Global Information Assurance Certification Paper

An Intrusion Detection System Process: Defense in Depth
Scott Manderscheid
February 9, 2001

Introduction:

When establishing an Intrusion Detection System Process, a **defense in depth process** concentrating on software, networks, and hardware is the key to success. Before operating systems can be hardened, system sensors installed, and networks monitored, a model must be created for each unique network segment; assumptions cannot be made - what worked once is not the guarantee for success the next time. First, "identify*ing* the systems that must be protected for business to continue or trust to be maintained[1]" must occur. Where does a company direct its personnel, hardware and monetary resources? Secondly, while levels of protection are informal processes for most companies, these informal security steps must be documented, defined, and firmly established formally as part of the Corporate Culture. According to a Computerworld "concerned organizations don't wait for a grand plan. Instead, as they identify internal and external threats and vulnerabilities, they recognize that they probably need to be safer than they are and they identify a set of basic controls and then systematically implement them.[2]" The key is to not to react, as these companies are doing, but rather to be proactive, establish standards and policies, and document where the company is suppose to evolve in a systematic process. This is possible by creating a **Systems Security Program**. This program, if designed correctly will stop intruders from entering into the "corporate jewels area." Equally important this Security Program must be a living model; it must be continuously evaluated and updated. Finally, the executives must "buy" into this process or it is destined to fail.

The Defense in Depth Model:

First Layer. "**The Perimeter"**. For any model to succeed, the perimeter must be defined. It is not only a question of where are the servers, switches, hubs and routers located, but also where are the doors and windows located that individuals can access to obtain "local control" of these devices? Are there metrics to validate entrance into those rooms and devices? A Company's Physical Security Program must include actively monitoring all personnel entering and exiting these Physically Protected Spaces. Additionally, routers must be configured to provide both passive and active defenses against hacking and Denial of Service (DOS) type attacks.

Second Layer. "**Passive Network Monitoring."** There are multitudes of network health processes providing System Administrators valuable information on the health of a network. These processes should be included as an Indications and Warning (I&W) network. (Acting much like an early radar warning system). MRTG, HP OpenView and a multitude of other programs provide information on bandwidth monitoring, CPU utilization, Disk Space usage, application usage, and other such valuable information. As System Administrators intuitively know what is considered "normal activity" for their networks, any "out of band" increases are

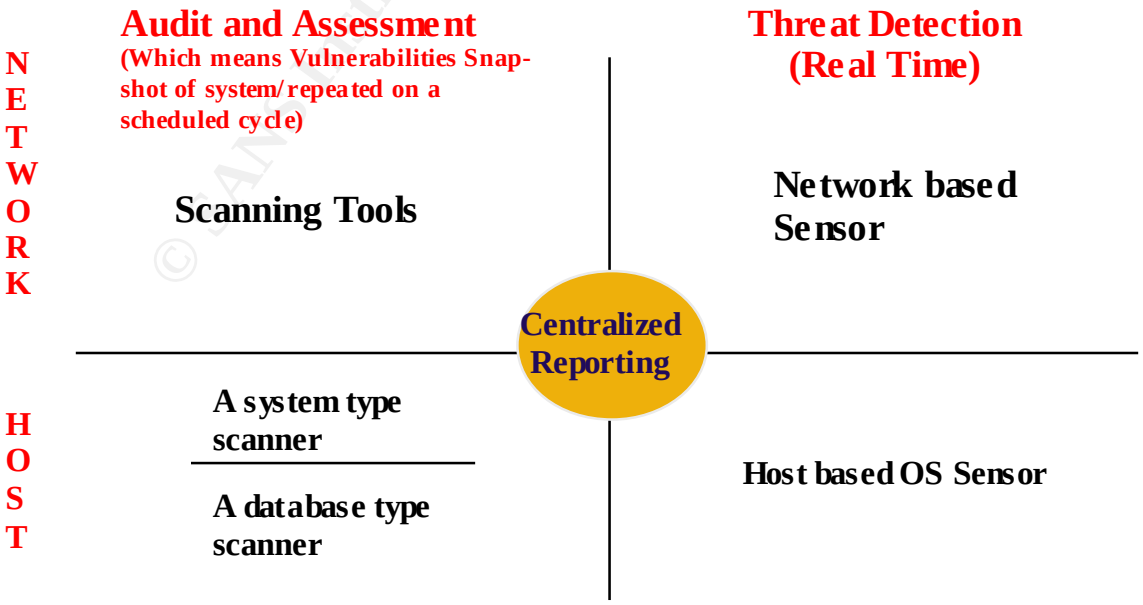
[1] Sans Institutes Resource, Essential Security Actions Step by Step, 1999 http://www.sans.org/newlook/resources/esa.htm
[2] Computerworld, Computer Security's Top Three Questions, 30 August

readily noticeable. Incorporating this raw information into a central area will allow Security and Systems Administrators another means to detect something going amiss.

Third Layer. **"Active Operating Systems Monitoring."** System Administrators and System Security Personnel must continuously audit the internal networks. Firewall logs, switch and router activity, computer system logs, and read/write permissions should be reviewed on a weekly or twice monthly basis. These audits will provide critical information on the activities occurring not only on the network, but also on each system. Once these systems are audited, and logs archived for forensic purposes, the activity of each system can not only be tracked and monitored, but changes immediately noticed during the audit. Furthermore, once normal system and network operating standards are created, unused services can be turned off, ports blocked, and systems hardened.

