Securing the Foundation of Information Technology (IT) Systems

What vulnerabilities are you exposed to with an unsecured operating system?

Everyone thinks about security today. Organizations deploy firewalls, anti-virus software, network security solutions, application security tools, and so on. One often overlooked area that every organization should protect is the operating system running on your servers. Recent studies show that securing the operating system is widely recognized as a necessary practice in an organization's overall security policy, but it is not being done on a regular, consistent basis across the enterprise. Operating systems control every function that the server provides. The operating system is responsible for the management and coordination of everything that happens on a computer, including how and where resources are shared.

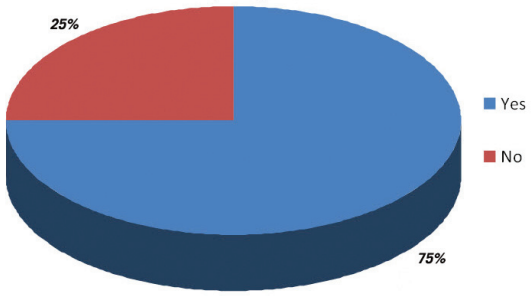
January 2010

Securing the Foundation of IT Systems

System Administration and Security

System administrators today understand security as well as, if not better than, anyone in an organization. With the current threat environment, security has become the focus of many system administrator's jobs. In an independent study conducted at the Large Installation System Administration (LISA) 2009 Conference in Baltimore, Maryland[1], it was determined that 75% of system administrators are responsible for security in their organizations.

As the system administrator, are you responsible for the security for your organization?



Most system administrators agree that locking down, or hardening, operating systems to a prescribed level of compliancy, and maintaining that compliancy across the enterprise is a best practice to follow. However, studies reveal that the majority of organizations are not locking down all of their servers and many are not even locking down all Internet facing servers, which are the most vulnerable. The vulnerability that organizations face when they do not lock down their operating systems consistently and persistently can be devastating. And, there is always the need for someone to blame.

"Special assignment, Chaswick. I need you to test our severance package."

1 Independent research study included live survey of 100 system administrators at the 2009 Large Installation System Administration (LISA) Conference, Baltimore, MD. http://www.trustedcs.com/news-andevents/PRLISASurveyResults.html

Why the Disconnect?

Unfortunately, companies and government agencies are faced with limited resources and increasingly shrinking IT budgets, while at the same time, threats to data and other sensitive and classified information is on the rise. When faced with budget decisions, securing assets can become a costly afterthought.

"In an effort to sustain growth and pick up new users, more social networks are opening up their architecture to allow third-party applications. Cybercriminals can take advantage of this by developing applications out of the social network environment to target users. In addition, access to social network APIs gives attackers a roadmap to vulnerabilities in legitimate third-party applications and a way to tap into user accounts."[2]

The 2010 security landscape is not getting brighter and there are fewer resources to protect our systems from the broadening threat environment.

45% of web servers with malicious reputations are hosted in the United States.[3]

Enterprise-Wide Security

In a constantly changing environment, locking down operating systems across the enterprise and maintaining an identified level of compliancy is no easy task. On blogs frequented by system administrators, questions always arise regarding the lock down process indicating the lack of straightforwardness about the actual process. Regardless of which operating system a company or government agency is running, there are a variety of methods that system administrators can implement to harden an operating system such as free lock down scripts. However, these scripts most often require modification in order to adhere to specific security policies. Modification is a manual process which also introduces the chance for error. What happens when errors are made? Applications do not run and users are unhappy. Scripts can be reversed, but then the operating system configuration is back to its initial state and you

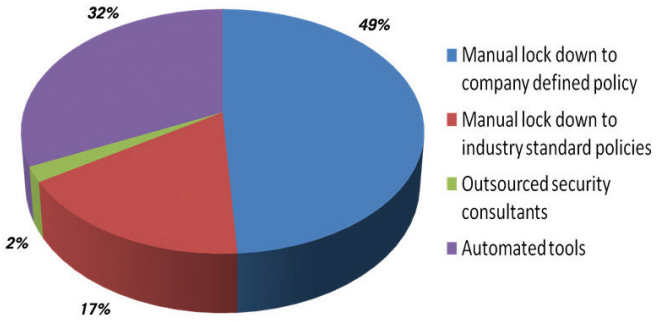
2 "Hackers to sharpen malware, malicious software in 2010," by Robert Westervelt, searchsecurity.com, 19 Nov. 2009

3 McAfee® Threats Report

find yourself starting over again. You cannot simply undo the one lock down that caused the problem. According to the survey of system administrators from the LISA conference, only 32% are using automated tools to assist with the lock down process.

