Global Information Assurance Certification Paper

Network Security Assessment

Abstract:

An essential part of any security plan should be a periodic security assessment. Security assessments are a way to look at the current state of your network, and determine if any new vulnerabilities exist, or if any policies or procedures can be refined to achieve a greater level of security. This often overlooked aspect of network security can be as elaborate or as simple as your security policies require.

Recommendations:

Despite the differences in network designs, there are some steps to keep in mind when doing your security assessment.

1) First off, gather all your policies and read them. While I agree this is not the most exciting part of a security assessment, it is an essential step! Examine the policies for obvious holes.

   Is there a policy giving you the right to perform an audit? If not, you should develop this policy first. Follow your company's procedures for creating and approving policies. Make sure that the policy specifies who is allowed to perform the audit, the scope of the audit, and to whom the audit results should be presented.

   For example, if you are planning on running a port scan on your Internet servers, be sure the policy states that you are allowed to perform these. Also, if you do things like password cracking or war driving on your network without specific permission to do so, you are asking for trouble!

   A good policy will also state the frequency of these audits. Some businesses may feel that a yearly audit is sufficient, while other larger companies may have several audits going on simultaneously.

   Next, examine the other policies relating to electronic security. These policies should cover the following topics.
   - Who is permitted to use the various pieces of equipment, and what is the purpose of that use? Is a janitor permitted to use computers to access the Internet? If there is no specific policy against this, you may not be able to take disciplinary action if an infraction occurs.
   - Whose property the information created on the company's property is. If a programmer uses company hardware and software to create a program on his own time, who owns that program? The policy should state these things clearly.

- What privacy rights do the users of the network have? Is it okay for someone to read another's email, or access their files stored on company servers? Is management permitted to do these things as part of an audit? Under what conditions can someone do these things, if at all?

2) The second step is to take an overview look at your network and assess the risks that exist at this level. The purpose of this overview is not to determine if vulnerabilities exist, but rather to determine the areas that you will examine to determine if there are vulnerabilities. At this level, look for the following things;
   - What are your assets? Where are they located?
   - What are the points of access to your assets? While physical access is the first step, often these days there are many other ways to access your data. Connections to the Internet, wireless access, VPN tunnels, and modem connections are all ways into your network, and all of them will need to be examined.
   - What are parts of your network, and how are they interconnected? Is there a separation between individual segments? How are these segments connected?
   - What is the level of user access to your assets? Are there sufficient levels of user access, or is everyone granted administrator privileges?
   - Is there sufficient separation of duties, or does one person have the responsibility to add users to the network as well as create them in applications?
   - What services are available on each of your hosts? Are extra services running that should not be running.
   - Are the hosts kept updated with all required patches and security updates?
   - How are the backups handled? Are frequent backups performed to ensure that vital data can be retrieved in case it is compromised? Also, make sure that the backup media is treated with the proper security in mind. Since the backup media contains the same data as your servers, they should be treated just as you treat your servers. Where are the backups kept? What is the physical access to this media? A common ploy in corporate espionage is to obtain copies of the backup media for whatever data they are trying to acquire. This would not only give easy access to the data but would probably go unnoticed if the media was replaced with similar looking media.
   - How informed are your employees about security concerns? Your employees are an essential part of your network. Be sure they are aware of security concerns, and what to do about them. Are the help desk personnel aware to verify the identity of the people they are talking to on the phone? Do your sales people know not to

divulge confidential information via email? All these concerns should be evaluated. This is often on of the hardest parts of the security assessment.

3) Now that we have an idea of what pieces make up your network, and the overall security concerns each piece may have, it's important to look at the individual pieces in depth.

Assets: Now is the time to bring out the list of assets you created earlier and look over them. I encourage you to actually write down your list of assets and follow along this exercise with each individual piece.

