Global Information Assurance Certification Paper

Juan Valbuena
GCUX version 1.9
Hardening Solaris 8 for Entrust Certification Authority
December 29, 2003

Abstract

This paper details the installation, configuration and a step-by-step procedure to harden a server that will function as a Certification Authority. Other security considerations such as logical and physical environment will be also discussed.

A Certification Authority is the core of any PKI implementation; hence the security surrounding this system is usually very high and should be supported by several security Policies such as a Certificate Practise Statement, Certificate Policy, PKI Disclosure Statement, Subscribers Agreements among others. The purpose of each of these policies is not within the scope of this paper.

This paper also discuss the Hardware and the Software required followed by a Risk Analysis identifying risk, threats, and vulnerabilities on this kind of system implementations.

At the end of this paper, the hardening process will be tested manually and with the use of other applications such as vulnerability assessment tools i.e. Nessus.

As this paper is about a Certification Authority implementation, PKI-specific concepts may be mentioned but not full explanation will be provided. Readers are expected to understand the behinds of Public Key Infrastructure. In some cases, short description may be provided as a footnote.

System Description

Within this section, the hardware and software components to be used are described. Normally these sorts of implementations (PKI) required more than one server, mainly for security reasons. For instance, the LDAP directory, which is used as certificate and revocation list repository, is meant to be public, while the CA is not. For the purpose of this PKI implementation, only one server will be used.

Hardware

The followings are the specifications for the server that has been chosen to set-up the Certification Authority (CA):

- Sun Fire V120
- UltraSPARC-IIe 648MHz

- 3072 MB of RAM
- 34730 MB of Hard Drive

Software

The Operating System (OS) used on this implementation is Sun Solaris version 8, with latest recommended patches.[1]

The CA, will required the following software:

- Critical Path LDAP-Directory version 4.0.1: Lightweight Directory Access Protocol (LDAP) directory software. It will be used as a repository for: Digital Certificates, Certificates Revocation Lists and Authority Revocation Lists (no used as it is a single CA). This is normally a corporate service component that uses LDAP protocol and is not specific to Entrust CA.
- Informix Database version 9.2.1: Database for the CA. It is used to store configuration information, subscribers details and backup encryption keys among other details.
- Entrust Authority version 6.0.1: Ultimate responsible to digitally sign and issue certificates for the subscribers of this PKI system.

Other software used will include:

- TCP Wrapper 7.6: Implements TCP Wrappers on this server to provide access to control for network services available i.e. SSH and FTPS
- OpenSSH 3.7.1: Implements SSH protocol on this server to provide secure shell connectivity. Used for administration purposes only.
- Libgcc 3.3.2: C Compiler libraries and other programs

Final System

Introduction

A PKI system is designed to provide trust to employees within a single organization or domain of trust by issuing digital identities that are recognised and trusted by other subscribers[2] or relying parties[3]

[1] Provided by SUN at http://sunsolve.sun.co.uk.
[2] PKI Subscribers are all entities (Persons or Devices) that are issued with a Digital Certificate within a PKI system.
[3] Relying parties are both subscribers and not-subscribers that trust other entities that have been issued with a digital certificate by a specific Certification Authority.

The main purpose of this PKI system is to function as an anchor of trust for subscribers and relying parties providing mechanisms to encrypt and to digital sign messages and files supporting also non-repudiation within a single organisation. PKI subscribers will be able to encrypt and/or digitally sign emails, perform local and permanent encryption (for individuals or group of individuals) as well as to trust others issued with digital certificates by the same CA i.e. web servers using SSL.

The main components of a PKI system are the CA, a database and a repository or directory. Normally, the CA and the Informix database are placed in highly secure environment available for just a few people for maintenance and administration purposes while the repository is made available for all subscribers and relying parties as they need to gather other's digital certificates and public keys (encryption) and verify that others' identity is still valid.

Interoperability – All together

This section describes how the three main components interoperate together. Also other systems or components not installed on this server may be mentioned. This section mentions extensively PKI concepts that are not in the scope of this article but if anybody interested, take the time to read Implementing PKI: A Real Challenge!! [See Reference section].

The way that the CA issues the certificates and manages their life cycle varies among PKI implementations. It is always different. In this case, the users will be initiated manually via Registration Authority (RA) software installed on a workstation and used exclusively by the PKI administrator.

Once the CA has issued a user with a certificate, the CA will store into the Database all relevant information for the new user, and the certificate will be published on the LDAP directory. The RA will be also used to revoke and recover user keys when lost by subscribers for any reason.

Users requiring other's subscribers Public keys (for encryption purposes) will get that users' digital certificate and public keys from the LDAP directory. Also when requiring to validate someone's identity, the LDAP directory will provide access to the Certificate Revocation List (CRL) which contains a list of certificates that have been revoked or expired and are not longer valid.

From time to time, subscribers might need to contact the CA for different causes such as key updates, key recovery, key revocation among others. In those cases, subscribers require a client application on their workstations to do so. This application will be configured to contact securely the CA and perform tasks needed[4].

[4] This client application varies from vendor to vendor. In this case, Entrust Entelligence will be required for such purposes.

Security

The CA system should be highly protected, as it is the main component of the PKI system. Should the CA be compromised, the entire trust domain will fall and be not operational anymore. To recover from this situation, re-deployment will be necessary.

It is necessary to implement security controls, both logical and physical, to prevent unauthorised access that may compromise the system. Here some recommendations.

Logical Security

The CA should be placed in a network logically isolated from the internal network, protected by a non-share firewall. No other services will be located inside this secure logical perimeter.

On the firewall only the following ports should be available as an inbound connections to the CA:

- TCP 709: Entrust Secure Exchange Protocol (SEP) from Internal network for Client request (old versions)
- TCP 710: Entrust Administration Service Handler (ASH) from Admin network for RA functions
- TCP 829: Entrust Public Key Infrastructure X.509 – Certificate Management Protocol (PKIX-CMP) from internal network for Client requests (version 5.0 and above)
- TCP 389: LDAP directory protocol from Internal Network
- TCP 22: SSH protocol from trusted administrators' workstations only

Remote access to the server should be only allowed to trusted administrators using SSH. TCP wrappers should be also used to control the access to the server. The access restriction should be by IP address, username and password. Not root user should be allowed to connect remotely, instead, users will use own username and password and SU to root once authenticated as a user.

Physical Security

The CA components (including the LDAP directory) should be located in a specific-built room inside the regular computer room. Normally, a computer room

is a large secure room where all the IT assets of a company are located. The idea now is to use that in-placed security controls to protect the CA as well but adding an extra layer: the new CA room.

