Global Information Assurance Certification Paper

Defense In Depth: From the Bottom Up

Bryon Buesser
May 15, 2004
GSEC Practical Assignment, version 1.4b, Option 1

Abstract

There is a Native American saying[1], “Tell me and I'll forget, Show me, and I may not remember. Involve me, and I'll understand.” Nothing can be closer to the truth when it comes to teaching people about secure computing. Usually the hardest part of securing a network lies in keeping the end user from doing something inadvertently, like opening a dangerous e-mail attachment or leaving passwords out where anyone can view. This document is to help the end user understand what they can do to help keep themselves secure and to explain and show examples of defense in depth. By the title, Defense in Depth: From the Bottom Up, I am not suggesting that this is the starting point in securing your computing environment if you are a network administrator. I am stating that this is the part that takes the most amount of time and is probably the area most neglected. If you educate the end user about best practices and get them used to hearing the terminology in the security field, then they will be a greater asset than a hindrance when it comes to secure computing.

Introduction

Defense in depth is the practice of applying security in layers. In this document we will look at some of the different layers of security that are essential to keeping your computing environment secure. First, an explanation of what a security policy is and why it is important to understand the concepts it covers. Tools of the trade are covered next. These are applications and practices such as anti-virus software, system updates and patches, personal firewalls, and passwords that build on each other to create layers of security. Next we discuss what security best practices should be applied to your every day programs such as web browsers, e-mail, and office suites. Lastly, we talk about physical security.

Policy Explanation

Creating a security policy is the starting point for establishing a position on computer security . Nothing will hurt the quest for a secure computing environment more or cause more headaches than users who do not understand or ignore your policies.

A security policy is there to protect people and information. The document should outline the goal of how to operate in a secure computing environment and define the user's role in achieving that goal.

According to a CompTIA survey[2], just over half of the organizations surveyed out of 900 said they had a written security policy in place. It is very hard to enforce rules that are not clearly defined. A security policy documents the

1Quotes about Education
2Spalding

questions that are asked when an event occurs. It instructs people how to react to certain situations and assigns the responsibility for executing each step towards event resolution.

Developing a security policy does not have to be a groundbreaking process. There are various resources that will guide an organization in developing and explaining the right policies for a given situation. Two examples are:

1) http://sbc.nist.gov/
2) http://www.sans.org/resources/policies/

Tools of the Trade

A good security policy should outline the framework of how a computing environment is going to be laid out. Once that is understood it is time to look at the tools of the trade that are used to secure that environment.

Passwords

Passwords may not seem like a tool, but setting up password security is the first thing you should do before someone is able to access or participate in any level of security. Passwords are the cornerstone to security, but unfortunately it is usually seen as an inconvenience[3]. Most people hate to change their password, probably because they forget their passwords or feel that it is an inconvenience for them to come up with something that fits within the password policy and rules.

A password policy[4] people may find inconvenient is one that says that passwords must be changed every sixty days and the past five passwords can't be reused, but there is a good reason for this. For example, if someone were able to get the main password file from a computer, put it on a separate computer and run a password cracking tool against it such as L0phtCrack, theoretically it can take more than 60 days of continuous brute force checking for them to crack the password depending on the speed of the hardware they are using. To illustrate a defense in depth strategy to protect against repeated password guessing, if an attacker is trying to log on to a user account by guessing passwords, accounts should be disabled if the wrong password is entered more than three times. This prevents someone from having an unlimited number of tries to break in. After the third time the account should be disabled automatically. If an authorized user with the correct password were to try to log in they would have to alert someone to unlock the account which would be a warning sign that there was an attempt to break into the system.

3Cole, p.400.
4Cole, p.413-416

Here are a few good rules of thumb to follow when trying to create a good password[5]:

1) Always use a combination of capital and lowercase letters, numbers, and special characters such as punctuation.
2) Passwords should not be based on dictionary words.
3) Do not use personal information that is easily accessible as a password such as telephone numbers, family member names (that includes pets) or anything else a person can get from viewing objects in and around your desk.
4) Passwords should be longer than 8 characters or be a variation of the last password you used, such as the last password plus one digit.

