Global Information Assurance Certification Paper

Unix Security Audit Report

GIAC Enterprises, Research Division

Scott M. McKenzie

Table of Contents

Executive Summary

GIAC Enterprises' Research Division has recently implemented an Internet-connected web/application server at *webby.giac.nil*, which is the focus of this security audit. The server has two primary purposes: to provide a web-to-database data entry system and a database-to-web information retrieval system for its external customers.

The security of this system is paramount to the operation of this aspect of GIAC Enterprises' business. A system compromise could have a number of results, including unauthorized access to company data, denial of service to GIAC Enterprises' customers, or increased risk of penetration of other Internet-connected systems or the private internal network.

It is clear from the analysis that some steps have already been taken to secure *webby* for public access from the Internet, but further modification of the system is necessary to obtain an acceptable level of security. Overall, most of the problems can be corrected by modifying current configurations, installing appropriate security-related software and implementing more thorough administrative procedures.

However, the system has been connected to the Internet and exposed to potential threats for several months. Although no indication of a security breach was discovered during the audit, there is no guarantee that some component has not been compromised. In addition, a significant amount of time would be required to analyze inter-package dependencies before removing extraneous software. The recommendation of this audit is to re-install the operating system from scratch using proven hardening techniques, then install the latest versions of all necessary third-party software. This is the most efficient route to a clean system build, and proactive measures can then be taken to detect and prevent any future exploit attempts that may occur.

Vulnerabilities and Recommended Corrective Actions

The following is an outline of the system's more significant vulnerabilities and recommendations for their resolution. Further detail on each vulnerability and associated information may be found in the analysis.

Prioritized List of Vulnerabilities

- Vulnerability detected in third-party web server software.
- Security patches not applied on a consistent basis.
- Remote logins using unencrypted connections.
- Insecure file permissions and ownership.
- Insufficient backup and disaster recovery procedures.
- Large number of unnecessary software packages installed which significantly increase vulnerability risks.
- DMZ firewall policy allows unnecessary internal network connections.
- System is not adequately protected from unauthorized physical access.
- Inadequate administrative practices, including system monitoring and logging.

Recommended Corrective Actions

Immediate Recommendations (Complete within 7 days)

- Upgrade to latest version of Apache web server and associated software.
    - Estimated cost: 2 hours
    - Considerations: Apache will need to be tested with the Oracle components to ensure compatibility.
- Set PROM password and security mode to 'command' to prevent unauthorized booting from alternate media.
    - Estimated cost: 5 minutes
    - Considerations: System administrators will need to be informed of the password.
- Apply latest vendor-provided security patches.
    - Estimated cost: 1 hour
    - Considerations: It would be desirable to test the patches on a development system, if possible, before applying them to the production system. After the patches are installed, the system will need to be tested to ensure no functionality was lost due to an updated patch. The system should then be patched on a regular, scheduled basis.
- Install and configure `tcp_wrappers` to control incoming connections based on originating IP address.
    - Estimated cost: 1 hour

    - Considerations: None. Administrators and other users of this machine are from only one division of GIAC Enterprises; remote access should be restricted to machines in that area.
- Install and configure secure shell to allow encrypted remote access; disable telnet and ftp; disallow root from ftp in `/etc/ftpusers`.
    - Estimated cost: 2 hours
    - Considerations: Staff will need training to use ssh/sftp instead of telnet/ftp. A minor note; SSH relies on random number generation to create its keys, and Solaris lacks a random number pseudo device (such as `/dev/random`). Instead, SSH calculates its keys using a variety of other items (such as variable output from system status commands). This slows down the authentication process, but given the speed of the system, the delay should be minimal. Sun has indicated it will include a random number generator pseudo device in Solaris 9.
- Remove compiler from system. Software should be compiled on a staging system, then moved to the production system.
    - Estimated cost: 5 minutes to remove compiler; Variable time and cost of hardware to create a development environment.
    - Considerations: A test system with the same versions of the operating system, patches and third-party software will need to be implemented to establish a proper development environment. Time for this implementation will vary.
- Adjust file permissions and ownership using `fix-modes`.
    - Estimated cost: 1 hour
    - Considerations: The modified configuration will need to be tested to ensure no functionality was lost. Afterwards, the system should be re-scanned and any remaining issues examined.

Short Term Recommendations (Complete with 30 days)

- Implement revision control system for tracking configuration file changes.
    - Estimated cost: 4 hours
    - Considerations: System administrators (as well as other staff) will need to be trained on the package in order to take advantages of its features, including audit trails and the ability to roll back to previous versions.
- Establish backup and disaster recovery policies and procedures.
    - Estimated cost: 8 hours
    - Considerations: A proper backup policy must be written, staff informed, and the procedure implemented. SSH should already be in place to allow remote backup over a secure channel.
- Remove as many unnecessary software packages as possible.
    - Estimated cost: 8 hours + variable time depending on thoroughness.
    - Considerations: Removing software packages from an existing system is challenging at best due to the myriad of inter-package dependencies. Given the large number of extraneous software packages, it would

probably be more efficient to simply rebuild the system (see Long Term Recommendations).

- Implement central logging and tools for log monitoring such as `logcheck` or `swatch`.
  - Estimated cost: Variable hours and possible cost of hardware depending on chosen solution.
  - Considerations: If the existing central loghost is used, it will need to be audited and secured. `syslog-ng` will then need to be installed and the firewall modified to log via TCP/IP to the internal loghost. Otherwise, a new loghost will need to be created in the DMZ.
- Implement `sudo` for granting privileges.
  - Estimated cost: 2 hours
  - Considerations: An analysis must be performed to determine what level of access is required for each user, and a policy regarding elevated privileges created. `sudo` can then be configured to grant the appropriate level of access to each party. Staff will need to be trained in its use if elevated privileges are not granted directly to their primary account.
- Restrict firewall to prohibit unnecessary network connections between systems in the DMZ.
  - Estimated cost: 1 hour
  - Considerations: The functions of other systems in the DMZ will need to be reviewed to determine if any access must be left enabled.
- Restrict firewall to prohibit unnecessary network connections from systems in the DMZ to the Internet.
  - Estimated cost: 1 hour
  - Considerations: The functions of this system will need to be reviewed to determine if any access must be left enabled.
- Restrict firewall to specifically block access to ports 111, 32771 and 32772 from any system other than `localhost`. Alternately, consider use of `rpcbind` and `portmap` replacements.
  - Estimated cost: 1 hour or variable time depending on chosen solution.
  - Considerations: Modifying the firewall should be relatively quick and painless. Implementing `rpcbind` and `portmap` will require testing to ensure they are compatible with and do not compromise the functionality of Solstice DiskSuite, which relies on RPC to operate. Given the seriousness of RPC vulnerabilities, both solutions may be implemented for additional security.
- Replace network hub in DMZ using a switch with redundant network backbone connections.
  - Estimated cost: 30 minutes plus hardware.
  - Considerations: Replacement of the hub will need to be scheduled during a period of light activity. Administrators of all affected systems will need to be notified of the outage.

Long Term Recommendations (Complete as soon as possible)

- Implement more thorough audit trail for physical access to DMZ server room, such as an ID-card reader.
    - Estimated cost: Variable time plus cost of materials.
    - Considerations: The DMZ room is not under the control of the GIAC Enterprises Research Division, so this is somewhat beyond their scope.
- Install a dry fire control system in the DMZ server room.
    - Estimated cost: Time and materials.
    - Considerations: Personnel will need training on the new system, including preventing accidental discharge, etc. However, the DMZ room is not under the control of the GIAC Enterprises Research Division, so this is somewhat beyond their scope.
- Rebuild system from scratch using approved hardening techniques, only including the minimal number of software packages necessary.
    - Estimated cost: 8 hours + variable time.
    - Considerations: Given the complexity of the Oracle application software hosted on this system, determining which packages are necessary will be a challenge. A test system will need to be established with a core OS install and security patches; additional packages can then be added as necessary to enable the operation of the Oracle and other third-party software.
- Install file integrity monitor such as `tripwire`.
    - Estimated cost: 1 hour
    - Considerations: This is only valuable if implemented after a clean system build; adding `tripwire` to an existing system will only detect future alterations of files.
- Perform a security audit on the GIAC Enterprises' database server.
    - Estimated cost: 8 hours
    - Considerations: *webby* has a SQLnet connection to a database server located inside the firewall. Although it is unlikely this connection would facilitate a compromise, it is important to ensure all connected systems are secure.

