Security Audit Report for ACME Corporation

Table of Contents

Acme Security Audit

Executive Summary

This report represents the final result of a security audit of the Acme web based systems. The audit was performed by examining the Acme security policy, taking a snapshot of the state of the systems, running a collection of analysis programs and staff discussions.

The security audit examined all significant facets of the Acme.com network that would affect its security level, including host and network security, physical security, network services and finally the overall security architecture of the network.

Major Issues

We found security issues in several different areas of the Acme.com network. The most serious are the following:

- The first line of defense, the firewall, has been setup properly, but the second line of defense, server configuration is lacking in network services security, user account security, password policy and file system security. If an intruder breaches the firewall, the system offers little defense for server security
- There is no separation between the Web servers and the Database servers on the production network. If an attacker gains access to a Web server, he has full network access to the Database servers. A DMZ network zone needs to be established in order to achieve this separation
- The network servers on the DMZ network of the Acme corporate office are exposed to Internet traffic. This makes it very easy for an attacker to gain access to the servers. This vulnerability is compounded by the fact that the corporate servers have a direct pathway into the production network by means of a VPN tunnel. By taking over a corporate server, an attacker will have little difficulty in penetrating the production network
- Several IIS installations display severe security holes. An attacker can exploit vulnerabilities within the IIS servers and can potentially gain remote administrative access to the servers. Patches and advisories are available for these vulnerabilities

Additional Issues

While not critical, these issues should be resolved in the near future:

- Antivirus implementation has occurred after infection (of Nimda and Code Red worms/viruses). The result of this is that these worms/viruses install backdoor programs that open the possibility of hackers to have full remote access to the servers
- Auditing and intrusion detection processes need to be put into place so that the system administration staff is notified of break-in attempts and other security breaches. We recommend

using readily available tools such as portsentry, logcheck and tripwire in order to automate these processes

- Patch installation processes need to be put in place so that security patches and hotfixes are applied to the servers as soon as security alerts are published. We recommend running, on a periodical basis, patch inspection tools available from Microsoft. For Linux servers, RedHat also offers an automated patch update service. We also recommend that the system administration staff subscribe to automated email notifications which contain security alerts and advisories from CERT and the SANS Institute

Conclusion

We have found several critical security inconsistencies in the Acme.com network that require immediate attention. The problems of the site are not insurmountable, and other than the DMZ zone setup within the production network, most of the issues can be resolved rapidly. Difficulties such as having numerous small problems on the individual hosts, as well as having some significant network issues indicate a general problem with allocating resources to solve basic security issues. The system staff is generally knowledgeable about security, but needs to spend more time on day-to-day system administrative tasks as well as achieving more consistency and order into the organization of the systems.

We recommend the system staff to concentrate on the major issues — fixing the configuration problems on the network and then methodically fixing all the host-based problems that were found. After the basic problems are resolved, the next effort should be focused on enforcing policy, updating documentation, and putting into place procedures and programs that would prevent security problems from recurring.

Overall Ranking

Overall Security Assessment (2.4 out of 5)	*	*	*		
Security Architecture and Design	*	*			
Network Security	*	*			
Linux / FreeBSD Host Security	*	*	*		
Windows Host Security	*	*			
Physical Security	*	*	*		

(ratings range from 1-5 stars, with 1 star being the worst and 5 stars being the best)

Security Architecture and Design

Introduction

This section discusses the overall layout of the system infrastructure of the Acme Web site, as well as the layout of the corporate network architecture. While not part of the production infrastructure, the corporate servers are very important from a security point of view because of the special trust relationships and patterns of access to the production servers. We have found significant security vulnerabilities in the corporate network infrastructure. We also discuss specific issues with the border router and the firewall which isolate the production network from general Internet network traffic.

Security Architecture & Design Assessment	*	*			
Production Network Architecture at Colocation facility	*	*			
Border Router	*	*			
PIX Firewall Implementation	*	*	*	*	
Corporate Network Architecture	*				

(ratings range from 1-5 stars, with 1 star being the worst and 5 stars being the best)

Summary

Strong points:

- The Acme production infrastructure is hosted at a colocation facility
- The Acme production infrastructure is protected by a robust firewall
- The firewall has almost all ports closed, with the exception of HTTP and SSL traffic
- IPSec is being used to access the production servers via client VPN software

Weak points:

- The network design of the production site is flat, with no separation between the Web servers and the Database servers
- The border router does not implement proper access control list in order to prevent spoofing and denial of service attacks
- The corporate network servers on the DMZ network are totally exposed to all Internet traffic
- There is a strong trust relationship between the corporate servers on the DMZ network and the production servers -- the former are allowed VPN access into the latter. This is particularly dangerous because of the exposure of the corporate servers to all Internet traffic

Production Network Architecture at the data center

Security Risk: High

- There is no DMZ (De-Militarized Zone) on the production network firewall at the data center
- Consider setting up DMZ on firewall in order to isolate Web servers from Database servers; this prevents intruders to gain access to the Database servers even if they do gain access to the Web servers

Border Router

Security Risk: High (SANS Top 20 Security Vulnerabilities)

- Set up rules against denial of service originating from production network
  - Allow only internal addresses to enter the router from the internal interfaces
- Set up rules against source routing

Firewall Implementation

Security Risk: Medium

- Do not allow incoming traffic over the Internet into the production network from unprotected servers at the corporate network; a VPN connection should be used instead
  - Traffic is currently allowed from several servers at the corporate network to ports 1433 (SQL Server) and 5631/5632 (PCAnywhere) on several production servers

Corporate Network Architecture

Security Risk: High

- Set up DMZ properly
  - The current setup is to use the DMZ port on the NetScreen firewall in transparent mode, which effectively leaves all servers on the DMZ open to the world
  - Implement NAT and block all incoming traffic

Network Security

Introduction

This section discusses the security of the Acme production servers as it relates to services and applications visible from the network. It is particularly important to look at vulnerabilities related to Web servers and applications, since the firewall does not block HTTP traffic. It is also important to look at the network security of not only the production servers, but also of the corporate servers, since they are enjoying a strong trust relationship in terms of security with the production environment. We also look at common network services such as mail, DNS and NFS.

Network Security Assessment	*	*			
Network Services	*	*			
Web Server Security	*	*			
Mail	*				
DNS	*	*	*		

(ratings range from 1-5 stars, with 1 star being the worst and 5 stars being the best)

Summary

Strong points:

- telnet and ftp access is disabled on the production servers
- tcp_wrappers is installed on the production Linux servers, enabling enhanced logging capabilities
- Unnecessary services are disabled on the production servers
- DNS servers are up-to-date in terms of software versions and do not allow zone transfers; reverse DNS lookups do not reveal server names that might help an attacker in guessing the function of the servers
- NFS is being used on only one production server and the NFS exports are restricted to a small number of servers

Weak points:

- All corporate servers on the DMZ network have a large number of open ports accessible by anybody on the Internet; the services running on these port numbers cover a large portion of the SANS Top 20 security vulnerabilities and can be easily exploited by attackers in order to gain full control over the servers
- A simple network scan reveals Web servers running on non-standard port numbers, which can be used to gain access to valuable information (Compaq Management Server for example)

- Several IIS installations on the corporate network display severe security holes which can be used to gain access to the servers; some of these vulnerabilities have been discovered two years ago and patches are available
- The corporate mail server allows relaying and can be used by spammers to send mail to third parties

Network Services

Security Risk: High

- Disable RPC/portmapper on Linux/FreeBSD servers which do not need to run NFS (ns1, ns2, mail) **(SANS Top 20 Security Vulnerabilities)**
- Fix the NULL session bug on all Windows servers; this allows an attacker to connect to the IPC$ share over the network with blank user name and password and then to enumerate shares, users and groups on the servers. This can be fixed by blocking the NetBIOS ports at the border router or at the firewall **(SANS Top 20 Security Vulnerabilities)**

