GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Layered Security – Inside and Out

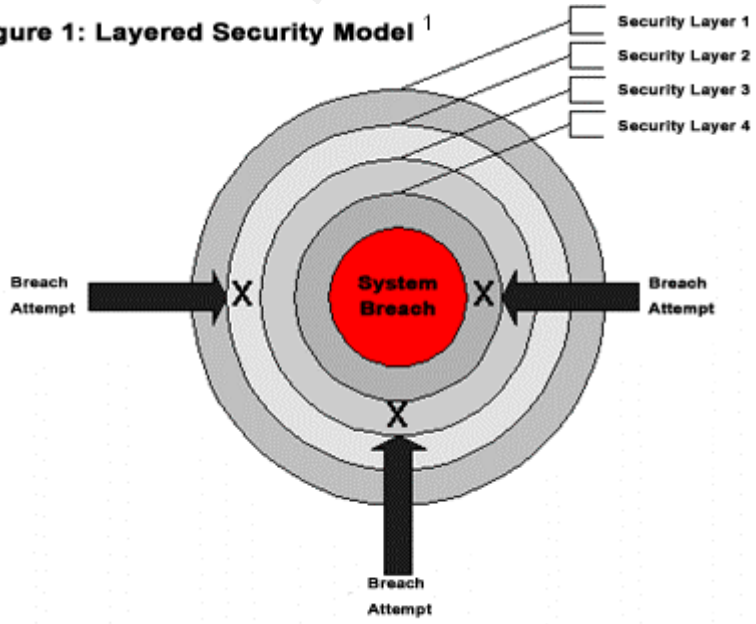
Chris Mclaren
January 20, 2003
GSEC Practical v.1.4b (option 1)

Introduction

Well as you probably guessed, layered Security or "Defense in Depth" is not a one-product solution but multiple applications and products integrated together that keep your network wrapped in a warm 'Security Blanket'. Or in this case several layers of blankets.

As shown in Figure 1 sometimes one of the first layers won't detect and stop a security breach from occurring. The idea behind the layered security model is that eventually all attack vectors are covered by one or more well placed security defenses. This effective model is used in many security designs and is not limited to information security but is also used in fields that implement any forms of security solutions. This paper will present some of the important steps that should be taken when developing and implementing a layered security solution for a site.

Figure 1: Layered Security Model [1]



Defining Layered Security

David Whyte Senior Incident Response, stated at a Carleton University seminar that:

> "Layered network security can best be described as the strategic deployment of appropriate risk-based security countermeasures thus reducing the possibility of circumvention through single points of failure." (Whyte)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

All layers should be implemented from where the risk is greatest and then on down to the smallest threat. Each defensive layer should be selected and situated to best counter the posing threat. There needs to be a security strategy in place, specific to your site to determine where security measures need to be taken. Simply said, the more security layers effectively deployed the harder it will be for an attack to reach your protected assets.

Who Is The Enemy?

With the ever-expanding growth of the Internet, information crime and warfare are reaching their highest levels ever, leaving the corporate world scrambling to protect themselves. As in any battle, the importance of knowing who the enemy is plays a key role on developing a strategy to protect and defend your territory.

A lot of times the most dangerous attacks can from within your own ranks. A layered security approach must protect you from external attacks but also from the all too often overlooked internal attacks on security.

> "The 2001 Computer Crime and Security Survey from the Federal Bureau of Investigation and the Computer Security Institute makes it clear that cybercrime is on the rise. But for the first time, according to survey respondents, incidents precipitated by outside hackers outnumbered those originated by internal threats.
>
> Experts said that trend is likely to continue as increasing numbers of outside intruders mount more attacks on computer networks and PCs. Symantec Security Response senior product manager, Dee Liebenstein told NewsFactor that a big reason for the increasing number of outside attacks is the almost infinite number of threats." (Layman)

A lot of times these inside users don't understand or realize the security implications of some of their actions. From opening an infected e-mail attachment or installing some form of spyware on their computers they can help outside attackers enter into the site and cause unwanted security breaches.

It is because of this inexperience and lack of security understanding that users, through no fault of there own, can cause much more dangerous security threats. On the other hand, some are malicious and know enough about the internal environment to go strait for the 'crown jewels'.