- What is the asset? Write down what form the asset takes. Is it a file server containing essential data? Is it a database that houses all of your payroll data? Is it an application that your customers use to place orders with you? Perhaps it's a listing of your customers. It's important to look at each one of your assets individually. This will allow us to be very specific when it comes to the types of security risks involved with this asset, and what we can do to mitigate the risks.
- Why is it important to you? Some things will be obvious. We need our inventory records to allow us to know how much of each item we have. Other things should also be assessed. How important is it that these records are not tampered with or modified by accident? How important is it that no unauthorized people can read this data? Would that exposure create a failure in customer confidentiality or allow your competitors to have an unfair advantage over you?
- What is the physical access to this asset? Is this a server located in a locked data center secured by a thumbprint scanner and an identification number, or is it located in a desk in the middle of the office space? As Microsoft states on http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/essays/10imlaws.asp, "If a bad guy has unrestricted physical access to your computer, it's not your computer anymore**."** This cannot be stressed enough. With tools like "NTFS Reader For Dos" from http://www.ntfs.com/boot-disk.htm, it is very easy to simply reboot a machine from a diskette or CD to gain unrestricted access to all the data on this machine. Anyone that keeps their servers in the middle of the office should now ask yourself, "How much to I trust my janitor?".
- What are the other forms of access to this asset? Computer networks have greatly increased how information is accessed. It's no longer accessed strictly by a user sitting in front of a terminal attached to the server. Oftentimes, it's a user accessing the data from around the world via the internet. It's important to determine how the asset is accessed so you can determine the vulnerabilities that may exist with those access methods.

- Who has access to the asset? Is access to the asset on a "need to know" basis only? Your job here is to balance manageability with security. The most secure data has no one that is authorized to access it; however, what good is data that no one can get to? Similarly, making everyone on your network an administrator may make your network very manageable, but it surely lacks the security that most networks find necessary. It's difficult to find the right balance of security and manageability, but we should constantly be reevaluating this balance.
- What is the risk involved with this asset? This is where you should assess the current level of risk for this asset. The risk to an important database may be rated at low if all the appropriate controls are in place. The risk to lesser important data may be considered high risk if many people have unrestricted access to change it. At this step, you should look at the answers to all of these questions for each individual asset, and answer what you feel is the current level of risk.

Now, let's look at the points of access to the network. It is important to look at the different ways for someone to get into your network. This allows us to determine if the correct security procedures are being followed for this access.

Points of entry into the network may include Internet access, VPN tunnels, wireless access points, private data circuits, and modems. Each of these items carries with them different risks, so we'll look at them individually.

- Internet access. This can include people from the internet connecting to your web servers or sending email to you via your mail server. These setups usually include a connection to the Internet and several pieces of security hardware and software, such as routers, firewalls, and intrusion detection devices. It is extremely important to ensure that these connections are well secured. The proliferation of the Internet means that literally millions of people have access to your machines. If the proper security measures are not taken, it is likely that your servers will be compromised within the first few hours they are connected to the Internet.

  Recent findings from the Honeynet Project (http://www.honeynet.org), an organization that connects test machines to the Internet to evaluate the attacks against them, states, "A default Windows98 desktop was installed on October 31, 2000, with sharing enabled, the same configuration found in many homes and organizations. The honeypot was compromised in less than twenty four hours. In the following three days it was successfully compromised another four times. This makes a total of five successful attacks in less than four days."

  Once again, I recommend that the strictest security policy be put in place. Routers should have access control lists in place that restrict access to internal resources from any unnecessary port or IP address. If

you want to provide http access to a server, then only port 80 should be open to that server. Similar "most restrictive" policies should be set on firewalls also.

- VPN Tunnels: FindVPN.com (http://www.findvpn.com/articles/what.php) states that "a virtual private network (VPN) allows two or more private networks to be connected over a publicly accessed network." This means that data can be transferred securely between two separate networks through a third unsecured network, such as the Internet. However, despite the security inherent in VPN's, there are still things to consider.

  First, who is connecting to your network, and how secure are they? If a vendor connects to your network, will their lack of security create vulnerabilities on your network? Viruses may be spread to you from infected systems on their network, or attacks may be perpetrated on you from someone that has compromised their network. To mitigate these risks, you should consider even VPN connections as insecure, and place properly configured routers, firewalls and intrusion detection devices between these networks, and allow only traffic that is considered necessary to pass to and from them.