Analysis Detail

Network Security

The system *webby.giac.nil* is located behind the corporate firewall in a DMZ (demilitarized zone). GIAC Enterprises places all of its Internet-connected systems in the DMZ, and maintains a separate internal corporate network. The firewall restricts external traffic to *webby* to only the TCP/IP ports required for its operation, including 80 (http), 443 (https/SSL) and 9000 (Oracle Forms Server). Additionally, the firewall blocks all UDP traffic entering or exiting the DMZ. This is a sound policy, and will help protect *webby* from a variety of attacks, but should not be relied upon as the only line of defense.

A single-port SQLnet over TCP/IP connection is permitted from *webby* to the Research Division's Oracle database server located on the internal corporate network. This is not the most ideal solution, as it would be preferable to disallow all connections to the internal network, but is unavoidable in the current topology. It would be even less desirable to place the database server in the DMZ, potentially elevating its exposure to compromise. Overall, the risk here is relatively minor. However, the database server should also be audited to ensure it is in as secure a state as possible.

Systems in the DMZ, including *webby*, are permitted unrestricted access to any other system in the DMZ. This setup should be changed immediately, so that no system in the DMZ may access any other system in the DMZ, unless required for a necessary business function. With this setup, one compromised machine may result in other compromises in the DMZ. This vulnerability may be resolved by modifying the firewall configuration, or employing a host-based access control system such as `tcp_wrappers` on *webby*.

Systems in the DMZ are also permitted unrestricted access to sites on the Internet. This setup should be terminated unless required for a necessary business function. Disallowing Internet access would offer some additional protection in that if a system is compromised, attackers will be impeded from downloading rootkits or other software from an external site. This may be resolved by modifying the firewall configuration.

All systems on the internal corporate network are permitted unrestricted access to all systems located in the DMZ. This setup should be changed immediately, so that unrestricted access to *webby* is permitted only from systems located in the GIAC Enterprises Research Division that require access for system administrative purposes or another necessary business function. This can be accomplished by modifying the firewall configuration, or employing a host-based access control system such as `tcp_wrappers` on *webby*.

Network connectivity to each machine in the DMZ is provided by CAT5 UTP connected to a 10 MBs hub, which is up-linked to a router port governed by the firewall. It is advisable to replace the hub with a switch to hamper any packet-sniffing attempts from another machine in the DMZ should it be compromised. There are no redundant network

connections for the DMZ itself; however, the corporate network does retain redundant Internet connections through two major ISPs.

Physical/Environmental Security

The logical DMZ, where *webby* is located, physically resides in a single room in the basement of the main corporate building. The walls are concrete/cinder block, and extend fully to the floor and ceiling, both made of concrete. A small vent connected to the air handling system ventilates the room. The vent is not large enough to permit physical access to the room, but the current setup also does not adequately cool the room. It would be advisable to increase the air conditioning capacity to maintain a more optimal temperature. The room is connected to the main sprinkler system and is wet, which would result in damage to the equipment if triggered. A better solution would be to disable the sprinkler system and install a carbon dioxide-based dry extinguishing system.

The door to the room is a metal fire door that opens into the room, and is controlled via a regular key lock. The door is not connected to an alarm system at this time. Only the corporate security office and two corporate network personnel possess keys to the door. The DMZ contains systems maintained by both the corporate IT department and by different business units of the corporation, so occasional access to the room is necessary for a number of personnel not associated with *webby*. When someone requires physical access to the DMZ, the person meets one of the three key-holding entities at the room, and presents photo identification before being allowed to enter. However, once access is granted, the access-granting entity usually departs, and the activities of the personnel remaining in the room are unmonitored. A solution would be to install a security camera, but care would have to be taken in the placement of the camera to prevent "shoulder surfing" attacks on personnel working on the system consoles. Plans to install card reader access to the room have been formulated but not yet implemented. This will allow for a more thorough audit trail. Ideally, card access should be required to both enter and exit the room, though that may not be feasible due to fire code regulations. The door should trip an alarm if propped open for an extended period of time.

Electrical power is provided to the room by standard wall outlets with no surge suppression, line filtering or generator backup. For this reason, *webby* is connected to a high-capacity UPS with an estimated 1.5 hour run time. However, the UPS is not configured to shut down the system in the event of a power failure and subsequent battery drain. The hub that provides network connectivity to systems in the DMZ is also connected to a UPS.

Since personnel not associated with *webby* have limited access to the DMZ room, the system should be further secured from unauthorized physical access. In its current state, unauthorized personnel have access to the console, CDROM drive and power switch. This access alone could be sufficient to compromise the system. *webby* currently resides on the floor, with a monitor, keyboard and mouse attached as the console. The system and its UPS should be enclosed in a locked cage, which would prevent access to the

console, CDROM drive and cable connections. The power and network cables that leave the cage should be enclosed in a metal conduit. The hub that provides network connectivity to systems in the DMZ should also be secured in a similar manner.

Operating System

webby.giac.nil is a Sun Microsystems Enterprise 250, running the Solaris 7 operating system, Sun's variant of UNIX. The configuration of Solaris on the system is a Full Install and includes approximately 370 packages. As a production machine accessible from the Internet, this is not recommended, as a full install of the OS includes a large number of packages unnecessary for the system to function as a web/application server. A defect in any of these packages could lead to a compromise. All packages not required for the proper operation of the system should be removed. However, given the large number of extraneous packages and inter-package dependencies, it would most likely be more efficient to rebuild the system from scratch, employing proper hardening techniques during the build process, such as those found in the "Securing Solaris Step-by-Step" document produced by SANS. Once the system has been set up and appropriately hardened, a file integrity checker such as `tripwire` should be installed before deployment. If a full system rebuild is not feasible, an alternative may be to use the security tools YASSP or Titan. Both apply a methodology to an existing system configuration similar to what would result from a properly secured system build, although a large number of unnecessary packages will still remain on the system.

If the system is re-installed, consideration should be given to using Sun Solaris 8, the current shipping version of the OS as of this writing. Sun has made an effort to make each revision of its system software more secure out of the box, and using the latest version guarantees support from the vendor. To Sun's credit, it does have a history of maintaining support on several older versions, and releasing security patches for the current revision and several previous revisions in tandem.

System Patches

System patches are relatively up to date, the last Recommended & Security patch cluster having been applied approximately three weeks prior to this analysis. However, there isn't a defined schedule for applying patches, so this is more likely the result of coincidence as opposed to sound administrative practice. It is recommended that a fixed schedule be established for applying the Recommended & Security patch cluster, perhaps on a monthly basis, and that other high-risk security-related patches be applied as they become available. Sun Microsystems makes all patches available to the public at http://sunsolve.sun.com, and offers a weekly SunSolve patch update mailing list, which describes new patches as they are released.

System Access

Logins are authenticated via the local `/etc/passwd` and `/etc/shadow` files. Since *webby* is a production system, these contain a limited number of active users, including the necessary system accounts, userids to operate components of the web/application server, and a small number of users who require access to update content. System accounts which are not used on the system have been disabled in `/etc/shadow`, but should probably be removed from the files altogether. Some disabled accounts still have valid shells, which should be changed to `/dev/null`. Password aging and history are not currently utilized, and should be activated, at least for the user accounts. Password minimum length is enforced to six characters and passwords must be alphanumeric. The password cracking tool John the Ripper was used to evaluate the existing passwords. Only one password of the existing seven accounts was discovered in a scan of considerable length; that password has since been changed.

The system and service account passwords should be changed on a regular basis. Some of the user accounts are generic (for web content and application updates) and used by more than one person. These accounts should be removed and replaced with an individual account for each user that requires access to allow more thorough auditing. This should be easy to implement, as there are fewer than ten individuals who need access to *webby*.

Users connect to *webby* via telnet and ftp, which means passwords are sent in cleartext across the network. Although these connections are made from the internal network to the DMZ and not across the Internet, care should be taken to prevent internal packet sniffing. Secure Shell should be implemented immediately to provide a secure channel for interactive and file transfer connections, after which telnet and ftp should be disabled. Direct root login via telnet is disabled, users must log in then `su` to root, but root may still log in via ftp. An `/etc/ftpusers` file should be created to prevent this. Root is permitted to log in on the system's console, which typically occurs only during physical system maintenance.