Access to this room should be restricted to no one but the highly trusted support personnel or system administrators who are responsible for the installation and support of the PKI system. Strict security policies should be in place too. These policies will enforce security controls such as dual-control (at least two individuals present at any specific time), separation of duties (more than one person required to complete a sensitive task), and need-to-know (only people that has a reasonable reason for being there). These policies will need to be aligned to PKI policies such as CPS and CP.

Risk Analysis

As mentioned before, the CA is the anchor of trust of any PKI implementation, and in spite of that the general public does not access it directly, the risk of being compromise from internal individuals is still high. It is well known that the most of the attacks to a system occur from employees and other internal-to-an-organization users rather that from outsiders.

The following threats can be considered:

- Physical Damage: Fire, Natural disaster, theft and breakage
- Hardware Malfunction: Server hardware failure
- Software Malfunction: Application malfunction
- Insider Attackers: Employees and/or Subscribers
- Outsider Attackers: Others not belonging to the organization
- Loss of Data: Data loss by any mean

Threats such as physical damage, hardware or software malfunction could be mitigated using regular and well known controls such as good fire detection and suppression systems, physical access controls for external/internal people to the computer room (only authorised people should be allowed in), Service Level Agreements (SLAs) with vendors for support, backup for application, data and redundant hardware in place and ready to use.

Natural disasters are quite difficult to defend from, but be ready for them will mitigate the impact caused. Controls such as off-site backup, external disaster

recover sites (cold, warm or hot) or even replication sites, but not without a good, well defined, documented and tested emergency incident response process.

External attacks are possible, but as this system is not accessible from outside, outsiders do not represent a high risk here (not Zero though, let's say it is low). Also, it is assume that the internal network is already protected by two-tier firewall architecture with a well-defined and tuned security policy so only necessary and publicly available services are open on the first firewall but none on the second, what make even more difficult to the outsider to succeed on any attack to the CA server.

However, internal attacks do still represent some risk; some of them may be, but not limited to:

- Employees and/or subscribers that use the service provided improperly;
- Mis-management and Mis-configuration by trusted administrators and operators that may create security breaches on the system
- Subscribers and /or employees that penetrate the secure boundaries with the intention of compromise the system by changing configuration, destroying data, corrupting CA private keys among others;

Strict security policies, well trained administrators and operators, the use of secure utilities such as SSH for secure remote access, well-defined procedures to handle sensitive processes will deter and some times stop intruders gaining access into the system.

Step-by-Step Guide

Operating System Installation

The first step is to install the operating system. As describe previously, Solaris 8 will be used. The following is the step-by-step process to run the installation from the CD.

1. Insert the CD "Solaris 8 Software 01/02" into the server's CD room drive. Start the Open Boot[5] and type "boot cdrom" to boot from the CD. To access the OpenBoot, if you are connected to the console, send a break signal from the Terminal window and you will see the OK prompt.
2. The installation will start prompting for initial system configuration questions. Answers to this initial question may vary depending the situation. For this specific systems the following answers were provided.

[5] OpenBoot software is firmware that controls the boot process and provides useful diagnostic capabilities [SUN]. To enter into the OK prompt, power on the server and send a break signal from the terminal window.

Question	Answer
Language	*English (Option 0)*
Locale	*English C-7bit ASCII (Option 0)*
Terminal	*DEC VT100 (Option 3)*

3. The system will then show a short introduction to the installation process. Press **F2** key to continue[6].

4. Now the system will identify the networking information. Following answers were provided:

Question	Answer
Networked	*Yes*
DHCP	*No*
Primary NIC	*eri0*
Hostame	*GCUX-CA-Server*
IP Address	*192.168.0.99*
Part of a Subnet	*Yes*
Maks	*255.255.255.248*[7]
IPv6	*No*

5. A summary page will appear with all information previously entered, so if any of the answers was mistyped, this is the chance to correct it. If everything is OK, type **F2** to continue.

6. Next, whether or not Kerberos security is going to be configured. For this installation, Kerberos will not be used. A confirmation will be then received.

7. Next, naming services that will be used for this system. This will not use any, so **None** is the answer. Confirmation of this answer will be received.

8. Next, Time Zone where the system will reside needs to be configured. As the CA software is very sensitive about time, **GMT offset** is recommended. **Cero (0)** offset for this particular case as this server will be in the UK.

9. Date needs to be provided. Confirmation for time configuration appears. **F2** to continue.

10. By now, system identification is completed. Now installation script is started. When prompted, choose **Initial Installation** (normally **F4**) and then **Standard installation**

[6] Some systems will required to type "ESC" + "2" keys instead of the F2 key.
[7] This network mask will allow 6 hosts to be part of the same subnet (192.168.0.96/27)

11. Now is the time to choose the Solaris Software that will be installed. I used **Entire Distribution**. Installing this option will required a lot more space (2.3GB) than installing only the Core System (800MB) and also will add a lot more of unnecessary services and hardening at the end will need more steps, but installing only Core System you will need to add many other patches, some of them are unknown to me yet. Next you choose the hard drive where the system will be installed.

12. When prompted for the disk layout, choose manual and configure the file system as follow:

Slice #	*Partition*	*Size*	*Description*
0	*/*	*5120KB*	*Operating System*
1	*/swap*	*4096KB*	*Swap drive*
2	*Overlap*	*34730KB*	*Used by Solaris as the entire disk*
3	*/usr*	*2048KB*	*User Binaries*
4	*/opt*	*5120KB*	*Applications*
5	*/var*	*11175KB*	*Logs and Entrust Authority Backup*
6	*/ifmxdata*	*5120KB*	*Informix Database*
7	*/export/home*	*2048KB*	*User folders*
		34727KB	

13. Once the file system is confirmed, choose the source for the installation. If remote choose F4 and if local choose F2. Remote installation is not recommended for security reasons, as Network File System could introduce some vulnerabilities on the system[8]

14. The software installation will begin.

Securing OpenBoot

15. Once the software has been installed the server will reboot automatically. During the booting process, send a break signal from the terminal window to enter to the OpenBoot and setup an Openboot password

    OK> password

[8] CERT(*) Advisory CA-94:15, http://pintday.org/advisories/cert/ca-94_15.html

NB: This server should also be protected from people that may gain unauthorised physical access to the server and be able change the configuration of the system or even worse change the root password[9].

16. Assigned the security mode to "command", so before a command is executed, the firmware password is required[10]

    OK>setenv security-mode command

17. Activate the changes

    OK> reset

Post-Installation and Networking configuration

18. When the OS has been just installed, the root account is not protected with password yet. When prompted for Login user, type "**root**" and then **<Enter>**.

19. Set new password for the Root user by typing the command "**passwd**". Enter and confirm the new password for the root user.

