A Client Assessment of Vulnerabilities of a SCO UNIX Mail and File Serving System

AUDITOR:
Harry W. Scott
hws1964@earthlink.net

Table of Contents

A Client Assessment of Vulnerabilities of a SCO UNIX Mail and File Serving System

Executive Summery

The client is a mid-sized organization involved in the transportation and security business. It is an established company with many years of successful computer operations. Currently the company has more than 4000 employees spread over numerous branch offices throughout the United States. The client asked to remain anonymous and as such will be referred to only as “the client”

The client has asked that the review focus on a SCO UNIX system used by the Information Technology Services Group for E-Mail and File Sharing. Given that this system models many other systems, it was felt that this was a valid choice.

The eight specific recommendations developed by the auditor are:

1. Replace Standard FTP and TELNET with secure encrypted versions of TELNET and FTP
2. Eliminate extraneous and unneeded services.
3. Improved Disaster response by creating a Disaster Response Plan
4. Completed the Computer Security Plan and distribute to the required personnel.
5. Replace the GroupWise platform with a more secure platform for electronic messaging.
6. Have regular security training for users and administrators
7. Train the Helpdesk Staff on Security, with special emphasis on Social Engineering prevention.
8. Evaluate flaws in the AFPS configuration to mitigate security concerns.

The auditor feels that items 1, 3 4 and 6 are high priority items. Others items are less pressing. In particular, removing the extraneous services, and creating the disaster and security plans need to be done as quickly as possible as they effect all other aspects of the operation.

The elimination of the extraneous services requires minimal resources, but the development of the plans will be a costly venture, both in time and in resources. It is vital that they have the highest priority.

Client Description

The client is a mid-sized organization involved in the transportation and security business. It is an established company with many years of successful computer operations. Currently the company has more than 4000 employees spread over numerous branch offices throughout the United States. The company has a history of limited but stable budgets for information technology.

The client has recently embarked on a review of its security posture to position its self for new ventures in the Internet environment. The client′s efforts to gain market share are directly affected by its ability to insure the dependability, flexibility, reliability and confidentiality of the data that is its possession. The client has hired this examiner as part of this ongoing effort.

Limitation of the Audit

The client, who has elected to remain anonymous for this report, will be known simply as "the client." Certain parts of this report will be sanitized to insure client confidentiality. All system names and IP addresses will be changed and the names of system administrators, users, managers, and others will also be sanitized. It is the opinion of the auditor that this restriction does not impact on the effectiveness of his duties or the validity of the results. The auditor working relationship with the principles was professional and courteous and he found no limits on his ability to audit the data.

Scope

The scope of this audit is limited to the Unix system used by the Information Technology staff of the client for their electronic mail and file sharing. This system is an important part of the client's information architecture as the client is reliant on this system to maintain interconnection between the IT staff and the rest of the organization. Many other systems in this company are configured similar to this system so the client would like to use this system as a template for what issues will be encountered thought the enterprise. This audit will look at the current systems as it installed, and recommended methods of improvement. Operations and administration will be reviewed in addition to system configurations, but a full evaluation of the client's physical security is outside the scope of this audit.

The client has asked that the auditor concentrate on changes that can be done with limited resources that can still have a major impact. Recommendation will be ranked, were possible by there relative cost. The report will be submitted to the Chief Information Officer (CIO) before it is released and the CIO may elect to edit the report before publication.

System Description

The system in question is an SCO Open Server 5.04 Unix system running on an ACER Altos 9100 series computer. This system is a duel Pentium-based server platform running a RAID 5 SCSI array. The system has over 10G of disk storage and over 256M of ram. The system supports 40 active users mostly as file sharing system. This file sharing is done using SCO Advanced File and Print Services (AFPS) which uses the SMB protocol to emulate a Microsoft NT server (www.sco.com/products/Datasheets/afps/).

Most of the users use the system to connect shares to their NT workstations. These shares are used for electronic messaging and for file sharing. Electronic messaging is done using GroupWise 4.1 which is an older messaging system originally done by WordPerfect Corporation and later bought by Novell (www.novell.com/groupwise). The vendor does not currently officially support the software, though Novell continues to give minimal support as a "good faith" effort. The client is a Windows 3.1-designed client that used a shared database stored on the SCO system accessed via mapped drives. The GroupWise Unix daemons then read this database and process the electronic mail. This configuration was never supported by the vendor and was only deployed via significant effort by the client. All clients mail less than 90 days old is stored in this database, making its security highly important.

The client also uses the system as file storage repository with over 5G of user data storage. This data varies greatly in its importance and sprawls over a significantly large directory structure.