System Security

Services not required for *webby*'s operation have been disabled in `/etc/inetd.conf` and in the various `rc` scripts. Services that remain active in `inetd.conf` are telnet, ftp, time and metadb (an RPC service for Solstice Adminsuite). Though time is enabled, the system is not actively synchronizing its clock. Network Time Protocol (NTP) should be installed and configured to provide time synchronization with a trusted time source.

A list of active network ports was obtained by using `netstat` (see Appendix A). *webby* was also scanned using `nmap` from a point on the internal network inside the firewall to obtain a network-based view of open ports (see Appendix B). Since the firewall blocks all UDP traffic, active UDP ports appear on the `netstat` output, but not on `nmap`. The results are consistent with ports that are known to be open on the system.

TCP/IP

Port	Service	Notes
21	FTP	Should be disabled and replaced with sftp
23	Telnet	Should be disabled and replaced with ssh
37	Time	Time synchronization; NTP needs to be configured
80	HTTP	Web server
111	Portmapper	Required for DiskSuite
443	HTTPS/SSL	Web server (Secure Sockets Layer)
9000	Forms	Oracle Web Forms Server
32771	RPC	Solstice DiskSuite
32772	RPC	Solstice DiskSuite

UDP

Port	Service	Notes
37	Time	Time synchronization; NTP needs to be configured
111	Portmapper	Required for DiskSuite
514	Syslog	Syslog should be configured to send messages only and not receive; this will close 514/udp
32771	RPC	Solstice DiskSuite

Solstice DiskSuite, which provides software RAID, uses the RPC portmapper (port 111) as well as ports 32771 and 32772. Given the inherent security flaws in RPC, it would be ideal to disable all RPC services, but that is not feasible in this situation. It is recommended to specifically block all access to ports 111, 32771 and 32772 at the firewall, and/or install Weitse Venema's `rpcbind` and `portmap` replacements. These are more secure than the OEM Sun distribution and allow filtering based on IP address. Since *webby* is the only system that needs to interact with these services, access can be restricted to 127.0.0.1.

The system does not have a security mode or password set in the PROM. Given that personnel not associated with *webby* have physical access to it, the system should have its security mode set to "command" and a PROM password set. This will prevent unauthorized personnel from booting the system from a CD.

TARA, an updated version of the system scanning tool Tiger, was used to analyze the system configuration on *webby* (see Appendix C). A large number of the warnings generated by TARA were related to improper ownership, group ownership or permissions on files. Many of these problems can be fixed by using `fix-modes`, a program that will change most files to be owned by root as well as remove unnecessary group and world write permissions. After running `fix-modes`, TARA should be run again to verify that file permissions have been modified properly and reveal any additional permissions that may need to be modified manually.

Administrative Practices

There is one primary administrator for *webby*, and three others who have the root password (another admin, IT manager and DBA). This is not a particularly secure arrangement, and does not provide any sort of accountability other than the `su` logs. Only the primary administrator should have and be permitted to use the root password in an active manner; it should also be stored with the IT manager for backup purposes. If individuals other than the primary admin require some degree of root privileges, `sudo` should be implemented to provide a more secure means of granting privileges and maintaining an audit trail.

System administrators and other users of *webby* should document their changes in a central log. Also, a revision control system should be implemented to monitor changes to configuration files.

System logs are stored locally, rotated weekly and retained for a month. Log entries should also be sent to a central loghost. Currently, GIAC Enterprises operates a central loghost on the internal network. Forwarding log entries to that loghost is not feasible as the firewall policy prohibits all UDP traffic. Two possible solutions are to implement a second, well-secured loghost in the DMZ, or use `syslog-ng` to forward log entries over TCP to the internal loghost. In any case, a utility such as `logcheck` or `swatch` should be implemented to review system logs.

The GNU `gcc` compiler and `perl` are installed on the system. Some software is compiled directly on *webby* using the installed `gcc`. Since this is a production system, it is recommended that software be compiled on a similar system elsewhere, then installed on *webby*. Compilers such as `gcc` should be removed. At this time `perl` does not appear to be used for any applications; if further examination supports this, it should also be removed.

Backups and Disaster Recovery

Backups for *webby* are currently implemented on a very ad hoc basis. A number of the configuration files that are complex or would be time consuming to reproduce are saved to a backup directory on *webby*, as well as on another system. These copies are manually updated when successful changes are made to the original files on *webby*. Changes to the configuration files are usually documented using comments within the file itself. However, no revision control system is in place to monitor configuration file changes, and backup of the files is not automated, which could result in the manual backups becoming out of date and thus useless. No formal documentation, procedures or policies for backups or disaster recovery are in place for this system. A plan should be created and implemented as soon as possible.

The system does not have an attached tape drive. However, given that administrators of the system do not have direct physical access to the system to change backup media, and

that the system is located in a building ten minutes from the Research Division that manages it, regular media swaps would prove to be an obstacle. If a tape drive were used, it is possible tapes would become full and critical backups would fail due to lack of available media. An alternative that should be explored is the implementation of a well-secured remote backup system capable of establishing a connection to *webby* using Secure Shell, and writing data out to a local tape drive via the encrypted tunnel.

webby is configured to offer some degree of fault tolerance. Solstice DiskSuite, a product provided by Sun that implements software RAID, is used to configure disk redundancy. The system contains six 9 GB SCSI hard disks. The /, /usr, /var, /opt and swap partitions are mirrored, so that in the event of a primary disk failure, the system may be booted by modifying the PROM to boot from the mirror disk. The other four disks are arranged in a RAID5 configuration, which is used to store third-party applications and data. The RAID5 setup will allow the volume to remain available in the event of a disk failure, providing time to obtain a replacement and perform a hot drive swap. *webby* is equipped with redundant, active power supplies. The system contains dual processors, and is able to operate on one CPU in the event of a processor failure. *webby* also includes a Remote System Control module, which allows the system to be powered on or off, or reset in the event of a system hang, from a remote location via a telnet connection. Unfortunately, there appears to be no way to implement Secure Shell for the RSC interface. No spare hardware is currently kept on site, but a service contract for *webby* is maintained with Sun Microsystems that provides overnight parts replacement and/or four hour on-site response time during normal business hours.

Failover options for the system have been considered but none have been implemented. Given the nature of the business activities that *webby* supports, a brief outage would be permissible. It is recommended that a second system be configured as a "warm spare." This system would also reside in the DMZ and would synchronize its data with *webby* on a daily basis. In the event of a total system failure on *webby*, the secondary system can be renamed and re-addressed to temporarily take its place.

Third-Party Applications

webby has several additional software packages installed that are not part of the Solaris operating system:

```
# pkginfo |grep -v SUNW
application LWperl          perl
application SMCgcc          gcc
application SMCgzip         gzip
application SMClsof         lsof
system      TSIpgx          PGX32 (Raptor GFX) System Software/Device
Driver
system      TSIpgxmn        PGX32 (Raptor GFX) Man Pages
application TSIpgxw         PGX32 (Raptor GFX) X Window System Support
system      TSIpgxx         PGX32 (Raptor GFX) System Software/Device
Driver (64-bit)
application WLtop           top
```

As mentioned previously, if the GNU `gcc` compiler and `perl` are not necessary for the system to function, they should be removed, as they provide valuable tools to attackers to facilitate or extend a compromise. The `lsof`, `gzip` and `top` utilities have useful administrative functions and may be permitted to remain. The PGX32 packages are required device drivers for the installed video card.

webby uses the popular Apache web server software. The version installed is 1.3.xx, which is several revisions behind the current release, and should be upgraded as soon as possible to take advantage of any security and bug fixes the latest release provides. SARA and Nessus, two network vulnerability scanners, were used to scan the system (see Appendix D and E). SARA lists a vulnerability for the currently installed version of Apache, reinforcing the need for an upgrade. Apache is configured with DSO support, and has been compiled to enable Secure Sockets Layer (SSL) support using `mod_ssl` and OpenSSL. Apache runs under a dedicated, non-privileged userid. Common Gateway Interface (CGI) support is enabled, but in a limited fashion. *webby* only permits CGI script execution from specific system directories; users do not have personal web space in which to upload or run their own CGIs. In addition, the only CGIs in use are those associated with the Oracle Forms and WebDB products described below. The CGI vulnerability assessment tool `malice` was used to check for known exploits (see Appendix E), but none were discovered. This is most likely due to the relative obscurity of the CGIs in use on the system, as CGI scanners don't appear to include the Oracle CGIs in their vulnerability databases. However, CGIs are prime targets for attack, so it would be ideal to use `chroot` to run Apache in its own directory structure if possible.

