# Global Information Assurance Certification Paper

# Hardening "X Fed Agency" Data Center AIX Servers

Yaowe Ong
SANS Security Essentials
GSEC Practical Assignment, Version 1.2e
June 2, 2001

## Preface

This document represent by understanding of current "X Fed Agency" Data Center Network and system security strength and how to improve it. The security is a join effort between the top management, network engineer, system administrator, and the security engineer. A policy has to be formulated to define what we are protecting, how will it be done, who is responsible for procuring the software/hardware tools, who is to set the policies, who is to implement them, and how are we going to respond to an incident. What is the scope and flexibility of the security engineer during the emergency time. Tools are good, but they have to be properly configured and periodically monitored to ensure that they are doing what they supposed to do

## I. Security Policy

"X Fed Agency" FMC mid-tier Unix support team does not allow the installation of network file system services. Sendmail was installed but disabled as daemon. We use the SANS (System Administrator and Network Security, http://www.sans.org) online documentation on security policies (http://www.sans.org/infosecFAQ/policy/policy.htm) as a basis for our security policy. The policy must at least have the following items defined:

- Security policy defining security personnel job responsibilities and scope of work
- Chain of reporting in the event of emergency incident
- Guidelines or step-by-step procedures for incident response

Before the policy or policies are defined and published, the security person must respond to an incident with the following suggested steps outlined below:

1. Identify the scope of assumed attack
2. Outline the suspected compromises
3. Work through the environment to distinguish type of attack (external or internal compromised hosts)
4. Check the system logs or validate the software's against the software fingerprint database (see section 2 of this document)
5. Document the discrepancies
6. Validate the suspicions with facts and data
7. Take actions to stop the damage or spread of damage and report to your manager
8. Ask for external helps SANS http://www.incidents.org or Federal Bureau of Investigation's National Infrastructure Protection Center, http://www.nipc.gov)

## II. Operating System and Application Software Fingerprinting

Create software fingerprinting of your system on removable media to allow you to validate the system in the time when a suspected incident does indeed happen. Tripwire is one of the best software available to accomplish this job. It can be downloaded from the AIX freeware site (http://www-frec.bull.com/docs/download.htm). The documentation for this software is available online for both the open source (http://www.tripwire.org) and commercial product licenses (http://www.tripewire.com).

An alternative to tripwire used is "poor-man software fingerprinting" as, suggested by SANS. The poor-man finger printing deploy common Unix find command in conjunction with '`ls -l`' and `sum` or `cksum` commands to create a database of all protected files. These commands provide information such as file size, checksum value, permission settings, modified date, and absolute path to the file or directory.

The best time to perform software fingerprinting is immediately after the installation of the operating system and patches. Every time the operating system and network configuration changes and new application software is installed, a new software fingerprint database should be created. These databases must be installed on removable media and removed immediately after being created. Every week or month, depending on how volatile the system is, the system administrator should recreate a new software fingerprint database and compare it with the "reference" database to verify that there are no "trojan horses" hidden in the system.

## III. **System Logging**.

Syslog server.
Protection of system log and audit files is the most important step of a system intrusion forensic investigation. A sophisticated hacker is as smart as the system administrator if not smarter. They know where to clean up the crime scene to avoid detection. To add another layer of protection the administrator should:

- Start the syslog daemon on both client and syslog server with –r option.
- Configure the /etc/syslog.conf to send another copy of log to the syslog server.
- Beef up the security on syslog server

Swatch (http://www.stanford.edu/~atkins/swatch) is a log analysis tool that can perform

- Rotate the log files
- Monitoring and inspecting system activities
- Alerting the system administrator for unusual activities

The CERT (Center for Emergency Response Team at Carnegie Mellon University Software Engineering Institute, http://www.cert.org/security-improvement/implementations/i042.01.html) has sample step-by-step procedures on how to setup this tool. It covers from download, installing, configuring, and running the package.

System logs rotation.
Extensive system logging and auditing can consume too much filesystems real estate. To calculate your required disk space, you may want to tune the log configuration settings by starting an extensive log for a short period of time. Check the log content to see if any "useless" data can be weeded out. Tune your configurations to fit your organization security requirements. Next, compress the old logs and archive the oldest logs to the magnetic tape to free up disk space. Write a small script to rotate the logs or use swatch.

