  1340  436 tty2     S    18:43   0:00 /sbin/mingetty tt
root       786  0.0  0.0  1340  436 tty3     S    18:43   0:00 /sbin/mingetty tt
root       787  0.0  0.0  1340  436 tty4     S    18:43   0:00 /sbin/mingetty tt
root       788  0.0  0.0  1340  436 tty5     S    18:43   0:00 /sbin/mingetty tt
root       789  0.0  0.0  1340  436 tty6     S    18:43   0:00 /sbin/mingetty tt
root       790  0.0  0.1  3320 1216 ?        S    18:43   0:00 /usr/bin/gdm -nod
root      1531  0.0  0.1  1564  732 ?        S    20:01   0:00 CROND
root      1532  0.0  0.1  1920  908 ?        S    20:01   0:00 /bin/bash /usr/bi
root      1534  0.0  0.0  1656  552 ?        S    20:01   0:00 awk -v progname=/
root      1535  0.0  0.1  1904  880 ?        S    20:01   0:00 /bin/sh /usr/lib/
root      1537  0.0  0.0  1352  512 ?        S    20:01   0:00 /usr/lib/sa/sadc
root      1582  0.5  1.0 54936 6596 ?        SL   20:06   0:03 /etc/X11/X -auth
root      1583  0.0  0.2  3960 1880 ?        S    20:06   0:00 /usr/bin/gdm -nod
dragon    1594  0.0  0.8 13916 5192 ?        S    20:06   0:00 ksmserver --resto
dragon    1700  0.0  0.8 17804 5140 ?        S    20:06   0:00 kdeinit: dcopserv
dragon    1702  0.0  0.8 18132 5740 ?        S    20:06   0:00 kdeinit: klaunche
dragon    1704  0.0  0.8 17800 5620 ?        S    20:06   0:00 kdeinit: kded
dragon    1707  0.2  0.4  4504 3064 ?        S    20:06   0:01 artsd -F 10 -S 40
dragon    1709  0.0  0.8 17852 5560 ?        S    20:06   0:00 kdeinit: kxmlrpcd
dragon    1715  0.0  0.7 17664 4740 ?        S    20:06   0:00 kdeinit: Running.
dragon    1717  0.0  1.0 17572 7032 ?        S    20:06   0:00 knotify
dragon    1718  0.0  1.1 18648 7480 ?        S    20:06   0:00 kdeinit: kwin
dragon    1720  0.1  1.5 20196 9904 ?        S    20:06   0:00 kdeinit: kdesktop
dragon    1725  0.1  1.5 20668 9820 ?        S    20:06   0:00 kdeinit: kicker
dragon    1729  0.0  1.1 18676 7672 ?        S    20:06   0:00 kdeinit: klipper
dragon    1731  0.0  1.0 18128 6508 ?        S    20:06   0:00 kdeinit: khotkeys
dragon    1733  0.0  1.0 18380 6852 ?        S    20:06   0:00 kdeinit: kwrited
dragon    1734  0.0  0.0  1532  512 pts/0    S    20:06   0:00 /bin/cat
dragon    1736  0.0  1.3 19428 8692 ?        S    20:07   0:00 kdeinit: konsole
dragon    1737  0.0  0.2  2416 1372 pts/1    S    20:07   0:00 /bin/bash
dragon    1760  0.0  0.0  2040  640 pts/1    S    20:07   0:00 /driders
dragon    1764  0.1  1.3 19400 8672 ?        S    20:08   0:01 kdeinit: konsole
dragon    1765  0.0  0.2  2408 1352 pts/2    S    20:08   0:00 /bin/bash
root      1928  0.0  0.3  3676 2056 ?        S    20:15   0:00 /usr/local/apache
dragon    1929  0.0  0.3  3864 2280 ?        S    20:15   0:00 /usr/local/apache
dragon    1930  0.0  0.3  3828 2244 ?        S    20:15   0:00 /usr/local/apache
dragon    1931  0.0  0.3  3864 2272 ?        S    20:15   0:00 /usr/local/apache
dragon    1932  0.0  0.3  3828 2236 ?        S    20:15   0:00 /usr/local/apache
dragon    1933  0.0  0.3  3828 2236 ?        S    20:15   0:00 /usr/local/apache
dragon    1936  1.0  2.4 24152 15828 ?       S    20:16   0:01 /usr/lib/netscape
dragon    1961  0.0  0.5 17220 3644 ?        S    20:16   0:00 (dns helper)
dragon    1965  0.0  0.3  3816 2144 ?        S    20:16   0:00 /usr/local/apache
dragon    1966  0.0  0.3  3816 2144 ?        S    20:16   0:00 /usr/local/apache
dragon    1967  0.0  0.3  3816 2144 ?        S    20:16   0:00 /usr/local/apache
dragon    1968  0.0  0.3  3816 2144 ?        S    20:16   0:00 /usr/local/apache
```