Security Risk: Medium

- Disable rsh, rexec and the other " r" services on all Linux/FreeBSD servers**(SANS Top 20 Security Vulnerabilities)**

Web Server Security

Security Risk: High

- Several IIS installations display severe security holes such as the MDAC RDS vulnerability (CVE entry CVE-1999-1011), the Index Server Directory Traversal vulnerability (CVE entry CVE-2000-0097) and various ISAPI filters and IIS/FrontPage extensions vulnerabilities (idq.dll, webhits.dll, etc.) **(SANS Top 20 Security Vulnerabilities)**
- Several production and corporate servers run the ColdFusion Administration server on publicly-accessible IP addresses

Mail

Security Risk: High

- mail.Acme.com allows relaying
    - malicious users are able to send unsolicited mail to third parties using mail.Acme.com as their SMTP server

DNS

Security Risk: Medium

- Recursive queries are allowed against ns1.Acme.com and ns2.Acme.com. This may allow DNS cache poisoning attacks against the servers.

Security Risk: Low

- Logging is not implemented; consider logging various aspects of DNS operations for easier auditing and monitoring

Host Security

Linux/FreeBSD Host Security

Introduction

In this section we examine the overall security of the servers running Linux and FreeBSD. We looked at security settings and processes at the host and operating system level, such as user accounts and passwords, file systems, auditing and intrusion detection. Most of the Linux servers we looked at are running RedHat 7.1, which provides a fairly good security out of the box. We recommend upgrading all servers to RedHat 7.1 and running Linux-specific security hardening tools such as Bastille on a regular basis.

Linux / FreeBSD Host Security Assessment	*	*	*		
User Account and Password Policies	*	*			
File System Security	*	*	*		
Services	*	*	*		
Apache Security	*	*	*	*	
Auditing and Intrusion Detection	*	*			
Security Patches	*	*			

(ratings range from 1-5 stars, with 1 star being the worst and 5 stars being the best)

Summary

Strong points:

- File system security is generally strong
- Services are well secured, with the exception of RPC services on some servers
- Security for the Apache web server is generally strong
- Syslog events are being sent from production servers to a central location
- Process is in place for subscribing to Red Hat automated patch updates

Weak points:

- There is no enforcement of strong user passwords and no aging and expiration of passwords
- There is no automated process in place for monitoring suspicious file permissions and ownership
- There is no automated process in place for monitoring log files events
- Security patches have not been applied recently

User Account and Password Policies

Security Risk: High

- Set password aging and expiration; currently no aging and expiration are set, in contradiction with the stated security policy

Security Risk: Medium

- Use sudo to execute commands which require root privileges; sudo logs all commands, as opposed to su

Security Risk: Low

- Set /bin/false as the default shell in /etc/passwd for system accounts (e.g. uucp, mail, news)

File System Security

Security Risk: High

- Do not allow world-writable files, especially owned by root

Security Risk: Low

- Look for suspicious SUID and SGID files
- Look for files with no real owner
- Write scripts to periodically monitor the file system for the file types listed above

Services

Security Risk: High

- Disable any RPC services which are not necessary

Apache Security

Security Risk: Medium

- Consider running the httpd daemon with a user and group other than “ nobody” , since “ nobody” is treated in a special way on NFS servers and clients

Auditing and Intrusion Detection

Security Risk: High

- There currently is no auditing process in place; exploits are being tried against servers with no alerts being triggered
- All logs need to be monitored periodically
- The implementation of sending syslog events to a remote server is incorrect on ns1.Acme.com; instead of syslog events being sent to the remote server, a file called “messages?@loghost” is being created

Security Patches

Security Risk: High

- Periodically download relevant security patches from the vendor sites and apply them

Windows Host Security

Introduction

In this section we examine the overall security of the servers running Windows NT/2000. We examined the servers to make sure that a strategy is in place for keeping up to date on the latest security patches and virus definition files. User rights and file permissions were analyzed to make sure that appropriate permissions are being applied. Lastly, we examined the setup of IIS, ColdFusion, and SQL Server for security vulnerabilities.