Anti-virus

Another common tool to protect computer data from malicious attacks is anti-virus software. Anti-virus software works on the file level on your computer. The anti-virus program will scan all files on a computer looking for tell-tale signs of a virus. These signs are known as virus signatures. Anti-virus programs also scan incoming e-mail attachments to intercept any worms or trojan horses that may be embedded in a word document. "A worm is a virus that replicates itself on other drives, systems, or networks[6]." "A trojan horse is A program that either pretends to have, or is described as having, a set of useful or desirable features, but actually contains a damaging payload. Most frequently, the usage is shortened to "Trojan". Trojan Horses are not technically viruses, since they do not replicate[7]."

There are many different vendors that provide anti-virus solutions. For example, there are enterprise class solutions that allow installation, distribution, updates and monitoring from a central location. Some products that offer that level of software are McAfee VirusScan, Symantec AntiVirus Enterprise Edition, and F-secure Anti-Virus Total Suite. At the other end of the spectrum we have software packages like AVG Anti-Virus from Gisoft that offer free personal anti-virus packages for home computers. Regardless of what package is being used, there are two important features that must be set up correctly in order for anti-virus software to work properly.

The first feature of anti-virus software that should be configured is how the software gets updated. Whether this is done manually or automatically, it is extremely important to keep anti-virus signatures up to date. Anti-virus software

5Cole,p.415.
6Network Associates, McAfee Security Virus Glossary of Terms
7Network Associates, McAfee Security Virus Glossary of Terms

compares files against a database of signatures. If the file does not match any of the signatures it is deemed safe. If virus signatures are not kept up to date the anti-virus software will still detect viruses that are in the signatures list, but any new viruses that come out will more than likely not be picked up by the software.

The second feature to keep in mind is scanning frequency and scheduling. Up to date virus signatures will not amount to a hill of beans if they are not actively scanning your system. Most anti-virus software include a scheduling component that specifies when and how often the computer file system is scanned. A better option is to choose an anti-virus software package that actively scans the computer file system in real-time, so when a file is modified it is immediately checked to see if it now matches any virus signatures.

Software Updates

It is extremely important to keep on top of software updates released by software manufacturers. These updates and "hot fixes" are provided to patch security holes or bugs in software which can be exploited. These exploits can be used to gain unauthorized access to a computer or used for other malicious purposes such as password harvesting or using the computer as a platform to attack other machines. Keeping track of these updates is yet another good example of defense in depth, using layers of security to protect a computing environment.

Anti-virus software will stop a virus, trojan horse, or worms that exploit vulnerabilities, but it is the manufacturer's update that actually fixes the vulnerabilities that the virus or worm is trying to exploit. Some worms and viruses are being written to disable your anti-virus software before it executes its malicious code.

Most operating systems (OS's) these days have built-in applications that will automatically search for updates from their manufacturers. Windows Update (http://v4.windowsupdate.microsoft.com/en/default.asp) and Red Hat Network (https://rhn.redhat.com/help/about.pxt) are two such types of programs bundled in their respected OS's. Unfortunately, the manufacturers sometimes leave this important feature turned off which leaves it up to the user to turn this feature on and configure it properly.

To this day some people are a little gun shy to install the latest patches from Microsoft. Several years back Microsoft released service pack 6 for its WindowsNT operating system. For the early adopters who installed the Service Pack when it was first available this proved to be a painful lesson. There was a problem[8] with the patch where users could not complete winsock calls to a program unless they had administrative rights to the computer. Mainly this affected Lotus Notes users. Microsoft quickly released service pack 6a to fix the problem that existed in the original service pack. As a result many IT

8Microsoft Corperation, Knowledge Base Article - 245678

departments developed a testing period of sometimes more than a month or two to allow for a patch to be throughly tested before it was implemented. That length of time is no longer a luxury we can afford. On April 13, 2004, Microsoft released software patch MS04-011[9] to fix a vulnerability that could allow an attacker to remotely execute code on a victim's computer. On April 28, 2004, Network Associates discovered[10] a trojan called W32/Gaobot.worm.ali[11] that takes advantage of this vulnerability. Another worm based on the same vulnerability was discovered on April 30, 2004[12].This worm went on to create large scale interruptions to many of the world's largest businesses and some hospitals[13]. Even more problematic was that on May 8, 2004, there were already five different variants of the virus "in the wild." The update that fixes this vulnerability will protect a computer from all of the different variants of the virus. They all exploit the same vulnerability. It is what they do after they have infected the system that is different. In nine days a virus was spread worldwide infecting millions of computers, disrupting businesses, and possibly endangering lives. This could have been avoided or had much less impact if the updates for this vulnerability had been installed in a timely manner. Almost all of the computers that were infected had the capability to install the patch automatically the day the patch was released.

