Global Information Assurance Certification Paper

"Retrofitting Security Onto Existing Production Systems"
GSEC, version 1.2f
Thomas Taylor
December 24, 2001

September 11th, 2001 Upper Management became painfully aware of the need for increased security. What does this mean? In simple terms, "Security n. 1. Freedom from risk or danger; …. 4. *Computer Science*. a. The level to which a program or device is safe from unauthorized use. b. Prevention of unauthorized use of a program or device."[1]. The existence of our Internet firewall and our haphazard, intermittent and informal security is no longer sufficient to prevent anxiety, doubt or fear in Upper Management. Their concern is that their systems are at risk. Upper Management wants to be assured that their systems have confidentiality, integrity and availability. The problem is how does this organization act upon their concerns and shift from an existing open access environment to a secure closed environment? The complexity of this shift is compounded by the fact that any changes will have to be implemented upon existing production systems. This is a large and daunting project, but it can be done.

Upper Management's desire for increased security needs to be transformed into documentation or into a set of Security Policies. Currently there are no Security Policies in our organization. Internet Security Policy: A Technical Guide [2], RFC 2196 Site Security Handbook [3] and SANS "Basic Security Policy" version 1.7 – July 5, 2001 [4] are excellent sources for gaining an understanding of security policies and how to create them. From the Internet Security Policy: A Technical Guide and SANS "Basic Security Policy", there are several types of security policies that need to be created. These policies are the Program Policy, the Issue-Specific Policy, the System-Specific Policy, and Security Procedures and Checklists. The Program Policy "sets the overall tone of an organization's security approach" [5] and is Enterprise-wide. Issue-Specific Policies "are intended to address specific needs within an organization" [6] and it can be Enterprise-wide, Department-wide or local. An Issue-Specific Policy would be a guide for single discrete issue such as Internet browsing, or email usage, or incident handling. System-Specific Policy is "directed toward each system individually" [7] and will be Department-wide or local and not Enterprise-wide.

The first task in this project is to create a System-Specific Security Policy. This Security Policy will be based largely on the Site Security Handbook section 1.5 "Basic Approach … (1) Identify what you are trying to protect. (2) Determine what you are trying to protect it from. (3) Determine how likely the threats are. (4) Implement measures which will protect your assets in a cost-effective manner. (5) Review the process continuously and make improvements each time a weakness is found."[8]. As stated in the Site Security Handbook, the fourth step will most likely determine if a security measure is implemented [9]. Each step is important. The process of creating the security policy will aid in better understanding the systems and thus foster a greater ability to protect them. This Security Policy will act as a guide for the project. Upon completion of the project, a revised Security Policy will have to be created. Presented below is the System-Specific Security Policy.

The purpose of this document is to guide in the process of retrofitting increased security onto critical production systems.

(1). The existing assets are:
2.6 Solaris Operating System, Solaris Disksuite,
3 Sun E3500 systems (2 production systems and 1 develop system) each with: 4 X 300 Mega-Hertz CPU's, 3 GB of RAM, A5000 arrays, 2 Fast Ethernet Network cards, Graphics cards, 19" Monitors, keyboards,
Oracle8 Database,
System Administrators, Database Administrators, Developers and Users.

Assets to acquire for this project are MD5, GZIP, PGP, the GNU C Compiler, Npasswd, Tripwire, OpenSSH, TCP-wrappers and a new version of "Sendmail".

(2). These assets will be protected from unauthorized use, including unauthorized access to the data, unauthorized use of hardware, and denial of service attacks. The production assets will be protected from a loss of availability caused by the implementation of this security policy.

(3). These systems have been install with the Solaris "Entire Distribution" meta-cluster. This can be confirmed by issuing the command "admintool" as root, which starts a graphical user interface. Drill down from "Browse" through to "Software". The first line in the window is "Entire Distribution 3.6". Double click this first line. The pop up window gives the further detail that this is the "SUNWCall" meta-cluster. This type of install has placed vulnerabilities onto the systems. There are many services and programs not being used by authorized users. These services and programs tend to have default configurations, which are well known. This makes those services and programs vulnerable to abuse. In addition, there are inherent vulnerabilities in the r-commands, telnet, ftp, "Sendmail" and other services. These systems have vulnerabilities that can be found and exploited using automated scanning and hacking tools. The existing vulnerabilities may already have been exploited and the systems compromised. Auditing is not occurring in a timely manner, and access is not controlled by the operating system in a secure manner. As these assets are secured, critical services might be removed which could cause a loss of availability.