Windows Host Security Assessment	*	*			
User Account and Password Policies	*				
File System Security	*				
User Rights	*	*	*		
Share Permissions	*	*	*	*	*
Auditing and Intrusion Detection	*				
Antivirus	*	*			
Hotfixes/Patches	*	*			
IIS/ColdFusion	*	*			
SQL Server	*	*			

(ratings range from 1-5 stars, with 1 star being the worst and 5 stars being the best)

Summary

Strong points:

- Shared folders are generally administrative shares, and as such, are hidden from view
- User Rights were generally well secured
- NTFS permissions are set using groups instead of individual users
- NTFS used for file partitions allowing for greater security and error recovery

Weak points:

- Auditing was incorrectly implemented resulting in no auditing being performed
- Password Policies were incorrectly implemented resulting in Windows default Password Policies being applied
- User accounts that were created with Administrator access to run critical processes (sqlexecservice) are currently being used to logon to the network
- Most directories are setup with Everyone Full Control access

- Spotty implementation of security patches
- Several servers infected with viruses including CodeRed II and Nimda

User Account and Password Policies

Security Risk: High

- Account Policies were setup incorrectly by using Domain Controller Security Policy instead of using Domain Security Policy. The Account Policies that were setup using the Domain Controller Security Policy window were overridden by the default values provided in the Domain Security Policy window. As a result, the only Account Policies that are in affect are the default Account Policies setup by Windows when it is first installed, which are very weak

    - No minimum password length required
    - No minimum/maximum password age
    - No password complexity requirements
    - No lockout after unsuccessful logon attempts

- Most passwords are setup to never expire. Most user accounts should be setup so that their passwords expire on a regular basis

Security Risk: Medium

- Administrator and Guest accounts should be renamed. If the Administrator and Guest accounts are renamed, it makes it more difficult for a hacker to gain unauthorized access into the network. Not only should this be done for the domain Administrator and Guests Accounts, but should also be done for the local Administrator and Guest accounts

Security Risk: Low

- The same password is being used for the local Administrator account on multiple Member Servers. User will not be prompted for password while accessing another server that has the same password when logged on using the Administrator account. This allows the user access to resources on multiple computers with only having to logon once
- The logon screen shows the last user logged on to the system. This gives a hacker a valid user name. Now all the hacker needs to do is to attempt to hack the password to gain access to the system
- The screen saver should be configured to password protect the screen after a number of minutes of inactivity. If the user forgets to logoff or lock the terminal, it will be done automatically after a number of minutes of inactivity

File System Security

Security Risk: High (SANS Top 20 Security Vulnerabilities)

- Everyone Group has Full Control on most directories (Windows default). Change to appropriate permissions

User Rights

Security Risk: Medium

- Tighten permission on the following User Account policies:

Auditing and Intrusion Detection

Security Risk: High (SANS Top 20 Security Vulnerabilities)

- On the Domain Controller, Auditing Policies were setup incorrectly by using Local Security Policy instead of using Domain Controller Security Policy. The Local Security Policies that were setup were overridden by the values provided in the Domain Controller Security Policy window. The Domain Controller Security Policies specified that no auditing was to be performed
- Event Logs are not being checked for security breaches. If they were being checked, the incorrectly configured Auditing Policies listed above would have been discovered

Security Risk: Medium

- Event Logs on some servers are only being kept for seven days. If a prolonged security breach takes place, critical log data used analyze the extent of the breach will be lost

Security Risk: Low

- Implement a warning logon message to warn intruders that Acme will prosecute unauthorized access attempts

Antivirus

Security Risk: High

- Antivirus software needs to be installed on all Windows servers on the network. Some Windows servers had no antivirus software installed
- Of the servers that did have antivirus software installed, the antivirus software should be configured to download antivirus definitions on a more frequent basis. The current configuration downloads new virus definitions once a week. Since new viruses come out every day, it is advisable that definitions be downloaded everyday

