Global Information Assurance Certification Paper

Security Audit and Review of Acme.com

Paul Leadingham

Executive Summary

This security audit and review was conducted to explore potential or existing security problems within Acme.com's Unix systems. The systems audited covered both internal back office support systems and production systems. The systems selected represent many different aspects of Unix based operations at Acme.com to include Development servers, MIS, Database servers, Fileservers, Webservers, and Backup servers.

Several security issues within the Unix systems audited were found. These findings were categorized into Sound, Questionable, and High-Risk security practices. Each issue has suggestions on how to correct the practice or procedure.

The Acme.com environment is reasonably protected fairly adequately by firewalls. Unfortunately this also gives management and engineering staff a false sense of security. Internal attacks are just as likely or more likely than external attacks, and in this case, a firewall does not protect the systems from this internal danger. One issue that plays into this scenario is the fact that Acme.com employees and also outside contractors run NT and routinely Linux systems on the Acme.com network. These systems could be compromised and used as a jump-off point for attacks against Unix systems within the Acme.com network.

A large percentage of the security flaws covered in this report can easily be corrected by establishing and implementing security guidelines for the systems. Some issues will require significant systems changes that will require down time or possibly reloading the operating system.

Scope of Audit and Review

Systems Analyzed

Unix systems, all running Sun Solaris, were analyzed covering a cross sampling of the following functional areas within Acme.com:

- Development
- Quality Assurance
- MIS, data tracking software
- Webservers
- Database servers
- Support Systems, including backup servers

Areas Audited on Unix systems

- Operating systems patch levels were compared with Sun's recommended patch levels
- Selection of passwords
- Password expiration and failures
- Unsecure services such as finger and echo
- Use of .rhosts, and remote types of commands
- Use of .netrc
- Versions of third-party applications such as Apache and WU-FTPd
- Implementation and use of third-party applications
- setuid files
- System logging
- chroot'ed directories and applications using chroot
- Sendmail configuration
- DNS configuration
- NFS exports/shares
- Physical security
- Backup & restore procedures

Methodology Used

The selected systems were probed with several security auditing tools to expose any vulnerabilities that might exist. These tools were:

- Nmap
- Nessus
- John the Ripper
- Tiger

The tools were downloaded (see Reference list) and installed on a Sun Ultra 5 that existed on the Acme.com network. The tools were used to probe the network and targeted systems. Systems were also reviewed at the command line shell to search for known security flaws and system administration misconfiguration.

A port scan of the internal networks was done to investigate what type of systems co-existed on the networks with the Unix systems. This is critical for a couple of reasons. It gives the organization an idea of other operating systems that could possibly be compromised and it identifies unauthorized systems on the networks.

Security Audit and Review Findings

Policies and procedures

The lack of policies is the root of many of the problems within Acme.com. There are very few policies to protect the company from system abuse and unauthorized use of systems.

Policy and/or procedural documentation is needed for:

- Backup Policies - although backups do take place, current policies are not documented. Backups are intermittently taken off site. Plans to

backup across high-speed NMLI network connection will possibly resolve some facets of this issue. Monthly restore tests are recommended to verify backup procedures and consistent storage of media offsite.

- User Password Policies – Users need instruction on how to manage Unix system accounts (periodic password changes, safeguard passwords, etc.)

- Introduction of foreign computers – employees and outside contractors are allowed to bring in computers and connect to company network. Policies need to be established to cover this issue. Any introduction of non-company systems introduces a significant risk to systems in the current infrastructure and should be avoided.

- Disaster Recovery procedures - most critical system have alternate systems but are currently located in the same location. Procedures should include offsite storage of data and periodic tests to recover and verify the data.

- Intrusion/Exploitation procedures - there are currently no contingency plans covering intrusions and exploitations or ACME.com systems. This is especially critical of webservers that can be defaced or attacked by Denial of Service (DOS) attacks. Procedures need to be developed that cover forensics of the attacked system and public relations to name a few. Everyone from the CEO down to the Information Technology department need fully understand their role in properly handling any type of system security breach.