If you visit the Windows Update website it will download and install an Active X program onto the computer so it can scan the computer to see what programs are installed, what updates have been installed, and what needs to be upgraded. The process is fairly simple and works very well. After the computer has been scanned it will break down the updates that are missing into three categories:

1) Critical Updates and Service Packs
2) Windows specific updates (depending on what version of windows)
3) Driver updates.

The user has full control over what updates are installed on the computer. Windows update can also be configured within your Windows operating system to automatically check for new updates. It can either download them to the computer and then let the user decide what to install or it can download and update the operating system automatically. The user will be notified by a small icon on the task bar when there are critical updates to install. The option to download and install later gives you the best flexibility, but as we have seen in the example of the sasser worm it is becoming more and more apparent that the automatic installation option needs to be turned on and left on.

---

9 Microsoft Security Bulletin MS04-011
10 Network Associates, Exploit-MS04-011
11 Network Associates, W32/Gaobot.worm.ali
12 Network Associates, W32/Sasser.worm.a
13 Keizer

Red Hat Network Update Module,[14] which is Red Hat's implementation of an auto-updating system for Red Hat Linux, has the same features of updating and notifying you when there is an update but it differs in what it updates. Windows Update will only notify and update Microsoft-based products. Red Hat Update Network will provide updates for the Red Hat Linux operating system as well as other open source programs that come packaged with Red Hat Linux.

Firewalls

Sometimes product updates are unable to be installed due to hardware or software incompatibilities so we need to look at another tool called a firewall. A firewall is a software or hardware device that filters incoming and outgoing network traffic to the computer. Since broadband Internet access is becoming more commonplace in many homes, personal firewalls create another layer of security that adds to anti-virus software and software updates. While most places of business have high level network equipment to filter most of the network traffic, the personal firewall still has its place in the business and home environment. An example for the business world would be a remote worker/traveler who is not under the umbrella of security provided by the corporate network and communicates over non-secured Internet connections. High speed Internet providers do not provide a level of security to the home user either. That responsibility lands squarely on the shoulders of the end user.

The main purpose of the firewall is to only allow the network traffic that you approve to access your computer. Just like anti-virus software, a firewall is not going to do its job effectively if it is not configured correctly. Most hardware based firewall appliances, like Cable modem and DSL routers for home use, come configured with one firewall rule that says deny all inbound connections and allow all outbound connections. While this does not completely secure the computer, it is a giant leap forward when combined with anti-virus software and a fully patched and updated operating system. Firewall configuration is not an easy task either. Software based firewalls like ZoneAlarm from ZoneLabs[15] help to make firewall configuration easier by notifying you with pop-up notices when an application is trying to pass through the firewall for the first time. This allows for a more graphical way to configure rules for future events.

To illustrate how a defense in depth strategy could be used to combat the sasser worm we will need to use the following tools: firewall, anti-virus, and an update patch. In the case of the sasser worm our first line of defense would be the firewall. The sasser worm first tries to find other computers on the network by sending a ping request. If we have our firewall configured to deny a ping request then we may have escaped the worm. Let's say that the worm was able to find out that our computer is on the network. Once the worm has found us it sends a

14 Red Hat
15 ZoneLabs

buffer overflow to the LSASS.exe file. This is the file where the vulnerability exists. The buffer overflow creates a command that now instructs your computer to send an ftp request on tcp port 9996 to the original infected machine at tcp port 5554. So again, if we have our firewall configured to block outbound ftp connections on tcp port 9996 we would have escaped infection. If we did not have our firewall configured correctly, or if we had inadvertently turned it off, then anti-virus software would have been our next layer of defense. When the sasser worm makes the ftp connection back to the original infected computer it downloads a file with a random file name such as 1234_up.exe. The worm executes this file which copies a file called avserve.exe to the windows directory and creates a registry entry that tells this file to run every time the computer starts. It is this file (avserve.exe) that is used to spread the worm to other machines. Anti-virus software with up to date virus signatures would be able to detect that the new file on the system (1234_up.exe) was related to the sasser worm and would have either deleted the worm or quarantined, depending on your anti-virus settings, so it was unable to execute. The best way to prevent the sasser worm form infecting your system is to first install the patch MS04-011 that is available from Microsoft. This would have fixed the buffer overflow problem in the file LSASS.exe and the sasser worm would have never been able to infect your computer.

Application Security

Documents and web pages have become so interactive it has opened up the door for malicious programs to compromise computers without your knowledge. The type of exploits that these programs cause can range from a keystroke logging program that is used in an attempt to find out passwords or credit card numbers to programs that give an attacker complete and total control over your computer as if they were sitting at the console themselves. This type of software is generally referred to as spyware. That is why it is now important to explore the security settings of the applications. The typical applications that are found on home and corporate computers alike are a web browser and an office suite.

While viewing some web pages, a small web page will open up in a window on top of the page you are trying to view. This is usually in the form of an advertisement for some product or a link to another web page. These small web pages are called “pop-up” ads. Since “pop-up” pages are bits of code that get launched without your direct approval they have been the tool of choice for delivering malicious programs and spyware. A tool or feature called a pop-up blocker has become an important feature in browsing the web. Firefox and Mozilla[16] web browsers both have these features built in. Firefox and Mozilla are free alternative web browsers to Internet Explorer which comes built into the Microsoft Windows operating system. Internet Explorer does not have a pop-up blocking feature built in, so to stop these extra windows from being launched a

16 Mozilla

third-party software tool like the Google tool bar will need to be installed.

It is very important to configure web browser security settings. If these are set to an unsecured level it can create a back door to allow an attacker to install malicious software. In Internet Explorer the security settings are set to medium by default. Some viruses and malicious programs have been known to change these settings to an unsafe level and then cause the browser to go to a web page that installs a program that can give them a back door to the computer. This will allow them to bypass the security settings on that computer. It is good to get in the habit of checking these settings to make sure they are at the level they were originally set.

E-mail has become the de-facto way to communicate for most people and organizations. E-mail has allowed people to communicate with text, voice, and video over the Internet. This has allowed people to share documents and ideas and the all important fw:joke of the day. E-mail is not without its downside as well. Since so many people are using this medium for communication you have those people that want to use it as an advertising medium - the same exact way that the postal system has been used. A quick comparison between electronic mail and postal mail: unsolicited mail can be sent to a U.S. postal mail box in the form of credit advertisements - great deals on consumer goods like food items and electronics sales, and financial advice that may or may not be in your best interest. The U.S. Postal Service has been used for malicious purposes such as mail bombs and chemically infected packages. The same types of unsolicited mail can be sent in electronic form and can be used for malicious purposes also like electronic viruses and worms. In the same way that the U.S. Postal Service has started screening its packages for infectious and explosive agents so has the the electronic world with anti-virus software that has been installed on the e-mail server to protect its recipients.

Just because an e-mail server has anti-virus software installed doesn't mean you are completely safe from any harmful messages. Virus writers are becoming more and more creative in delivering and sending these messages. Most e-mail spreading viruses are spoofed from their original source so just because you receive an e-mail from your uncle Bob doesn't mean he is the one who actually sent it. Uncle Bob's address could have been on the mail list of someone else's computer and the message could have originated there. So let's take this situation to the real world: would you be the least bit suspicious if you received a rather large box that was delivered to your mailbox from your uncle Bob? It's not your birthday, it is not near any holiday where sending gifts in the mail is appropriate. Would you open the package, or would you call uncle Bob and ask why he sent you a package? The same type of cautiousness should be taken in the Electronic world. If you receive an e-mail form someone who you regularly communicate with that has an attachment that looks legitimate but it kind of came without warning, it would only take a second to confirm with that person to make sure that they actually sent you a legitimate attachment.

Instant messaging is rapidly becoming an easy way to keep in contact with friends, family, and business contacts while connected to the Internet. It is also becoming more commonplace for employees at businesses to communicate and collaborate using this application. Instant messaging is a great real-time way to communicate on a one-on-one basis or with a group of people. The downside of using free publicly accessible networks to conduct business is that when you use a free product such as AOL Instant Messenger to communicate, you are connecting to a third party network and you should expect no privacy or security.

An easy way around this would be to set up a secure internal instant messaging server. I define secure in this context as not open to the Internet. The only people that should have access to this server are your employees. There are several products available for setting up such a service. There are open source products such as Jabber[17], which is an open source instant messaging server that works cross-platform and works with a wide variety of clients. On the other hand, Microsoft's Exchange E-mail server has an instant messaging component to it as well.