Fourth Layer. **"The Bait."** No matter how well protected your system is, you must assume it will be penetrated. If the attack and system compromise does not originate from an outside source, it will be from a disgruntled employee, System Administrator accident, or internal intruder. Therefore, a "Honey Pot" or dummy LAN generating enticing data patterns, promising folder descriptors and other such fronts can lure the intruder/hacker away from the actual network and systems and provide you time to recover from a successful network penetration. This Honey Pot should be equipped with probes, Operating System sensors, and tracking software to identify the intruders who "mistakenly" negotiate through the outer layers. Additionally this "Bait" will provide valuable resources on I&W.

Fifth Layer. **"Intrusion Detection."** An "umbrella" Intrusion Detection System (IDS) software program will allow the System Security team to determine when critical software files and./or programs on all systems are changed, added, or deleted. This system needs to be multifaceted and integrate each level of data collection and reporting, and compliment upper and lower tiered programs. This **Systems Security Program** must be tiered and cover network and operating systems issues.



The two major categories for the System Security Program are audit and assessment and threat detection. Audit and assessment begins with how does the hacker view your network. It also includes being able to "implement a file integrity (cryptographic fingerprinting) system to ensure that you can tell which files were changed in an attack[3]." Finally, it ties in database type scanners with the system type scanner. These two programs allow you to know what the read/write permissions are for every file/executable program with the system, and who has access to which files. Threat detection focuses on network probes and OS sensors providing real time alerts on what is happening with network traffic, bandwidth utilization, OS registry changes, etc. All of these sensors, agents and probes need to deposit the data into a central "repository". This data repository then provides vulnerability and risk assessments, intrusion detection attempts and successes, and network analysis reports.

Sixth Layer. "**Administration/OS software and patches"**. The most fundamental layer of security is OS and application patches. Without patch updates and fixes, even the most physically isolated computer can be compromised in minutes. Statistically speaking, every computer will be probed at least 5 times during its live cycle. I have witnessed a server compromised (rooted) in less than 1 day after it had been connected to the Internet. The System Administrator forgot to install the updates and patches. These updates will provide protection against software related vulnerabilities and hazards. Simply quoted: "Implement the latest applicable patches, remove or tighten unnecessary services, and tighten system settings on each host operating system (as described in SANS Step-by-Step guides).[4]" These simple steps will solve two thirds of a company's problems. After all, there is always an easier target down the (internet) freeway.

Seventh Layer. **Administration/Routine Administrative functions"**. Never allow unrestricted, unencrypted, and unvetted access to the operating system. Simply stated: never conduct sysadmin processes from an unvetted link. It is as easy as never transmitting clear text passwords, and ensuring a trusted relationship is established between the two systems. Ensuring all remote communications to a system is using a SSH2 or like process is akin to putting a guard at the entrance to a bank. It adds a layer of protection, calms the customers (your bosses), and tells the criminals that it will take more effort to break into your system.

Eighth Layer. "**Procedural/Formal and informal"**. Every informal process will fail without proper documentation during a critical phase. Documenting security policies and procedures will provide an integral standard that guarantees efficient, reliable, and responsive security practices to meet all security requirements for safeguarding the facility, personnel, and your customers.

Ninth Layer. "**Staff".** No one knows the network and system devices like the Security and System Administrators, who are continuously monitoring the network health and current status

[3] Sans Institutes Resource, Essential Security Actions Step by Step, 1999 http://www.sans.org/newlook/resources/esa.htm

[4] Sans Institutes Resource, Essential Security Actions Step by Step, 1999 http://www.sans.org/newlook/resources/esa.htm

of IDS activity. These individuals will often know something is going wrong before a sensor or probe will provide an alert. Additionally, they often provide early I&W's to management that "something" is wrong. While this is an informal byproduct, the System Security Engineer and System Administrator needs to have a means to provide these symptoms to management for evaluation as a situation is developing and to the Security Incident Response Team (SIRT) if warranted.

Tenth Layer. "**Quality Assurance"**. Finally, an independent third party needs to conduct a documented annual audit. This audit validates current procedures and policies and provides a general indication to the relative health of the systems and network, and provides the checks and balance to the entire system.

Conclusion:

This defense in depth model provides multiple levels of system and security hardening. While it might be impractical for a company to implement every layer of defense (costs, staffing and level of knowledge constraints) without outsourcing, it is possible to initiate some of these protections. Additionally, as companies depend more and more on the Internet as a communication resource, B2B and B2C process, and streamline department functionality, system security becomes critical. Microsoft has proven numerous times, size does not matter, if a dedicated hacker wants to cause your business harm, it will. They have the time, knowledge (script kiddie programs and internet chat groups) and resources (internet and Mom's computer) to ultimately interrupt your service. With that said, it is possible, even likely, that you can cause the criminal (read hacker) to go elsewhere. All you have to do is to harden your system more than the CEO's down the (Internet) highway. After all, would you rather rob a bank with or without a guard and alarm system? Soft targets are easy targets.

Bibliography:

1. Delio, Michelle, Microsoft Crashes: The Fallout, 11:15 a.m. Jan. 26, 2001 PST, http://www.wired.com/news/business/0,1367,41454,00.html

2. McClure, Stuart, and Scambray, Joel, "Hacking Exposed", Osborne/McGraw-Hill 1999. And the following link http://www.hackingexposed.com/

3. SANS Institute, "Windows NT Security Step by Step", version 2.15, July 30, 1999. http://www.sans.org/newlook/publications/ntstep.htm

4. SANS Institutes Resource, "Essential Security Actions Step by Step", 1999 http://www.sans.org/newlook/resources/esa.htm

5. Tipton, Harold F. and Krause, Micki, "Information Security Management Handbook, 4th Edition, Auerbach, 2000.

Last Updated: July 26th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS