Systems Administrators: The First Line of Defense

Elizabeth Frank

Systems Administrators: The First Line of Defense

By Elizabeth Frank
GSEC Practical Assignment
Version 1.2e

Introduction

As computers and networks have assumed critical functions in many aspects of today's business world, the need for their security has increased as well. Businesses depend increasingly on email, web sites, and databases of customer credit card numbers for day to day transactions. A company's immediate financial state as well as its reputation depend on the integrity, availability and reliability of its data. A single system compromise can result in untold financial losses as well as a lack of confidence in the company itself. Protection of electronic information has taken on new importance in the light of increased attacks and thefts. The systems administrators are the people responsible for the defense of a company's cyber structure. Their job is to ensure an organizations' systems are functioning properly while secure from various threats. Because even a single mis-configuration in a computer or network setup can provide a means of unauthorized access, systems administrators must have adequate technical and managerial skills to ensure their security. A properly trained and experienced systems staff is essential to the security of an organization's computer network.

Discussion

Over the past ten years, the internet has evolved from an exclusive environment of collaboration and communication within a relatively small intellectual community to a critical component of business infrastructure. This evolution has in turn driven the systems administration profession. Initially computers were isolated systems, maintained by their users or a single individual. As workstations and PCs appeared on more and more desktops and networking became an issue, an individual within an organization would often be assigned to manage the systems in addition to their regular tasks. Usually this position would fall to the most technically-able body available such as a teenager who liked computers, a student, a secretary or maybe even the person with the most floppy diskettes. In fact, most systems administrators are not recognized as such by their job titles. In their 1999 salary studies, the the Systems Administrators' Guild (SAGE) reported that fewer than half of all people actually doing systems administration are employed by that title [1].

These newly designated systems administrators had no actual training or experience. They learned on the job by trial and error. Since relatively few systems were on the internet, security was not a primary issue. Focus was on keeping the computers available and functional to legitimate users. Organizations with inadequate funding for technical positions often didn't have enough personnel for the task, therefore ease of administration became a primary concern for already overworked administrators. The combination of insufficient training and understaffing often resulted in extremely insecure systems. A few real life examples of security holes introduced by systems administrators and their effects are listed below:

- No backups. Restoration of user data is a key element of any response to an intrusion. Not only do backups protect users' data from loss due to hardware failures, but preserve data integrity in the event of an intrusion or even theft of a hard drive. Although most systems administrators know the importance of saving all data to tape on a regular basis, a new administrator may not. Management of one particular organization discovered their systems group had been doing no backups whatsoever only after a user's data had been lost. The same organization then instituted backups on network drives only, but continued to setup users' home directories on their local drives. Again, this resulted in a loss of data for several users.

- Several UNIX systems on a LAN with .rhosts files in the root directory containing only a +. This not only permitted all users on the LAN, including root, to move from one system to another without a password, but anyone external to the LAN also had full access as well. Luckily, this hole was caught and closed by a new administrator before it could be exploited.

- No password protection on xterminals. Not knowing of a remote administration feature on their xterminals, the systems group of an organization did not set the administrator password. This made it possible for a remote user to login as the administrator and reboot the terminal, effectively creating a denial of service attack.

- Ghosts in the machines. Although procedures were in place to add a new user in an organization, no policy or mechanism existed to remove or lock an account when a user left. In addition, some accounts existed for the sole purpose of forwarding email announcements and had never been used. Because every account on a system is an additional point of entry to the network, each one should be well protected and monitored by its owner. Compromises are often detected and reported by users who find unusual files in their directories. Such activity can go undetected on an unused account for quite a while. In one instance, a user's password was compromised on an active account. Since the user had the same password on a system they no longer accessed, the attacker then had instant access to a second computer and network. Since the account was legitimate, the administrator had no reason to suspect the activity was an attack until the system was compromised.

Now that the internet is infested with "script kiddies" launching DOS attacks, viruses, worms and stealing credit card information, the trial and error approach to system administration no longer suffices. The people managing systems and networks must be trained and experienced to maintain system integrity. Not only must they be technically capable, but must know how to manage tasks and workloads such that security is never compromised. Quick solutions without regard to their impact on the overall infrastructure of a network can compromise an entire site within hours. Real life compromises as a result of quick fixes are listed below:

- A site had several presentations scheduled which required PowerPoint slides. As a convenience to the presenters, an anonymous ftp site was setup to allow presentations to be uploaded in advance. Instructions detailing the dropzone location and upload procedure were put on the organization's web page. It didn't take long for the system to become a *warez* distribution site.