```
dragon    1969  0.0  0.3  3816 2144 ?       S    20:16   0:00 /usr/local/apache
```

System Init Settings

```
[dragon@dnids1 dragon]$ /sbin/chkconfig --list
atd                     0:off   1:off   2:off   3:on    4:on    5:on    6:off
rwhod                   0:off   1:off   2:off   3:off   4:off   5:off   6:off
keytable                0:off   1:on    2:on    3:on    4:on    5:on    6:off
nscd                    0:off   1:off   2:off   3:off   4:off   5:off   6:off
syslog                  0:off   1:off   2:on    3:on    4:on    5:on    6:off
gpm                     0:off   1:off   2:on    3:on    4:on    5:on    6:off
kudzu                   0:off   1:off   2:off   3:on    4:on    5:on    6:off
kdcrotate               0:off   1:off   2:off   3:off   4:off   5:off   6:off
lpd                     0:off   1:off   2:on    3:on    4:on    5:on    6:off
autofs                  0:off   1:off   2:off   3:on    4:on    5:on    6:off
sendmail                0:off   1:off   2:on    3:on    4:on    5:on    6:off
rhnsd                   0:off   1:off   2:off   3:off   4:off   5:off   6:off
netfs                   0:off   1:off   2:off   3:off   4:off   5:off   6:off
network                 0:off   1:off   2:on    3:on    4:on    5:on    6:off
random                  0:off   1:off   2:on    3:on    4:on    5:on    6:off
rawdevices              0:off   1:off   2:off   3:on    4:on    5:on    6:off
apmd                    0:off   1:off   2:on    3:on    4:on    5:on    6:off
ipchains                0:off   1:off   2:on    3:on    4:on    5:on    6:off
iptables                0:off   1:off   2:on    3:on    4:on    5:on    6:off
identd                  0:off   1:off   2:off   3:off   4:off   5:off   6:off
portmap                 0:off   1:off   2:on    3:on    4:on    5:on    6:off
nfs                     0:off   1:off   2:off   3:off   4:off   5:off   6:off
nfslock                 0:off   1:off   2:off   3:on    4:on    5:on    6:off
pppoe                   0:off   1:off   2:on    3:on    4:on    5:on    6:off
crond                   0:off   1:off   2:on    3:on    4:on    5:on    6:off
anacron                 0:off   1:off   2:on    3:on    4:on    5:on    6:off
xfs                     0:off   1:off   2:on    3:on    4:on    5:on    6:off
isdn                    0:off   1:off   2:on    3:on    4:on    5:on    6:off
ypbind                  0:off   1:off   2:off   3:off   4:off   5:off   6:off
sshd                    0:off   1:off   2:on    3:on    4:on    5:on    6:off
rstatd                  0:off   1:off   2:on    3:on    4:on    5:on    6:off
rusersd                 0:off   1:off   2:off   3:off   4:off   5:off   6:off
rwalld                  0:off   1:off   2:off   3:off   4:off   5:off   6:off
xinetd                  0:off   1:off   2:off   3:on    4:on    5:on    6:off
yppasswdd               0:off   1:off   2:off   3:off   4:off   5:off   6:off
ypserv                  0:off   1:off   2:off   3:off   4:off   5:off   6:off
httpd                   0:off   1:off   2:off   3:off   4:on    5:on    6:off
tux                     0:off   1:off   2:off   3:off   4:off   5:off   6:off
named                   0:off   1:off   2:off   3:off   4:off   5:off   6:off
snmpd                   0:off   1:off   2:off   3:off   4:off   5:off   6:off
arpwatch                0:off   1:off   2:off   3:off   4:off   5:off   6:off
smb                     0:off   1:off   2:off   3:off   4:off   5:off   6:off
xinetd based services:
            rexec:      off
            rlogin:     off
            rsh:        off
            chargen:    off
            chargen-udp:            off
            daytime:    off
            daytime-udp:            off
            echo:       off
            echo-udp:   off
            time:       off
            time-udp:   off
            finger:     off
            ntalk:      off
            talk:       off
            telnet:     off
            wu-ftpd:    off
            rsync:      off
```

Recommended Change to /etc/rc.d/init.d/syslog

The line `SYSLOGD_OPTIONS="-m 0"` should be modified to read

```
SYSLOGD_OPTIONS="-r -m 15"
```

Recommended Changes to /etc/sysconfig/syslog

The line `SYSLOGD_OPTIONS="-m 0"` should be modified to read

```
SYSLOGD_OPTIONS="-r -m 15"
```

Recommended /etc/logrotate.conf Configuration

```
# rotate log files monthly
monthly
# keep a years worth of backlogs
rotate 12
# see "man logrotate" for details


# rotate log files weekly
# weekly
# rotate log files monthly
monthly

# keep 4 weeks worth of backlogs
# rotate 4
# keep 12 months worth of backlogs
rotate 12

# send errors to root
errors root

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp -- we'll rotate them here
/var/log/wtmp {
    monthly
    create 0664 root utmp
    rotate 12
}

# system-specific logs may be configured here
# Apache Logs
/var/log/httpd/access_log" /var/log/httpd/error_log {
    monthly
    rotate 12
}

# Up2date Logs
/var/log/up2date {
    monthly
    rotate 12
}
```

Recommended /etc/login.defs Configuration

```
MAIL_DIR    /var/spool/mail

#           PASS_MAX_DAYS           Maximum number of days a password may be used.
#           PASS_MIN_DAYS           Minimum number of days allowed between password changes.
#           PASS_MIN_LEN            Minimum acceptable password length.
#           PASS_WARN_AGE           Number of days warning given before a password expires.
#
PASS_MAX_DAYS           60
PASS_MIN_DAYS           0
PASS_MIN_LEN            6
PASS_WARN_AGE           14

UID_MIN                              500
```

```
UID_MAX                          60000

GID_MIN                            500
GID_MAX                          60000

USERDEL_CMD /usr/sbin/userdel_local

CREATE_HOME yes
```

Current Secure Shell Daemon Configuration

```
#           $OpenBSD: sshd_config,v 1.38 2001/04/15 21:41:29 deraadt Exp $
# This sshd was compiled with PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin

Port 22
Protocol 2,1
HostKey /etc/ssh/ssh_host_key
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
ServerKeyBits 768
LoginGraceTime 600
KeyRegenerationInterval 3600
PermitRootLogin yes
IgnoreRhosts yes
StrictModes yes
X11Forwarding yes
X11DisplayOffset 10
PrintMotd yes
KeepAlive yes

SyslogFacility AUTH
LogLevel INFO

RhostsAuthentication no
RhostsRSAAuthentication no
HostbasedAuthentication no
RSAAuthentication yes

PasswordAuthentication yes
PermitEmptyPasswords no

Subsystem   sftp        /usr/libexec/openssh/sftp-server
```

TCPDump 3.6.1 Output from X11 Forwarded Session
NMAPFrontEnd was started and the DNIDS server was portscanned from the remote host.

