Global Information Assurance Certification Paper

Purpose
This paper is a brief overview about host security considerations. A host could be an individual's box or server. Security is a process that should ensure the confidentiality, availability and integrity of systems and information. Security takes a lot of consideration, education and planning to implement. This paper should also provide links that will aid in locating more information on the topics briefly discussed here.

Word Central defines the word "process" as, "A series of actions or operations leading to a result." This definition fits what security needs to be. Security needs to be a series of operations that lead to a secure box. Security is not just a user id or a password. One way to view security is as an onion. Onions have many layers. Security should provide many layers of protection. Id's and passwords are only a piece of the onion.

Risk Analysis
The outer layer of the onion is risk analyses. Risk analyses is the questioning stage. We need to take a look at the scope of what we need to secure and define the risks. Questions to ask may include:

- What are we protecting?
- What is the value? Value may include a lot more than physical value. Value may also include customer confidence, reputation, data and other over looked items.
- What are the risks?
- What types of things could potentially happen? Look at both real and imagined possibilities.
- If something does happen, what is the impact to the organization?
- What is the worst case scenario?
- How can risk be minimized?
    - Will the benefits of minimizing the risk to the organization outweigh the cost?

If it is cost effective then risk needs to be minimized.

Polices
Once we know what the risks are, and what we need to protect, we need to develop a plan, this is where good policies come in. Good policies will help you manage your risks. Find out how your organization develops policy and who needs to sign off to get your policy implemented. Draft and refine your policies. Policies should make a statement identifying the purpose of their existence. Polices should identify who, what, when, where, why and how. Language used should be understandable, realistic and to the point. For more information on developing polices see GIAC Basic Security Policy by Stephen Northcutt. Including some users in the development stage may also be a good idea. In researching and including other views, you may learn information that will help later in implementation. User involvement may also help get user buy in of policies in some circumstances.

An organization may have several policies. These might include policies on such things

as: acceptable use, passwords, ethics, incident response, backups, remote use, laptops, physical security, access controls, software, applications, viruses, screen savers, hardware and the list goes on.
For more information on policies see http://www.cert.org and http://www.boran.com/security/

Once the policy is established and signed off on by management, it needs to be communicated to the users who are to be responsible for adhering to its contents. Communication and education play a great role in security. Once the policy have been communicated, get it in writing, that each user has read and understands both the policies and the penalties for not adhering to the policies.

Users
Education and training belong in each layer of the process. Although many of the layers have some overlap, education is special and actually helps bond the layers of the onion together.

Users are a layer of the onion. Their understanding and attitude can have a major impact on the security of boxes they are responsible for. The role of education can't be stressed enough. Users are one of the biggest makers or breakers of security. Sometimes the simplest changes can make a big difference. Many times users don't understand the issues or see the risks as sufficient to adhere to the policies that have been set. They may believe that they don't need strong passwords because "What would anyone want with my account" or "So what if my box gets hacked, there is nothing on it anyhow." They don't understand the potential issues and importance of what they have access to. People also tend to want to be helpful so they will easily be fooled into providing information that could be costly to organizations. This is one of the reasons social engineering is so successful. Helpdesk are a great target for information gathering and changing. Users also may think nothing of sharing passwords or writing them down and taping them to their monitors. Users also will leave computer logged in and leave their desk without providing some sort of password protected lock on their system. Education of users can go along way in reducing risks.
For more information on passwords see:
http://www.oc.nps.navy.mil/~cook/Security/oc2020_password.html
http://www.unb.ca/csd/student/unix/passwords.html
http://www.adpc.purdue.edu/BSC-Pete/passwrds.htm

For more information about social engineering see:
http://packetstorm.securify.com/docs/social-engineering
http://netsecurity.about.com/compute/netsecurity/cs/socialengineering/index.htm

Other topics worth educating users on include:
- Opening unsolicited email and running executables.
- Applying patches to applications and operating systems.
- Understanding effects of being a "weak" link.

- Using encryption to encrypt information that is proprietary or sensitive.
- Installing software that is not approved.
- Putting systems on a network without first patching and securing them.
- Running unnecessary services.
- Updating virus definitions.

The list goes on and on.