    NB: The root user must have strong password, which should have no less than 8 characters, include upper and lower case characters, and numbers.

20. Configure the default router for this server, creating the defaultrouter file. This file should contain the default router IP address.

    #echo "192.168.0.98" > /etc/defaultrouter

21. Disable IP forwarding by creating notrouter file. This file will be empty.

    #touch /etc/notrouter

22. Prevent routing protocols from start at boot process. To do so, create in.routed and in.rdiscd files. These files should be empty as well.

    #touch /etc/in.routed /etc/in.rdiscd

23. The host file will perform naming resolution. No DNS will be used for the CA server. This needs to be reflected on the nsswitch configuration file. Copy nsswitch.files to nsswitch.conf to do so.

    #cp /etc/nsswitch.files /etc/nsswitch.conf

[9] Recover the root password is very simple and just need physical access to the server, the Solaris media (CD) and console access. See instructions at http://isp-lists.isp-planet.com/isp-solaris/0110/msg00043.html - How to recover a root password.
[10] to disable this password, set the environment variable to none instead of command

Verify the host file will be used to resolve names for host. A line similar to this one should appear

hosts: files

To do so, type

#more /etc/nsswitch.conf

24. Reboot the server

#reboot

Recommended Patches Installation

25. Download the recommended Solaris patch cluster from http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access.

26. Using FTP, transfer the file (8_Recommended.zip) to the server and save it on /tmp directory. Uncompress the file using unzip:

unzip 8_Recommended.zip

The Directory 8_Recommended will be created (/tmp/8_Recommended).

27. Install the cluster by typing:

#./install_cluster –q –nosave

28. Reboot the server

#reboot

Application Installation and Configuration

At this stage we will install the Certification Authority and all its supporting software; LDAP Directory and Informix Database. If using Hardware Security Module[11] (HSM) this also the time to install it and configure it.

It is recommended that the applications should be installed before hardening otherwise it may not work properly. For instance, applications like the Informix

[11] HSM is a tamper-proof security device that stores the cryptographic keys used by the CA. [Chrysalis and nCipher]

database will not work and entrust authority may not go through the configuration process. Also, during this installation, system files are modified and many system users are created, which will require some files to be re-harden again i.e. /etc/passwd, /etc/group.

The overall installation plan is as follow:

1. Pre-installation tasks
2. Install LDAP Directory Software
3. LDAP directory creation for the CA
4. Install and configure Informix Database
5. Install and configure Certification Authority (CA) software
6. Create the instance of the Certification Authority (CA's Keys generation)

Pre-installation

A. User Accounts and Groups: Application such as Critical Path LDAP directory, Informix Database and Entrust CA required specific users to be created. The following users/groups need to be created (name; group; home directory)

- idsadmin; ids; /exports/home;
- informix; informix; /export/informix;
- entrust;entrust; /export/entrust;
- master1;entrust;export/entrust;
- master2;entrust;export/entrust;
- master3;entrust;export/entrust;

B. Kernel Configuration: Informix database requires a specific kernel configuration parameters, so the following lines need to be added to the /etc/system file[12]

```
set shmsys:shminfo_shmmax=268435456
set shmsys:shminfo_shmmin=100
set shmsys:shminfo_shmmni=100
set shmsys:shminfo_shmseg=100
set semsys:seminfo_semmap=64
```

[12] Make a copy of any file that you are intending to modify

```
set semsys:seminfo_semmni=4096
set semsys:seminfo_semmns=4096
set semsys:seminfo_semmnu=4096
set semsys:seminfo_semmsl=100
set semsys:seminfo_semume=64
set noexec_user_stack=1
```

C. Directories creation: The following directories need to be created for the Informix Database and Entrust Backup.

- /var/ifmxdata
- /var/entbkup/

29. Create the following groups by typing:

```
#groupadd ids

#groupadd informix

#groupadd entrust
```

30. Create the following user accounts by typing:

```
#useradd –d /export/home/idsadmin –m –g ids idsadmin

#useradd –d /export/home/informix –m –g informix informix

#useradd –d /export/home/entrust –m –g entrust entrust

#useradd –d /export/home/entrust –m –g entrust master1

#useradd –d /export/home/entrust –m –g entrust master2

#useradd –d /export/home/entrust –m –g entrust master3
```

31. Copy to a backup file the /etc/system file by typing

```
#cp /etc/system /etc/system.bk
```

32. Add the following lines at the end of the /etc/system file

```
# cat <<'FF'>>/etc/system
*Added for Informix database
set shmsys:shminfo_shmmax=268435456
set shmsys:shminfo_shmmin=100
set shmsys:shminfo_shmmni=100
set shmsys:shminfo_shmseg=100
set semsys:seminfo_semmap=64
```

```
set semsys:seminfo_semmni=4096
set semsys:seminfo_semmns=4096
set semsys:seminfo_semmnu=4096
set semsys:seminfo_semmsl=100
set semsys:seminfo_semume=64
set noexec_user_stack=1
FF
```

33. Create the entrust backup directories by typing:

```
#mkdir /var/entbkup
```

34. Change ownership and permissions for the following directories

```
# chown entrust:entrust /var/entbkup

# chown informix:informix /ifmxdata
```

35. Reboot the server by typing:

```
#reboot
```

LDAP Installation

It is important that the Distinguished Name (DN) for the CA has been defined already and that the PKI vendor has provided the schema for this LDAP server; Entrust Technologies in this case.

For this installation the CA DN will be: **cn=ca-gcux,o=sans-practical,c=GB**

We will use a command line tool included in the software to be used for Entrust implementations.

36. Insert the Critical Path LDAP directory software on the CDROM

37. Mount the CD drive:

```
#mount –F hsfs /dev/dsk/c0t0d0s0 /cdrom
```

38. Install the package by typing:

```
#pkgadd –d /cdrom IDS
```

39. Answer the questions using the following information:

User to administer IDS	idsadmin
Which group will idsadmin belong to?	ids
Should user belonging to this group be able to run LDAPservices on low ports numbers?	y
Path to install the software	/opt/ids/ids4
Do you want automatic iCon service?	n
location of iCon	/opt/ids/iCon
Default port for iCon	1500
IP address	192.168.0.99
idsadmin uses /bin/sh, do you want to update the .profile?	y
idsadmin uses /bin/sh, do you want to update the .cshrc?	y
Path to package base directory	/opt/ids/ids4

LDAP Instance Creation

Now that the LDAP software has been installed, we will create the instance that will hold the CA information.

40. As root, create a directory that will hold the LDAP directory data. This directory will be created on /opt/ids/gcux-ldap.

