Global Information Assurance Certification Paper

SANS GIAC
Level 1 Security Essentials Paper

Hardening in the Enterprise: Always an After Thought?

Introduction

This paper covers in a general and non-technical way the topic of operating system hardening. I have deliberately tried to keep this paper as non-technical as it is not the intention of this paper. There are a wealth of technical documents in this field written by much more experienced people than myself, and this is not a technical blow by blow on performing operating system specific procedures for this process.

I have come across many good technical articles on hardening the most commonly used operating systems on the market today, for example, Windows 9x/NT/2000, Solaris, Linux and BSD variants. However it is also apparent that these procedure/policies are not being used en-masse as the alarming number of machine break-ins continues without respite.

This paper tries to look at some of the non-technical issue's related to the what/why/how's of the hardening process, and why you should address it at multiple levels within your organization.

What is Hardening?

For me the easiest way to describe "hardening" is the making of modifications to an operating system before it is put into use to increase its security and performance. By operating system I am including:

- General purpose OS's:
  - Unix (all flavours)
  - Windows (all flavours)
- Infrastructure
  - Routers
  - Switches
  - Load Balancing
  - Network Traffic Bandwidth Management
  - Caching

Securing a system involves implementing a set of procedures, practices, and technologies to protect the information technology (IT) infrastructure as well as software and associated data throughout the organization. From a practical implementation angle these are best developed and tested prior to major deployments of technology within an organization to allow the process to be automated to ensure

consistency and speed of applying the changes so deployment is both timely and tested for security and performance.

Because computer security involves the enterprise's total set of exposures, from the local workstation or server to the Intranet and beyond, it cannot be attained by simply implementing a "magic bullet" software product solution or by installing various security solutions. Computer security must be implemented by reliable mechanisms that perform security-related tasks at each of several levels in the environment. Implementation also involves applying security procedures and policies at each of these levels. The process of hardening can address security across multiple environments and applications with an organization.

As an overview, areas to look at for what should be covered in a complete hardening process in a heterogeneous environment are listed below:

- Operating system
- File system
- Network Services
- System services
- Applications
- Performance tuning

The operating system itself comes under a heavy scrutiny during the hardening process and the following areas are normally covered:

- Kernel tuning parameters can also be additionally configured
- Operating system patches are also applied to bring the OS up to the most recent and secure version

Every operating system uses some type of file system to control access to physical storage of the machine. Some of the areas off interest here are:

- File permissions need to be modified from their default settings as most OS's ship with a more open set of permissions than is needed in the majority of environments today
- Encryption of local and remote file systems may be configured, depending on the nature of the information being stored

The network services of an OS, which are a critical component of any OS today, and as such, must also be addressed in the process of hardening a machine. Below are some points of note during this phase of the hardening process:

- The IP configuration of the machine can be very important in itself, for example, private vs. public addressing of the hosts
- Is a more secure method of moving sensitive data around the network required? If that is the case then a VPN of some sort needs to be taken into consideration during the hardening process
- What path does information take to get to/from the host? The routing a machine uses should also be taken into consideration during the installation process. The general rule of thumb is that no machines should be running dynamic routing (RIP, OSPF etc) themselves, but let infrastructure devices decide the best path for network traffic

- The configuration of routing devices should also be taken into consideration during the hardening process with templates used to define global default access-lists, routing and filtering rules

Most general purpose OS's in use today also offer system specific services that are used to deliver functionality to users. The majority of these can be modified to improve both the security and performance of the service. Some of these are listed below:

- File Sharing
- Network Printing
- Network Time Synchronisation
- Name Resolution
- Network Based Authentication

Applications are the main reason people use computers. Below is a very simple list of applications.

- File Transfer
- Web Browsing
- Mail
- Newsgroups

However the point to be made here is that just because you go to the extra lengths to address the previous areas, unless you look at the applications themselves, you are missing one of the most important areas when performing any hardening process. As the core of the majority of OS's become more stable, more and more attacks are aimed not at the OS itself, but the application running on the machine, as the easiest entry point of malicious users.

With applications there are also business logic rules, which should be noted and performed as part of the hardening process. Certain businesses have processes which systems emulate. These should also be added to the hardening process so they are applied consistently throughout the organizations resources.

Performance tuning in itself is a form of hardening because in general it is increasing the capacity, throughput and performance of an OS or application. Many vulnerabilities exist today not because of faulty software as such, but software which, with modifications, can out perform a standard configuration both in security, availability and throughput, for example, http://www.checkpoint.com/techsupport/documentation/FW-1_VPN-1_performance.html.

Some people perform the hardening process after the machine is in use, however I strongly recommend that this process be completed before any production related work is completed with the machines. I have seen too many times a development server placed into production without full consideration of the security implications, which end up in a under performing resource and a risk to the organization.

Why is Hardening Important?

The starting point for any hardening model is to assure that security standards and policies are in place to protect the system from external attacks and unauthorized internal usage. Securing computer resources, applications, and related data is an integral part of securing an enterprise and hardening is the cornerstone of that model.

The proof is in the pudding as they say, and nowhere is it more evident when it comes to hardening. Organizations that take this seriously rarely have problems relating to performance and security if a good hardening practice is adopted. For example:

- Every resource is commissioned with a specific purpose in mind and considerations are taken into account based on load, purpose etc. as to how the machine is hardened
- All resources received a basic list of "know good" modifications. Local knowledge is quite valuable here as experience can help greatly in always applying modifications, which you know, work in your environment and not just in a text book. Sitting down at a system and actually performing the recommended steps can prevent errors such as this. This a critical step that should always be performed prior to publishing a security guide. Securing a system can be difficult and frustrating, having impossible instructions in the guide will not make the experience any easier for the system administrator. Also to make the hardening process even harder, some applications simply do not work when certain recommended modifications are made. The best way to do this is to keep the application specific hardening steps separate from the more universal OS modifications.
- All OS's receive modifications based specifically around their function, i.e. web server. So any service specific modifications are additionally performed on top of the more general procedures

You need look no further that the http://www.sans.org/topten.htm list of commonly exposed vulnerabilities to see the results. All of the vulnerabilities listed there all well publicized by the vendors and other interest groups (newsgroups, mailing lists etc). The vast majority of break-ins occur on machines for which there is almost always a relatively easy process to gain information and software to fix the issue. A good hardening process would reduce the vast majority of the vulnerabilities listed in the SANS top ten along with a great many other well know applications and OS related vulnerabilities. Thus giving the organization much more reliability and integrity of its services and information.

Why Hardening Isn't Being Performed

The hardest question of all to answer in the puzzle is this one. If the many documented hardening procedures and policies stop the majority of vulnerabilities, then why isn't every one doing it?

The vast majority of administrators have the skills to perform hardening procedures on machines, but don't. Below I cover some potential reasons as to why this is the case.

The makers of the operating systems are partly to blame for this issue. Almost every operating system that is installed without modification to the standard installation process will have a number of commonly known holes in security. If these remain in place, and the machine becomes accessible by the Internet, then the machine is in a high-risk state to be compromised. Because the main aim of the OS manufacturers is functionality of the product, security is often sacrificed at the expense of functionality. However the average system administrator will have a level of trust of most vendors, in that they think "surely they wouldn't ship an insecure OS". This level of trust is abused on a daily basis with administrators blindly believing in the security of an un-modified operating system.

Change control of production systems can be difficult timing wise. Because hardening is ever a moving target, a big part of maintaining security is through the application of regularly released patches or updates from vendors for their software. In some environments administrators will generally have to go through a change control process, which involves paperwork, and usually after hours work to make these changes. Most administrators aren't especially keen to stay back a couple of times a week applying patches to their machines.

The number of patches released is daunting in their number for the average administrator. If you were to add up the combinations of OS's and the applications which run on them, it would not take long to get large list of products requiring regular updating. It is quite easy to see how average administrators do not get around to applying these as soon as is sometimes warranted due to the sheer number of updates required. Again vendors do not always make the process easy as sometimes instructions can be confusing on which service pack and minor update to apply in which particular order, which in itself is a black art sometimes.

In today's Internet environment applications have very fast development cycles and usually security is the first loser in the hunt for the latest and greatest killer function for an application to perform. All developers should (in a perfect world anyway) keep security issues in mind while application development is performed. This often saves more time in the long run, due to a smaller amount of patching/updating being required.

Interdepartmental boundaries confusing responsibilities for the hardening process are a major issue in big organizations. Most big organizations will have a large IT staff covering different areas of responsibility, for example, servers only, the mail application, backup only etc. As such different groups have very specific and non-overlapping roles. So the hardening process can be muddled by questions like:

- Who is responsible for applying the patches for the OS itself?
- Does the server group which maintains the OS also maintain the application, for example, I'm in the server group and am responsible for the Windows NT OS only organization wide, so who applies the latest MS Exchange Server patch? Our group or the mail server group?

Also the cost of generating good hardening procedures is sometimes viewed as an unnecessary cost by management and they might prefer to place budget money elsewhere. A good hardening and build process requires time and extra resources. Upper management might not always place a priority on the extra costs needed to achieve correctly built servers, wanting only to "just get it going".

Risks to an Enterprise If Hardening Isn't Performed

The potential risks to an organization can be quite considerable if a good hardening process is not in place for the building process of all resources deployed in an enterprise. These risks can be put into the following general categories:

- Monetary – Financial Loss relating to under performing and unsecured resources being used within the organization
- Productivity – Cost of fixing machines affected in terms of end-user and administrator lost productively due to a loss of functionality (server crash or compromise) and performance
- Trust – Loss of good faith of customer/users, which in a modern e-commerce world is a must to succeed. Once lost, this is sometimes impossible to regain and if a company needs the trust of its customers it is then vitally important to protect it
- Legal – What are the legal ramifications in your organizations field of operation relating to your information and its security

I feel that time spent on developing a strong procedure for the deployment of resources initially at inception, pays big dividends in the short, medium and long term time period, in terms of reducing the risks mentioned above to an organization.

Conclusion

If they is any conclusion that I would want the readers of this to take away with them, it is this, the more time spent developing and testing a strong baseline for a particular resource, the more an organization benefits. Most importantly an awareness of the implications of doing this process must be brought to the attention of, and agreed upon, by people in multiple levels of an organization for it to be the most effective.

References:

Security Entities Building Block Architecture
http://www.microsoft.com/technet/security/secentbb.asp

Security Considerations for End Systems
http://www.microsoft.com/technet/security/sconsid.asp

Craig Donovan "**Strong Password**"
http://www.sans.org/infosecFAQ/policy/password.htm

Steven Krychiw: **SecurID: A Secure Two-Factor Authentication**
http://www.sans.org/infosecFAQ/authentic/securid.htm

Todd Arnold: **NT Security**
http://www.sans.org/infosecFAQ/win/NTsec.htm

Common Errors in OS Hardening Instructions, Security Audit Findings and Security Patch Information for Windows NT
Dave Loschiavo
http://www.sans.org/infosecFAQ/win/common_errors.htm

The SANS Institute Consensus of the Top Ten commonly found vulnerabilities on the Internet
http://www.sans.org/topten.htm

Hardening Procedures, Policies and Tools
www.securityfocus.com

Open Source Software Resources
www.freshmeat.net

Performance Tuning (Checkpoint Firewall-1)
http://www.checkpoint.com/techsupport/documentation/FW-1_VPN-1_performance.html