Another option is to turn to a consulting organization that provides services, including scans of the operating system that show how it fares against a set of security best practices. These organizations may also offer lock down services but this can be costly over time. And once the consultants are gone, who will maintain the lockdown? There are configuration management tools available that assess the security of operating systems and make recommendations as to what needs to be done to remediate vulnerabilities. But again, the operating system configuration is manual and therefore the same costs and risks remain.

What is the primary method of system hardening you or your organization engage in today?



What is the Responsibility of the Software Vendor?

It would be optimal if new off-the-shelf operating systems were shipped with fully enabled lock downs, but the vendors that provide these systems would soon be out of business. Operating system installation would be cumbersome at best and once installed, there would be a high probability not all applications would run successfully. So, operating systems are shipped unsecure, so that they can be easily installed and applications can run with minimal configuration. Therefore, system administrators are tasked with locking down all new out-of-the-box operating systems before installing applications, in addition to maintaining lock down after new applications and patches are installed.

Unused Services…..a Prime Target

When new software is installed on an operating system, services required for installation are enabled, but these services may not be needed beyond initial installation. Unused services are a prime target for attackers. They know that services are frequently turned on without the system administrator's knowledge, which make an operating system susceptible to widespread attacks. As part of the lock down process, system administrators should disable as many unused services as possible, including network, peer-to-peer, file sharing and general services. The challenge comes in determining which unnecessary services are enabled, and then disabling them. In the lock down process, system administrators should adjust the kernel's TCP/IP settings to help prevent denial-of-service attacks and packet spoofing. Security at the operating system level fortifies your environment so if penetration occurs through a firewall or application, the operating system is locked down to provide further protection. These additional measures are often referred to as *layered security* or *in-depth-defense*. All of these things help minimize an organization's potential attack surface. If you don't need it, delete it.

The Less You Have, the Less the Worry

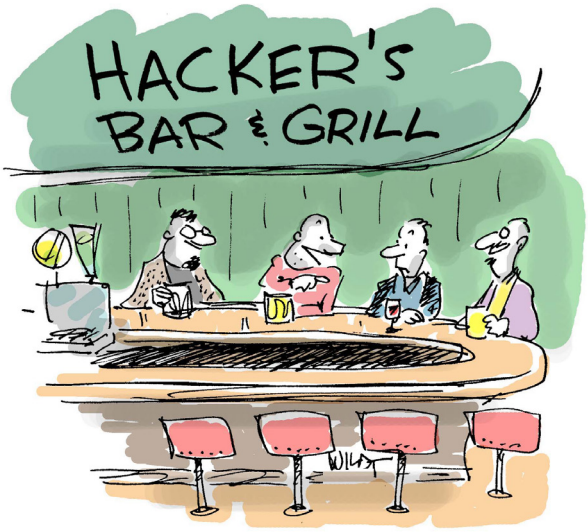
Some of you are thinking, "I have disabled the service, I am using a system-based firewall and I am already blocking those ports, so why the fuss? Besides, if I remove the service and someone needs the software for something, it's a pain to get it back on the system." Another excuse is "I'm on an isolated network and getting software on and off the system is difficult." These are valid issues, but what if your firewall rules fail to parse and the daemon doesn't start? Secondly, the less you have on your system, the less you have to worry about disabling, configuring, and patching. Thirdly, why are you wasting system resources on unused services?

Password Misuse Can be Deadly

Administrative password misuse is another example of a potential vulnerability. According to the "Top 20 Critical Security Controls for Cyber Defense: Consensus Audit Guidelines,"[4] published by the SANS Institute, the misuse of administrator privileges is the number one method used by attackers to infiltrate an enterprise. The second most

4 The Twenty Critical Security Controls: Consensus Audit Guidelines, The SANS Institute, http://www.sans.org/critical-security-controls/

common technique is the elevation of privileges by guessing or cracking a password for an administrative user to gain access to a targeted machine. As part of the operating system lock down practice, organizations must ensure that administrative passwords have a minimum of 12, somewhat random, characters and that all administrative accounts are configured to require password changes on a regular basis. Further enforcement of securing administrative accounts should ensure that machines cannot be accessed remotely.



"Sure, I remember you. I'm terrible with faces but I never forget a username, pin, or password."

Awareness Versus Hindsight

Another best practice to protect an organization's system from attackers is to maintain the highest possible degree of awareness. Logging is key. Without it, you might not know an attack has occurred. Even if you are aware, without logging and analysis, there are no details provided about the attack. Knowing the details allows action to be taken to prevent the attacker from instigating broad-based damage to your enterprise's vital information. An organization's operating system lock down practices must include logging access control events when users try to gain access without having the appropriate permission. And lastly, extensive logging is worth little if potential attackers can gain access to log files. These files should be maintained on separate machines from those that are generating the events.