Errpt
In addition to syslogd facility, AIX has this nice tool to report the system errors.

- Errpt, display summary of error (time stamp, error id)

- Errpt –a, provides detail suspected cause of error, process id, program name, library modules involve, etc.

This valuable information should be examined daily and mail to system administrator.

## IV. Password and User Management

A. Password and user management

User authentication is the first line of defense against unauthorized access to a system resource. AIX provides

- Strong User Account Management
    - Administrator can setup account expiration date. This feature was not implemented until late 2000.
    - Administrator can set the initial password but require the user to change the password upon first login.

- Password Strength/Re-Use
  AIX can be configured to force users to select good passwords on an individual account basis such as
    - Minimum number of alpha characters
    - Minimum number of non-alpha character
    - Maximum repeated characters
    - Minimum age, time between changes
    - Maximum age, time password to be expired
    - Password history, number of previous passwords not to be repeated used
    - Dictionary file to be used for disqualifying password

  These features are not uniformly implemented on all AIX servers and it should. There is several cracking password tools use by the hacker to illegally break into Unix based systems. They are free and very effective. If the hackers are using them, the system administrator should use them too. May be used it before the hacker did. These tools and their download website are:
  Crack (http://www.users.dircon.co.uk/~crypto/) and
  John the Ripper (http://www.openwall.com/john/)

- Access Restrictions
  System administrator should develop a habit of monitoring the system resources access by properly configure the authentication log, sudo log, and su log in /etc/syslog.conf. AIX saves the failed logins in /etc/security/failedlogin. The administrator can create an equivalent to *lastb* command in HP-UX and Linux by adding the command alias in root profile:
  *alias='/usr/bin/who /etc/security/failedlogin'*

The following system access restriction is part of AIX features and should be implemented.

- Allowed time that user may log into the system by time-of-day and day-of week
- Allowed remote access to the system from specific terminal or network domain or disallowing remote access (this is usually than on root account to avoid network-based root login attacks).

## V. Network Services

A. Network services manage by super daemon, inetd

Network services are just like doors and windows, which allow curious or malicious outsiders to take a peek at or worst, get into your house. Most of the Unix or Microsoft operating system, by default, enable all the services whether you needed or unessential in your environment. The hacker loves them. We worry about them but do nothing until one-day, the in-house team decided to run a network scanning and penetration test on all the hosts. As a result, the following ports are currently identified by the "X Fed Agency" network management team to be shutdown or replaced.

| | | | |
|---|---|---|---|
| echo | 7 TCP/UDP | | |
| discard | 9 TCP/UDP | | |
| systat | 11 TCP | | |
| daytime | 13 TCP/UDP | | |
| netstat | 15 TCP | | |
| chargen | 19 TCP/UDP | | |
| ftp | 20 TCP | | |
| ftp-data | 21 TCP | | |
| telnet | 23 TCP | | |
| smtp | 25 TCP | | |
| time | 37 TCP/UDP | | |
| Domain | 53 TCP | | |
| tftp | 69 UDP | | |
| link | 87 TCP | bootp | 67 UDP |
| sunrpc | 111 TCP/UDP | | |
| NeWS | 144 TCP | | |
| snmp | 161 UDP | | |
| xdmcp | 177 UDP | | |
| exec | 512 TCP | biff | 512 UDP |
| login | 513 TCP | who | 513 UDP |
| shell | 514 TCP | syslog | 514 UDP |
| printer | 515 TCP | | |
| route | 520 UDP | | |
| uucp | 540 TCP | | |
| NFS | 2049 TCP/UDP | | |

X11 6000 to 6000+n TCP (where n is the max number of X servers you will have)

Our respond was to write a script to shutdown all non-essential network services by modified the /etc/inetd.conf, /etc/inittab (NFS services, AIX does not use system V /etc/rc*.d structure), and /etc/rc.tcp (Sendmail service, another AIX unique way of doing thing). We do have to open some ports to support our environment need. These ports will be protected by tcp_wrappers or replaced by Secure shell (See next section).

B. TCP Wrappers and Secure Shell

(1) Tcp_wrappers (http://www.porcupine.org/)

There are some network services that will be opened to support system administration activities as well as Tivoli Enterprise Management software. This security of these services can be improved with the deployment of tcp_wrappers. This is how TCP Wrappers work:

- When a connect request comes in, the tcpd (tcp_wrappers daemon) can be configured to take over the initial contact.
- It checks to ensure that the requesting party is in the ALLOW access control list or not in the DENY access control list.
- It can be configured to do reverse lookup on the incoming IP address to make sure the other guy is who he says he is. This can minimize the tcp hijacking or spoofing.
- It can send mail to alert the system administrator for suspicious attempt.

More information on where to get the software, how to install it, how to configure it, etc are available on these websites: http://www.cert.org/security-improvement/implementations/i042.01.html, http://www.cert.org/security-improvement/implementations/i003.04.html, and http://www.porcupine.org/ as well as IBM red book on Additional AIX Security Tools. I had configured several HP-UX servers on GSFC environment and still getting the Email from tcp_wrappers. Apparently, the current system administrator does not bother to change the sendmail aliases.

(2) Secure Shell (http://www.openssh.com or http://www.ssh.com)

Most UNIX systems provide the Berkeley r-commands: rlogin, rsh, and rcp, and the telnet for remote access to network host. These very user-friendly commands depend on either the local host file (/etc/hosts, /etc/host.equiv, $HOME/.rhosts) or the Domain Name Service (DNS) for host name resolution, and either a login/password or DNS-based trust for user authentication. The hacker on the wild

Internet can easily down load hacking tool to create network packages necessary to gain access to the system. Beside, these r-commands and telnet perform network transaction in clear text, which can easily view by tcpdump, snort, or equivalent tools.

The SSH family of tools (sshd, sftp, scp), public key cryptography, and the problem of clear text data transmission by using strong data encryption. These tools resolve three of our most concerned issues:

- Authentication, you say you are who you are.
- Encryption, the data transmission channel between the system are protected from spoofing.
- Integration, the information is not hijacked and altered while on the way to the destination.

There will come a time when all network traffic is encrypted and strong DNS and IP security is widespread, eliminating the need for security tools like SSH. Until that time comes, SSH is a strong defense against network sniffing, DNS spoofing, and IP spoofing. http://www.cert.org/security-improvement/implementations/i062_01.html

C. X11

**Guide to Encrypted Exceed Sessions**

First, download Teraterm (see http://hp.vector.co.jp/authors/VA002416/teraterm.html) and TTSSH for Teraterm (http://www.zip.com.au/~roca/ttssh.html). Then, install sshd with the following 2 directives set in the sshd_config file:

**X11Forwarding yes**
**X11DisplayOffset 10** # Can be a higher value if deemed necessary

Once the Teraterm was installed, unzip all the ttssh files to the teraterm install dir.

Launch TTSSH with the ttssh.exe, not ttermpro.exe.

There are three additional configuration files in the Setup menu for SSH. You will need to get your private ssh id file from **/export/home/ssh/id_keys** on the AIX server. This is best to be done via floppy and not over the network. **<secret>***Remember, NO ONE should get to see this file***</secret>** so put it somewhere safe (i.e. not on a network drive)

Next, in the **Setup -> SSH Authentication** ... menu fills in your connection id name (Unix login) and check "Use RSA key to login". You then point to where you

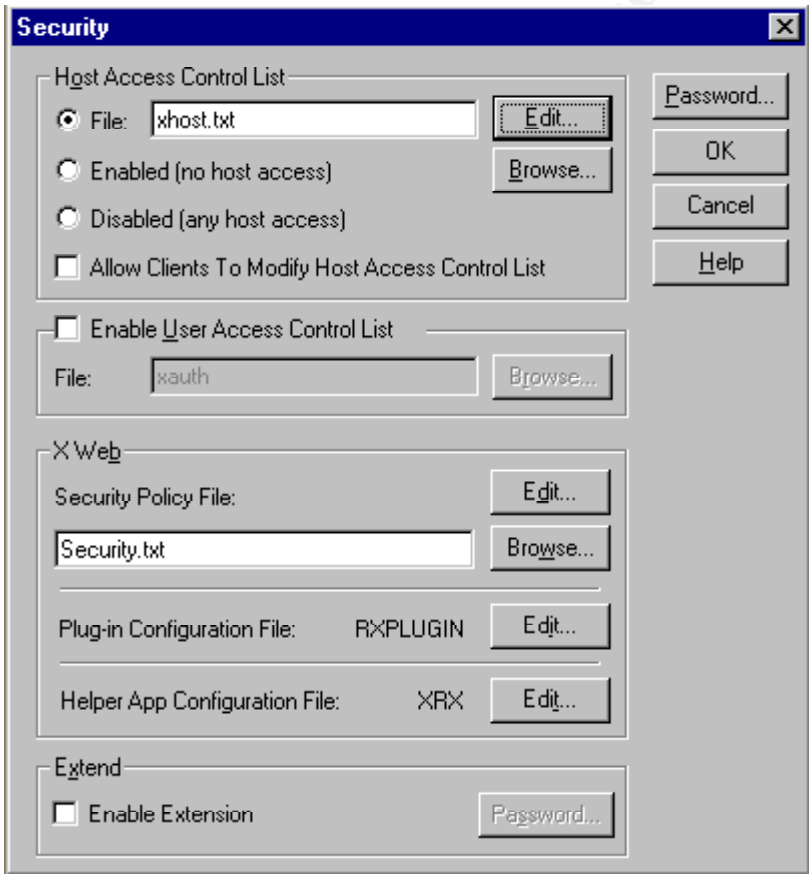
copied your private id key on your hard drive.

Now in the **Setup -> SSH Forwarding** menu check the "Display remote X applications on local X server". Nothing needs to be put in the port forwarding block

No real rocket sciences for eXceed either; just use standard session (tailor to suit). When you login to workstation, ttssh will automatically setup your display with the correct offset.

Start-up your favorite window manager or application e.g. Xterm. These will now forward over your encrypted ttssh session and display on your NT box in exceed.

Add an entry **localhost** to your xhost.txt file (in Exceed -> configuration -> Security) otherwise someone can just use xkeys and see everything you type. The settings in the Security section should be as follows:




## Remember

Security on your NT workstation should also be adequate so lockdown all unnecessary services, implement screen locking after short timeout and also put your private key in an encrypted part of your drive.

**Resources**
http://www.vector.co.jp/authors/VA002416/teraterm.html
http://www.zip.com.au/~roca/ttssh.html
http://www.hummingbird.com/

Note: *Xhost authentication by ip address or host name is vulnerable to spoofed IP addresses and is deemed insufficient. All X clients should be authenticated using MIT-MAGIC-COOKIE. This is automatically created when logging in via xdm. The remote Xclient will need to have a copy of the magic cookie exported to it (see the xauth command - I believe hummingbird X supports this).*

*SSH quite happily tunnels X-Windows encrypted. Simply enable at each end in the relevant Ssh and sshd config files. It is also possible to tunnel other TCP ports. SSH tunneling, I believe, bypasses MIT-MAGIC-COOKIE authentication as the client appears to be local to the X server (the tunnel end-point).*

*Tunneling/VPN are fine so long as the VPN endpoints are maintained at the same security policy (i.e. are the same company or are two companies with contractual obligation to maintain their networks/systems at the same security level/policy). If the end-points are of differing levels of security or are two different companies etc then the VPN endpoints must terminate outside of the respective firewall at each end (and inside a firewall to any untrusted networks such as the internet!). Some/many VPNs have rudimentary packet-filtering capability on the end-points - again don't leave these facing untrusted networks. If you are using a VPN that is packaged within a firewall, make sure you fully understand where the VPN terminates with respect to the internal and external networks.*

D. NFS and SUN-RPC, NIS, DNS

(1) NFS and Sun-RPC
"X Fed Agency" policy as I was told, does not allow nfs services. This is almost true as implemented in the "X Fed Agency" data center. There are, however two exception, namely IBM SP and SP Nodes as well as Sun Enterprise 10000 and its domains.
These two "Enterprise-class" super servers depend on control workstations to provide access to peripherals such as magnetic tape drive and CD-ROM drive. Since access to these peripherals is sporadic, the NFS services turned on when needed and immediately turn off when it is no longer needed.