```
[root@dnids1 /root]# tcpdump -vn -r /tmp/sshx11 ip and host MY.DNIDS.server | more
02:19:38.271498 MY.DNIDS.server.32972 > MY.Audit.laptop.22: S [tcp sum ok] 1321470482:1321470482(0) win 5840
<mss 1460,sackOK,timestamp 3704716 0,nop,wscale 0> (DF) (ttl 64, id 36254, len 60)
02:19:38.271498 MY.Audit.laptop.22 > MY.DNIDS.server.32972: S [tcp sum ok] 3682731474:3682731474(0) ack
1321470483 win 16060 <mss 1460,sackOK,timestamp 19204063 3704716,nop,wscale 0> (DF) (ttl 64, id 32997, len
60)
02:19:38.271498 MY.DNIDS.server.32972 > MY.Audit.laptop.22: . [tcp sum ok] ack 1 win 5840 <nop,nop,timestamp
3704716 19204063> (DF) (ttl 64, id 36255, len 52)
02:19:38.281498 MY.Audit.laptop.22 > MY.DNIDS.server.32972: P [tcp sum ok] 1:24(23) ack 1 win 16060
<nop,nop,timestamp 19204064 3704716> (DF) (ttl 64, id 32998, len 75)
Three-Way-Handshake with initial data push
<<<snip>>>
02:20:38.761498 MY.Audit.laptop.63548 > MY.DNIDS.server.13: S [tcp sum ok] 2559472882:2559472882(0) win 2048
(ttl 57, id 25275, len 40)
02:20:38.761498 MY.DNIDS.server.13 > MY.Audit.laptop.63548: R [tcp sum ok] 0:0(0) ack 2559472883 win 0 (DF)
(ttl 255, id 0, len 40)
02:20:38.761498 MY.Audit.laptop.63548 > MY.DNIDS.server.22: S [tcp sum ok] 2559472882:2559472882(0) win 2048
(ttl 57, id 5885, len 40)
02:20:38.761498 MY.DNIDS.server.22 > MY.Audit.laptop.63548: S [tcp sum ok] 1407292643:1407292643(0) ack
2559472883 win 5840 <mss 1460> (DF) (ttl 64, id 0, len 44)
02:20:38.761498 MY.Audit.laptop.63548 > MY.DNIDS.server.22: R [tcp sum ok] 2559472883:2559472883(0) win 0
(ttl 255, id 34305, len 40)
02:20:38.761498 MY.Audit.laptop.63548 > MY.DNIDS.server.8: S [tcp sum ok] 2559472882:2559472882(0) win 2048
(ttl 57, id 15120, len 40)
02:20:38.761498 MY.DNIDS.server.8 > MY.Audit.laptop.63548: R [tcp sum ok] 0:0(0) ack 2559472883 win 0 (DF)
(ttl 255, id 0, len 40)
NMAP scan, discovering that TCP port 22 was open
```

<<<snip>>>

Netstat prior to recommendations

```
[dragon@dnids1 dragon]$ netstat -ln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:32768           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:515             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN
tcp        0      0 DNIDS.Server:80         0.0.0.0:*               LISTEN
tcp        0      0 DNIDS.Server:443        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:9111            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:32768           0.0.0.0:*
udp        0      0 0.0.0.0:665             0.0.0.0:*
udp        0      0 0.0.0.0:111             0.0.0.0:*
```

Netstat after recommendations

```
[dragon@dnids1 dragon]$ netstat -ln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp        0      0 0.0.0.0:6000          0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:80            0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:22            0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:443           0.0.0.0:*              LISTEN
udp        0      0 0.0.0.0:514           0.0.0.0:*
udp        0      0 192.168.1.2:123       0.0.0.0:*
udp        0      0 127.0.0.1:123         0.0.0.0:*
udp        0      0 0.0.0.0:123           0.0.0.0:*
```

List of Open Files after recommendations

```
[root@dnids1 dragon]# /usr/sbin/lsof -i -P
COMMAND    PID   USER   FD   TYPE DEVICE SIZE NODE NAME
syslogd    475   root    7u  IPv4    805       UDP *:514
sshd       599   root    3u  IPv4    942       TCP *:22 (LISTEN)
X          790   root    1u  IPv4   1172       TCP *:6000 (LISTEN)
httpd     7142   root   16u  IPv4  29534       TCP *:443 (LISTEN)
httpd     7142   root   17u  IPv4  29535       TCP *:80 (LISTEN)
httpd     7143   root   16u  IPv4  29534       TCP *:443 (LISTEN)
httpd     7143   root   17u  IPv4  29535       TCP *:80 (LISTEN)
httpd     7144   root   16u  IPv4  29534       TCP *:443 (LISTEN)
httpd     7144   root   17u  IPv4  29535       TCP *:80 (LISTEN)
httpd     7145   root   16u  IPv4  29534       TCP *:443 (LISTEN)
httpd     7145   root   17u  IPv4  29535       TCP *:80 (LISTEN)
httpd     7146   root   16u  IPv4  29534       TCP *:443 (LISTEN)
httpd     7146   root   17u  IPv4  29535       TCP *:80 (LISTEN)
httpd     7147   root   16u  IPv4  29534       TCP *:443 (LISTEN)
httpd     7147   root   17u  IPv4  29535       TCP *:80 (LISTEN)
```

Contents of fstab