Physical Security

Physical security must be considered just as important as network perimeter security. When we talk about physical security we are talking about any way someone can obtain access to information with in your organization without having appropriate authorization. This includes building access, physical access to the computer to install software or hardware, and access to sensitive computer related documents. Patching and firewalls will not be able to prevent someone from walking up to an unattended computer console to create a security breach.

You may or may not be able to control how much access someone has to your building. It is easier for small businesses and home users to secure access to their space than retail and large businesses located in a single building. In any case, it is not wise to allow non-authorized people to roam about unsupervised. It is best to have a central access point for all visitors to come in from so they can sign in. It is good to keep a log of all people that visit your place of business, what time and date they arrived, who they came to see, and time and date of when they left. This is just like a security log on any firewall. It is also good to label visitors with a badge of some sort so employees can see if someone is roaming around unescorted.

Just because you sit in an office that has locked doors does not guarantee that sensitive information you leave out on your desk or in common areas will stay confidential. This is most prevalent in this day of cube farms and cost cutting

17 Jabber Software Foundation

open office space. Every work area should have some kind of storage space that is secured by a lock. Things that you should place in that secure area while you are not around your work area are things such as employee telephone lists, sensitive procedure manuals, password lists, and any other work product that is proprietary to your business.

A desk, like a computer, has files on it and those files need to be physically secure as well. According to an article published by the Carnegie Mellon Software Engineering Institute[18], if someone has physical access to a computer they have the opportunity to install either software or hardware that can be used to bypass a network's perimeter security. An example of hardware tampering would be someone installing a wireless network card that allows them to view files on a computer or to access an internal network. As an extra layer of security you can secure physical access to a computer by using third party locks and cables to prevent unauthorized access.

Conclusion

Technology is changing at a rapid pace which forces us to adapt to any security challenges that may arise. We have seen month-long software testing periods dwindle to days. There will be a day when a security flaw is found and reported, and in that same day a virus will be released based on that vulnerability. The term is called a zero day virus. The only way to be protected from such an attack is through the application of secure procedures, products, and education.

18Carnegie Mellon

References

"Quotes about Education." Inspirational-Quotes. 2003.
URL:http://www.inspirational-quotes.info/quotes-about-education.html

Spalding, Elizabeth; Babich, Jennifer. "Human Error at Center of Most IT Security Breaches, CompTIA Survey Finds." 31 March 2004.
URL:http://www.comptia.org/pressroom/get_news_item.asp?id=424

Cole, Eric; Fossen, Jason; Northcutt, Stephen; Pomeranz, Hal. SANS Security Essentials with CISSP CBK, version 2.1. SANS Press, 2003 p400-416

"McAfee Security, Virus Glossary of Terms." May 2004.
URL: http://www.networkassociates.com/us/security/resources/glossary.htm#w

"McAfee Security, Virus Glossary of Terms." May 2004.
URL: http://www.networkassociates.com/us/security/resources/glossary.htm#t

"Microsoft Knowledge Base Article-245678." 14 May 2003
URL:
http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/q245/6/78.asp&NoWebContent=1

"Microsoft Security Bulletin MS04-011" 4 May 2004
URL: http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

Network Associates. "Exploit-MS04-011." 28 April 2004.
URL: http://vil.nai.com/vil/content/v_124974.htm

Network Associates. "W32/Gaobot.worm.ali." 28 April 2004
URL: http://vil.nai.com/vil/content/v_125006.htm

Network Associates. "W32/Sasser.worm.a." 28 April 2004
URL: http://vil.nai.com/vil/content/v_125007.htm

Keizer, Gregg. "Sasser Worm Impacted Bussinesses Around the World." 7 May 2004.
URL: http://www.internetwk.com/allStories/showArticle.jhtml?articleID=20300011

"Red Hat Network Update Module." May 2004
URL: http://www.redhat.com/software/rhn/update/

" ZoneLabs" May 2004
URL: http://www.zonelabs.com/store/content/home.jsp

"Mozilla." May 2004
URL: http://www.mozilla.org/

"Jabber Software Foundation." May 2004
URL: http://www.jabber.org/

Carnegie Mellon Software Engineering Institute. "Allow only appropriate physical access to computers." 12 June 2000.
URL: http://www.cert.org/security-improvement/practices/p074.html