- General computer security procedures need to be documented and presented to all employees on a quarterly basis via formal classroom

discussion, email, and bulletins posted throughout the company. The information disseminated should cover good password selection and usage, social engineering, and the company's policies prohibiting viewing pornography, etc.

Sound security practices in use

- Secure shell is used extensively by Unix system administrators to safeguard passwords and sensitive data. This includes the transfer of data from system to system. This is much better than using NFS mounts or ftp-based shell scripts that send passwords in the clear text across the network, however, the version of Secure shell is quite old and needs updated.

- Separate networks exist for Unix systems and personal computers except for those in the IT department and a few personnel that need access to the Unix servers.

- Root passwords were not guessable/crackable and change periodically. Also root is only allowed to login directly to systems from the console, except for ssh connections.

- Sudo is used to allow non-root users to execute selected commands and scripts. It is also used by system administrators to allow for an additional level of auditing. This sudo policy is not to point blame on system administrators but to help in diagnosing mistakes and changes of systems by reviewing sudo logs.

- ntp, network time protocol is implemented on all systems to allow synchronization of events across systems. This is very important when correlating events across multiple systems.

Questionable security practices in use

- Recommended and Security patches updated 2-3 times a year. Several respectable and trusted security websites such as CERT, CERIAS, CIAC, and SANS should be monitored daily for new exploits on installed operating systems. These exploits normally have patches offered immediately by operating system and application companies.

- NIS & NIS+ are not used. This is good in the aspect that NIS has known security problems and NIS+ can leave exploitable holes if not configured properly. The drawback is users are created on systems as necessary, but not normally deleted upon departure. Procedures need to be developed to remove accounts as users leave the company for any reason. This is also true for contractors. LDAP might be used to keep accountability of users and user id numbers.

- Unneeded services such as printing, automounting, and sendmail are running but are not used. Services should be evaluated and shut down if possible.

- Open Boot Prom password is not set. This can be done as an added layer of security although some danger of being locked out of a machine is introduced if the password is forgotten.

- Remove unnecessary packages, especially GNUgcc compiler off all systems unless absolutely necessary. Xwindow support should be removed where possible.

- Unix systems were accessible by networks outside of Acme.com that belong to the parent company. Firewalls are planned to block this traffic in the very near future.

High-risk security practices in use

- Unnecessary services running on Unix systems such as echo, finger, shell, uucp, printer, etc which can be used as security exploits. Many services are in the default installation and can be turned off in /etc/inetd.conf.

- telnet should be shut down and all connections made to the Unix systems using Secure shell

- Many user passwords were easily guessable using freely available tools such as John the Ripper. Password expiration needs to be turned on. Login failures need to be logged. Passwords that are not alphanumeric should not be permitted as valid passwords.

- ftp shut down unless absolutely necessary for particular systems. If needed, Solaris OEM ftp daemon should be replaced with WU-ftpd or NcFTPD. Patches to the replacement ftp daemon should be done regularly. FTP logging should be sent to another filesystem.

- .rhosts located on several machines for several users. Although convenient, .rhosts files open a system up to unauthorized logins by having the connecting system spoof an IP address. Publish policy on .rhosts usage and disable the usage in /etc/pam_conf.

- Several systems have NFS mounts from systems outside of system administrators' control. There are two systems that mount filesystems from sister company. Remove these links and find alternate method of sharing data.

- Systems should have /usr mounted read-only. Systems should attempt to mount all other filesystems set nosuid to deny exploits of creating executable binaries or scripts running under root privileges.

- Unknown list of setuid files on systems. Create lists of acceptable suid files and periodically check against master list either manually or via scripts.

- Sendmail running on most systems. Systems allow mail-relay, which is often used to relay spam email from unsuspecting systems. This would be nearly impossible to exploit in the Acme.com environment based upon firewall settings. A secure sendmail infrastructure is being designed and will be implemented in the near future.

- Apache should be configured to run as a non-root user. Also cgi scripts should be individually audited for secure programming methods.