    #mkdir /var/gcux-ldap

41. Change ownership to idsadmin and group ids

    #chown idsadmin:ids /var/gcux-ldap

42. Change to idsadmin user by typing:

    #su – idsadmin

43. From /var/gcux-ldap, create the instance by typing:

    #odsecreate

44. Answer the questions as follow:

name of DSA	cn=gcux-dsa
DSA Administrator	cn=manager
DSA Administrator password	Passw0rd[13]
The DSA can support RFC1006 comms, or IDM, or both	y

[13] Do not use symbols on this password, but still use strong password

Will the DSA support RFC1006 comms (Y/N) ?	
Please enter the port number for RFC1006 DAP/DSP	1750
Please enter the port number for RFC1006 shadowing. Press return for no shadowing, this can be added later	<Enter>
Shadowing protocol will not be added Will the DSA support IDM comms (Y/N) ?	n
Please enter the port number for LDAP. Press return for no LDAP, this can be added later	389
Please enter the license key	XXXXXX[14]
Do you wish to include the extensibleObject defined in RFC 2252 (Y/N) ?	n
Do you wish to include the Java(tm) Objects schema defined in RFC 2713 (Y/N) ?	n
Do you wish to include the CORBA Objects schema defined in RFC 2714 (Y/N) ?	n
Please enter 'Y' to configure an empty Entrust DSA or 'N' to add the CA, Search Base (CP) and EntrustDirectory Manager entries.	n
Please enter the name of the search base in the	c=GB
Please enter the name of the CA in the DSA	cn=ca-gcux,o=sans-practical,c=GB[15]
You have requested a CA using an attribute type of 'cn' The object class of the CA is also required. This can be: 'or' for organisationalRole or 'ap' for applicationProcess or 'de' for device. Please enter the CA's object class	ap
CA's password	Passw0rd
Entrust Directory Manager	cn=dir_manager
Entrust Directory Manager's password	Passw0rd
Do you wish to start the DSA	y

Informix Database Installation

45. Insert the Informix Database Software CD on the CD Rom and mount the CD drive if necessary

    #mount –F hsfs /dev/dsk/c0t0d0s0 /cdrom

46. From the based directory, start the installation script

[14] Provide license information provided by the vendor
[15] No spaces

```
# ./install.sh
```

47. Agree with the License Agreement (if you really agree)
48. Agree as well on the packages to be installed
49. Answer the coming questions using the following the table above

Installation directory	/opt/informix9.21
Number of users for data sizing (5000 - 190000)	XXXX
This will use approximately XXX MB of data. OK (y/n) ? [y]	y
Mirroring	<Enter> (No mirroring)

Entrust Certification Authority Software Installation

50. Insert now the Entrust Authority software CD into the CD-Rom drive
51. Mount the CD-rom if is not already
52. Execute the installation script from the CD-Rom

```
#./install.sh
```

53. Accept the Licence Agreement (If you agree)
54. Accept all the packages to be installed
55. Answer all the ongoing questions using the information on the table above

CA Software location directory	/opt/entrust/authority6
User that owns the installation	entrust
Group that owns the installation	entrust
Install Documentation	n
Configure the CA now	y
Location of the CA instance	/opt/authdata/gcux-ca
License Serial Number	XXXXXXX
Enterprise Users limit	10
Enterprise License Code	CCCCCC
No web license to be installed	<Enter>
Is the Directory Service running using Microsoft Active Directory?	n
IP Address of LDAP Directory	192.168.0.99
TCP Port Number LDAP	389
Version of LDAP	v.3
CA DN	cn=ca-gcux,o=sans-practical,c=GB
CA DN password	Passw0rd
DN for First Officer	Accept default
Dir Administrator	cn=dir_manager

Dir Administrator password	Passw0rd
Port for Entrust Secure Exchange Protocol (SEP)	default (709)
Entrust Administration Protocol port [710]	default (710)
Port for Certificate Management Protocol (PKIX-CMP)	default (829)
Are you using a hardware device for the CA keys (y/n) ? [n]	n
Enter the algorithm that Entrust/Authority will use to digitally sign certificates.	RSA 2048
Enter the algorithm that you would like Entrust/Authority to use for certificate hashing.	SHA1
Enter the algorithm that will be used for creating Entrust users' digital signatures	RSA 1024
Enter the algorithm that will be used for creating Entrust users' encryption key pairs	RSA 1024
Do you wish to interoperate with Microsoft (TM) CryptoAPI-enabled Applications? (y/n) ? [n]	n
Name for the Informix database	gcux-ca
Enter the algorithm that will be used for database encryption	cast-128
Enter the full pathname of the UNIX directory that will be used for storing backups of the database:	/var/entbkup/gcux-ca
Root or Subordinate	root
Enter the CA certificate lifetime in months (120-420)[240]	120
Enter the CA private key usage period (20-100)[100] >	100
Enter the policy certificate lifetime in days (1-3650)[30]	30

56. Once all the information above has been entered, a confirmation page appears. Verify all details have been entered properly. Type **yes** if agree.

57. At the end of the configuration process, a question if the CA is to be initialised. Choose initialise with Command Line Master Control. (Option 2)

Initialise The CA

58. The command line master control will start. Once in there, initialise the CA by typing:

```
entsh$ init
```

59. Provide the following roles passwords[16]:

    - Master User 1
    - Master User 2
    - Master User 3
    - First Officer

Starting the CA service

To start the CA service, you will need to start the following applications in specific order: LDAP directory, Informix database and the Entrust Authority. I am assuming, user is log into the sever as a root

60. To start the LDAP directory

    #su – idsadmin

    #cd /var/gcux-ldap

    #odsstart

    #exit

61. Start the Informix Database

    #su – entrust

    #cd /opt/entrust/authdata/gcux-ca

    #. ./env_settings.sh[17]

    #startstop.sh start ifmx

62. Start the Entrust Authority

    #entsh

    entsh$ login

    Login as a Master User 1 (Master1)

    cn=ca-gcux,o=sans-practical,c=GB.Master1 $ service start

[16] These passwords are meant to be very strong. Actually, the Master Control will only accept passwords longer that 8 characters, mix between upper and lower cases and digits.
[17] Notice that there two dots ". ." before the "/"

Verify system is UP

#service status

```
sep Entrust SEP              enabled  up  2 processes
keygen  Key Generator        enabled  up  1 processes
backup  Automatic Backup     enabled  up  1 processes
integ   Database Integrity Check  enabled  up  1 processes
amb     CRL and Maintenance  enabled  up  1 processes
ash     Admin Service Handler  enabled  up  4 processes
cmp     PKIX-CMP             enabled  up  2 processes
```

The Hardening

Create Statutory Banners

Statutory banners are important to warn users about the proper use of this server and the implication of unauthorised access to the system. As these banners may have legal implication, the legal department of the organization should approve them. The banners are created on these two files: /etc/issue and /etc/motd. The following is just an example of a statutory banner.