webby uses the Forms Server and WebDB products by Oracle to provide application server functionality. Forms Server allows data entry forms created with Oracle Developer to be run as Java applets within a remote user's web browser. WebDB is used to create managed web sites with dynamic content as well as some applications. *webby* primarily functions as a conduit between web-based clients and the back-end database server; very little data is stored on the system itself. Forms and WebDB applications are written by GIAC Enterprises application developers, so it is recommended they follow good coding practices and obtain knowledge on the creation of secure web applications. Both products require users to provide a username and password for access. Logins to WebDB are encrypted using SSL via Apache; Forms uses its own encryption between the downloaded Java applet (Forms client) and the Forms server on *webby*, so no authentication information is sent in the clear over the Internet. Both Forms and WebDB are implemented using CGI scripts provided by Oracle. They are either compiled C executables or shell scripts for which the source code is available; the latter should be scrutinized to ensure they are not exploitable. As previously mentioned, CGIs are potentially dangerous. Oracle provides an alternate method for using these technologies through its Internet Application Server product, which may be considered as an alternative to the current CGI-based implementation. However, a separate analysis would need to be performed to determine which method maintains a better level of security while continuing to meet the business requirements of the system.

Appendices

Note about network ports: `netstat` (Appendix A) was run on the system to obtain a list of active ports. *webby* was also scanned using `nmap` (Appendix B) from a point on the private network inside the firewall which has full, unfiltered TCP access to the DMZ. However, since the firewall blocks all UDP traffic, open UDP ports appear on the `netstat` output but not on the `nmap` or `nessus` (Appendix E) scans.

Appendix A – Netstat

The output below reflects the open ports on the system. The two established connections are the telnet session used to obtain this information and the SQLnet connection from *webby* to the database server.

```
# /usr/bin/netstat -an

UDP
   Local Address         Remote Address     State
-------------------- -------------------- -------
      *.111                                Idle
      *.*                                  Unbound
      *.32771                              Idle
      *.37                                 Idle
      *.514                                Idle
      *.*                                  Unbound

TCP
   Local Address        Remote Address    Swind Send-Q Rwind Recv-Q  State
-------------------- -------------------- ----- ------ ----- ------ -------
      *.*                  *.*              0      0     0      0 IDLE
      *.111                *.*              0      0     0      0 LISTEN
      *.*                  *.*              0      0     0      0 IDLE
      *.21                 *.*              0      0     0      0 LISTEN
      *.23                 *.*              0      0     0      0 LISTEN
      *.37                 *.*              0      0     0      0 LISTEN
      *.32771              *.*              0      0     0      0 LISTEN
      *.32772              *.*              0      0     0      0 LISTEN
      *.9000               *.*              0      0     0      0 LISTEN
      *.443                *.*              0      0     0      0 LISTEN
      *.80                 *.*              0      0     0      0 LISTEN
      *.*                  *.*              0      0  8576      0 IDLE
      *.*                  *.*              0      0     0      0 IDLE
192.168.x.y.34814     192.168.s.t.1500      9100     0  9100      0 ESTABLISHED
      *.*                  *.*              0      0     0      0 IDLE
192.168.x.y.23        192.168.u.v.53022     9100     1  9100      0 ESTABLISHED
      *.*                  *.*              0      0     0      0 IDLE
```

Appendix B – Nmap

A full connect TCP scan was selected for `nmap` since this was a legitimate scan. The firewall blocks UDP traffic to and from the DMZ where *webby* is located, so `nmap` could not be used to display open UDP ports.

```
# ./nmap -sT -v -v webby.giac.nil

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Host webby.giac.nil (192.168.x.y) appears to be up ... good.
Initiating TCP connect() scan against webby.giac.nil (192.168.x.y)
Adding TCP port 443 (state open).
Adding TCP port 80 (state open).
Adding TCP port 37 (state open).
Adding TCP port 21 (state open).
Adding TCP port 23 (state open).
Adding TCP port 9000 (state open).
Adding TCP port 32771 (state open).
Adding TCP port 32772 (state open).
Adding TCP port 111 (state open).
The TCP connect scan took 1 second to scan 1523 ports.
Interesting ports on webby.giac.nil (192.168.x.y):
(The 1514 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
23/tcp     open        telnet
37/tcp     open        time
80/tcp     open        http
111/tcp    open        sunrpc
443/tcp    open        https
9000/tcp   open        sd
32771/tcp  open        sometimes-rpc5
32772/tcp  open        sometimes-rpc7

Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds
```

Appendix C – TARA

webby was scanned using TARA, an updated version of Tiger. Below is the `tigerrc` configuration file used.

```
#
# 'rc' file for tiger.  This file is preprocessed, and thus
# can *only* contain variable assignments.
#
#
# TAMU version
#
# Note:  This disables many of the checks.  You should not use this.
#        The checks enabled here are the ones we definitely want done
#        but all of them should be done.
#
#-----------------------------------------------------------------------
-
#
# Select checks to perform.  Specify 'N' (uppercase) for checks
# you don't want performed.
#
Tiger_Check_PASSWD=Y          # Fast
Tiger_Check_GROUP=Y           # Fast
Tiger_Check_ACCOUNTS=Y        # Time varies on # of users
Tiger_Check_RHOSTS=Y          # Time varies on # of users
Tiger_Check_NETRC=Y           # Time varies on # of users
Tiger_Check_ALIASES=Y         # Fast
Tiger_Check_CRON=Y            # Fast
Tiger_Check_ANONFTP=Y         # Fast
Tiger_Check_EXPORTS=Y         # Fast
Tiger_Check_INETD=Y           # Could be faster, not bad though
Tiger_Check_KNOWN=Y           # Fast
Tiger_Check_PERMS=Y           # Could be faster, not bad though
Tiger_Check_SIGNATURES=N      # Several minutes
Tiger_Check_FILESYSTEM=Y      # Time varies on disk space... can be
hours
Tiger_Check_PATH=Y            # Fast for just root... varies for all
Tiger_Check_EMBEDDED=N        # Several minutes
#
# Should messages tagged with INFO be shown?
#
Tiger_Show_INFO_Msgs=Y
#
# In order for this to be effective, you must set 'CRACK' in a
# 'site' config file.
#
Tiger_Run_CRACK=N               # First time, ages; subsequent fairly
quick
#
# Line size (for formatting of output)... default is 79...
# Specifying '0' means unlimited
#
Tiger_Output_Width=79
#
# Same as above, except used when run via 'tigercron'...
```

```
# You should set this once and never change it, 'cause if you
# change it, you'll get lots and lots of new stuff according
# to the scripts (the diff's against previous reports will find
# lots of changes due to the formatting changes).
#
Tiger_CRON_Output_Width=0
#
# If an embedded pathname refers to an executable file, this executable
# will in turn be checked.  This will continue "recursively" until
# either no new executables are found, or a maximum reference depth
# is reached.  Setting this variable to 0 is equivalent to infinity.
# On a Sun 4/490, SunOS 4.1.2, 6GB disk, an infinite depth check
# took about 30 minutes.  Your milage will vary.
#
# On small memory systems, a large search depth can result in out
# of memory situations for 'sort'... :-(...
#
Tiger_Embed_Max_Depth=3
#
# Only search executables for embedded pathnames.  If this is
# set to 'N', then all regular files will be searched.  Otherwise
# only executable files will be searched.
#
Tiger_Embed_Check_Exec_Only=Y
#
# Check all setuid executables found.  This will cause 'tiger'
# to run longer on many systems, as it will have to wait for the
# file system scans to complete before it can begin checking the
# embedded pathnames.
#
Tiger_Embed_Check_SUID=Y
#
# Only report executables which are writable or not owned by root.  If
set
# to 'Y' only the executables will be reported.  Any other value will
result
# in regular files and directories being reported as well.
#
# Note that currently, device files are never reported.
#
Tiger_Embed_Report_Exec_Only=Y
#
# Who do you allow to own system files.
# List of usernames separated by '|'... no whitespace
#
Tiger_Embedded_OK_Owners='root|bin|uucp'
#Tiger_Embedded_OK_Owners=root
#
# What groups can have write access to system files?
# List of group names separated by '|'... no whitespace.
# No value means no groups should have write access.
#
Tiger_Embedded_OK_Group_Write=
#
# Should all users' PATH variables be checked.  This has the potential
# of being dangerous because of the way it is done.  You might want to
```

```
# take a look at check_path and decide for yourself whether the
precautions
# are sufficient before enabling this.
#
Tiger_Check_PATHALL=N           # Check all user PATHs in startup files.
#
# Who can own executables in 'root's PATH?
# List of usernames separated by '|'... no whitespace
#
Tiger_ROOT_PATH_OK_Owners='root|uucp|bin|sys|daemon'
#Tiger_ROOT_PATH_OK_Owners='root'
#
# What groups can have write access to executables in 'root's PATH?
# List of group names separated by '|'... no whitespace.
# No value means no groups should have write access.
#
Tiger_ROOT_PATH_OK_Group_Write=
#
# Who can own things in other users PATH?
# List of usernames separated by '|'... no whitespace
#
Tiger_PATH_OK_Owners='root|bin|uucp|sys|daemon'
#
# What groups can have write access to executables in non-root user
PATH?
# List of group names separated by '|'... no whitespace.
# No value means no groups should have write access.
#
Tiger_PATH_OK_Group_Write=
#
# Should 'tiger' wait for Crack to finish?  If set to 'Y' it will wait
# until it finishes.  If set to 'N', it will collect the output if
# Crack finishes before the rest of the checks.  If it isn't finished
# 'tiger' will simply report where the output will be stored.
#
Tiger_Collect_CRACK=N
#
# Run Crack on local password sources only?  If set to Y, no network
# sources will be used.  If set to 'N', NIS, NIS+, NetInfo, etc
# sources will also be used.
#
Tiger_Crack_Local=N
#
# Who gets output from 'tigercron'?
#
Tiger_Mail_RCPT=root
#
# List of '/' separated filename globs (NOT pathnames) to look for
# on the filesystems.
#
Tiger_Files_of_Note="..[!.]*/.* */.*      */.[!.]/.log/.FSP*"
#
# File system scan - things to look for
#
Tiger_FSScan_Setuid=Y         # Setuid executables
Tiger_FSScan_Devs=Y           # device files
Tiger_FSScan_SymLinks=N       # strange symbolic links
```

```
Tiger_FSScan_ofNote=Y         # wierd filenames
Tiger_FSScan_WDIR=Y           # world writable directories
Tiger_FSScan_Unowned=N        # files with undefined owners/group
#
# Should we scan read-only filesystems
#
Tiger_FSScan_ReadOnly=N
#
# List of dot files commonly found in user home directories.  These
# will be checked by check_accounts for proper access permissions.
#
# Note that .rhosts and .netrc need not appear here, as they will
# be checked by scan_rhosts or scan_netrc.
#
USERDOTFILES=".cshrc .profile .login .mailrc .exrc .emacs .forward
.tcshrc .zshenv .zshrc .zlogin .zprofile .rcrc .bashrc .bash_profile
.inputrc .xinitrc"
#
# Rhost sites which are expected to be in the .rhosts files.
# Anything that doesn't match will be reported.  The patterns
# are simple patterns as used in Bourne Shell 'case' statement.
#
#RHOST_SITES='*.tamu.edu|jupiter'
```

Output from TARA

```
# ./tiger
Security scripts *** 2.0.9 ARC, 1999.0907.2100 ***
Sat Feb 17 17:23:55 EST 2001
17:23> Beginning security report for webby (sun4u SunOS 5.7).

# Performing check of passwd files...

# Performing check of group files...

# Performing check of user accounts...
# Checking accounts from /etc/passwd.
--WARN-- [acc005w] Login ID adm is disabled, but has a 'cron' file or
      cron entries.
--WARN-- [acc005w] Login ID sys is disabled, but has a 'cron' file or
      cron entries.
--WARN-- [acc006w] Login ID acrn's home directory (/web/acrn) has group
      `webadmin' write access.
--WARN-- [acc006w] Login ID adm's home directory (/var/adm) has group
      `sys' write access.
--WARN-- [acc006w] Login ID appdev's home directory (/apps) has group
      `dba' write access.
--WARN-- [acc006w] Login ID bin's home directory (/usr/bin) has group
      `bin' write access.
--WARN-- [acc006w] Login ID lp's home directory (/usr/spool/lp) has
      group `lp' write access.

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

```
# Checking accounts from /etc/passwd...

# Performing check of .netrc files...

# Checking accounts from /etc/passwd...

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

--WARN-- [root002w] Remote root access allowed in /etc/ftpusers


# Performing check of PATH components...
# Only checking user 'root'


--WARN-- [path002w] /usr/sbin/accept in root's PATH from .profile is not
owned by root (owned by lp).
--WARN-- [path002w] /usr/sbin/in.uucpd in root's PATH from .profile is
not owned by root (owned by 5).
--WARN-- [path001w] /usr/sbin/install.d in root's PATH from .profile is
group `bin' writable.
--WARN-- [path002w] /usr/sbin/lpadmin in root's PATH from .profile is
not owned by root (owned by lp).
--WARN-- [path002w] /usr/sbin/lpfilter in root's PATH from .profile is
not owned by root (owned by lp).
--WARN-- [path002w] /usr/sbin/lpforms in root's PATH from .profile is
not owned by root (owned by lp).
--WARN-- [path002w] /usr/sbin/lpshut in root's PATH from .profile is not
owned by root (owned by lp).
--WARN-- [path002w] /usr/sbin/lpsystem in root's PATH from .profile is
not owned by root (owned by lp).
--WARN-- [path002w] /usr/sbin/lpusers in root's PATH from .profile is
not owned by root (owned by lp).
--WARN-- [path002w] /usr/sbin/reject in root's PATH from .profile is not
owned by root (owned by lp).
--WARN-- [path001w] /usr/sbin/static in root's PATH from .profile is
group `bin' writable.
--WARN-- [path002w] /usr/bin/coraenv in root's PATH from .profile is not
owned by root (owned by oracle).
--WARN-- [path002w] /usr/bin/dbhome in root's PATH from .profile is not
owned by root (owned by oracle).
--WARN-- [path002w] /usr/bin/disable in root's PATH from .profile is not
owned by root (owned by lp).
--WARN-- [path002w] /usr/bin/enable in root's PATH from .profile is not
owned by root (owned by lp).
--WARN-- [path002w] /usr/bin/oraenv in root's PATH from .profile is not
owned by root (owned by oracle).
--WARN-- [path001w] /usr/bin/prodreg in root's PATH from .profile is
group `root' writable.
--WARN-- [path001w] /usr/bin/prodregdir in root's PATH from .profile is
group `root' writable.
--WARN-- [path002w] /usr/bin/uudecode in root's PATH from .profile is
not owned by root (owned by 5).
--WARN-- [path002w] /usr/bin/uuencode in root's PATH from .profile is
not owned by root (owned by 5).
--WARN-- [path002w] /usr/bin/uulog in root's PATH from .profile is not
owned by root (owned by 5).
```