- Some production servers are currently infected (or have been infected in the past) with the Nimda and CodeRed II viruses. A Trojan program (Trojan.VirtualRoot) has been installed on these servers that can allow a hacker to have full remote access to these servers by issuing a HTTP GET request to run scripts\root.exe on the infected web server. It is recommended that a CodeRed removal tool be run against these servers. Once a computer has been attacked by W32.Nimda.A@mm, it is possible that your system has been accessed remotely by an unauthorized user. For this reason, it is impossible to guarantee the integrity of a system that has had such an infection. If you need to be certain that your organization is secure, you must reinstall the operating system, and restore files from a backup that was made before the infection took place, and change all passwords that may have been on the infected computers or that were accessible from it. This is the only way to ensure that your systems are safe

Hotfixes/Patches

Security Risk: High

- Windows hotfixes/patches have not been applied equally across all servers in the network. While some servers were up to date with the latest patches, some servers were very far behind. We recommend that Acme download the latest version of HFNETCHK.EXE from the Microsoft web site. When run this tool tells you which hotfixes/patches are missing from a server or workstation

IIS/ColdFusion

Security Risk: High (SANS Top 20 Security Vulnerabilities)

- Setup appropriate permissions on inetpub, wwwroot, ftproot, and script directories. On most of the servers, users were given too much access permissions to these directories because permissions were set to Everyone Full Control
- Setup appropriate permissions on Consumer, Corporate, and Admin WWW directories. Users were given too much access permissions to these directories because permissions were set to Everyone Full Control

SQL Server

Security Risk: Medium

- Any user in the local Admin group has complete access into SQL server. Remove all users within the local Admin group that do not need local Admin rights, or remove the BUILTIN\Administrators group from SQL Server.

Miscellaneous Items

Security Risk: High

- Only one Domain Controller exists in the domain. Active Directory security information gets distributed to all domain controllers in the domain. With only one domain controller, there is no redundancy for this information

Security Risk: Medium

- Unnecessary services should be turned off. Each network service you run has the potential to open unknown and unprotected security holes. Additionally, they may be useful in helping an intruder attack other parts of the system

Security Risk: Low

- Emergency Repair Disks are not being generated on a frequent basis. On some servers this has not been done in over a year. Without updated Emergency Repair Disks, it makes disaster recovery more difficult

Physical Security

Introduction

This section discusses the physical security of the Acme production servers. We looked at the security of the data center where the production servers are collocated, at the physical security of the servers themselves, and also at the disaster recovery procedures in place for the Acme production infrastructure.

Physical Security Assessment	*	*	*		
Colocation Facility Security	*	*	*	*	
Computer Security	*	*	*		
Disaster Recovery	*	*	*		

(ratings range from 1-5 stars, with 1 star being the worst and 5 stars being the best)

Summary

Strong points:

- The production servers are hosted at the Acme data center in downtown Los Angeles
- The servers are locked in cabinets with combination locks
- Backups are being done for the Windows servers and the backup tapes are stored off-site

Weak points:

- Users are not logging off or locking the screen when using PCAnywhere to access the Windows servers
- The production Linux servers are not being backed up

Computer Security

Security Risk: High

- Users are not logging off from the console when they are done working on the server. If a malicious user gets past the PCAnywhere login, he has full access to the server desktop. Acme should consider implementing a User Policy that logs off users after a number of minutes of inactivity

Security Risk: Medium

- CMOS/BIOS access is not password-protected on Linux and Windows servers
- LILO is not password protected on Linux; a user with physical access to the console can boot in single-user mode and gain root access

Security Risk: Low

- Consider disabling the CTRL-ALT-DEL combination on Linux servers to prevent users from rebooting the servers

Disaster Recovery

Security Risk: High

- The production Linux servers are not being backed up