The Box- Building and configuring

Before putting a machine on the network, the machine should have logging turned on and all unneeded services and protocols turned off and patches applied. Most operating systems are very friendly and install with most things turned on and wide open. The average user is not usually aware of this. The average user is also not aware that patches exists and should be applied to the system. Vendors typically have websites that indicate what public security issues their software has and how to apply patches. Most also have mailing list to send users updates and information when available. Another great source of software vulnerabilities is http://www.securityfocus.com/. For information on securing nt- http://www.microsoft.com/technet/winnt/winntas/technote/planning/secnt2.asp and http://www.enteract.com/~lspitz/nt.html, SANS also provides a great papers on securing NT and Linux available through http://www.sansstore.org/ or the GIAC training.
For information on securing linux- http://www.enteract.com/~lspitz/linux.html SANS also provides a great paper on this topic as well.
For information on securing Solaris- http://www.enteract.com/~lspitz/armoring.html
It is also very important to keep up on new patches and updates once a system has been built and in production.

Logs

Users should review their logs daily to look for possible intrusions, malicious activity or simply misconfiguration. Logs often give information that can be handy in telling us of potential trouble. Looking at them can be well worth the time invested. By default the logging in NT is not on. For more information on logging in NT and 2000 see http://www.microsoft.com/TechNet/security/monito.asp.
Many Linux systems store logs in /var/log.

Virus Software

Windows machines should have a good virus checker installed. The definitions should be the newest and should be updated monthly or as often as updates are available. There are several decent products available. More information on virus and virus definitions can be found at http://www.cert.org/other_sources/viruses.html.

Logging on and File Transfers

Users should also have access to a secure mechanism for logging on to other boxes and for file transfers. Telnet and ftp are not secure protocols. They send passwords in clear text and that can be sniffed.
Products for securely connecting to other boxes include:

- Secure CRT, http://www.vandyke.com/ SecureCRT uses secure login and data transfer capabilities of Secure Shell.
- OpenSSH, http://www.openssh.com/
- F-Secure, http://www.europe.fsecure.com/products/ssh/. F-Secure provides secure login connections over unknown or untrusted networks.

Secure Email

Users should have access to some sort of encryption mechanism to send encrypted mail or files. Without using encryption, sending email over the Internet is equivalent to sending a postcard. For more information on secure email please see,
http://coverage.cnet.com/Content/Features/Howto/Encryption/ss02.html
http://www.earthlink.net/internet/security/encryption/email.html
http://www.home.es.netscape.com/security/basics/email.html

Applications

Applications that run on a box should also be examined for possible security breaches. Unknowingly people will install insecure software and think nothing of it. New software should go through some type of testing and review process before being installed on machines. New software often opens new vulnerabilities. New software should not be run without a thorough understanding of the technology with all of its strength and limitations. One instance that comes to mind, was an instance when a backup software package created a copy of the SAM file, and put it in a special directory for the backup software. This directory by default gave everyone full access to the SAM file (even guest).

Firewalls

The next layer for securing a box should include some type of firewall. There are several types of firewalls. Firewalls look at incoming packets and discard those that don't meet a specific rule based on what they are programmed to accept. The firewall product will deny access to unauthorized connections and show you where those attempts originated from and where they were headed. You can also tell what ports they were destined to. There are many types of personal firewalls that can exist on the host. There are also firewalls that are used to protect networks. Information gathered from logs can be used to find patterns, misconfigured equipment and break-in attempts. You may wish to use this information to communicate those attempts to the owners of the originating hosts. For more information on personal firewalls for Windows see http://grc.com/su-firewalls.htm.
For more information on linux filtering and firewalls see
http://www.openwall.com/scanlogd/,
http://www.psionic.com/abacus/portsentry/,
http://cheops.anu.edu.au/~avalon/ip-filter.html.
For additional info on firewalls and choosing one that suits your needs see
http://www.boran.com/security/it12-firewall.html.
http://www.robertgraham.com/pubs/firewall-seen.html
SANS also has a good reference of Trojan port numbers available at
http://www.sans.org/newlook/resources/IDFAQ/oddports.htm