Quick Fixes based upon ease of implementation and cost

- Run hardening scripts such as YASSP or fix-mode on Solaris systems. These scripts will correct poor security configurations on the default install of Solaris.

- Install tripwire or Solaris Fingerprint Database to safe guard against binary changes.

- Install and run from cron John the Ripper to periodically check user password selection. Send notification to rouge users and lock accounts if not resolved within acceptable time.

- Turn off all services run by inetd. Prior to this Secure shell should be inplemented. If ftp is absolutely necessary then install WU-FTPd or NcFTPd.

- Install OpenSSH. This will allow implementation of ssh version 2 while updating current version of Secure Shell. ssh should not allow root connections, shut this off in /etc/ssh_config.

- Consider replacing bind, sendmail, and portmapper with more secure versions. At a minimum stay current with patches supplied by Sun Microsystems.

- Create procedures and steps for handling intrusion incidents. This should include steps in collecting and handling logs, contact information for FBI and computer incident centers such as CERT, and prepared statements for marketing or public affairs officers in case company is contacted by the media.

- ISS Real Secure license has been purchased. This product should be implemented and run on as many systems as possible.

Other cost-effective means of securing Unix Systems at Acme.com

- Implement syslog servers at key infrastructure points to allow for consolidated logging. These syslog servers can then be monitored

using logcheck, swatch, or watcher. This provides central points of logging and may provide a sterile copy of intrusion activity of a system. Will require purchase of low cost Unix systems.

- Install cameras in server room to provide an additional layer of physical security

Concerns about future versions of Unix

It was mentioned that other Unix operating systems are being discussed for future implementation into the Acme.com environment. Specifically, Linux was mentioned as a possible low cost solution for some applications and services. Many companies are moving to Linux for this very reason, but few have implemented it in a true production role and there are several reasons for that.

First of all Linux is distributed by almost a dozen companies. These software distributions all contain the core Linux kernel developed by Linus Torvalds. The distributors then bundle other services with the kernel. Some low-lying services are the same throughout the many distributions, but many can have their own version of programs. One recent distributor had a security exploit discovered in their implementation of telnet while the other distributors of Linux were not affected. If Linux is used in the future, care should be taken to find the distribution that appears to be tenacious on security concerns.

The Linux project has been open-source since it's inception. This has been a double-edge sword. On one side the availability to the source code has allowed hackers to exploit poorly or overlooked programming. On the flip side, the more individuals reviewing the code and finding these exploits make the Linux operating systems that much stronger. It is an argument that can be attacked from either side. Most industry experts agree that Linux will eventually come to being a robust and secure Unix operating system that can be used in

any facet of a business infrastructure. The decision on when to move to Linux at Acme.com should be thoroughly discussed and researched prior to implementation.

References

Documents and Reference Sites

- University of Georgia Computer Security and Ethics http://www.uga.edu/compsec
- The Solaris Security FAQ http://www.sunworld.com/common/security-faq.html
- Sun AnswerBook http://docs.sun.com
- SANS Institute's Solaris Security, Step by Step Version 1.0
- CERT http://www.cert.org
- CERIAS http://www.cerias.purdue.edu
- CIAC http://ciac.llnl.gov
- SANS http://www.sans.org

Software Tools

- nmap ftp://ftp.cerias.purdue.edu/pub/tools/unix/scanners/nmap/
- nessus http://www.nessus.org
- John the Ripper ftp://ftp.cerias.purdue.edu/pub/tools/unix/pwdutils/john/
- tiger ftp://ftp.cerias.purdue.edu/pub/tools/unix/scanners/tiger/
- logcheck http://www.psionic.com/download
- Solaris Fingerprint Database http://sunsolve.sun.com
- sudo http://sunfreeware.com
- Solaris Patches http://sunsolve.sun.com
- OpenSSH http://www.openssh.com
- NcFTPd http://www.ncftp.com
- wu-ftp http://sunfreeware.com

Last Updated: July 27th, 2017

Upcoming Training

SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**