```
--WARN-- [path002w] /usr/bin/uupick in root's PATH from .profile is not
owned by root (owned by 5).
--WARN-- [path002w] /usr/bin/uuto in root's PATH from .profile is not
owned by root (owned by 5).
--WARN-- [path002w] /usr/local/bin/coraenv in root's PATH from .profile
is not owned by root (owned by oracle).
--WARN-- [path002w] /usr/local/bin/dbhome in root's PATH from .profile
is not owned by root (owned by oracle).
--WARN-- [path002w] /usr/local/bin/oraenv in root's PATH from .profile
is not owned by root (owned by oracle).
--WARN-- [path001w] /etc/acct in root's PATH from .profile is group
`adm' writable.
--WARN-- [path002w] /etc/acct in root's PATH from .profile is not owned
by root (owned by adm).
--WARN-- [path001w] /etc/default in root's PATH from .profile is group
`sys' writable.
--WARN-- [path001w] /etc/dfs in root's PATH from .profile is group `sys'
writable.
--WARN-- [path001w] /etc/dhcp in root's PATH from .profile is group
`sys' writable.
--WARN-- [path001w] /etc/dmi in root's PATH from .profile is group `sys'
writable.
--WARN-- [path001w] /etc/fn in root's PATH from .profile is group `sys'
writable.
--WARN-- [path001w] /etc/fs in root's PATH from .profile is group `sys'
writable.
--WARN-- [path001w] /etc/init.d in root's PATH from .profile is group
`sys' writable.
--WARN-- [path001w] /etc/lib in root's PATH from .profile is group `sys'
writable.
--WARN-- [path001w] /etc/log in root's PATH from .profile is group `adm'
writable.
--WARN-- [path002w] /etc/log in root's PATH from .profile is not owned
by root (owned by adm).
--WARN-- [path001w] /etc/lp in root's PATH from .profile is group `lp'
writable.
--WARN-- [path002w] /etc/lp in root's PATH from .profile is not owned by
root (owned by lp).
--WARN-- [path001w] /etc/openwin in root's PATH from .profile is group
`bin' writable.
--WARN-- [path001w] /etc/opt in root's PATH from .profile is group `sys'
writable.
--WARN-- [path001w] /etc/rc0.d in root's PATH from .profile is group
`sys' writable.
--WARN-- [path001w] /etc/rc1.d in root's PATH from .profile is group
`sys' writable.
--WARN-- [path001w] /etc/rc2.d in root's PATH from .profile is group
`sys' writable.
--WARN-- [path001w] /etc/rc3.d in root's PATH from .profile is group
`sys' writable.
--WARN-- [path001w] /etc/rcS.d in root's PATH from .profile is group
`sys' writable.
--WARN-- [path001w] /etc/snmp in root's PATH from .profile is group
`sys' writable.
--WARN-- [path001w] /etc/tm in root's PATH from .profile is group `sys'
writable.
```

```
--WARN-- [path002w] /etc/uucp in root's PATH from .profile is not owned
by root (owned by 5).
--WARN-- [path002w] /usr/ucb/lpc in root's PATH from .profile is not
owned by root (owned by lp).
--WARN-- [path002w] /usr/ucb/lptest in root's PATH from .profile is not
owned by root (owned by lp).
--WARN-- [path002w] /usr/sbin/accept in root's PATH from default is not
owned by root (owned by lp).
--WARN-- [path002w] /usr/sbin/in.uucpd in root's PATH from default is
not owned by root (owned by 5).
--WARN-- [path001w] /usr/sbin/install.d in root's PATH from default is
group `bin' writable.
--WARN-- [path002w] /usr/sbin/lpadmin in root's PATH from default is not
owned by root (owned by lp).
--WARN-- [path002w] /usr/sbin/lpfilter in root's PATH from default is
not owned by root (owned by lp).
--WARN-- [path002w] /usr/sbin/lpforms in root's PATH from default is not
owned by root (owned by lp).
--WARN-- [path002w] /usr/sbin/lpshut in root's PATH from default is not
owned by root (owned by lp).
--WARN-- [path002w] /usr/sbin/lpsystem in root's PATH from default is
not owned by root (owned by lp).
--WARN-- [path002w] /usr/sbin/lpusers in root's PATH from default is not
owned by root (owned by lp).
--WARN-- [path002w] /usr/sbin/reject in root's PATH from default is not
owned by root (owned by lp).
--WARN-- [path001w] /usr/sbin/static in root's PATH from default is
group `bin' writable.
--WARN-- [path002w] /usr/bin/coraenv in root's PATH from default is not
owned by root (owned by oracle).
--WARN-- [path002w] /usr/bin/dbhome in root's PATH from default is not
owned by root (owned by oracle).
--WARN-- [path002w] /usr/bin/disable in root's PATH from default is not
owned by root (owned by lp).
--WARN-- [path002w] /usr/bin/enable in root's PATH from default is not
owned by root (owned by lp).
--WARN-- [path002w] /usr/bin/oraenv in root's PATH from default is not
owned by root (owned by oracle).
--WARN-- [path001w] /usr/bin/prodreg in root's PATH from default is
group `root' writable.
--WARN-- [path001w] /usr/bin/prodregdir in root's PATH from default is
group `root' writable.
--WARN-- [path002w] /usr/bin/uudecode in root's PATH from default is not
owned by root (owned by 5).
--WARN-- [path002w] /usr/bin/uuencode in root's PATH from default is not
owned by root (owned by 5).
--WARN-- [path002w] /usr/bin/uulog in root's PATH from default is not
owned by root (owned by 5).
--WARN-- [path002w] /usr/bin/uupick in root's PATH from default is not
owned by root (owned by 5).
--WARN-- [path002w] /usr/bin/uuto in root's PATH from default is not
owned by root (owned by 5).

# Performing check of anonymous FTP...

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

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

--WARN-- [cron003] cron entry for root uses `/usr/lib/newsyslog' which
contains `/usr' which is group `sys' writable.

--WARN-- [cron003] cron entry for root uses `/usr/lib/newsyslog' which
contains `/usr/lib' which is group `bin' writable.

--WARN-- [cron003] cron entry for root uses `/usr/lib/fs/nfs/nfsfind'
which contains `/usr' which is group `sys' writable.

--WARN-- [cron003] cron entry for root uses `/usr/lib/fs/nfs/nfsfind'
which contains `/usr/lib' which is group `bin' writable.

--WARN-- [cron003] cron entry for root uses `/usr/lib/fs/nfs/nfsfind'
which contains `/usr/lib/fs' which is group `sys' writable.

--WARN-- [cron001w] cron entry for root does not use full pathname:

--WARN-- [cron001w] cron entry for root does not use full pathname:
--WARN-- [cron003] cron entry for root uses `/usr/lib/gss/gsscred_clean'
which contains `/usr' which is group `sys' writable.

--WARN-- [cron003] cron entry for root uses `/usr/lib/gss/gsscred_clean'
which contains `/usr/lib' which is group `bin' writable.

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

--WARN-- [cron003] cron entry for root uses `/usr/lib/gss/gsscred_clean'
which contains `/usr' which is group `sys' writable.

--WARN-- [cron003] cron entry for root uses `/usr/lib/gss/gsscred_clean'
which contains `/usr/lib' which is group `bin' writable.

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

--WARN-- [cron003] cron entry for root uses `/usr/lib/sendmail' which
contains `/usr' which is group `sys' writable.

--WARN-- [cron003] cron entry for root uses `/usr/lib/sendmail' which
contains `/usr/lib' which is group `bin' writable.


# Performing check of 'services' and 'inetd'...
# Checking services from /etc/services.
--FAIL-- [inet003f] The port for service pop2 is assigned to service
pop-2.
# Checking inetd entries from /etc/inet/inetd.conf