```
[dragon@dnids1 dragon]$ more /etc/fstab
LABEL=/                 /                       ext2    defaults        1 1
LABEL=/LOG              /LOG                    ext2    defaults        1 2
LABEL=/home             /home                   ext2    nosuid,nodev,noexec     1 2
/dev/fd0                /mnt/floppy             auto    noauto,owner    0 0
LABEL=/usr              /usr                    ext2    defaults        1 2
LABEL=/var              /var                    ext2    defaults        1 2
none                    /proc                   proc    defaults        0 0
none                    /dev/pts                devpts  gid=5,mode=620  0 0
/dev/hda3               swap                    swap    defaults        0 0
/dev/cdrom              /mnt/cdrom              iso9660 noauto,owner,kudzu,ro 0 0
/dev/cdrom1             /mnt/cdrom1             iso9660 noauto,owner,kudzu,ro 0 0
```

SUID files

```
[root@dnids1 dragon]# find / -type f \( -perm -04000 \) -fls suid.txt | more suid.txt
find: /proc/7335/fd/5: No such file or directory
::::::::::::::
suid.txt
::::::::::::::
 16690   40 -rwsr-xr-x   1 root     root        37764 Apr  4  2001 /usr/bin/at
 16804  784 -rws--x--x   2 root     root       795092 Mar 23  2001 /usr/bin/suidperl
 16804  784 -rws--x--x   2 root     root       795092 Mar 23  2001 /usr/bin/sperl5.6.0
 16862   16 -rwsr-xr-x   1 root     root        14332 Feb  5  2001 /usr/bin/rcp
 16864   12 -rwsr-xr-x   1 root     root        10844 Feb  5  2001 /usr/bin/rlogin
 16865    8 -rwsr-xr-x   1 root     root         7796 Feb  5  2001 /usr/bin/rsh
 16903   36 -rwsr-xr-x   1 root     root        34588 Mar  9  2001 /usr/bin/chage
 16905   36 -rwsr-xr-x   1 root     root        36228 Mar  9  2001 /usr/bin/gpasswd
 17007   16 -r-s--x--x   1 root     root        13536 Jul 12  2000 /usr/bin/passwd
 17417   16 -rws--x--x   1 root     root        13048 Apr  8  2001 /usr/bin/chfn
 17418   16 -rws--x--x   1 root     root        12600 Apr  8  2001 /usr/bin/chsh
 17436    8 -rws--x--x   1 root     root         5460 Apr  8  2001 /usr/bin/newgrp
 17474  212 -rwsr-xr-x   1 root     root       212940 Jun 17 04:32 /usr/bin/ssh
 17491   24 -rwsr-xr-x   1 root     root        21312 Mar  8  2001 /usr/bin/crontab
 17719    8 -rwsr-xr-x   1 root     root         7300 Apr  3  2001 /usr/bin/kcheckpass
 18117   84 ---s--x--x   1 root     root        81020 Feb 23  2001 /usr/bin/sudo
211025   20 -rwsr-xr-x   1 root     root        18256 Dec  1  2000 /usr/sbin/traceroute
211191  416 -r-sr-xr-x   1 root     root       417828 Mar  3  2001 /usr/sbin/sendmail
211758    8 -rwsr-xr-x   1 root     root         6392 Apr  7  2001 /usr/sbin/usernetctl
211933   24 -rws--x--x   1 root     root        20696 Feb 14  2001 /usr/sbin/userhelper
212117   12 -r-s--x---   1 root     apache      10976 Mar 29  2001 /usr/sbin/suexec
 81477    8 -rws--x--x   1 root     root         6040 Mar 31  2001 /usr/X11R6/bin/Xwrapper
227527  488 -rwsr-x---   1 dragon   dragon     494796 Nov 22  2000 /usr/drider/driders
 73304   24 -rwsr-xr-x   1 root     root        22620 Jan 16  2001 /bin/ping
 73516   60 -rwsr-xr-x   1 root     root        56444 Mar 22  2001 /bin/mount
 73517   28 -rwsr-xr-x   1 root     root        24796 Mar 22  2001 /bin/umount
 73548   16 -rwsr-xr-x   1 root     root        14112 Jan 16  2001 /bin/su
 17268  108 -rws--x--x   1 root     bin        106192 Sep 11 15:16 /opt/schily/sbin/rscsi
 73532   16 -r-sr-xr-x   1 root     root        14960 Apr  7  2001 /sbin/pwdb_chkpwd
 73533   16 -r-sr-xr-x   1 root     root        15448 Apr  7  2001 /sbin/unix_chkpwd
```

SGID files