- Wireless Access Points: Wireless access is a very convenient technology that allows people to take their computers with them everywhere from the corporate boardroom to outside the building. The downside of this convenience is the lack of viable security. Most wireless access devices use WEP to ensure that only those with the proper key can decrypt the encoded messages between the access points and the remote devices. Cisco states "WEP encryption scrambles the radio communication between bridges to keep the communication private. Communicating bridges use the same WEP key to encrypt and unencrypt radio signals." (http://www.cisco.com/en/US/products/hw/wireless/ps5279/products_configuration_guide_chapter09186a0080184b01.html) Because of flaws in the WEP protocol (see http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html), you should not rely on WEP alone. My recommendation is to use VPN technology to add an additional layer of encryption to your wireless devices. Whether or not you decide to use VPN technology, or another technology like Cisco's LEAP Server, I would recommend treating this like an unsecured link and add properly configured routers and firewalls between the wireless access points and your internal network to ensure that only the requires services are accessed via the wireless links.

- Data Circuits: Private point-to-point circuits are probably the most secure method to tie network segments together. These links are connections between one network and another without traveling out through the internet. While the risk is reduced, you may still feel justified in using access control lists on any routers that connect these networks. Other types of data circuits may use different technologies, such as frame-relay

or ATM. These technologies introduce a slightly higher level of risk because they rely on a switched network environment. As with point-to-point circuits, you may wish to use ACL's or firewalls to protect your network from possible intrusions via a data circuit.

- Modems: Modems can provide necessary communications to other networks or computers. Dialup connections to anything from vendors to the Internet allow vital communications very inexpensively. However, we should take great care with modems to be sure that they are not used for unauthorized purposes. Hackers may use programs called war dialers to find modems on your network. Then later try to access these modems to compromise your security. Also, if you allow your users to access your network through dial-up modems, this could likewise allow hackers to connect to your network. If at all possible, things like remote dial-back, and strong passwords should be used to make sure that only authorized personnel use these connections. At the very least, modems should only be connected where necessary, and external modems should be powered off when not in use.

You should now look at the different segments of your own network, to see how they are connected. Are different buildings connected via fiber-optic cable? Are different departments separated by VLANS? You should examine any such segment, and decide if there is a need for greater security. If sensitive information is kept on the research and development network segment, it may require adding an ACL or a firewall to properly secure this segment.

Users Access: You should look at who has access to what is on your network. Do people have access to only the resources they need to perform their job functions? It's easy to allow users to have elevated permissions, but this practice should not be permitted. A network is only as secure as it's administrators are trustworthy. Permitting too many administrators just increases the likelihood that someone will do something that they shouldn't.

You should also look at separation of duties. In small organizations it may be necessary to have one person who has access to everything on the network; however, whenever possible you should try to make sure that administrative duties on the network are separated and assigned to different employees. An example would be a manager who could create a user account in the domain and grant that user access to applications, such as accounting software. In this example, it would be possible for this manager to create a bogus user on the network, grant this user access to the accounting application, and then sign on as this user and access the accounting system essentially anonymously. This allows for dual control and provides a much more secure environment.

Now, let's look at the hosts on your network. What services are used on each server? Are there services running on your servers that aren't necessary? How would you know? It is advantageous to scan your internal host to determine what is running on each of them. Port scanners are available from a variety of sources. The ISS System Scanner from Internet Security Systems(http://www.iss.net) is an example of a commercial scanner. NESSUS (http://www.nessus.org) is an example of a free security scanner. According to their website, Nessus is "A security scanner is a software which will audit remotely a given network and determine whether bad guys (aka 'crackers') may break into it, or misuse it in some way." Due to possible vulnerabilities in services, it is essential that you understand what services are running on each host, and turn off any service that is not needed. Even necessary services should be examined for vulnerabilities. For example, a host running Microsoft's IIS unnecessarily could be compromised buy exploiting a vulnerability is the IIS Service. If the IIS Service is not needed, it should be turned off to ensure that these types of things can't happen.

Patches: It's very important that all necessary security updates are applied to your servers. I can't stress this step enough! More servers are compromised by exploiting known vulnerabilities, then any other means. The most recent example of this is the Blaster worm. A patch for the vulnerability that the Blaster worm exploited was released several months prior to the release of the Blaster worm. Then, why, you ask were so many servers compromised by this worm? They simply were not patched in time. Another example of this would be the Code Red Worm. Both these worms exploited vulnerabilities that were reported much in advance, and administrators just didn't take the time or effort to patch their systems.