(4). The major measures implemented to protect the assets are: the hardening of Solaris, the hardening of Oracle, the training of administrators in better security practices, and the conformation of previous, existing and continued system integrity. The development system will be used to test changes that will be implemented onto the production systems. This will reduce the risk of availability loss to the production systems.

"If you are hardening a machine on which you have already installed Solaris, first remove all packages not needed of the operation of your server" [10]. In Solaris, the command "pkgrm" is used to remove packages that are not needed. After removing packages that are not needed, the remaining packages will be similar to the initial install of the "Core Systems Support" meta-cluster. The "Core Systems Support" is the installation recommended by CERT, SANS and Sun Microsystems. Oracle8 requires additional packages and one of the Sun Microsystems window managers that support Motif. These window managers are "dtwm", "twm" or "olwm" [11].

The remaining packages should include,

For the Core System: SUNWcar, SUNWcsd, SUNWcsl, SUNWcsr, SUNWcsu, SUNWesu, SUNWkvm, SUNWlibms, SUNWntpr, SUNWntpu, SUNWswmt, [12]
For SunFastEthernet/FastWideSCSI-2 Adapter: SUNWhmd, SUNWhmdu,
For GX device driver and header file: SUNWcg6, SUNWcg6h
For Frame Buffer Device Drivers: SUNWdfb, SUNWdfbh
For Enterprise Network and Array Drivers & Utilities: SUNWluxl, SUNWluxd, SUNWluxop,
For Solaris DiskSuite: SUNWmd, SUNWmdg, SUNWmdn,
For Oracle8: SUNWarc, SUNWtool, SUNWlibm, SUNWlibms, SUNWsprot.
For the Motif window manager,
The CDE End User: SUNWdticn, SUNWdtwm, SUNWtdst, SUNWtezt, SUNWdthe, SUNWdthev, SUNWdthez, SUNWdthj, SUNWdtim, SUNWdtrme, SUNWpdas,
The CDE Runtime: SUNWdtbas, SUNWdtdmn, SUNWdtdte, SUNWdtlog, and SUNWdtbax.
This list of packages will not be authoritative until it has been tested. The packages for the Core System are less than that of the "Core Systems Support" meta-cluster. Some packages have been included so that the system will be able to access its hardware resources. As packages are removed, dependencies will be revealed through the "rmpkg" program. Additional packages may be required for system functionality.

After removing the unnecessary packages, test the assets to confirm their availability and integrity. Check and make sure that Solaris and Oracle function in the expected manner. Check and make sure that the users have access to these assets. The system administrators will confirm the system. The database administrators will confirm the functionality and connectivity for Oracle. The users will confirm that the data is as they expect.

The further hardening of Solaris will be accomplished by following the instructions in CERT's Installing and Securing Solaris 2.6 Servers [13], which heavily references and relies upon SANS' Solaris Security Step By Step [14]. Both these documents will be available and used during this process. The tasks will include modifying Solaris configurations, removing some services, and installing new security programs. The tools MD5, GZIP, PGP, and the GNU C Compiler will be installed and exist only on the development system. These tools are required for installing the new security assets, Npasswd, Tripwire, OpenSSH, TCP-wrappers, and a new version of Sendmail. The new security programs will then be installed, tested, and accepted, on the development system, and then exported to the production systems.

Tripwire is being installed and applied to existing systems. Tripwire will not show if the systems have been previously compromised without additional work. A Tripwire comparison, between the existing systems programs and the original Solaris release with patches, is required to confirm the integrity of the systems. The original Solaris release, for comparison, will be obtained from the CDROM media. The patches, for comparison, will be obtained online from Sun Microsystem, Incorporated. OpenSSH and TCP-wrappers will be configured to allow access, for authorized users, to the systems.

Tripwire, OpenSSH, TCP-wrappers and configuration changes made to Solaris create additional information rich audit and log files. These files will be monitored daily by the systems administrator. They will look for unauthorized access attempts, unauthorized access or for any other irregularity. In order to recognize irregularities, the systems administrators will have to

become familiar with what are considered *normal* events on the systems. The daily inspection of audit and log files will aid them in this familiarization process.

The Oracle application on our systems needs to be secured. As Operating Systems become less vulnerable to exploitation, hackers will target vulnerabilities in applications. Oracle Corporation recognizes this and has formed a security group to find and repair vulnerabilities in their applications. A reference source for hardening Oracle is the Oracle8 DBA Handbook: Chapter 9 "Database Security and Auditing"[15]. One excellent procedure for securing Oracle is to set the ORA_ENCRYPT_LOGIN=TRUE in the user environment and to set the DBLINK_ENCRYPT_LOGIN=TRUE in the ora.init parameter file [16]. The will cause Oracle passwords to be encrypted, thus preventing *in the clear* passwords from being sniffed on the network. This guide also has detailed SQL statements that will enable account locking [17], password aging [18], password expiration [19], password history [20], and password complexity verification [21]. Before these utilities are enabled, the administrators, developers and users will have to accept them as necessary, and to be trained on secure password policies and practices.

The Oracle application is a very large and complex program. Large size and complexity in an application increases the likelihood that it will contain vulnerabilities. The entire Oracle product suite should not be loaded. Load only the minimum amount of product required for functionality. The Oracle application has already been install. The command "runinstall" will show installed products, will install products, and will uninstall products. Our initial install of Oracle was a minimal one. Use the "runinstall" command to verify that there are not any unnecessary Oracle programs on the system.

System administrators need to understand their systems and the new security tools that are being installed. The security tool and system log files must be audited. A false sense of security will do more harm than no security, and this would be a step in the wrong direction as we try to move away from our existing state of vulnerability. The administrators need security training. The administrators will have to be allocated time and resources to familiarize themselves with the systems and the system changes.

(5). Upon completion of this project, the project will be reviewed. From that review, a new production System-Specific Security Policy will be created. Layering the defenses for the core systems should be considered. Trip-wire is a host based intrusion detection system. It will act like a security camera at a convenience store. It will not stop a crime in progress or, in our case, stop an intrusion as it occurs but will only detect intrusions that have occurred. Increasing security by an acquiring intrusion detection system that will detect intrusion attempts and acquiring an internal firewall to protect the core production systems should be considered, during this review process.

The System-Specific Security Policy, from above, has the benefit of largely being transparent to the user community.

The second task in this project is to begin the process of creating a broad Enterprise-wide Program Policy. This task is more visible. For Program Policy to be successful, it requires the input and acceptance of management, administrators and users. This is a big project. The first

step in this task is to identify who is responsible for creating the Program Policy. Should it be Management, a group of department heads, Human Resources, the Information Technology group, or the Attorneys? It should be a group representing these various interests. If there are individuals in this group creating the Program Policy that are not security aware, then guidelines and information documentation to aid them in understanding what is needed will be required. A quick security awareness course in a nutshell for them might be:
We have assets. We want Confidentiality, Integrity, and Availability for these assets. Assets have vulnerabilities. Threats exploit vulnerabilities. The probability of this happening is risk. A risk that has been actualized results in the loss of Confidentiality, Integrity and/or Availability. This loss is detrimental to the enterprise. Risk needs to be mitigated. The mitigation measure should not cost more than the loss.

When the Program Policy Group initially meets, the task for the group should be defined, such as "A security policy is a formal statement of rules by which people who are given access to an organization's technology and information assets must abide" [22]. This can be a starting point for the group. The policy writers will need to formulate a purpose or mission statement for the Program Policy that fits the enterprise.

The Policy group also needs to understand that the desired increased security placed upon the enterprise is going to happen to an existing production environment. There will be a general resistance, in the enterprise, to the loss of availability as it is exchanged for security. The policy writers have to carefully consideration each element of the policy and its effect. For example, if a stringent password policy is implemented, will the users' frequently changing and hard to remember passwords start showing up on post-it notes attached to monitors? If this occurs, then this policy will have failed.

The group creating the policy will need help identifying assets. It needs to be understood by the group that personnel should be considered assets, along with software, hardware, and enterprise and department functions. An asset list for them to consider prior to starting their process is:
Operating Systems,
Database engines, Database front ends,
Applications for Document Storage, Engineering, Financial, Human Resource, Law Enforcement, Library, Utilities, Utility Billing,
Email, Web browsing, and various other desktop applications,
Servers and applications for Firewall, Web hosting, FTP, Proxying, mail, network files, DNS, VPN, …
Server systems: CPU's, RAM, disks, tape drives, tapes, monitors, keyboards, mice, network connections, UPS's, modems,
Desktop systems: CPU's, RAM, disks, monitors, keyboards, mice, network connections, UPS's, modems,
Network: LAN, WAN, Internet, routers, switches, concentrators, wire, optical fiber, T-1's, racks
Departments of Fire, Human Resources, Information Technology, Law Enforcement, Parks and Recreation, Public Libraries, Public Utilities, Public Works,
Managers, Administrators, Developers, Users, Attorneys, Engineers, Electricians, Firemen, …
"Use of Electronic Systems And Tools" signature form,
Policies and Rules imposed by outside Regulatory Agencies.

These assets have vulnerabilities. They need to be identified for and by the group. The following are examples of enterprise-wide vulnerabilities that should be brought to the attention of the Policy group. The public has walk up access to the browse the Internet from enterprise's Local Area Network. Operating systems, applications and hardware have vulnerabilities. The enterprise's "Use Of Electronic Systems And Tools" signature form does not have mechanisms that allow exceptions. Some exceptions are required for employees to do their jobs. These exceptions are informally being allowed. This makes the form legally unenforceable and thus creates vulnerability for the enterprise. The employees that have been given an informal exception to the signature form might still be discipline or even terminated. These employees are vulnerable due to the signature form not allowing exceptions.

There are threats to the assets. These threats are cyber terrorism, script kiddies, corporate espionage, "malware" (viruses and hack tools), and disgruntled or former employees. The policy group needs to understand that even by dismissing the human threat element as neglible, threats coming from automated sources are a certainty. A system placed onto the Internet will be probed in less then fifteen minutes [23]. A vulnerable system can be compromised in less than one minute. All this can happen with automated hack tools, which are readily available on the Internet.

It is not the job of the group to mitigate the risks created by the threats and vulnerabilities. The Program Policy should set the duties and responsibilities of risk mitigation to the appropriate employees. This Policy should delineate the rights, if any, of the employees. This Policy should take into account any regulatory agencies rules and policies that apply to this enterprise. The Program Policy should set the tone for Issue-Specific and System-Specific Policies. These policies should be limited to one or two pages. They should individually address the issues of passwords, web browsing, Email, FTP, Incidents, Backups, viruses, firewalls, encryption, remote access through modem or VPN, employee exits or hires, networks, and privacy. These should be able to be incorporated into the Program Policy. The group that writes the Program Policy should be the same group that convenes to review it and change it.

In conclusion, the large project of retrofitting security onto production systems will be difficult. It needs to be done carefully, so as not to create a self inflected denial of service. It is possible as describe above, but it will take time.

References:

[1]. The American Heritage Dictionary Of The English Language, 3rd ed. (Houghton Miffin Company, 1992), p. 1632.

[2]. Internet Security Policy: A Technical Guide, URL: http://csrc.ncsl.nist.gov/isptg/html/ISPTG.html

[3]. B. Fraser, RFC 2196: Site Security Handbook. URL: http://www.ietf.org/rfc/rfc2196.txt?number=2196

[4]. Gary Kessler, "Basic Security Policy", 1.2 SANS Security Essentials II: Network Security, (2001), pp. 2-1A – 2-39A.

[5]. Ibid., p. 2-6A.

[6]. Ibid.

[7]. Ibid.

[8]. RFC 2196: Site Security Handbook, p 4.

[9]. Ibid.

[10]. "Installing and Securing Solaris 2.6 Servers". URL: http://www.cert.org/security-improvement/implementations/i027.02.html

[11]. Table 1-2 Operating System Software Requirements, Chapter 1: Requirements and Features, Oracle8: Release 8.0 for Sun SPARC Solaris 2.x Installation Guide, (Oracle, December 1997), p. 1-4.

[12]. Alex Noordergraff and Keith Watson, Solaris Operating Environment Minimization For Security: A Simple, Reproducible, and Secure Application Installation Methodology, (December 1999), p.10, URL: http://www.sun.com/blueprints/1299/minimization.pdf

[13]. Ibid. "Installing and Securing Solaris 2.6 Servers".

[14]. Hal Pomeranz, The SANS Institute: Solaris Security, Step by Step Version 2.0, (Deer Run Associates, 2000).

[15]. Kevin Loney, Oracle8 DBA Handbook: What Every System Administrator Needs to Know for Effective and Efficient Database Management, (Osborne McGraw-Hill, 1998).

[16]. Ibid. p. 329.

[17]. Ibid. p. 309.

[18]. Ibid.

[19]. Ibid. p. 310

[20]. Ibid. p. 311

[21]. Ibid. pp. 312-316

[22]. RFC 2196: Site Security Handbook, p.7.

[23]. Keith Johnson, "Hackers Caught In Security 'Honeypot'", Wall Street Journal Online, (December 19, 2000 6:01 AM PT), URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2666273,00.html