```
[root@dnids1 dragon]# find / -type f \( -perm -02000 \) -fls sgid.txt | more sgid.txt
find: /proc/7341/fd/5: No such file or directory
::::::::::::::
sgid.txt
::::::::::::::
 16724   36 -rwxr-sr-x   1 root     man          35676 Feb  4  2001 /usr/bin/man
 16729  168 -rwxr-sr-x   1 root     uucp        167324 Feb 23  2001 /usr/bin/minicom
 16815   12 -rwxr-sr-x   1 root     mail         11124 Jan  6  2001 /usr/bin/lockfile
 16917   24 -rwxr-sr-x   1 root     slocate      24508 Feb 26  2001 /usr/bin/slocate
 17075    8 -r-xr-sr-x   1 root     tty           6492 Apr  4  2001 /usr/bin/wall
 17447   12 -rwxr-sr-x   1 root     tty           8692 Apr  8  2001 /usr/bin/write
 17728   60 -rwxr-sr-x   1 root     root         55400 Apr  3  2001 /usr/bin/kdesud
 17874   40 -r-xr-s--x   1 root     games        40268 Feb 27  2001 /usr/bin/gataxx
 17875   24 -r-xr-s--x   1 root     games        20636 Feb 27  2001 /usr/bin/glines
 17876   72 -r-xr-s--x   1 root     games        69260 Feb 27  2001 /usr/bin/gnibbles
 17877   80 -r-xr-s--x   1 root     games        75772 Feb 27  2001 /usr/bin/gnobots2
 17878   56 -r-xr-s--x   1 root     games        52648 Feb 27  2001 /usr/bin/gnome-stones
 17879   76 -r-xr-s--x   1 root     games        71884 Feb 27  2001 /usr/bin/gnomine
 17880   28 -r-xr-s--x   1 root     games        25644 Feb 27  2001 /usr/bin/gnotravex
 17881   24 -r-xr-s--x   1 root     games        23144 Feb 27  2001 /usr/bin/gnotski
 17882  236 -r-xr-s--x   1 root     games       234076 Feb 27  2001 /usr/bin/gtali
 17883   48 -r-xr-s--x   1 root     games        47900 Feb 27  2001 /usr/bin/iagno
 17884   48 -r-xr-s--x   1 root     games        45356 Feb 27  2001 /usr/bin/mahjongg
 17885   24 -r-xr-s--x   1 root     games        20988 Feb 27  2001 /usr/bin/same-gnome
211029    8 -rwxr-sr-x   1 root     utmp          6584 Jul 13  2000 /usr/sbin/utempter
211672   12 -rwxr-sr-x   1 root     utmp          9180 Mar 16  2001 /usr/sbin/gnome-pty-helper
 73706    8 -rwxr-sr-x   1 root     root          4160 Apr  7  2001 /sbin/netreport
```

Game Package identified for removal

```
[dragon@dnids1 dragon]$ rpm -iq gnome-games
Name        : gnome-games                  Relocations: (not relocateable)
Version     : 1.2.0                        Vendor: Red Hat, Inc.
Release     : 10                       Build Date: Tue 27 Feb 2001 08:33:41 PM GMT
Install date: Wed 23 May 2001 07:10:38 PM GMT      Build Host: porky.devel.redhat.com
Group       : Amusements/Games             Source RPM: gnome-games-1.2.0-10.src.rpm
```

```
Size        : 5521899                   License: LGPL
Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
URL         : http://www.gnome.org
Summary     : GNOME games.
Description :
The gnome-games package includes games for the GNOME GUI desktop
environment, including GnomeScott, ctali, freecell, gnibbles, gnobots,
gnobots2, gnome-stones, gnomine, gnotravex, gnotski, gtali, iagno,
mahjongg, same-gnome, and sol.