- A user on a UNIX system had an urgent and legitimate need to run a process as root, therefore the systems administrator setup *sudo* to allow access. Because it was done in a hurry, sudo was configured incorrectly and allowed all users to execute all commands as root, including the *su* command. By executing "*sudo su -*" any user could simply login as root.

- A vulnerability in an old version of Solaris NFS allowed any system to mount an exported partition if the list of systems it was exported to was longer than 256 characters. Sun released a patch for the vulnerability that claimed to fix it, but didn't. Rushed system administrators installed the patch, but didn't test the fix and unknowingly remained vulnerable to a relatively simple, but dangerous, exploit.

Bad management decisions by an administrator can also result in system compromises. For example, an organization's manager chose to have a SPARC station run linux rather than Solaris. The linux distribution had more known vulnerabilities which had in fact already been compromised on several of the organizations' existing systems while their Solaris systems had not been successfully attacked. The SPARC station running linux was compromised shortly after being put on the network.

All but the smallest organizations usually have more than one systems administrator managing the computers and networks. In this case, it is essential that all members of the group work as a team to maintain security. Usually, a lead systems person will oversee the coordination of all systems, assigning specific tasks to other members of the group. Although an individual can be assigned primarily to issues of system and network security, it is not a single task or procedure and must be taken into account for every change to the current configuration or new system setup. Lack of coordination or communication can severely compromise a network. For example, an administrator within a group sets up a new NIS server for the network and neglects to inform all members of the team. If done correctly, the new server could go unnoticed by any or all of the other administrators. When one of several NIS vulnerabilities ([2] ,[3] or [4]) is announced, this server will not get patched if the individual assigned the task of patching the NIS servers does not know of its existence and the network will remain vulnerable to attack.

Extensive security training and expensive tools weren't necessary to prevent these holes, whereas education and basic systems administration training would have. Finding qualified personnel for the systems administration task has become quite a challenge for many organizations. Often an organization will promote a lower level system administrator to a vacated or just opened upper level position. This can be advantageous in that there is a minimal learning curve. The newly appointed individual can be expected to know the organization's current configuration and how to maintain it as is. If the current infrastructure is good, then this will work well. However, if the new systems administrator has never managed systems elsewhere and assumes the current setup is "the" way to do it, an already dysfunctional network will deteriorate. This seems to occur frequently within universities, possibly explaining their reputation as an easy target for hackers. A good systems administrator doesn't necessarily need to know how an organization's existing setup, but how it *should* be configured.

Because there are currently no degree programs offered specifically in systems administration, it can be difficult to gauge a candidate's expertise. A degree in a related or other technical field, as in any profession, demonstrates an applicants' abilities to meet deadlines, follow-through and problem solve. On average, those with more education receive higher salaries. However, only slightly more than half (54.1%) of system administrators surveyed by SAGE had a bachelor's degree in a computer related field. In fact, according to the 2000 SAGE Systems Administrators Salary Survey, 83.7% learn system administration on the job and 83.1% are self-taught. Only 14.4% learn through a formal university program [5]. Other sources of training include certification programs, vendor-specific courses, conferences and non-degree courses. SAGE offers general systems administration training and has also begun a mentor program designed to provided guided and supervised on-the-job training [6]. In addition to the general systems courses offered, there are specialized classes in such topics as specific operating systems, networking technologies and even security. The SANS Institute [5] has established a certification program in general security issues as well as specialties in UNIX and Windows operating systems. CISSP [7] also offers security certifications. It is interesting to note however, that years of experience have a more significant impact on salary than either level of education or certification.

Better education at the systems administrator level is not the only means of improving security within an organization. Stuart Campbell of KPMG stated that while companies are spending more towards security, they are spending it in the wrong way [8]. Money is going to buy new technology rather than educating and training employees which would produce better results. For example, many users still don't understand the importance of keeping their passwords secret. Sticky notes under keyboards are not uncommon in many companies and pose a difficult security hole for systems administrators to close. Oftentimes, social engineering is still a viable means of obtaining internal access.

Employees at all levels within a company should be trained in information security just as they would be in physical security measures such as arming door alarms. If new security procedures are implemented, all employees should be informed and instructed in their use. They should also be provided with system administration contact information in the event of suspicious or questionable activity.

Firewalls, intrusion detection systems and other tools have come into existence to combat cyber threats. Lists of such resources can be found on the internet at sites such as SANS [9], CERT [10]and CIAC [11]. The responsibility of deploying these tools within a network falls to the systems administration staff. System administrators must choose the tools most suited to their organizations' needs as well as install and configure them properly. Knowing which tools are available to choose from, as well as how to use them properly, is a key component of system administration. For example, SSH and Kerberos both provide a means of encrypting network transactions. However, SSH is relatively easy to install and configure while Kerberos can be quite complex. Some organizations may require Kerberos while others can be adequately protected by SSH. Still others may have a need for both. It is the system administrator's task to know which method to implement and ensure it is done correctly.