It is therefore imperative to create strategies, standards and security rules to harden security layers and to protect against all attacks, inside and out.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Where To Put Security Layers

Put them anywhere and everywhere! But be smart and educated about it. Any asset that has a risk attached to it should be secured. Risk management is a very important tool to determine where security needs to be deployed and also how much security, depending on the risk.

Why don't we just secure everything with the biggest and baddest protection we can find? We'll because most of us operate on a limited budget and resources. That's why it's important to know your risks. Managers don't like risks and a risk annalist might help you 'sell' the needed security solution.

There should be a layered defense at three important points: on the network, at the Server, and at the Desktop. If you neglect one of these points, it will become your weakest link. A lot of times in organizations the desktops and users are the weakest link in your security defense. Remember your Security Defense is only as strong as its weakest link. It is always a good idea to start with the biggest hole first.

Because of the increasing mobility of devices in networks (making the boundaries of networks virtual in nature) it is important to make sure that security strategies also include remote access (VPN/Modem) for Home users and telecommuters. Also take into consideration the ever-increasing use of PDA's and other wireless devices. One of the greatest assets you will need to protect is information and therefore every device that holds and communicates information will need to be encompassed.

Security From The Inside And Out

There are many sources that have put together a list of important security layers needed for a complete layered security defense. I only wish to add to what they have established in a less vendor specific dialog. I will cover several of the most important steps that should be taken as part of developing a fully layered security defense.

The topics focused on are as follows:

Security Policies
Hardened Perimeters
Intrusion Detection Systems
Vulnerability Assessments
Scaleable Security
Security Trends

I hope this information will be valuable, insightful and will help in better securing your network.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Security Policies

As you can see developing a security policy is at the top of the list and should be at the top of yours. All users need to be on your side if you're going to win this battle for better security. They must be your first concern and must be kept on the same page.

A security policy is a list of security rules. The need to develop such a strategy within the organization is a very important first step in securing your site. There needs to be management endorsement, user education and more user education and maybe even more user education. With the most dangerous security threat existing inside your network it is important to have some leverage to protect the enterprise site from internal compromises.

> "A generally accepted approach to follow when creating a security policy is suggested by Fites, et. al. [Fites 1989] and includes the following steps:
>
> 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." (Fraser)

A security policy should be clear and concise and should encompass what needs securing and why. A risk assessment will help in deciding which direction the policy will take. Once the assets that need protecting are identified it is necessary to determine what it is they need to be protected from and then take the proper steps to minimize the associated risk.

Make sure the policy is always enforced. Depending on the size of the organization this could be a huge job. The first step is to get backing from management and get the policy endorsed. Next, educate the users on the security policy and of best practices to insure internal security. Also communicate any threats that users should be aware of - they need to understand their part in the overall security defense of the organization.

Also when any changes take place in an organization it is very important that the security policy is reviewed and changes are also made accordingly. For example, if a new server based application is deployed on the network, what security implications and weaknesses must be looked at to maintain the level of security needed in the organization? A security policy should be continuously reviewed.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Hardened Perimeters

A firewall will most likely be your first line of defense against outside attacks. It usually sits at the entry point of your network. This entry point or line is most likely becoming blurrier because of the new mobile, wireless and remote office world we are now a part of. It will have many more entry points that will need protecting.

> "The ideal perimeter is transparent as possible to properly authenticate clients utilizing legitimate services on the network but at the same time be impossible for untrusted clients to get packets past the perimeter". (Hoskins)

Firewalls usually come in two forms: those that operate at the Protocol level and those that operate at the application level.

Most routers will use packet-filtering and stateful inspection as they route network traffic. It is possible to close unwanted Ports to help control unwanted network access on routers. A well-designed and configured network is an important key to a secure network. If you plan to use routers as firewalls it is important to understand the associated limitations. I recommend not relying solely on routers for a secure perimeter, but using them in conjunction with an application-based firewall to provide a much more secure perimeter.

Application level firewalls usually run on a Proxy server that routes traffic at the application level. The proxy won't let outside parties have direct communication inside the network. It accomplishes this by intercepting the communication and then forwarding it inside the internal network where the request originated. If you use an application firewall it is important to run a proxy for each of the applications that need protection.

Important Note: As important as it is to harden your firewalls and mainstream servers you should also harden all devices within the DMZ zone. It is imperative that you keep utilities, applications and operating systems up-to-date and that you only install needed components. A default install should never be preformed on a device that is connected to the network.

In order to accomplish this and keep up-to-date systems, stay in contact with vendors for patches, updates and fixes for security threats. Most security breaches are due to inadequate configuration and not taking the time to fix holes that have been discovered. A lot of threats still target old security holes because the industry hasn't caught up yet.

The most common attacks that penetrate a perimeter are Viruses and Trojans. This is why it is important to run Virus scans on your firewall or gateway as well as on all hosts (servers and Desktops).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Remote users have become a huge security risk to companies. A hacker would much rather attack a home PC that is unsecured and used for work purposes, than to try and hack through the corporate firewall. He might find information that will allow him to gain access to the company assets. Make sure that remote systems have a layered security perimeter which should include a firewall, virus scan and maybe an personal Intrusion detection program together with an encrypted VPN connection will help secure your network.

Another important tool in hardening a perimeter is an intrusion detection system (IDS) IDS is covered in more detail in the following section.

Intrusion Detection Systems (IDS)

Intrusion detection systems (IDS) are an important part of a layered security defense. There are two layers to well-configured IDS. A network based monitor and a host based monitor. Both systems will help you see and track any attacks that try or succeed in entering the network. There are also hybrid ID systems that combine Network and Host based monitors.

Network Based Monitors

A network monitor looks at live packets that are being passed through the network to determine if there are signs of attacks or even anomalies. If a packet looks suspicious it is stopped and recorded for later analysis. These systems can sit in front of firewalls or at other entry points.

Cisco has developed several well-designed network monitors that can be added to monitor your network.

Host Based Monitors

A host monitor uses system logs and Audit tools to look for suspicious application activity in real time. It also watches system files for evidence of tampering and suspicious processes

Generally you want to monitor stable servers because the more often the configuration is changed the less accurate the IDS will be at detecting a threat. Also have the logs written to a different computer so that the attacker won't easily be able to easily erase his tracks.

It is recommended that all core servers such as web servers, firewall servers, mail servers, DNS servers and even application servers have an intrusion detection system installed and configured. You can install IDS on any devices within the DMZ. Just remember to install it on the devices with the greatest risk of attack before installing it on those devices of lesser risk.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

There are several popular HIDS systems such as TCP Wrappers and Tripwire that help track any undesired connections to you servers. There are several personal IDS/firewalls available as well for any home users.

Hybrid Monitor

The network based IDS should complement a host based IDS because it doesn't have the same limitations as the HIDS. If possible, find an ID System that inspects both network and hosts and that logs to one location.

A Hybrid Intrusion Detection System combines a Network Intrusion Detection System with a Host Intrusion Detection System. Exactly how the Hybrid system works varies from product to product. (SEC-1)

Vulnerability Assessments

The key to doing vulnerability assessments is to find the holes in the network and computer systems before the attacker does. Most holes are found in applications; therefore, it is imperative to keep all applications and operating systems updated with current security patches. Being proactive and one-step-a-head of the game is an important part of maintaining a secure defense against unwanted attacks.

There are several good vulnerability scanners available. Some popular scanner application providers may include Symantec or ISS. There are also several freeware scanners that are effective for finding important vulnerabilities. You will have to choose the tools that best suite your organization assessment needs and budget.

The down turn to running these scanners is that things can go wrong. First make sure you have permission to run the scan. The scan can cause certain systems to crash. Make sure that those individuals who may be affected by the scan are forewarned.

Remember that the greatest risks are created from improper configuration and setup. Take the time to configure applications and security defense mechanisms properly the first time.

Scaleable Security

There is a lot to be said about doing it right the first time. This usually isn't the case since a well-designed security defense often takes years to perfect. For this reasons it is a good idea to make layered security scaleable.

Security servers and services can become strained and unable to operate correctly as demands on the network increase. Often this is due to the rapidly

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

growing need for remote site connections and access to applications and services through those connections. This causes the load for the security mechanism to be more than it can handle efficiently, allowing vulnerabilities to arise that can open up all kinds of unwanted security holes. This can best effectively be resolved with a separation of applications and services into zones of varying levels of risk.

Now you have a system that is scaleable and that can be better added upon in the future. Since each zone is not dependent on shared resources it can be easily expanded and tailored as the companies operation expands. Scaleable solutions also let's you better layer security depending on the level of risk that exists in any given zone. Avoid allowing certain unsecured services such as FTP, telnet, SMTP or SNMP that might not be needed in a zone dedicated to a particular application. This will make monitoring traffic and picking up on abnormal activity easer.

Having a scaleable security defense is taking a proactive approach in creating a security solution. We have seen this happen many times where security systems had to be redesigned a few years down the road because they couldn't handle the network growth.

Security Trends

Staying up to date on current trends could help you better manage you information security layers. Make sure to investigate each trend to better determine if it would be beneficial for you organization to incorporate.

For example, according to Tim Finnegan, who manages security practices for Alphanumeric Systems Inc. in Raleigh, there are three trends in network security

A move toward implementing a "managed vulnerability assessment." There are a number of application companies that will run regularly scheduled scans on your network for any security holes that may exist. Few companies have the resources to keep up with all the vulnerabilities that keep occurring. They don't become aware of a security hole till the application makes them aware of any patches or upgrades that are available.

Moving away from frame-relay technology to virtual private network technology. With the ease of encrypting data using VPN and the setting up a high-speed connections provided by a local ISP, the need to spend a lot more on a dedicated line is not practical.

A "single sign-on." How many of us have a username and password for every application we have access to. Some users don't want the hassle that comes with remembering all those passwords (especially if you have a password policy that forces users to change their passwords every 45 days). So they start writing

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

them down everywhere. A single sign-on would help users to be more secretive with their passwords. (Rogoski)

All of these new trends can better help security professionals secure their networks. You might already have a strategy in place that works for doing vulnerability assessments but on the other hand replacing expensive dedicated lines and multiple logins might be more appealing then existing practices. It is important to stay on top of such trends to simplify security measures. The simpler you can make the security architecture the easer it will be to manage. The easer it is to manage the better you are able to track and kill attacks.

Conclusion

Layered security can best help organizations to implement a trusted security configuration. Trusted Security meets three requirements:

> Availability – assurance that systems work promptly and that service is not denied to authorized users.
>
> Integrity – Data has not been altered in an unauthorized manner while in storage, during processing, or while in transit. Systems operate while performing its intended function in an unimpaired manner, free of unauthorized manipulation.
>
> Confidentially – Private or confidential information is not disclosed to unauthorized individuals. Confidentiality protection applies to data in storage, during processing, and while in transit. (Tripwire)

Currently there is no 'silver bullet' or one complete security solution that solves all security holes. I believe this is contributed to how the security world sees security. Security is too important to trust it that one system and prevent loss from attacks.

Most of us who own a vehicle not only lock our doors and roll up our car windows but we also have to have a security alarm and some even put a anti theft club on the steering wheel. There are a lot more anti theft devices out there for your car but if your driving a '78 rusted out Honda you probably won't spend a lot on anti-theft.

It is the same situation that exists in the Information security world. It all comes down to the risk and how much you have to lose. Develop a security strategy that will meet the trusted security requirements for your organization. The larger the potential risk the more security layers you should deploy.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

1) Setrin, Jeff, “Driver’s License Authentication” September 23, 2002, http://www.biometritech.com/features/imageauto.htm

2) Whyte, David, “The Role of Intrusion Detection Technology in Implementing Layered Network Security (abstract),“ January 31 2001, http://www.scs.carleton.ca/semnet/310101.html

3) Lyman, Jay, “Outside Hackers vs. the Enemy Within: Who’s Worse”, February 5, 2002.
Http://www.newsfactor.com/perl/story/16157.html

4) Fraser, Barbara, "Site Security Handbook," FYI 8, RFC 2196 September 1997. http://www.faqs.org/rfcs/rfc2196.html

5) Hoskins, Mike, “Multi-Layered Security”, March 2002, http://ezine.daemonnews.org/200203/multilayersec.html

5) SEC-1, “Network Security Solutions, Intrusion Detection Systems”, http://www.sec-1.com/intrusion_detection_systems.html

6) Mackey, Richard, “Security Architecture – Layered Insecurity” June 2002, http://www.infosecuritymag.com/2002/jun/insecurity.shtml

7) Rogoski, Richard, **“**Layered Approach Key to IT Security”, November 1 2002, http://triad.bizjournals.com/triad/stories/2002/11/04/focus3.html

8) Tripwire White Paper, “Data Integrity Assurance In A Layered Security Strategy - Providing The Essential Foundation For Data Security”, http://www.tripwire.com/files/literature/white_papers/Layered_Security.pdf

© SANS Institute 2003, Author retains full rights.