# Performing NFS exports check...

# Performing check of system file permissions...
```

```
--WARN-- [perm001w] /export should not have group write.
--WARN-- [perm001w] /sbin should not have group write.
--WARN-- [perm001w] /usr should not have group write.
--WARN-- [perm001w] /usr/4lib should not have group write.
--WARN-- [perm001w] /usr/openwin should not have group write.
--WARN-- [perm001w] /usr/games should not have group write.
--WARN-- [perm001w] /usr/bin should not have group write.
--WARN-- [perm001w] /usr/lib should not have group write.
--WARN-- [perm001w] /usr/ucb should not have group write.
--WARN-- [perm001w] /dev should not have group write.
--WARN-- [perm001w] /etc/dfs should not have group write.
--WARN-- [perm001w] The owner of /etc/uucp/Permissions should be root
(owned by 5).
--WARN-- [perm001w] The owner of /etc/uucp/Systems should be uucp (owned
by 5).
--WARN-- [perm001w] The owner of /usr/bin/uulog should be root (owned by
5).
--WARN-- [perm001w] The owner of /usr/bin/uuglist should be uucp (owned
by 5).
--WARN-- [perm001w] The owner of /usr/bin/uuto should be root (owned by
5).
--WARN-- [perm001w] The owner of /usr/bin/uupick should be root (owned
by 5).
--WARN-- [perm001w] The owner of /usr/bin/uustat should be uucp (owned
by 5).
--WARN-- [perm001w] The owner of /usr/bin/cu should be uucp (owned by
5).
--WARN-- [perm001w] The owner of /usr/bin/tip should be uucp (owned by
5).
--WARN-- [perm001w] /usr/bin/tip should not have owner write.
--WARN-- [perm001w] The owner of /usr/bin/uucp should be uucp (owned by
5).
--WARN-- [perm001w] The owner of /usr/bin/uux should be uucp (owned by
5).
--WARN-- [perm001w] The owner of /usr/bin/uuname should be uucp (owned
by 5).
--WARN-- [perm021w] Disk device /dev/md/dsk/d2 has read access for group
sys.
--WARN-- [perm021w] Disk device /dev/md/rdsk/d2 has read access for
group sys.
--WARN-- [perm021w] Disk device /dev/md/dsk/d11 has read access for
group sys.
--WARN-- [perm021w] Disk device /dev/md/rdsk/d11 has read access for
group sys.
--WARN-- [perm021w] Disk device /dev/md/dsk/d15 has read access for
group sys.
--WARN-- [perm021w] Disk device /dev/md/rdsk/d15 has read access for
group sys.
--WARN-- [perm021w] Disk device /dev/md/dsk/d14 has read access for
group sys.
--WARN-- [perm021w] Disk device /dev/md/rdsk/d14 has read access for
group sys.
--WARN-- [perm021w] Disk device /dev/md/dsk/d5 has read access for group
sys.
--WARN-- [perm021w] Disk device /dev/md/rdsk/d5 has read access for
group sys.
```

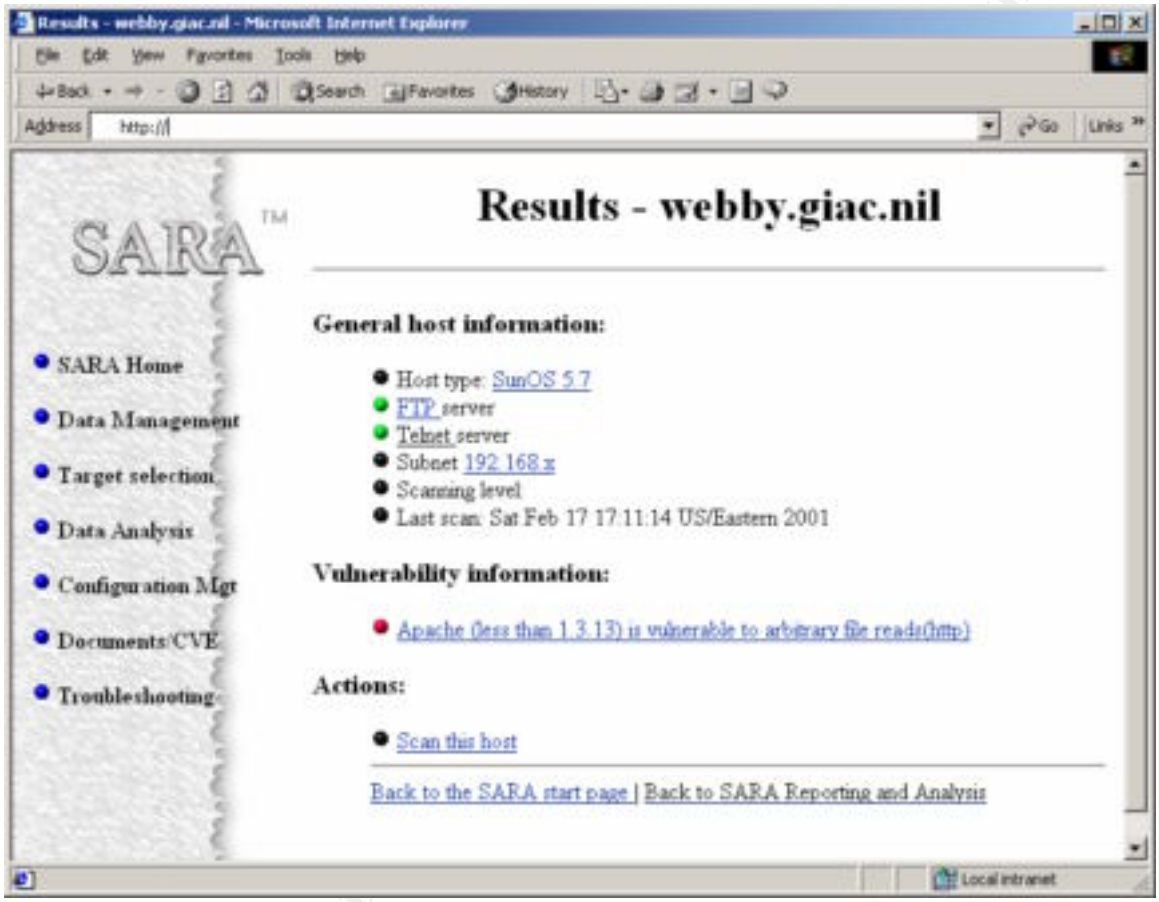
```
# Checking for known intrusion signs...

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

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

# Checking sendmail...

# Checking setuid executables...
--FAIL-- [fsys001f] File /etc/lp/alerts/printer is a setuid script:
-r-sr-xr-x   1 lp       lp           203 Sep 10  1998
/etc/lp/alerts/printer
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/4.0.8/bin/cmadmin has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/4.0.8/bin/cmctl has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/4.0.8/bin/cmgw has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/4.0.8/bin/dbsnmp has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/4.0.8/bin/oemevent has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/4.0.8/bin/onrsd has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/4.0.8/bin/oratclsh has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/4.0.8/bin/osslogin has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/4.0.8/bin/tnsping has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/4.0.8/bin/trcasst has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/4.0.8/bin/trcroute has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/4.0.8/ows/4.0/bin/owslctl has relative
pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/6i/bin/dbsnmp0 has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/8.1/bin/cmadmin has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/8.1/bin/cmctl has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/8.1/bin/cmgw has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/8.1/bin/dbsnmp has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/8.1/bin/lsnrctl has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/8.1/bin/oemevent has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/8.1/bin/onrsd has relative pathnames.
```

```
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/8.1/bin/oratclsh has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/8.1/bin/osslogin has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/8.1/bin/tnslsnr has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/8.1/bin/tnsping has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/8.1/bin/trcasst has relative pathnames.
--WARN-- [fsys002w] setuid program
/raid5/dba/oracle/product/8.1/bin/trcroute has relative pathnames.
--WARN-- [fsys002w] setuid program /usr/bin/nispasswd has relative
pathnames.
--WARN-- [fsys002w] setuid program /usr/bin/passwd has relative
pathnames.
--WARN-- [fsys002w] setuid program /usr/bin/yppasswd has relative
pathnames.
--WARN-- [fsys002w] setuid program /usr/lib/fs/ufs/ufsrestore has
relative pathnames.
--WARN-- [fsys002w] setuid program /usr/openwin/bin/kcms_calibrate has
relative pathnames.
--WARN-- [fsys002w] setuid program /usr/openwin/bin/kcms_configure has
relative pathnames.
--WARN-- [fsys002w] setuid program /usr/sbin/pgxconfig has relative
pathnames.
--WARN-- [fsys002w] setuid program /usr/sbin/static/rcp has relative
pathnames.

--INFO-- [fsys004i] The following setuid programs are non-standard:
-r-sr-xr-x root     bin      /usr/sbin/pgxconfig
-rwsr-s--x oracle   dba      /raid5/dba/oracle/product/4.0.8/bin/cmadmin
-rwsr-s--x oracle   dba      /raid5/dba/oracle/product/4.0.8/bin/cmctl
-rwsr-s--x oracle   dba      /raid5/dba/oracle/product/4.0.8/bin/cmgw
-rwsr-s--x oracle   dba
/raid5/dba/oracle/product/4.0.8/bin/oemevent
-rwsr-s--x oracle   dba      /raid5/dba/oracle/product/4.0.8/bin/onrsd
-rwsr-s--x oracle   dba
/raid5/dba/oracle/product/4.0.8/bin/osslogin
-rwsr-s--x oracle   dba      /raid5/dba/oracle/product/4.0.8/bin/tnsping
-rwsr-s--x oracle   dba      /raid5/dba/oracle/product/4.0.8/bin/trcasst
-rwsr-s--x oracle   dba
/raid5/dba/oracle/product/4.0.8/bin/trcroute
-rwsr-s--x oracle   dba      /raid5/dba/oracle/product/8.1/bin/cmadmin
-rwsr-s--x oracle   dba      /raid5/dba/oracle/product/8.1/bin/cmctl
-rwsr-s--x oracle   dba      /raid5/dba/oracle/product/8.1/bin/cmgw
-rwsr-s--x oracle   dba      /raid5/dba/oracle/product/8.1/bin/lsnrctl
-rwsr-s--x oracle   dba      /raid5/dba/oracle/product/8.1/bin/oemevent
-rwsr-s--x oracle   dba      /raid5/dba/oracle/product/8.1/bin/onrsd
-rwsr-s--x oracle   dba      /raid5/dba/oracle/product/8.1/bin/osslogin
-rwsr-s--x oracle   dba      /raid5/dba/oracle/product/8.1/bin/tnslsnr
-rwsr-s--x oracle   dba      /raid5/dba/oracle/product/8.1/bin/tnsping
-rwsr-s--x oracle   dba      /raid5/dba/oracle/product/8.1/bin/trcasst
-rwsr-s--x oracle   dba      /raid5/dba/oracle/product/8.1/bin/trcroute
-rwsr-s--x root     dba      /raid5/dba/oracle/product/4.0.8/bin/dbsnmp
-rwsr-s--x root     dba
/raid5/dba/oracle/product/4.0.8/bin/oratclsh
```