(2) NIS and NIS+
NIS and NIS+ are not implemented in the data center. It is currently not an issue.

(3) DNS
All Domain Name Servers are Microsoft Windows NT 4.0 based. It is not a

Window NT security issue. We will not touch it on this document.

E. Electronic Mail

Sendmail-8.11.3 (http://www.sendmail.org, http://www.sendmail.com) is ran as daemon in Oracle server machines. IBM patches are applied on all mail servers. Sendmail is being enabled on all Oracle servers to support customized "X Fed Agency" mail software written by Oracle consultant to allow Oracle DBMS to communicate with DBA. Since sendmail was created initially with extensive used of SUID and mail is executed as a root process. It had been in the past frequently use by hacker for intrusion attack and gained system access as root. IBM Emergency and Repair Services team had recommended the use of postfix (another Simple Mail Transfer Protocol compliant mail software, see http://www.postfix.org) as a replacement for sendmail. This mail software was designed with system security and performance as primary concerns. IBM in the hope that it will become widely adopted is making postfix available for free, in source code form. The "X Fed Agency" facility management contract Unix support team will recommend testing of Postfix on "X Fed Agency" ITF (integrated testing facility) and deploy it on all Oracle servers. Postfix source is available from http://postfix.mercea.net/sources/index.html and IBM Alphaworks site (http://www.alphaworks.ibm.com/) as the "IBM Secure Mailer". The binary file for AIX 4.3 is now available in http://www-frec.bull.com/cgi-bin/list_dir.cgi/download/aix432/ site.

F. Web Server
HTTP web service is not activated on AIX servers.

## VI. Perimeter Security and Firewall

A. Removable media: CD-ROM, Magnetic Tape, Floppy Disk and single-user mode access.
The intruder can use the bootable removable media if he/she has physical access to the system. The procedure is no brainer. All the intruder need to do is to push the reset button if the system does not have a lock key or simply unplug the power cord and plug in back again. Viola, he/she can boot the system from his/her bootable removable media with Trojan horse softwares, virus, worm, etc. The solution to this is to disallow booting from removable media and configure the single-user mode password.

B. Firewall
"X Fed Agency" Data Center uses CheckPoint ™ Firewall-1. The firewall is a mystery to the system administrators by design. I suspect that the current philosophy on firewall is "obscurity is the best security" policy. If I do not know what it is trying to block or protect and how the rulesets were formulated, I cannot judge whether it is performing its job or not.

C. Dial-in access
"X Fed Agency" has allowed system support personnel dial-in access through the WinFrame server which perform the separate user authentication.

## VII. Tools

A. Intrusion monitoring can catch the thief while they are in action. There are two very popular tools currently being used by the internet community. The tcpdump (windump for windows platform) and snort. Read the Australian CERT emergency response on Intrusion checklist and be prepared to react to the incident. Intrusions happen every day, every hour. One day, it will reach "X Fed Agency", and we have to be prepared.

(1) TCPdump (www.tcpdump.org) is a network scanning and monitoring tool. It depends on the packet capture library, libpcap software. A feature of Tcpdump is to have the network interface card enter into promiscuous mode and dump packet header information. It provides with an understanding of your network behaviors and recognize "weird" behaviors.
Tcpdump does not perform any analysis on your network traffic. It has the option to limit the scope of the dump, dump format (Hexadecimal or translated), or to send it to a file, and more.

(2) Snort (http://www.snort.org) is another lightweight network intrusion detection tool that provide both hex and ascii output of the packet side-by-side for easy viewing. It can perform protocol analysis and content searching/matching. User can alter the behavior or snort by setting up ruleset to perform scope of detection.

(3) Australian Center for emergency response Intrusion checklist (ftp://ftp.auscert.org.au/pub/cert/tech_tips/intruder_detection_checklist)

B. Host-based self-vulnerability scanning tools such as tara, sara, and others allow the administrator see the vulnerability their network and hosts. This will allow the administrator to present the facts to his/her management and take proactive measure to prevent future attacks. These tools are only useful if you use them constantly and pay attention to the new development in the internet world. Beware that the security issues are a continuous process. New threads and new vulnerabilities are discovered by amateur and malicious people around the world. Here are a short list of tools that can make our live a little bit easier.

(1) TARA (Tiger Analytic Research Assistant, http://www-arc.com/tara/index.shtml). This is an upgrade of Tiger which in term in an improvement over COPS. It had been thoroughly tested by ARC (Advance Research Corporation) on Linux, SGI, and SunOS 5.x. Tiger had been ported to AIX 4.3 in the past. Since TARA basically fixes the bugs in Tiger. It

should be a minimal work to be ported to AIX server.

Tiger (http://www.net.tamu.edu/network/public.html) Tiger is an integrated thorough machine checking tools. It was an improvement of COPS on Texas A & M University environment. There was not much work done on it since 1994.

COPS (Computerized Oracle Password System, http://dan.yosemite.ca.us/cops/, http://dan.yosemite.ca.us/cops/documentation/farmer-spaff-cops.html). Dan Farmer wrote this integrated security packages. It was one of the most popular securities in the early 90's. The package was written in Unix shell script and c language. Some early day hacker uses it to security flaws. It check the file/directory access permission setting, CRC check key system binary file, discover password and group files weakness, examine SUID file, cron files, and /etc/rc* files, check anonymous ftp setup weakness and tftp vulnerability, decode sendmail aliases, on and on. More information can be found in http://www.fish.com/cops/.

(2) SARA (Security Administrator's Research Assistant, http://www-arc.com/sara/index.shtml). This is a third generation of SATAN. The new features added to this SATAN-like network vulnerability self-assessment tool are:

- False positive editor
- Improved windows testing
- Support CIS Initiatives

SARA interfaces with the popular NMAP network-scanning tool to provide excellent OS fingerprinting. ARC has integrated a configurable SARA Pro Report Writer into standard SARA product to allow users to generate a wide variety of output. The latest version is 3.4.3. This tool allows the security support personnel to finger print the OS and network service "behaviors" and use them to compare with later day "behaviors" to detect the changes. This tool is a SANS and ISTS (Institute For Technology Studies, Dartmouth University) certified, if this mean something to anyone.

SAINT (Security Administrator Integrated Network Tool, http://www.wwdsi.com/saint/). SAINT was being crowned as second generation of SATAN. World Wide Digital Security, Incorporation, currently supports it. It had added SAINT writer to provide personal easy to use report. SAINT express provides automatic upgrade to latest version of SAINT. It has added new vulnerability checks on

- Solaris rpc.yppasswdd backdoor vulnerability

- Sendmail signal handling of race condition,
- WFTPD long pathname buffer overflow, and
- Viewsrc.cgi vulnerability

There are a lot of useful and not so useful features added in their writer. You have to check it out on their website to see if you like it or not. This tool is also certified by SANS and ISTS. We start to see a lot of cooperation or competition between these two prestigious organizations.

SATAN (Security Administrator Tool for Analyzing Networks, http://www.porcupine.org/). The original release of this tool in 1995 generated a lot of media attention. I had downloaded it and got permission from my boss to run on my subnet. It sucks up the resources on target host being exploited (just like DoS symptom). The interface is web browser based and very easy to use. The report was a wake up call to my manager and me. It was long and extensive. Here is what Wietse's site has said about this tool: *For more than one year, the most famous piece of Internet vaporware. SATAN closes much of the knowledge gap between intruders and system administrators, by proposing how to fix problems. CERT-UU wrote a nice overview of the program, of vendor bulletins, and of alternative archive sites. Additional information can be found on this really slow site. This unusual program is the result of an even more unusual cooperation between unusual people: Wietse Venema and Dan Farmer.*

**References**:


Crash Course in X Window Security, http://bau2.uibk.ac.at/matic/ccxsec.htm, (May 22, 2001)
AIX Security Checklist, http://www.cop.vt.edu/unix/aix.security.html, (May21, 2001)
Element of Security: AIX 4.1, IBM Redbook Document Number GCG 24-4435-00
Additional AIX Security Tools on IBM@Server pSeries, IBM RS/6000, and SP/Cluster, by Abbas Farazdel, Marc Genty, Bruno Kerouanton, Chune Keat Khol
Exploiting RS/6000 SP Security: Keeping It Safe, by Abbas Farazdel, Chris DeRobertis, Marc Genty, Maarten Kreager, and Michael Wilkop