The system is tied to a local and wide area network with the base IP address of 89.9.0.0". This WAN has more than 200 sub nets throughout the United States. The network is router-based with a router at all WAN node. In addition, a Firewall/Router combination limits INTERNET traffic to Electronic Mail and outgoing HTTP.

Methodology and Human Factors

The auditor was given access to the system as administrator to fully evaluate the system. The primary methodology employed was to evaluate the system using the standard Unix tools (ls, find, etc). The auditor also worked with the system administrator to identify concerns, and known problems. In addition, the Nessus (www.nessus.org) port-scanning tool was used to look for services that were currently running. This audit was done with the fully knowledge and support of the system administrator. No resistance was noted from the technical staff or management towards the auditor or his effort.

Vulnerabilities

Operating System Vulnerabilities

Significant Published SCO OpenServer System Vulnerabilities.

2000-06-05: BRU BRUEXECLOG Environment Variable Vulnerability
The Client does not use or load this software.

2000-02-15: SCO MMDF Buffer Overflow Vulnerability
It is SCO's position that this vulnerability was fixed buy previous patches that are installed on the clients system. Some researches contend that the vulnerability still exists in the patched versions. At this time, the auditor considers this fixed until proved otherwise.

2000-02-07: SCO OpenServer SNMPD Default Community Vulnerability
This Vulnerability effects only version 5.05 of the operating system.

1999-12-20: Multiple Vendor LibX11/X11 Toolkit/Athena Widget Libraries Buffer Overflows Vulnerability
This is a real vulnerability. Currently there is not patch released and no workaround is currently available. The client should implement a patch as soon as it is available.

1999-10-11: SCO OpenServer 5.0.5 'userOsa' symlink Vulnerability
This is a real vulnerability. Currently there is not patch released and no workarounds currently available. The client should implement a patch as soon as it is available.

1999-10-08: SCO OpenServer cancel Buffer Overflow Vulnerability
This Vulnerability effects only version 5.05 of the operating system.

1999-09-09: SCO OpenServer X Library Buffer Overflow Vulnerability
This Vulnerability effects only version 5.05 of the operating system.

1999-09-09: SCO OpenServer xlock Buffer (-bg) Overflow Vulnerability
This Vulnerability effects only version 5.05 of the operating system.

1999-09-09: SCO OpenServer Doctor Command Execution Vulnerability
This vulnerability is real. Suggested fix is to change the permissions on the /bin/doctor to 700. This change is not currently activated

1999-09-09: SCO OpenServer sar Buffer Overflow Vulnerability
This Vulnerability effects only version 5.05 of the operating system.

1999-09-09: SCO OpenServer X Library Buffer Overflow Vulnerability
This Vulnerability effects only version 5.05 of the operating system.

1999-07-14: BMC Patrol SNMP Agent File Creation/Permission Vulnerability
The client does not use or load this software

1999-06-14: SCO OpenServer XBase Buffer Overflow Vulnerability
The Client does not use or load this software.

This information is current as of 08/08/2000 from BugTrack (www.securityfocus.com).

Published AFPS Operating system vulnerabilities.

At this time there are no know published vulnerabilities for AFPS version 3.5.2. This was confirmed with a search on BugTrack (www.securityfocus.com).

Configuration Vulnerabilities

TELNET allowed as Root user

Standard Telnet is currently enabled for all users including root. This is an issue because TELNET uses and unencrypted protocol and can be easily be "sniffed" off the network. In addition, the root account, if used by multiple administrators, does not provide adequate tracking. Ideally, the root account should be accessible from the console only. If network access is needed then an encrypted Telnet Replacement like SSH is preferred. (Unix@Night: The Secure Shell (SSH), Acheson, 2000)

HTTP enabled in default configuration

The SCO HTTP configuration is in its standard mode. It is unused and not required. This should be disabled. (Linux Practicum, Brotzman, 2000)

FTP allowed for root user

Standard FTP is currently enabled for all users including root. This is an issue because FTP uses an unencrypted protocol and can be easily be "sniffed" off the network. In addition, the root account, if used by multiple administrators, does not provide adequate tracking. Ideally, the root account should be accessible from the console only. If network access is needed then an encrypted FTP Replacement like SSH is preferred. (Linux Practicum, Brotzman, 2000)

File system rights are too permissive

The GroupWise user partition and all of the files in this partition are set to permission 777, which means that they are readable, write-able, and executable for all users. This is done to eliminate file right issues for the GroupWise Desktop Clients using the AFPS Shares. This configuration provides no protection for the GroupWise database or executables. (www.novell.com/groupwise)

AFPS Shares allow for users to change files from an NT Share

AFPS is software from SCO that allows directory trees to be shared so that they look like NT shares to Microsoft Clients. Users can use NT tools to change and edit these files. Permissions are set to fully open on most AFPS shares. (www.sco.com/products/AFPS)

The named daemon is running in default configuration with nobody using it.