```
-rwsr-s--x root     dba      /raid5/dba/oracle/product/8.1/bin/dbsnmp
-rwsr-s--x root     dba      /raid5/dba/oracle/product/8.1/bin/oratclsh
-rwsr-sr-x root     other
/raid5/dba/oracle/product/4.0.8/ows/4.0/bin/owslctl


# Checking setgid executables...

--CONFIG-- [fsys003c] No setgid list... listing all setgid files

# Checking unusual file names...

# Looking for unusual device files...

# Checking symbolic links...

# Checking for writable directories...
--INFO-- [fsys008i] The following directories are world writable:
/raid5/dba/oracle/product/8.1/network/log/
/raid5/dba/oracle/product/8.1/network/trace/
/var/crash/
/var/dt/tmp/
/var/mail/
/var/preserve/
/var/spool/pkg/
/var/tmp/
/var/tmp/.oracle/
```

Appendix D – SARA

SARA uses an HTML browser-based interface to initiate scans and display the results. A screenshot of the scan results from *webby* is below.



Appendix E – Nessus

Nessus uses a graphical interface to run scans and display results. The output from this scan of *webby* has been saved in ASCII format for inclusion in this document. As noted earlier, since this scan was performed from a point on the private network inside the firewall, UDP ports do not appear in the output.

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

SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 0
 - Number of security warnings found : 3
 - Number of security notes found : 5


TESTED HOSTS

 192.168.x.y (Security warnings found)


DETAILS

+ 192.168.x.y :
 . List of open ports :
   o ftp (21/tcp) (Security notes found)
   o telnet (23/tcp) (Security warnings found)
   o time (37/tcp)
   o http (80/tcp) (Security notes found)
   o sunrpc (111/tcp)
   o unknown (443/tcp) (Security warnings found)
   o unknown (9000/tcp)
   o general/udp (Security notes found)
   o general/tcp (Security warnings found)


 . Information found on port ftp (21/tcp)

    Remote FTP server banner :
     webby ftp server (sunos 5.7) ready.


 . Warning found on port telnet (23/tcp)

    The Telnet service is running.
    This service is dangerous in the sense that
    it is not ciphered - that is, everyone can sniff
    the data that passes between the telnet client
    and the telnet server. This includes logins
    and passwords.

    You should disable this service and use OpenSSH instead.
    (www.openssh.com)
```

```
    Solution : Comment out the 'telnet' line in /etc/inetd.conf.

    Risk factor : Low
    CVE : CAN-1999-0619


. Information found on port telnet (23/tcp)

    Remote telnet banner :

    SunOS 5.7

. Information found on port http (80/tcp)

    The remote web server type is :
    Apache/1.3.12 (Unix) mod_ssl/2.6.5 OpenSSL/0.9.5a

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

. Warning found on port unknown (443/tcp)

    a web server is running on this port

. Information found on port unknown (443/tcp)

    The remote web server type is :
    Apache/1.3.12 (Unix) mod_ssl/2.6.5 OpenSSL/0.9.5a

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

. Information found on port general/udp

    For your information, here is the traceroute to 192.168.x.y :
    192.168.a.b
    ?

. Warning found on port general/tcp

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

    An attacker may use this feature to determine if the remote
    host sent a packet in reply to another request. This may be
    used for portscanning and other things.

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


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

Appendix E – Malice

Malice is a perl script that checks for known CGI-based vulnerabilities.

```
# perl malice5.2.pl

                    Malice .5.2

 Anti IDS scanner that uses null scans with HEAD requests

        Much props to doom for editing this.

Host: webby.giac.nil
Port: 80

HTTP/1.1 200 OK
Date: Sat, 17 Feb 2001 16:15:06 GMT
Server: Apache/1.3.12 (Unix) mod_ssl/2.6.5 OpenSSL/0.9.5a
Last-Modified: Tue, 13 Feb 2001 19:40:35 GMT
ETag: "243b7e-830-3a898db3"
Accept-Ranges: bytes
Content-Length: 2096
Connection: close
Content-Type: text/html

Checking webby.giac.nil for CGI holes.....:

webby.giac.nil either doesn't use CGI scripts, or has some tight
security


                    Malice .5.2

 Anti IDS scanner that uses null scans with HEAD requests

        Much props to doom for editing this.

Host: webby.giac.nil
Port: 443

HTTP/1.1 200 OK
Date: Sat, 17 Feb 2001 16:15:12 GMT
Server: Apache/1.3.12 (Unix) mod_ssl/2.6.5 OpenSSL/0.9.5a
Last-Modified: Thu, 20 Jul 2000 13:39:48 GMT
ETag: "204ca-37-39770124"
Accept-Ranges: bytes
Content-Length: 55
Connection: close
Content-Type: text/html

Checking webby.giac.nil for CGI holes.....:

webby.giac.nil either doesn't use CGI scripts, or has some tight
security
```

References

Documents

Common Issues and Vulnerabilities in Unix; Hal Pomeranz; Capitol SANS 2000
Unix Security Tools and Their Uses; Matt Bishop; Capitol SANS 2000
Topics in Unix Security; Steve Acheson, John Green, Hal Pomeranz; Capitol SANS 2000
Running Unix Applications Securely; Lee Brotzman, Hal Pomeranz; Capitol SANS 2000
Linux/Solaris Practicum; Lee Brotzman, Hal Pomeranz; Capitol SANS 2000
Securing Solaris Step by Step 1.0; Hal Pomeranz, SANS Institute; http://www.sans.org
Solaris Security; Peter H. Gregory; Prentice Hall/Sun Microsystems Press 2000

Software

Apache -- Home page for popular open-source web server; http://www.apache.org
fix-modes -- Fixes default permissions on files; ftp://ftp.fwi.uva.nl/pub/solaris/fix-modes.tar.gz
John the Ripper -- Password cracker; http://www.openwall.com/john/
logcheck -- System log parser; http://www.psionic.com/abacus/logcheck
Malice -- Web server/CGI scanner; http://packetstorm.securify.com/UNIX/cgi-scanners/malice5.2.pl
mod_ssl -- Apache interface to OpenSSL; http://www.modssl.org
Nessus -- Network-based security scanner; http://www.nessus.org
Nmap -- Network port scanner; http://www.insecure.org/nmap
NTP -- Network Time Protocol; http://www.ntp.org
OpenSSL -- Open source Secure Sockets Layer implementation; http://www.openssl.org
portmap and rpcbind -- Replacements for OEM versions; ftp://ftp.porcupine.org/pub/security/index.html
Revision Control System (rcs) -- Audit trail for configuration file changes; ftp://ftp.gnu.org/gnu/rcs
SARA -- Security Auditor's Research Assistant; http://www-arc.com/sara/
Secure Shell (ssh) -- OpenSSH; http://www.openssh.com
Sudo -- Granular control of elevated privileges; http://www.courtesan.com/sudo
Sun Microsystems -- Company home page; http://www.sun.com
SunSolve -- Patches for Solaris; http://sunsolve.sun.com
Swatch -- System log parser; http://www.stanford.edu/~atkins/swatch
syslog-ng -- Replacement for OEM syslog; http://www.balabit.hu/products/syslog-ng/
tcp_wrappers -- Filter by IP address; ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.tar.gz
TARA -- Tiger Analytical Research Assistant; http://www-arc.com/tara/
TITAN -- System security package; http://www.fish.com/titan/
Tripwire -- File integrity checker; ftp://coast.cs.purdue.edu/pub/tools/unix/Tripwire
YASSP -- Yet Another Solaris Security Package; http://www.yassp.org