Patches should be installed in a test environment whenever possible to be sure that the patch doesn't cause any problems with applications. After sufficient testing, patches should be installed in the production servers.

Administrators should subscribe to security mailing lists that tell them when new vulnerabilities exist. Microsoft maintains a mailing list for their products. CERT maintains a mailing list that spans various products from Microsoft products, to UNIX, Linux, and even Cisco's IOS platforms.

When new patches are released, immediate attention is required to determine if the patch applies to any host on your network, and then start the testing and implementation process.

Backups: Backups are a necessary part of any good disaster recovery and business resumption plan. While these subjects are beyond the scope of this paper, some parts of the backup plan should be examined with security in mind.

Where are your backups kept? Who has access to the physical media that your data is stored on? Much as you wouldn't allow unrestricted access to the data stored on your servers, you shouldn't allow unrestricted access to the data stored on your backup media. Care should be taken to ensure that the backup media, whether it is tapes, CD-ROM's or other media, is always transported and stored in a secure environment.

Do you have offsite storage for your backups? These also need to be stored in a secure way.

Employees: Employee training is an often overlooked part to network security. While not always the first thing that comes to mind, it is still a very important step. If you employees are unaware of your policies, they cannot be expected to follow them.

If you intend to take the security of your network seriously, you need to be sure that your employees receive periodic training on what is expected of them. The following subjects at the very least should be addressed with your employees.

- Policies: You need to discuss your policies with your employees, and be sure they understand what is expected of them. Be sure to discuss with them what they can do, and what they cannot do. Talk with them about what privacy rights they should expect, and who owns the documents that they create on company equipment.
- Viruses: Employees need to be aware what viruses and other malware are. A good understanding of how viruses, trojans and worms work will help them to avoid them. It may not be the best strategy to tell your employees to never open any attachments. Educate them what attachments are dangerous, and why, and you will be much further ahead.
- Social Engineering: Social Engineering is a very dangerous thing these days. The University of Rochester offers some good advice to their students on their site. (http://www.seas.rochester.edu:8080/CNG/docs/Security/node9.html) Some excerpts from this page you should include in your include is that your employees should not give anyone their passwords, nor allow someone to use a computer they have signed onto.
- Passwords: Educate your employees on how to create secure passwords. They may be resistant to use a complex password until they understand why secure passwords are so important, so be sure to talk over both these issues with them.

Conclusion:

In closing, I believe that a thorough security assessment is an essential part of any security plan. A security plan should be an ever evolving process. Being "secure" is not a destination, but rather a journey.

Following these steps, and continuing to evolve your security plans will help ensure that you keep your network as secure as possible. There is always room for additional security, but you should try to achieve a balance between totally secure, and unusable, and totally convenient and insecure.

References:

Microsoft Inc. "The Ten Immutable Laws of Security" URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/essays/10imlaws.asp (September 28, 2003)

NTFS.com "DOS NTFS boot disk to access NTFS partitions in Windows XP 2000 or NT" URL: http://www.ntfs.com/boot-disk.htm (September 28, 2003)

The Honeynet Project "Know your enemy: Statistics" July 22, 2001 URL: http://www.honeynet.org/papers/stats/ (September 25, 2003)

FindVPN.com "What is a VPN? Explaining Virtual Private Networks" URL: http://www.findvpn.com/articles/what.php (September 27, 2003)

Cisco.com "Cisco Aironet 1400 series configuring WEP and WEP features" URL: http://www.cisco.com/en/US/products/hw/wireless/ps5279/products_configuration_guide_chapter09186a0080184b01.html (September 28, 2003)

Borisov, Nikita; Goldberg, Ian; and Wagner, David "Security of the WEP algorithm." URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (September 25, 2003)

ISS.Net "Enterprise Protection > Vulnerability Assessment" URL: http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_system.php (September 28, 2003)

Deraison, Renaud "Nessus: Introduction" URL: http://www.nessus.org/intro.html (September 28, 2003)

Last Updated: July 25th, 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
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
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
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
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
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
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
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
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 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
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
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event