> "Authorise Users only. Activity may be monitored. Any unauthorised access could be prosecuted"

63. Create /etc/issue and /etc/motd files

    #echo "Authorise Users only. Activity may be monitored. Any unauthorised access could be prosecuted" > /etc/issue

    # echo "Authorise Users only. Activity may be monitored. Any unauthorised access could be prosecuted" > /etc/motd

64. Eliminate the "welcome" message for Telnet service. These banners may provide too much information to an intruder.

    #echo "BANNER=\"\"" > /etc/telnetd

65. Eliminate "welcome" message for FTP service

    #echo "BANNER=\"\"" > /etc/ftpd

66. Modify permissions and ownership for the banner files

    #chmod 644 /etc/issue /etc/issue

    #chown root:sys /etc/motd

    #chown root:root /etc/issue

67. Modify banner in the eeprom

    #eeprom oem-banner=" Authorise Users only. Activity may be monitored. Any unauthorised access could be prosecuted"

    #eeprom oem-banner\?=true

The login file

68. Prevent the root user to be able to login remotely to the system. Edit the /etc/default/login file

    #vi /etc/default/login

    Uncomment (remove the symbol # in front of "") CONSOLE line. The line should read similar to "*CONSOLE=/dev/console*"

69. Limit the maximum number of attempts allowed for a user to fail login to the server. Once the limit has been reached, the user will initiated again the login process

    Locate RETRIES and make the line similar to "RETRIES=3" to limit the maximum number to 3.

User Accounts

70. By default, root working directory is / and attackers will try to modify profile and login configuration files on this directory to gain access to the system. Modify the location of the home directory for the root user is then recommended.

    #passmgmt –m –h /export/home/root root

71. Change to a null shell all these users with system accounts or other users that are not regular users. Some of these users but not limited to are: adm bin lp smmsp nobody noaccess uucp nuucp smtp listen nobody4. To modify this, use the following command:

    ```
    #for user in adm bin lp smmsp nobody noaccess \
    uucp nuucp smtp listen nobody4 daemon sys; do
    passwd -l $user
    passmgmt -m -s /dev/null $user
    done
    ```

72. Verify that there are not user accounts with empty passwords

    #logins –p

    This should return no lines.

73. Create default UMASK for root:

```
#echo “umask 077” >> /export/home/root/.profile
```

74. Create default UMASK for users. This script modify the default for users at the /etc/default/login file

```
# cd /etc/default

#awk '/UMASK=/ { $1 = "UMASK=077" };{ print }' login >login.new

#mv login.new login

#chown root:sys login

#chmod 444 login

#echo umask=077 >>ftpd

#echo umask 077 >>/etc/profile

#echo umask 077 >>/etc/.login
```

Disabling no-needed network services

Inetd normally controls the network services that will be active on the server. For this particular case, the CA server will not require any of these services, so inetd can be deactivated.

As stated previously, only one network services will be required on this server: SSH for remote administration. For more information about inetd.conf file see reference section [10 & 11].

75. The following scripts will remove all services not required for this server:

```
        #cd /etc/inet
        # for svc in time echo discard daytime chargen fs dtspc \
exec comsat talk finger uucp name xaudio sun-dr; do
awk "(\$1 == \"$svc\") { \$1 = \"#\" \$1 }; {print}" \
inetd.conf >inetd.conf.new
mv inetd.conf.new inetd.conf
done


#for svc in 100068 100146 100147 100150 100155 100221 \
100232 100235 100234 100134 100083 rquotad \
rstatd rusersd sprayd walld 300326; do
awk "/^$svc\/ { \$1 = \"#\" \$1 }; { print }" \
inetd.conf >inetd.conf.new
mv inetd.conf.new inetd.conf
done
```

```
#for svc in printer shell login telnet ftp tftp; do
awk "(\$1 == \"$svc\") { \$1 = \"#\" \$1 }; {print}" \
inetd.conf >inetd.conf.new
mv inetd.conf.new inetd.conf
done
```

76. Change ownership and permissions to the inetd.conf file.

```
# chown root:sys inetd.conf

# chmod  444 inetd.conf
```

Inetd Service

77. Modify the inetsvc starting script to not start the inetd service.

    The following script will do this by deleting the line starting the inetd.

```
#cd /etc/init.d

# grep -v /usr/sbin/inetd inetsvc >newinetsvc
```

78. Change ownership and permissions for the new inetsvc file (newinetsvc)

```
#chown root:sys newinetsvc

#chmod 744 newinetsvc
```

79. Delete current starting script on /etc/rc2.d and create a new link to the new modified script.

```
# rm -f /etc/rc2.d/S72inetsvc

#ln -s /etc/init.d/newinetsvc /etc/rc2.d/S72inetsvc
```

Syslog

80. As this server is not intended to be a logging server, Syslog should be unable to listen to external request on port UDP 514 to log data from other servers. So, the starting script for Syslog, syslogd, should be modified to be started with the option –t, that means that will not listen to external requests on port UDP 514. The following script will create the new starting syslogd file.

```
# awk '$1 ~ /syslogd/ && !/-(t|T)/ { $1 = $1 "  -t" };\
{ print }' /etc/init.d/syslog >/etc/init.d/newsyslog
```

81. Same as with other starting scripts modified, we need to change ownership and permissions.

```
#chown root:sys /etc/init.d/newsyslog

#chmod 744 /etc/init.d/newsyslog
```

82. Now, let's replace the old script link with the new one. This script is also located on /etc/rc2.d

```
#rm -f /etc/rc2.d/S74syslog

#ln -s /etc/init.d/newsyslog /etc/rc2.d/S74syslog
```

Disable Start scripts from RC2 and RC3 directories

83. Disable other services. All services in the for-in list will be disable by adding "_NO" in front of each file. The following script will do so:

```
#cd /etc/rc2.d
#for file in S47asppp S89bdconfig S47pppd S90wbem S75cron \
S91afbinit S75flashprom S91ifbinit S92volmgt S71ldap.client S76nscd \
S93cacheos.finish S94ncalogd S95ncad S72autoinstall S80PRESERVE \
S70uucp S72inetsvc S80lp S20sysetup S72slpd S80spc S99dtlogin \
S73cachefs.daemon S85power S73nfs.client S88sendmail S40llc2 \
S74autofs S71rpc; do
[ -s $file ] && mv  $file _NO$file
done

#cd /etc/rc.3
#for file in S34dhcp S50apache S76snmpdx S80mipagent; do
[ -s $file ] && mv $file _NO$file
done
```

Kernel Tuning

We will now start adding few lines to the system file, with the intention of tuning the system kernel and reduce some of the vulnerabilities of the system. It is recommended to start with a comment line explaining the purpose for each of the line or group of lines (same purpose). Comments on the system file begin with start (*) symbol.

84. Disable core dumps by adding the following line at the end of the /etc/system file.

```
# cat <<'FF'>>/etc/system
* Disable the system to generate dump files
```

```
set sys:coredumpsize = 0
FF
```

85. Log and prevent buffer overflow attacks

```
# cat <<FF>>/etc/system
*Prevent stack crashes
set nonexec_user_stack=1[18]
set nonexec_user_stack_log=1
FF
```

86. Modify the Network Settings parameters. Download the nddconfig from http://www.sun.com/solutions/blueprints/tools/. Copy the nddconfig script into the server and follow implementation procedures [19]

```
#cp nddconfig /etc/init.d/nddconfig

#chmod 744 /etc/init.d/nddconfig

#chown root:sys /etc/init.d/nddconfig

#ln /etc/init.d/nddconfig /etc/rc2.d/S70nddconfig
```

This script contains recommended values for IP, TCP and UDP parameters. If necessary, these values can be modified directly on the nddconfig script and next reboot, changes will take effect.

87. Remote services such as rexec, rlogin and rsh are often targeted for attacks as they are weak and easy to break. Prevent the attacker to write to its configuration files is important.

```
#touch /.rhosts /.netrc  /.shosts /etc/hosts.equiv

#chmod 000 /.rhosts /.netrc  /.shosts /etc/hosts.equiv
```

88. Attackers using system accounts may gain unauthorised access into the system using services such as FTP. Configuration files such as /etc/ftpusers should include a list of users that cannot use FTP service. It is a good practise to include all users from the /etc/passwd file into the /etc/ftpusers file. One way of doing this is:

```
#cat passwd | cut –f1 –d: > /etc/ftpusers
```

[18] The line is also recommended by Informix database
[19] Solaris Operating Environment Network Settings for Security, By KeithWatson - Alex Noordergraaf, Sun BluePrints™ OnLine - December 2000. http://www.sun.com/solutions/blueprints/1200/network-updt1.pdf

#chmod 600 /etc/ftpusers

#chown root:sys /etc/ftpusers

89. Only root user should be running CRON jobs. To only allow root to run CRON jobs, /etc/cron.d/cron.allow and /etc/cron.d/at.allow are created.

#cd /etc/cron.d

#rm -f cron.deny at.deny

#echo root >cron.allow

#echo root >at.allow

#chown root:root cron.allow at.allow

#chmod 400 cron.allow at.allow

90. Configure the NTP service to listen to a specific server. This service is necessary and recommended for the CA server for time accuracy. The NTP server used for this server to gather the time from is 10.0.0.1. the /etc/ntp.conf file is configure as follow:

#echo “server 10.0.0.1”> /etc/ntp.conf

Logging Activity

Logging activity is very useful control to detect if a system has been compromised or if there has been an attempt to do it.

91. To capture logging information, add the following line to /etc/syslog.cong file

#echo “auth.info \t\t\t/var/log/authlog/” >>/etc/syslog.conf

#touch /var/log/authlog

#chown root:sys /var/log/authlog

#chmod 600 /var/log/authlog

92. To start logging fail logging attempt messages, the file loginlog needs to exist. The parameter SYSLOG_FAILED_LOGINS might be modified as well to determine how many attempts need to occur before a log entry is generated. 0 means that all fail attempts generate an entry.

#touch /var/adm/loginlog

#chown root:sys /var/adm/loginlog

#chmod 600 /var/adm/loginlog

```
#cd /etc/default

#awk '/SYSLOG_FAILED_LOGINS=/ \

{ $1 = "SYSLOG_FAILED_LOGINS=0" }; \

{ print }' login >login.new

#mv login.new login

#chown root:sys login

#chmod 444 login
```

93. Cron tasks should also be logged, as any unusual activity could be detected by the administrator. To enable logging for CRON tasks, modify the parameter CRONLOG in the file /etc/default. The line should look similar to “CRONLOG=YES”

```
# cd /etc/default

#awk '/CRONLOG/ { $1 = "CRONLOG=YES" }; { print }' cron > cron.new

#mv cron.new cron

#chown root:sys cron

#chmod 444 cron
```

File System Security

94. Apply fix-modes to the servers. To do this, download from ftp://ftp.science.uva.nl/pub/solaris/ the file fix-modes.tar.gz into the server.[20]

```
# gunzip fix-modes.tar.gz

#tar xvf gunzip fix-modes.tar

#make

#fix-modes
```

95. Read only option for /usr and nonsuid for others file systems. I find it safer to run an script to perform this change, as if you do a small mistake during the file modification, you will loose access to your file system, in which

[20] For more information about Fix-modes, please read the README.fix-modes inside the tar file. It is also possible to get a pre-compiled copy of this application.

case, you will need to boot from other media i.e. Solaris Installation CD, mount the file system manually and rollback the changes. Anyway, the script I used is as follow[21]

```
#awk '($4 != "ufs" || $3 == "/" || $3 == "/opt") { print; next; }
($3 == "/usr") { $7 = "ro"; print; next; }
($3 != "/" || $3 != "/opt") { $7 = "nosuid"; print; }' \
vfstab-BK >vfstab.new

#mv vfstab.new vfstab

#chown root:sys vfstab

#chmod 664 vfstab
```

NB: As you can notice, I have not set the nosuid on /opt directory. This is because applications not always work with it. For instance, Informix database will not even start.

Open SSH installation

To install Open SSH, few other applications are required, but before anything else the Solaris patch **112438-02** needs to be installed. Download the patch from **http://uk.sunsolve.sun.com/pub-cgi/retrieve.pl**. Transfer the ZIP file then to the server.

96. Uncompress the file by typing:

    ```
    #zip 112438-02.zip
    ```

    A directory named 112438-02 will be created. This directory contains all the packages required for this patch and also the README.112438-02 file that contains instructions to install the patch.

97. Install the patch 112438-02 by typing

    ```
    #patchadd ./112438-02/
    ```

98. Then, download the following packages from **http://sunfreeware.com**

    - openssh-3.7.1p2-sol8-sparc-local.gz
    - openssl-0.9.7c-sol8-sparc-local
    - libgcc-3.3-sol8-sparc-local

[21] Taken from Solaris Benchmark

- tcp_wrappers-7.6-sol8-sparc-local.gz

99. Transfer all files to the server and uncompress them using gzip

    #gunzip <name of the gz file>

100. Install all packages above by typing

    #pkgadd –d openssh-3.7.1p2-sol8-sparc-local

    #pkgadd –d openssl-0.9.7c-sol8-sparc-local

    # pkgadd –d libgcc-3.3-sol8-sparc-local

    # pkgadd -d tcp_wrappers-7.6-sol8-sparc-local

101. Reboot the server by tying

    #reboot

102. Include /usr/local/bin and /usr/local/sbin directories in the root PATH directory. Add these tow directories to the PATH variable by typing:

    #echo PATH=:$PATH:/usr/local/bin:/usr/local/sbin >> /export/home/root/.profile

103. Create a new directory /var/empty by typing:

    #mkdir /var/empty

    This directory is required by SSH 3.7.1p2 as a new security method called privilege separation, by which operations that require root privilege are performed by a separate privileged monitor process[22]

    NB: This file should not contain any files.

104. Change the directory ownership to **root** and group to **sys** by typing

    #chown root:sys /var/empty

105. Change the directory permissions to 755 by typing

    #chmod 755 /var/empty

106. Create a new group called sshd by typing

[22] http://www.sunfreeware.com/README.privsep

```
#groupadd sshd
```

107. Create a new user called “sshd privsep” by typing:

```
# useradd -g sshd -c 'sshd privsep' -d /var/empty -s /bin/false sshd
```

108. Generate the keys for the server by typing:

```
# ssh-keygen -t rsa1 -f /usr/local/etc/ssh_host_key -N ""

# ssh-keygen -t dsa -f /usr/local/etc/ssh_host_dsa_key -N ""

# ssh-keygen -t rsa -f /usr/local/etc/ssh_host_rsa_key -N ""
```

109. Create and open sshd_config file. SSH deamon reads the configuration parameters from this file. More information about this file can be found at http://www.biostat.wisc.edu/cgi-bcg/man.cgi?section=5&topic=sshd_config

```
#cat <<'FF'>>sshd_config
ListenAddress 192.168.0.99:22
Protocol 2
SyslogFacility AUTH
LogLevel INFO
PidFile /etc/sshd.pid
HostDSAKey /usr/local/etc/ssh_host_dsa_key
HostKey /usr/local/etc/ssh_host_key
KeyRegenerationInterval 900
ServerKeyBits 1024
LoginGraceTime 180
X11Forwarding no
StrictModes yes
KeepAlive no
UseLogin no
CheckMail no
PrintMotd no
PasswordAuthentication yes
PermitEmptyPasswords no
PermitRootLogin no
IgnoreRhosts yes
RhostsAuthentication no
RhostsRSAAuthentication no
IgnoreUserKnownHosts yes
RSAAuthentication yes
DSAAuthentication yes
FF
```

110. Set ownership and permissions to sshd_config file as follow:

```
#chown root:root /etc/sshd_config

#chmod 600 /etc/sshd_config
```

111. Create a start/stop script file to start SSH daemon at boot. Use a text editor like VI to create this file.

#vi /etc/init.d/sshd

Add the following lines to this file:

```
#!/sbin/sh
case "$1" in
'start')
if [ -x /usr/local/sbin/sshd -a -f /etc/sshd_config ]; then
/usr/local/sbin/sshd -f /etc/sshd_config
fi
;;
'stop')
kill `cat /etc/sshd.pid`
;;
*)
echo "Usage: $0 { start | stop }"
;;
esac
exit 0
```

112. Change the ownership of the sshd file and make it executable

#chwon root:root /etc/sshd

#chmod 744 sshd

113. Link it to a file on RC2 directory. This will start SSH service at boot time.

#cd /etc/rc2.d

#ln –s ../init.d/sshd S75sshd

TCP Wrappers

At this stage we will configure TCP wrappers on the system. The TCP wrapper package has been added in previous steps above. More information about TCP wrappers can be found on:

http://www.sunfreeware.com/README.tcpwrappers

In short, the TCP wrapper will provide monitoring and filtering for incoming requests using protocols like FINGER, FTP, TELNET, RLOGIN, RSH among others. This server will be only using SSH and all other services will be disable.

114. Create the host.allow and host.deny files. These files will be used to allow or deny connections to this server on specific protocols or network services

#touch /etc/hosts.allow /etc/hosts.deny

#echo sshd:192.168.1.1[23] > /etc/hosts.allow

#echo ALL:ALL > hosts.deny

115. Set ownership and permissions to hosts.allow and hosts.deny files as follow:

#chown root:root /etc/hosts.allow /etc/hosts.deny

#chmod 600 /etc/hosts.allow /etc/hosts.deny

Ongoing Maintenance

Regular Backup

System backups are not only important in the event of a disaster or hardware malfunction but also when a system has been compromised and the last known clean backup will need to be restored. Backups may be divided in different types: Operating system files, Application Files and Data files.

In this particular case, system and application backups are important but not critical for the system. But the data loss may cause the whole system to fall and the need to start over again deployment, what may cost to the company quite a lot, not only in time but also in productivity (in case PKI is required for day-to-day job).

Data incremental backups should be scheduled daily while full backups should be schedule at least once a week. Off-site vault is a must.

Database replication is also an option for this kind of system, but as cost is quite high, it will depend on a cost/benefit analysis to determine whether it is worth to spend the budget or not.

Patching

Keeping the system up-to-date is very critical as security vulnerabilities are discovered every day. Sun website is the best place to get latest patches. Also is recommended that the System Administrator subscribe himself to a distribution lists about new vulnerabilities and countermeasures.

Log Files Checking

[23] This IP address is just an example of a single workstation to be used. If more, a list of IP addresses can be added or if possible a sub-network.

As mentioned before, the logs on the system may be one of the best mechanisms to detect when a possible attack has occurred. However, log files can be quite large and difficult to read and time consuming for an administrator making this as not very useful tool. Therefore, the use of parsing scripts to filter known-to-be-ok information out of the "unusual behaviour".

There are also several tools available on the market to this job. There are some of this tools that will function as a Host-based IDS, detecting unusual activity based on the log files.

It is also important to include a log rotation script. Logging information may cause the system to fill up complete file systems and bring the system down. Log files require to be archived on a periodic basis.

Vulnerability Assessment

The best way to ensure the system is as secure as it was after the first hardening is to perform a vulnerability assessment periodically, so if flaws have been some how inserted into the system they can be detected. The most often we do this vulnerability assessment the higher the assurance that the system is kept to an appropriate security level.

Checking Configuration

Verify applications are running

I think the first thing to verify is if the server is doing its job. the best way to do it is to check if the LDAP, Informix and Entrust processes are running. This can be accomplished by running the command "ps –ef" and the outcome should be similar to:

```
   UID   PID  PPID  C    STIME TTY      TIME CMD
idsadmin  292     1  0 18:00:43 ?       0:00 odssched
idsadmin  293   292  0 18:00:43 ?       0:00 odsmdsa -d"/var/gcux-ldap"
idsadmin  294   292  0 18:00:43 ?       0:00 odssdsa
idsadmin  295   292  0 18:00:43 ?       0:00 odscomms -P0
   root  296   292  0 18:00:43 ?       0:01 odsldap3 -ldap:389 -ldaps:0 -http:0 -https:0 -charsetv2:iso8859-1
   root  354   352  0 18:06:30 ?       0:00 /opt/informix/bin/oninit
   root  355   352  0 18:06:31 ?       0:00 /opt/informix/bin/oninit
   root  353   352  0 18:06:29 ?       0:00 /opt/informix/bin/oninit
   root  352   351  0 18:06:29 ?       0:00 /opt/informix/bin/oninit
entrust  351     1  0 18:06:29 ?       0:08 /opt/informix/bin/oninit
   root  356   352  0 18:06:32 ?       0:00 /opt/informix/bin/oninit
   root  357   352  0 18:06:33 ?       0:00 /opt/informix/bin/oninit
entrust  609   573  3 19:04:08 ?       0:01 entcmp cmp -socket=6
entrust  601   573  3 19:04:04 ?       0:01 entbackup backup -socket=1
```

```
entrust   597   573 12 19:04:03 ?       0:03 entkeygen keygen -socket=1
entrust   591   573  3 19:04:02 ?       0:01 entsep sep -socket=1
entrust   587   573  3 19:04:01 ?       0:01 entash ash -socket=2
entrust   583   573  3 19:03:59 ?       0:01 entcmp cmp -socket=6
entrust   577   573  3 19:03:58 ?       0:01 entamb amb -socket=1
entrust   573     1  3 19:03:57 ?      0:01 entmon mon -sepsocket=1 -ashsocket=2 -cmpsocket=6
```

On the table above, only relevant processes are shown. In case any of the application is not running, the issue should be investigated.

Verify SSH access

As SSH will be the mechanism used to connect to the server, we need to have the assurance that it is properly configured. One way to do so, is to attempt SSH connection from IP addresses that have not been included in the /etc/hosts.allow file. If the connection is allowed, something is not right.

Verify file system

Few things to check on the file system are:

- NOSUID have been applied to file system on vfstab
- /usr is Read-only, also in the vfstab
- Check that World-writable directories have their sticky bit set, so files can not be modify by other users others that the owner

```
for part in `awk '($4 == "ufs" || $4 == "tmpfs"){ print $3 }' /etc/vfstab`
do
find $part -xdev -type d \( -perm -0002 -a ! -perm -1000 \) -print
done
```

- Permissions and ownership of files such as /etc/passwd, /etc/shadow/, /etc/group
- Confirm permissions and ownership on system log files such as /var/log/authlog, /var/adm/loginlog, /var/cron/log, /var/adm/messages, /var/log/syslog, etc.
- Verify there are not unauthorised world-writable files

```
for part in `awk '($4 == "ufs" || $4 == "tmpfs"){ print $3 }' /etc/vfstab`
do
find $part -xdev -type f -perm -0002 -print
done
```

- Verify there are not unauthorised SUID/GUID system executable files

```
for part in `awk '($4 == "ufs" || $4 == "tmpfs"){ print $3 }' /etc/vfstab`
do
find $part -xdev -type f \( -perm -04000 -o -perm -02000 \) -print
```

done

Fix-modes

Run fix-mode periodically and always that the system has been modified i.e. installation of a new patch.

CIS Scoring tool

Center for Internet Security (http://www.cisecurity.org) has developed a security-scoring tool for few operating systems, including Solaris, which analyses and reports compliance with technical control settings in the Benchmarks (see Reference Section).

I have used this scoring tool during the hardening process on this server, and I really found it quite useful, as the reports are quite comprehensive. However, as it is doing is checking your system against CIS benchmark, and not all the recommendations apply to your system, so you may finish with a quite low score, not exactly meaning that your system is not secure.

At the end, it is good practise to check in detail the report, so you may find something interesting that you have not see before.

Nessus

Nessus is a security scanner tool that is able to simulate an attack to a single host or the whole network. More information about Nessus can be found at www.nessus.org.

During the hardening process for this server, I used Nessus several times correcting each time the vulnerabilities found. Some of them cannot be performed on the server itself but a firewall will mitigate the risk i.e. ICMP type 17[24]

Nessus offers different types of scans regarding the plugins to be used during the scan: Enable all and Enable all but dangerous plugins.

Enable all but dangerous is the recommended, but some times I think it is good to include the dangerous. (Of course not on a live system).

[24] ICMP type 17 can be used by an attacker to gather information about the network i.e. netmask.

Once scan has finished, report can be safe in several formats including HTML and XML, what makes a nice looking report. Above, one of the tables presented in the report.

		Analysis of Host
Address of Host	Port/Service	Issue Regarding Port
192.168.0.99	ssh (22/tcp)	Security notes found
192.168.0.99	ldap (389/tcp)	Security hole found
192.168.0.99	entrustmanager (709/tcp)	No information
192.168.0.99	general /icmp	Security warning found
192.168.0.99	general /udp	Security notes found
192.168.0.99	general /tcp	Security warning found

References:

1. Sun Certified System Administrator for Solaris 8.0, Syngress, McGraw Hill
2. Advance Installation Guide. http://docs-pdf.sun.com/806-0957/806-0957.pdf
3. Solaris Security step-by-setp, SANS Institute, version 2.0
4. Installing Entust PKI 6.0 on Unix with Informix, Entrust Technologies, http://www.entrust.com
5. Solaris Operating Environment Networking Settings for Security, by Keith Watson and Alex Noordergraaf, November 2000. (http://www/sun.com/bluprints)
6. Solaris Benchmark v1.2.0, The Center for Internet Security, February 19, 2003. http://www.CISecurity.org/
7. Introduction to LDAP Security, Sasha Faust, http://ist.uwaterloo.ca/security/howto/2000-08-17/
8. InJoin Directory Server Administrator's Guide, Injoin Directory Server 4.1.Critical Path Inc, http://www.cp.net/
9. Implementing PKI: A Real Challenge!!, Juan Valbuena, Practical for the GSEC certification, SANS Institute 2003. http://www.giac.org/practical/GSEC/Juan_Valbuena_GSEC.pdf
10. Back to the Basics: Solaris and inetd.conf Part One, Hal Flyn, March 20, 2000 http://www.securityfocus.com/infocus/1490

11. Back to the Basics: Solaris and inetd.conf Part Two, Hal Flyn, March 20, 2000 http://www.securityfocus.com/infocus/1491