Install gnome-games if you want games to play within GNOME.
```

Search for Unowned Files

```
[root@dnids1 /]# find / -nogroup
/home/test
/home/test/.bash_logout
/home/test/.bash_profile
/home/test/.bashrc
/home/test/Desktop
/home/test/Desktop/kontrol-panel
/home/test/Desktop/.directory
/home/test/Desktop/Linux Documentation
/home/test/Desktop/www.redhat.com
/home/test/Desktop/Printer
/home/test/.kde
/home/test/.kde/Autostart
/home/test/.kde/Autostart/.directory
/home/test/.emacs
/home/test/.screenrc
/home/test/.bash_history

[root@dnids1 /]# find / -nouser
/home/test
/home/test/.bash_logout
/home/test/.bash_profile
/home/test/.bashrc
/home/test/Desktop
/home/test/Desktop/kontrol-panel
/home/test/Desktop/.directory
/home/test/Desktop/Linux Documentation
/home/test/Desktop/www.redhat.com
/home/test/Desktop/Printer
/home/test/.kde
/home/test/.kde/Autostart
/home/test/.kde/Autostart/.directory
/home/test/.emacs
/home/test/.screenrc
/home/test/.xauth
/home/test/.bash_history
```

Search for World Writable Files

```
[root@dnids1 /root]# find / -perm -2 -not -type l -ls | grep -v dev
 81424  332 -rw-rw-rw-   1 root     root       333432 May 27 18:54 /usr/dict/6of12.txt
 83683  428 -rw-rw-rw-   1 root     root       430156 May 27 17:00 /usr/dict/2of12.txt
 83999   24 -rw-rw-rw-   1 root     root        23995 May 27 16:45 /usr/dict/ReadMe.txt
 84001  860 -rw-rw-rw-   1 root     root       876477 May 27 18:12 /usr/dict/2of12inf.txt
 16109    4 drwxrwxrwt   2 root     root         4096 Feb 12  2001 /var/spool/vbox
 64428    4 drwxrwxrwt   2 root     root         4096 Apr  5  2001 /var/spool/samba
 48291    4 drwxrwxrwt   2 root     root         4096 Oct  3 14:08 /var/tmp
 29315    4 drwxrwxrwt  14 root     root         4096 Oct  4 00:01 /tmp
  2104    4 drwxrwxrwt   2 xfs      xfs          4096 Oct  3 14:03 /tmp/.font-unix
  2227    0 srwxrwxrwx   1 xfs      xfs             0 Oct  3 14:03 /tmp/.font-unix/fs7100
 17204    4 drwxrwxrwt   2 root     gdm          4096 Oct  3 18:07 /tmp/.X11-unix
 17155    0 srwxrwxrwx   1 root     gdm             0 Oct  3 18:07 /tmp/.X11-unix/X0
 75016    4 drwxrwxrwt   2 root     root         4096 Oct  3 18:07 /tmp/.ICE-unix
 75017    0 srwxrwxrwx   1 root     root            0 May 23 22:10 /tmp/.ICE-unix/953
 75019    0 srwxrwxrwx   1 root     root            0 Sep 28 17:22 /tmp/.ICE-unix/986
 74945    0 srwxrwxrwx   1 root     root            0 Oct  3 18:07 /tmp/.ICE-unix/1667
 75037    0 srwxrwxrwx   1 root     root            0 May 28 19:59 /tmp/.ICE-unix/6634
 73639    0 srwxrwxrwx   1 root     root            0 Jun 14 19:45 /tmp/.ICE-unix/1145
 74884    0 srwxrwxrwx   1 root     root            0 Jul  2 15:01 /tmp/.ICE-unix/987
```

```
74885    0 srwxrwxrwx   1 root     root            0 Aug  1 15:08 /tmp/.ICE-unix/983
75034    0 srwxrwxrwx   1 root     root            0 Sep 13 01:53 /tmp/.ICE-unix/832
75118    0 srwxrwxrwx   1 dragon   dragon          0 Sep 14 15:09 /tmp/.ICE-unix/909
75153    0 srwxrwxrwx   1 root     root            0 Sep 14 15:38 /tmp/.ICE-unix/1757
75051    0 srwxrwxrwx   1 root     root            0 Sep 22 18:40 /tmp/.ICE-unix/1031
75074    0 srwxrwxrwx   1 root     root            0 Sep 22 19:46 /tmp/.ICE-unix/1850
75079    0 srwxrwxrwx   1 root     root            0 Sep 22 19:57 /tmp/.ICE-unix/1018
```