The SCO named configuration is in its standard mode and is enabled by default. It is unused because the network has a separate DNS server and as such, the server does not require the daemon running. This should be disabled. (Running Unix Applications Securely, Brotzman-Pomeranz, 2000)

The Berkeley "R "commands are enabled and active for Root.

The system has the Berkeley "R" commands (rsh, rcp, rlogin) available and the standard non-encrypted versions are running. The system /.rhost file has:

89.9.232.42 root
alexunix root

This will allow root access from host 89.232.42 and alexunix to the box without prompting for a password. It is the intention of the technical staff that this will be eliminated in the future, but no action has been taken as of yet. Given that the trusted systems share many of the same security vulnerabilities as this system, this is a significant issue. (Linux Practicum, Brotzman, 2000)

The MMDF daemon a SCO Sendmail replacement is enabled and not used.

The SCO MMDF configuration, which is used as a replacement for sendmail is in its standard mode and is enabled by default. It is unused and not required as GroupWise is used as the system mail package. This should be disabled. (Linux Practicum, Brotzman, 2000)

Risks for 3 Party Software

GroupWise 4.1

Currently the primary purpose of the system is run a 3rd-party application called GroupWise 4.1 for electronic messaging. The software version is over 5 years old and no longer supported by the vendor. Attempts to upgrade to a new version, or even to a new software product, have been hampered by the choice of operating system platform and by political complications.

The software has a major weakness in that the mail is stored on the server in mail database directories and is encrypted with a simple bit-shifting algorithm. Any user on the system can read these database and can with minimal effort, read other users Electronic Mail. With minimal effort a user can fabricate a mail and send it into the system.

Administrative practices

Physical Location

The system is in a secure locked room. This room has two locks protecting the location. One electronic keypad is used to enter the operations facility and a second mechanical lock is used to secure the server room. The first lock is known by more than 35 people and the second by approximately 15. The space is usually unmanned, and runs “light out” 24 hours a day.

Additional Physical Protection

The system has no intrinsic physical protection other than the protection given by the room.

Fire

Fire alarms are installed in all work areas. Room is normally is not staffed and on the top floor of the building. In the event of a fire, there would be no easy access to the space to shut down equipment. The room is not protected with an automatic fire retardant system. (ref SANS Pub)

Building Security

The building is over public shopping mall. Shoppers can get to any floor. In addition, other companies share the building. Company workspaces are locked from the halls, but cleaning staff has access to the office spaces. Some users lock their offices and clean their own rooms, because of fear of cleaning staff. (Linux Practicum, Brotzman, 2000)

Helpdesk

A sub-contractor mans an on-site help desk. This help desk has the technical skill to handle low-level calls and available from 8:00 am to 7:00 p.m. EST, Monday through Friday. The staff was given an information security brief when they came on board, but have no direct in-house computer security training. The staff is helpful, friendly and well liked and this could leave them open to Social Engineering attacks.

Backup Policies

Backup strategy

Full system backups are done on a daily basis, Monday - Saturday in the early morning hours. Backup tapes are rotated for 30 days with the 30th day going off-site for an additional month's storage. Tapes are not regularly checked for their integrity, but the backup software has been used in the past to recover other machines. System backups are performed with the cpio utility via a shell script run out of cron. System error messages are written to a file where they can be reviewed latter. System logs are checked on an informal basis, averaging approximately one a week.

Backup Storage

Backups are secured n a locked container in the computer facility. Access to the container is limited to approximately 10 individuals who are all cleared information technology personnel. Every 30th tape is sent off site for permanent storage in a secure location approximately 5 miles from the main computer facility. Tapes are secured in a secure locked location in storage site also.

Other vulnerabilities

The organizations security plans are being updated, but current operating versions are very out of date. Overall, they are not ready to defend themselves from a concerted network attack. They have the technical skills and quality people to do well, but lack the organization and discipline too effectively combat an attack.

Recommendation

1. Replace Standard FTP and TELNET with secure encrypted versions of TELNET and FTP

Action

Priority
High
Cost
Moderate/High
Workload Impact
High

2. Eliminate extraneous and unneeded services.

Action
The Information Technology staff in cooperation with its user base should evaluate all network services with the goal of eliminating unneeded and extraneous services. With this in mind, the DNS, HTTP, NTP, and MMDF at a minimum should be disabled.
Priority
High
Cost
Minimal
WorkLoad impact
Low

3. Improved Disaster response by creating a Disaster Response Plan

Action
The Information technology staff should prepare a Disaster Response Plan to enable an effective response to computer security incidents. This report should include malicious, non-malicious, and natural treats to the system with appropriate responses to each. An Executive Summery Report should also be created and distributed to all concerned parties. A listing of emergency number and common critical responses should be posted in the Computer Facility and in the workspace occupied by the Information Security Staff.
Priority
High
Cost
Moderate
Workload Impact
Moderate

4. Completed the Computer Security Plan and distribute to the required personnel.

Action

The Computer Security Plan should be completed and a final copy approved by management. The lack of an effective security plan effects the client's ability to adequately manage its computer security effort. Without a plan, it is difficult to assign priorities and to manage the necessary resources. This major ongoing effort is vital to the enterprise. This plan needs to define what level of security is needed for each system and what will be the rules of operation. This plan needs to include a description of all application both off-the-shelf and in house developed, with what security impact each application will have on the overall operation of the network. This plan needs corporate level approval, and should be signed off by the highest officers in the company.

Priority

High

Cost

High

Workload Impact

High

5. **Replace the GroupWise platform with a more secure platform for electronic messaging.**

Priority

Moderate

Cost

High

Workload Impact

High

6. Have regular security training for users and administrators

Action

A lack of regular security training is a major issue because most of the technical staff is not used to thinking about security. There has been very little confirmed intruder activity in the organization and most people view security the threats as being minimal. Regularly security training should include an overview of the security plan, user responsibilities, common treats, and common mitigating factors. This training should be required of all employees.

Priority

High

Cost

Moderate

Workload Impact

Moderate

7. Train the Helpdesk Staff on Security, with special emphasis on Social Engineering prevention.

Action

The Helpdesk staff is a potential vulnerability because of their professionalism and helpful manner. This is a double-edged sword; you want your helpdesk too helpful to the customer, but not helpful to hackers. The Helpdesk is run by a sub-contractor and are an effective tool. It is recommended that the helpdesk staff be trained in computer security with emphases on Social Engineering. There is training available in the area and it would show a good payback, in increased resistance to these attacks. I feel that the Helpdesk function is truing trying to help the users and that this would be a way of making them aware without making them feel like they are causing problems.

Priority

Moderate

Cost

Moderate

Workload Impact

Moderate

8. Evaluate flaws in the AFPS configuration to mitigate security concerns.

Action

The current AFPS configuration was created with little regard for security and data integrity, and was initially a stop gap measure to allow the client to move off an even older terminal based mail solution. The client should tighten the current AFPS configuration to limit access to the shares. In addition, user should be discouraged from using the same passwords for their AFPS account as the do for their workstation. The system administrator stated that in testing that was done by a sub-contractor, AFPS password were easily cracked by cracking the users workstation and then retrieving the acl databases. These were cracked with a cracker program and were used to penetrate the system.

Priority

Moderate

Cost

Low

Workload Impact

Moderate

Conclusion

In the view of the auditor, the client's security issues are more organizational than technical. There some significant technical issues like the AFPS share rights and issues related to the non-encrypted TELNET, FTP and Remote Access software such as the Berkeley "R" commands. Even given these issues the moist significant areas of concern are non-technical. The client needs to complete its security plan and start an effective computer-security training program. Backups need to be tested and these tests need to be documented. A consistent effort needs to be applied to replacing the legacy messaging system, or if this is unattainable, attempting to mitigate the security vulnerabilities inherent in the package. With proper training and consistent management support of these efforts, we feel that the system can be made run securely enough to meet the needs of the organization.

References

Santa Cruz Operations (SCO) HOME Web Page, www.sco.com, SCO Inc., 2000

Santa Cruz Operations (SCO) AFPS Web Page, www.sco.com/products/Datasheets/afps, SCO Inc., 2000

Novell Home Web Page, www.novell.com, Novell Inc, 2000

Novell GroupWise Web Page, www.novell.com/groupwise, Novell Inc, 2000

Security Focus "Bugtraq" Web page, www.securityfocus.com, Securityfocus.com, 2000

NESSUS Port Scanning Tool, www.nessus.org, Nessus.org, 2000

Linux Practicum: Track 6 Unix Security, Lee Brotzman, SANS, 2000

Running Unix Applications Securely, Lee Botzman-Hall Pomeranz, SANS, 2000

Unix@Night: The Secure Shell(SSH), Steve Acheson, SANS, 2000