Because so much of today's commerce takes place electronically, many organizations have appointed a Chief Information Officer to oversee electronic business functions such as email reliability, web site availability, customer credit card number and personal information storage. However, too few of these corporations have also appointed a Chief Information Security Officer [12]. Also, while most businesses believe the biggest threat to their network security comes from outside sources such as hackers, according to KPMG internal threats are a greater risk [13]. More damage can be done undetected over a longer period of time by someone familiar with the internal structure of an organization. KPMG also reports that executives mistakenly optimistic about their network security are often misinformed by their own poorly trained and/or poorly qualified system administration staff.

Since system administrators are responsible for the security of an organization's computers and networks, they are the first line of defense and must be chosen carefully. In the old days, systems administrators were occassionally hired by an organization after demonstrating their abilities by hacking into that companys' computers thus proving they knew more about the systems than the current staff. Although this method may have a certain charm, most companies prefer the more traditional approach. Applicants submit résumés and applications in response to job postings in newspapers, trade journals or on the web. The human resources department sorts through the submissions and forwards the most likely candidates to a hiring committee. An interview process further screens the applicants and eliminates those that would not fit the company profile or who may have severely exagerated their abilities on paper.

Assessing a candidate's knowledge can be difficult. Some will spew forth technical information such as disk drive model numbers and corresponding transfer rates in an effort to impress an interviewer. While it may be tempting to hire such individuals, these facts can be looked up if needed whereas experience establishing and maintaining a secure network would be more beneficial to the company in the long run. The interview process itself should be approached with caution. Some candidates are not really interested in working for a company and are actually researching an organization's equipment for their own purposes. These are known as "trojan interviews" [14]. Based on specific job requirements for a position or a tour of the facilities, an individual can easily research vulnerabilities. Seeing Cisco 12000 routers on a rack, a hacker will know to try exploiting the recently released list of security holes [15]. Or knowing which system houses a credit card database may narrow a hacker's search for their target.

Conclusion

Systems administration is a complex task in and of itself. Convincing various pieces of hardware running a variety of operating systems to work together as one big happy network is the first step. Providing a usable computing environment to those with legitimate access while keeping out those who don't belong is quite a challenge to any systems administrator. The variety of security packages available today makes it possible to secure systems and networks from many threats, but only if the appropriate tools are chosen, installed and configured properly. It should also be noted that these additional measures will only be effective if the site is already configured securely. Knowing what to do and how to do it is absolutely essential. Companies can no longer afford the trial-and-error approach to training systems administrators as a single mis-configuration of a single component can expose a site to any number of exploits. Hiring a qualified systems staff must be a priority if an organization is to maintain computer and network security.

References

[1]"Careers in System Administration" by Barbara Dijker, Fall 1999 http://www.ddj.com/documents/s=894/ddj9914d/9914d.htm

[2] Sun rpc.passwd Security Vulnerability, http://www.ciac.org/ciac/bulletins/m-008.shtml

[3]Sun ypbind Buffer Overflow Vulnerability, http://www.ciac.org/ciac/bulletins/l-103.shtml

[4] Red Hat Linux "ypbind" Vulnerability, http://www.ciac.org/ciac/bulletins/l-009.shtml

[5] Sage Salary Survey (PDF Download, Usenix/Sage membership , or registration required)http://www.usenix.org/sage/jobs/salary_survey/salary_survey.html

[6] Sage Student Sys Admin Program,

http://www.usenix.org/sage/projects/internship/index.html

[7] (ISC)2: International Information Systems Security Certificaiton Consortium, Inc., http://www.isc2.org

[8] "Report: Business fails on global security" by Robert Lemos, November 14, 2001, http://www.zdnet.com/zdnn/stories/news/0,4586,5099609,00.html?chkpt=zdnpltp02

[9] SANS Institute Online, A Cooperative Education and Research Organization, http://www.sans.org

[10] CERT (Computer Emergency Response Team), http://www.cert.org

[11] CIAC (Computer Incident Advisory Capability), http://www.ciac.org/ciac

[12] Metro Atlanta Information Systems Security Association, Information Security Quarterly, July/August 2001 http://www.issaatlanta.org/Index/July_August_2001_Newsletter.pdf

[13] KPMG 2001 Global e.fra@d.survey, (PDF format) http://www.kpmg.co.uk/kpmg/uk/Image/EFRAUD.PDF

[14] "Security Manager Explains How Not to Get a Job", by Vince Tuesday, October 8, 2001 http://www.computerworld.com/itresources/rcstory/0,4167,KEY73_STO64480,00.html

[15] Cisco - Multiple Vulnerabilities in ACL Implementations, http://www.ciac.org/ciac/bulletins/m-018.shtml

Last Updated: October 16th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

Purple Team Summit & Training 2019	**Las Colinas, TXUS**	**Oct 21, 2019 - Oct 28, 2019**	**Live Event**
SANS Santa Monica 2019	**Santa Monica, CAUS**	**Oct 21, 2019 - Oct 26, 2019**	**Live Event**
SANS Training at Wild West Hackin Fest	**Deadwood, SDUS**	**Oct 22, 2019 - Oct 23, 2019**	**Live Event**
SANS Houston 2019	**Houston, TXUS**	**Oct 28, 2019 - Nov 02, 2019**	**Live Event**
SANS Orlando 2019	**Orlando, FLUS**	**Oct 28, 2019 - Nov 02, 2019**	**Live Event**
SANS Amsterdam October 2019	**Amsterdam, NL**	**Oct 28, 2019 - Nov 02, 2019**	**Live Event**
SANS Mumbai 2019	**Mumbai, IN**	**Nov 04, 2019 - Nov 09, 2019**	**Live Event**
Cloud & DevOps Security Summit & Training 2019	**Denver, COUS**	**Nov 04, 2019 - Nov 11, 2019**	**Live Event**
SANS DFIRCON 2019	**Coral Gables, FLUS**	**Nov 04, 2019 - Nov 09, 2019**	**Live Event**
SANS Paris November 2019	**Paris, FR**	**Nov 04, 2019 - Nov 09, 2019**	**Live Event**
SANS Sydney 2019	**Sydney, AU**	**Nov 04, 2019 - Nov 23, 2019**	**Live Event**
SANS London November 2019	**London, GB**	**Nov 11, 2019 - Nov 16, 2019**	**Live Event**
MGT521 Beta One 2019	**Crystal City, VAUS**	**Nov 12, 2019 - Nov 13, 2019**	**Live Event**
GridEx V 2019	**Online,**	**Nov 13, 2019 - Nov 14, 2019**	**Live Event**
SANS Gulf Region 2019	**Dubai, AE**	**Nov 16, 2019 - Nov 28, 2019**	**Live Event**
European Security Awareness Summit 2019	**London, GB**	**Nov 18, 2019 - Nov 21, 2019**	**Live Event**
SANS November Singapore 2019	**Singapore, SG**	**Nov 18, 2019 - Nov 23, 2019**	**Live Event**
Pen Test HackFest Summit & Training 2019	**Bethesda, MDUS**	**Nov 18, 2019 - Nov 25, 2019**	**Live Event**
SANS Austin 2019	**Austin, TXUS**	**Nov 18, 2019 - Nov 23, 2019**	**Live Event**
SANS Atlanta Fall 2019	**Atlanta, GAUS**	**Nov 18, 2019 - Nov 23, 2019**	**Live Event**
SANS Munich November 2019	**Munich, DE**	**Nov 18, 2019 - Nov 23, 2019**	**Live Event**
SANS SEC401 Madrid November 2019 (in Spanish)	**Madrid, ES**	**Nov 18, 2019 - Nov 23, 2019**	**Live Event**
SANS Cyber Threat Summit 2019	**London, GB**	**Nov 25, 2019 - Nov 26, 2019**	**Live Event**
SANS Tokyo November 2019	**Tokyo, JP**	**Nov 25, 2019 - Nov 30, 2019**	**Live Event**
SANS Bangalore 2019	**Bangalore, IN**	**Nov 25, 2019 - Nov 30, 2019**	**Live Event**
SANS Paris December 2019	**Paris, FR**	**Dec 02, 2019 - Dec 07, 2019**	**Live Event**
SANS Nashville 2019	**Nashville, TNUS**	**Dec 02, 2019 - Dec 07, 2019**	**Live Event**
SANS Security Operations London 2019	**London, GB**	**Dec 02, 2019 - Dec 07, 2019**	**Live Event**
SANS San Francisco Winter 2019	**San Francisco, CAUS**	**Dec 02, 2019 - Dec 07, 2019**	**Live Event**
SANS Frankfurt December 2019	**Frankfurt, DE**	**Dec 09, 2019 - Dec 14, 2019**	**Live Event**
SANS Cyber Defense Initiative 2019	**Washington, DCUS**	**Dec 10, 2019 - Dec 17, 2019**	**Live Event**
SANS Austin Winter 2020	**Austin, TXUS**	**Jan 06, 2020 - Jan 11, 2020**	**Live Event**
SANS Cairo October 2019	**OnlineEG**	**Oct 19, 2019 - Oct 24, 2019**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**