In addition to knowing that an attack has occurred and having the details to prevent widespread damage, an awareness of changes in the operating system configuration is an important aspect of minimizing your potential attack surface. This is a process known as baselining. Baselining can be defined as:

The identification of significant states within the revision history of a configuration item is the central purpose of baseline identification.[5]

In case this definition is a little too "high brow," this may help. You have just finished building a series of complex systems hosting an important application. You have locked down the systems, passed all of the required security audits, and your application is working. You consider this to be the "initial state" or "good state". Now you want to take a snapshot of the initial state to include a detailed inventory of installed software packages and versions, a list of critical files, networking configurations, and general hardware configurations, to list a few. As time goes by, software updates and patches are installed, and software is removed. Any of these actions could potentially change the behavior of your secured system. If the system or one of its applications malfunctions, the system administrator begins the fault management process, which consists of identification, isolation, and remediation. They ask the question, "what changed?" as that typically identifies the crux of the malfunction.

What if you were able to take a second snapshot and automatically compare it to the snapshot taken of the initial state and see only the differences? You could immediately identify or eliminate configuration changes as the culprit. As a best practice, system administrators should periodically perform a baseline comparison to identify changes that could potentially become a fault. In the case of authorized, expected changes, the baseline comparison can be used as evidence to your change management process that in fact, a specific change has been completed. In many high-availability configurations, you may have systems working in parallel or as a simple fail-over configuration. In these situations, it is critical that the two system configurations be as similar as possible. Running a baseline on each and then a baseline comparison can quickly accomplish that.

5 CMMI Product Team, "Chpt 7, Maturity Level 2: Managed, Configuration Management, SP 1.3," in Capability Maturity Model Integration, Version 1.1 (CMMI-SE/SW/IPPD/SS, V1.1): Staged Representation, Carnegie Mellon Software Engineering Institute.

Consistency Breeds Predictability

Maintaining a predetermined "good state" or configuration policy on every server across the enterprise provides you with control and eliminates downtime and ugly surprises. You will be far less susceptible to malicious attacks, be able to rebound more rapidly when attacks occur, and enjoy more up-time and happy users. Oh, and you might be named "System Administrator of the Year." So, where do you begin?

- Identify and group servers based on the level of security required.
- Identify organizational security policies or look to industry standard practices if internal policies do not exist.
- Define the process you will use to lock down your servers (manual, automated tools, external resources, etc.).

The size of the organization and the number of servers running business-essential systems usually determines the number of resources you will need. However, if you embrace the use of automated tools, the number of resources may be reduced. Of course, it is easier to harden 15 servers and maintain that state than it is to harden 1,500. But either way, you have to start somewhere. Many system administrators begin with research and discover that there are countless published tips and tricks on locking down operating systems. There are web postings, articles, printed and online publications, and guidelines. Everyone has an opinion of the best methods and practices and typically defends their opinions to the bitter end. So how do you determine who really knows what they are talking about?

Standards and Compliancy

Many people turn to standards developed by government organizations, research institutions, and industry. Dr. Andrew Tanenbaum once stated, "the nice thing about standards is that there are so many to choose from." Indeed there are, but they provide a starting point and have been likely vetted by experts.

72% of small businesses have no formal Internet security policy. [6]

The Center for Internet Security (CIS)[7] is one organization that provides standard practices or guidelines for many types of security, including operating system security. Their mission is to help organizations reduce risk by implementing strong technical security controls. They accomplish this mission by developing and making publicly available, security configuration benchmarks. CIS members develop benchmarks across private and public sectors. Many organizations utilize the CIS as a resource to provide best practices for securing workstations, servers, operating systems, networks, and applications.

The Defense Information Systems Agency (DISA)[8] is another source for security guidelines. DISA is chartered with providing information technology and communications support to the President, Vice President, Secretary of Defense, military services, and combatant commands. Part of that mission is to provide the Department of Defense (DoD) with configuration standards for information assurance systems. Known as the STIGs (Security Technical Implementation Guides), these guidelines are a set of instructions or procedures for locking down or hardening a system to a baseline level of security. Although developed for the DoD, the STIGs, or a subset of them, are used by commercial organizations and civilian government agencies. Because they were developed to protect information assurance enabled systems run by the DoD, they are considered to be one of the most stringent set of hardening guidelines available.

Another reputable source of security guidelines is the SANS Institute. SANS is regarded by many as the largest source of information on IT security in the world. They provide training, certification, and the largest available collection of research on security. Part of the research provided by SANS includes security best practices. Most recently, SANS has published The Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG). These include recommended controls for blocking attacks and finding and mitigating the attacks that get through. A consortium headed by the former Chief Information Officer (CIO) of the US Department of Energy and the US Air Force, John Gilligan developed the CAGs. The consortium included

6 National Cyber Security Alliance / Symantec

7 The Center for Internet Security, http://www.cisecurity.org/

8 Defense Information Systems Agency, Security Technical Implementation Guides, http://iase.disa.mil/stigs/stig/

people from the National Security Agency, DoD, Department of Energy Nuclear Laboratories, Department of State, DoD Cyber Crime Center, and security experts that support banking and the critical infrastructure community. The CAGs cover a variety of IT security areas, some of which can be addressed through operating system hardening. Another source for organizations to rely on to provide expert guidance.

Unless you are a defense agency working with information assurance systems, in which case it is mandated that you are compliant with the STIGs, you are not going to fully adopt any set of guidelines, but rather use the guidelines as a basis for establishing your own security policy.

Automated Lock Down with Security Blanket™

Trusted Computer Solutions (TCS) has spent the last 14 years developing, accrediting, and deploying secure solutions for the US Government. These solutions provide government customers with the ability to securely access and transfer classified information, something that is critical to our national security. Leveraging the company's extensive expertise in developing security solutions, TCS has developed a tool that automates the process of locking down an operating system, thus significantly reducing the attack surface.

Many organizations already use configuration management tools to scan their operating systems to determine whether or not they are in compliance with policy. Security Blanket takes it one step farther. It assesses whether the operating system is compliant with policy and then enables the user to automatically lock down the operating system to be compliant. Customers comment that each license of Security Blanket pays for itself after two uses. Manually locking down an operating system is at best a half-day task. If you figure that your system administrator makes $50 per hour, or $400 per day and in one day, he or she can realistically manually lock down two server operating systems, a $360 tool makes a lot of sense.

But the value does not stop there. The Security Blanket Administration Console enables a system administrator the ability to manage any number of servers from a central location. Servers can be assigned to groups based upon the level of security they require. A group of Internet facing servers, for example, might require a tighter lock down than a group of internal servers. Assessments can be run on an entire group of servers as can the automatic operating system configuration of security settings. This makes it very easy to maintain consistency across your enterprise. And, unlike manual lock down, if something goes wrong, Security Blanket enables you to automatically "undo" the lock down, back to the original state or on an individual security setting basis.

Implementing your organization's own security policy via Security Blanket is easy too. The product comes with pre-defined lock down configurations from the CIS, the DISA STIGs, SANS and many more. These pre-defined industry standards that can be used as is or modified to create your own configuration to support your security policy.

Security Blanket supports a number of operating systems including, Red Hat® Enterprise Linux®, Fedora™, Solaris™, CentOS, and SUSE®. It runs on any x86 or SPARC platform, as well as Linux® on the IBM® System z® mainframe.

Conclusion

While there is no one process to make any organization 100% secure, establishing a company-wide security policy based on industry-standard best practices is a good place to start. Many of these best practices can be implemented as part of the operating system assessment and lock down process. Securing the foundation on which your IT organization runs is not easy to do. It takes time, money, and resources, but the potential for an attack is too great and costly to ignore. By implementing a consistent, enterprise-wide operating system assessment and lock down process, a company can stop malicious attacks and keep them at bay.

"Who can hope to be safe? Who sufficiently cautious? Guard himself as he may, every moment's an ambush." Horace (Quintus Horatius Flaccus, Venusia, December 8, 65 BC – Rome, November 27, 8 BC)

Security the Foundation of IT Systems

Who Is Trusted Computer Solutions

Founded in 1994, Trusted Computer Solutions (TCS) is an industry leader in cross domain and cyber security solutions and services that facilitate compliance with security requirements that support business objectives. The company's flagship cross domain solutions enable government to securely share information, striking the right balance between information protection and information sharing, a vital component to national security. Known as the SecureOffice® Suite, these products adhere to stringent security standards set by US Government and are installed and accredited in operational systems around the world. TCS's cyber security solutions automate, accelerate and simplify the application of high levels of security. Security Blanket™ is an award-winning tool that automatically locks down enterprise-wide operating system server deployments, according to security best practices. CounterStorm™ uses behaviorial, statistical, and content-based anomaly detection to identify non-signature, targeted and zero day attacks, with unprecedented speed and accuracy. TCS is headquartered in Herndon, VA, with offices in Champaign, IL, and San Antonio, TX.

For more information, visit **www.TrustedCS.com**

For More Information

443.459.4141

TMurphy@TrustedCS.com

TRUSTED
COMPUTER SOLUTIONS

TCS Corporate Office
2350 Corporate Park Drive, Suite 500
Herndon, VA 20171
866.230.1307

TCS Trusted Operating Systems Lab
2021 S. First St, Suite 207
Champaign, IL 61820
217.384.0028

TCS Texas Office
10010 San Pedro, Suite 220
San Antonio, TX 78216
210.340.3151