Ids
Another layer may be to deploy an IDS system. An IDS (Intrusion Detection System) detects malicious activity. There are host based and network based systems. They can generally be configured to give you much more information than a firewall. They may also be set up to perform some action based on rules that are set for the IDS. The entire packet can also be captured to review later. IDS like firewalls and other mechanisms mentioned have limitations. For more info on IDS see
http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm
http://packetstorm.securify.com/papers/IDS/ids.ps

So what does it all mean? While no system is totally secure, protecting a system with a layered approach should help offset some of the risk. Testing and auditing the layers to ensure they are functioning well and as expected should be completed on a routine basis. Policies should also be reviewed and updated periodically to ensure they still make sense and tested to make sure they are being followed. If you happen to come across and intruder take a look at http://www.cert.org/tech_tips/.

Written by: Robin Tremblay –please don't post real name. 11/13/00

REFERENCES

GIAC Basic Security Policy –Stephen Northcutt

Word Central Dictionary, 2000 Merriam-Webster, Incorporated, (2000 Nov) URL:
http://www.wordcentral.com/

Boran, Sean. "IT Security Cookbook ", 30 August 2000 URL:
http://www.boran.com/security/

CERT Coordination Center, May 2, 2000, URL: http://www.cert.org

Cook, Mike. "Password Tutorial" 1 Jul 99, URL:
http://www.oc.nps.navy.mil/~cook/Security/oc2020_password.html

jaf@unb.ca. "Passwords -- Why yours is important", July 5, 1999 URL:
http://www.unb.ca/csd/student/unix/passwords.html

implement@purdue.edu. "Setting Strong Passwords", http://www.adpc.purdue.edu/BSC-Pete/passwrds.htm

Packetstorm, Several papers available, non-specific for this paper.
http://packetstorm.securify.com/docs/social-engineering

About.com, Several papers available, non-specific for this paper, 2000.URL:
http://netsecurity.about.com/compute/netsecurity/cs/socialengineering/index.htm

Security Focus. Several papers and info available, nothing specific for this paper .URL:
http://www.securityfocus.com/.

Microsoft Corporation. "Securing Windows NT 4.0 Installation"12 January 2000, URL:
http://www.microsoft.com/technet/winnt/winntas/technote/planning/secnt2.asp

Lance Spitzner,"Armoring Solaris", 22 October 2000 URL:
http://www.enteract.com/~lspitz/armoring.html
Lance Spitzner "Armoring Linux ", 19 September 2000, URL:
http://www.enteract.com/~lspitz/linux.html
Lance Spitzner, Armoring NT, 16 April 2000, URL:
http://www.enteract.com/~lspitz/nt.html

Van Dyke Technologies, Inc., Vendor site, 2000 URL: http://www.vandyke.com/
OpenBSD. Vendor site, 1999-2000. URL: http://www.openssh.com/
"F-Secure. Vendor Site. "Protecting Data in Transit - F-Secure SSH"
http://www.europe.fsecure.com/products/ssh/

CNET Networks. "Protect Your Email", 1995-2000 URL:
http://coverage.cnet.com/Content/Features/Howto/Encryption/ss02.html

EarthLink. "Using the Internet: Security: Encryption:"2000. URL:
http://www.earthlink.net/internet/security/encryption/email.html

Netscape."Secure Email," 2000. URL:
http://www.home.es.netscape.com/security/basics/email.html

Gibson, Steve. "Shields UP," 2000. URL: http://grc.com/su-firewalls.htm.

Psionic Software, Inc. "Psionic PortSentry 1.0". 10 May 2000.URL:
http://www.psionic.com/abacus/portsentry/

Reed, Darren. "IP Filter", URL: http://cheops.anu.edu.au/~avalon/ip-filter.html

Graham, Robert."FAQ: Firewall Forensics (What am I seeing?)" 20 June 2000 URL:
http://www.robertgraham.com/pubs/firewall-seen.html

von Braun, Joakim. "Intrusion Detection FAQ" 2000. URL:
http://www.sans.org/newlook/resources/IDFAQ/oddports.htm

Northcutt, Steve. “Information Assurance Foundations”. 2000. URL: located at SANS level 1 training from http://www.sans.org

Various Authors see each portion of FAQ. “Intrusion Detection FAQ.” 2000. URL: http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm