Defense In Depth

Todd McGuiness

Todd McGuiness
Version 1.2E
Defense In Depth

Introduction

Defense in depth is the concept of protecting a computer network with a series of defensive mechanisms such that if one mechanism fails, another will already be in place to thwart an attack. Because there are so many potential attackers with such a wide variety of attack methods available, there is no single method for successfully protecting a computer network. Utilizing the strategy of defense in depth will reduce the risk of having a successful and likely very costly attack on a network.

This paper will look at three common scenarios for network attacks, likely methods of attack, and countermeasures to protect the network from the attacks. The first scenario is an attack by a script kiddie from the Internet, the second is an attack from a skilled hacker and the final attack is from a trusted user who has access to the network.

This paper does not attempt to provide a comprehensive discussion of who attackers are, the methods they use in their attacks, or methods to protect against the attacks. A work of that sort would fill volumes and is obviously far beyond the scope or intention of this essay. This paper instead, uses a number of examples simply to illustrate the need to implement a strategy of defense in depth.

The Script Kiddie

The paper “Know Your Enemy III” [1], from The Honeynet Project, describes who a script kiddie is.

> The script kiddie is someone looking for the easy kill. They are not out for specific information or targeting a specific company. Their goal is to gain root the easiest way possible. They do this by focusing on a small number of exploits, and then searching the entire Internet for that exploit. Sooner or later they find someone vulnerable.

Despite a lack of technical know-how, script kiddies are dangerous because they do not care who they attack and because they are able to capitalize on the technical abilities of others. A person can go to a site like http://neworder.box.sk which has lists of exploits, discussions about the exploits, information about how to identify vulnerable systems and the code to launch an attack. This is essentially everything needed to launch an attack.

Attacks by script kiddies happen with amazing frequency. In an interview with MSNBC[2], Lance Spitzner, Director of the Honeynet Project, said:

> The fastest one of our honeypots has ever been hacked is 15 minutes. This should scare the hell out of you. We do nothing to advertise. We just put the systems out there. This is my ISDN line in my home bedroom. It's not IBM or something like that.

A strong perimeter defense is the best defense against script kiddies. A firewall manages both incoming and outgoing traffic on a network and is essential to a strong perimeter defense. In May 2001, Information Security Magazine printed an interview with Stephen Northcutt, Director of the Global Incident Analysis Center [3], which said:

> **Early in 1999, you said, "The good news is, of everything that I've seen in 1998 and 1999 so far, there is nothing that really presents a danger to a well-configured, proxy-based firewall site. Almost every technique that I've seen in use will not pass through that firewall; you do have to watch your backdoors, but that's really good news." Is this still true?**
>
> Yes, but with a modifier. You also have to have a content sensor for e-mail attachments. The improvements in malicious code are significant. Insiders are a big threat, but any software running on any system in your organization is an "insider" as well. It has the same advantages as any human insider.

Firewalls are extremely effective, but they cannot be relied on as the only means of securing a network perimeter. In fact, the SANS Institute determined that relying primarily on a firewall is one of the seven most common mistakes management makes to jeopardize network security [4].

Network based intrusion detection systems (IDS) provide another layer of perimeter defense.Iin his book, Network Intrusion Detection An Analyst's Handbook,[5] Stephen Northcutt said:

> The signature line of the hymn *Amazing Grace* is "I once was blind, but now I see." This is what an intrusion detection system does: It helps an organization go from a blind state to a seeing state. This is a good thing! (Page 226)

A network based IDS will monitor network traffic to identify scans or traffic patterns that indicate an attack. These systems can recognize defined attack signatures or anomalous behavior that might be indicative of an attack. A network based IDS can identify attacks that would likely otherwise go undetected, will sometimes take defensive measures such as interacting with the firewall to stop certain traffic, alert an administrator of a problem and can help identify the vulnerability that was exploited in the event of a successful attack.

Despite the strongest of perimeters, a script kiddie will sometimes find a method to successfully attack a network. Some of the most devastating incidents to date have been random attacks perpetrated by script kiddies. Because there are ways around a firewall, it is imperative that individual systems be protected. Systems need to be hardened by making sure that the system has all current vendor patches installed, that anti-virus software is current and that all unused services are disabled. The Honeynet project provides the following insight in the paper "Know Your Enemy." [6]

> …the script kiddie is going for the easy kill, they are looking for common exploits. Make sure your systems and networks are not vulnerable to these exploits…

The Code Red worm, for example, was an exploit that took advantage of a vulnerability in Microsoft's IIS web server software. The Code Red worm ran rampant on the Internet starting July 19, 2001 [7] despite the fact that Microsoft had released a

patch for the vulnerability on June 18, 2001 [8] more than a month earlier. The W32.Nimda worm took advantage of two different vulnerabilities. The worm came into the wild and crippled networks on September 18, 2001 [9] even though Microsoft had released fixes for the two vulnerabilities on August 10, 2000 [10] and March 29, 2001 [11].

To avoid attacks like Code Red and W32.Nimda, basic system security measures need to be defined and implemented before a computer becomes part of a network. There are several sources available to help accomplish this. For instance, AusCERT [12] and The SANS Institute [13] both have excellent information on basic measures to secure systems.

System administrators also need to be aware of new threats and fixes to maintain secure systems. SANS [14], Bugtraq [15] and CERT [16] provide current information on vulnerabilities for the administrator.

Anti-virus software is an essential tool for securing any system on a network. Anti-virus software with current signatures will recognize known viruses, worms and Trojans, take specified actions to deal with the infection and notify users or systems administrators of the problem.

Social engineering is a common method of attack to get an exploit past a firewall. Script kiddies are likely to implement social engineering by email as was done with the I Love You virus and the variants that came out soon after the original virus was introduced. The most important line of defense against this type of attack is user education. In his article "Security Awareness Program" [17] Tom Peltier identified the user community as critical to the network security process; he wrote:

> A strong security architecture will be less effective if there is no process in place to make certain that the employees are aware of their rights and responsibilities. All too often, security professionals implement the "perfect" security program and then forget to factor the customer into the formula. (page 197)

The user community needs to be made aware of threats to the security of the network. For instance, they should know the risks of opening email attachments, sending sensitive information across the network, and so on.

Another threat to network security created by the script kiddie is denial of service (DoS) attacks. A DoS attack is an attack on network resources to prevent users from getting to what they need. For instance, a smurf attack takes advantage of improperly configured routers on another network to fully consume a network's bandwidth so legitimate users cannot access network resources. Syn flood attacks take advantage of a built-in weakness of TCP/IP to bind a system's resources so users can't get to a particular host. There are countless other attacks that can lock user accounts, fill disk drives, crash CPU's and so on.

When the script kiddie cannot do anything else, he often resorts to a DoS attack. Many DoS attacks can be prevented by a strong perimeter and properly configured systems, but some of these attacks cannot be stopped. Sometimes, the most that can be done is take precautions so network resources cannot be used by an attacker in an attack on another network.

The Skilled Attacker

Attacks by skilled attackers happen with less frequency but are successful much more frequently. Kevin Mitnick boasted in testimony to the U.S. Senate [18]:

> I have successfully compromised all systems that I targeted for unauthorized access save one…I have gained unauthorized access to computer systems at some of the largest corporations on the planet, and have successfully penetrated some of the most resilient computer systems ever developed.

The skilled attacker is able to be more successful by researching the company being attacked, utilizing additional methods of attack, and being more aggressive with the same tools as the script kiddie. It is even more important to use properly configured firewalls, secure each individual system, employ intrusion detection systems and anti-virus software but additional methods also need to be employed.

Making information about the network easily available is tantamount to rolling out the red carpet for attackers. In Hacking Exposed: Network Security and Solutions [19] the authors say:

> Even the most skilled attackers often spend days researching their targets, painstakingly building a list of possible avenues of entry. Once a vulnerability is identified, the actual exploitation of the hole likely occurs in milliseconds… (page 4)

Skilled attackers study the company and it's network to discover every entry point to the network. These entry points may be from the Internet, a company intranet, an extranet, dial-in modems, or even the front door of the building. Once all entry points are identified, the attacker will determine the best way to breach one of these entrances to gain access to the network.

The skilled attacker will use company information to mount more successful social engineering attacks. For instance, these attackers might call the help desk posing as the CEO and demand that his password be changed or send a Trojan in an email to one employee posing as another employee. These attacks tend to be very successful because the attacker can be very believable by referencing names of upper management or by referencing situations at the company like recent acquisitions or layoffs. These attacks are also successful because they play on a person's desire to be helpful or even to keep one's job. The only way to combat this type of attack is through education. Kevin Mitnick, who said he has gotten into all but one site that he targeted, continued in his Senate testimony [18] that:

> The methods that will most effectively minimize the ability of intruders to compromise information security are comprehensive user training and education. Enacting policies and procedures simply won't suffice. Even with oversight the policies and procedures may not be effective: my access to Motorola, Nokia, ATT(sic), Sun depended upon the willingness of people to bypass policies and procedures that were in place for years before I compromised them successfully.

To combat a social engineering attack, companies need to raise the awareness of all employees to a point where any unusual request for information is seen as a threat. Network security can not be left to just the system administrators. Everybody

from the janitors to the executive staff need to be trained to recognize the threat that can be created by divulging even seemingly trivial information.

Because a skilled attacker might simply walk through the front door of a facility, physical security also needs to be addressed. The attacker might carry in a laptop or CD or floppy diskettes and install Trojans or network sniffers. Once inside, the attacker might also gather more intelligence or mount a social engineering attack.

Physical security can be implemented in many different ways. Twelve foot chain link fences with three strands of barbed wire around the physical perimeter of a property with armed guards at each gate and at building entrances, biometric controls for doorways, motion detectors and surveillance cameras may be in line at some sites while merely training users to be aware of unrecognized people or unusual activity may be more appropriate at other sites.

Strong passwords are essential to a secure network. A skilled attacker will frequently simply guess passwords. Eric Cole, in Hackers Beware, [20] notes that

> Eighty percent of all salespeople that I came in contact with had a password of either golf or bogey. (page 286)

An attacker who is able to access a password file will also employ password cracking software. Eric Cole points out in Hackers Beware [20] that:

> … all passwords can be cracked; it is just a matter of time. The length of time it takes to crack a password changes as computers get faster and cheaper. A password that took over 50 years to crack 10 years ago can be cracked now in less than a week. (page 311)

Using strong passwords and changing them frequently will make it much more difficult for an attacker to gain access to the network through password guessing or cracking. Passwords should not be dictionary words or names. They also should not be words or names with numbers concatenated to them. A strong password will be a mix of upper and lower case alpha characters, special characters (i.e. ~,!,@,#,$,%,^) and numbers. Passwords also need to be something the user will remember so it won't be written down and taped to the computer monitor.

There are better strategies for user authentication than passwords. For instance, one-time passwords can be generated by software or hardware to be used for a specific period of time. There are different methods to implement this, but one way is for a user to have a special calculator that generates a new password every minute. At the end of the minute, the password is useless. This one-time password in combination with a traditional password provides a much more secure method of authentication. Biometrics is another example of a more secure method of user authentication. Biometric devices use biological identifiers like fingerprints or retinal scans to identify a user.

The Inside Attacker

The attacker who has the strongest position going into an attack is the trusted employee. In his May 2001 interview with Information Security Magazine, Stephen Northcutt [3] said:

> Insiders are without a doubt the largest threat. They know where the crown jewels are. They know the processes on the inside. They already have logins. If they have something to gain, there's not much to prevent them from doing the wrong thing.

Additional measures need to be taken to discourage the inside attacker. Policies and procedures, employee screening, separation of duties and rotation of assignments are important methods to secure the network from attackers who already have trusted access to it.

Security policies and associated procedures are necessary to a secure network. Policies and procedures raise awareness of network users so they will know if they have crossed a line and are doing something that they shouldn't. Policies and procedures also make the expectations of management clear for all the people involved in the security process. Charles Cresson Wood in Information Security Policies Made Easy 8th Edition [21] said:

> Management must first decide which users should be given access to which information resources, preferably defining the ways to make these decisions in a policy. Management must also establish procedure so that technical people can set-up access controls in a manner consistent with these decisions. (page 7)

Employee screening can be anything from checking references to reviewing tax records to obtaining a security clearance. Obviously the level of screening done should be related to the magnitude of the risk presented to the company if the employee were to betray the faith placed with him.

In nearly all cases, the concept of least privilege should be implemented. This is to say that nobody should have access to anything that they do not explicitly need to do their job.

Separation of duties requires actions by at least two people to complete a given task. This creates the need for collusion and reduces the opportunity for an individual to breach system security. For instance, cryptographic keys that are being held in escrow can be split in two with one individual holding the first part of the key and another individual holding the second part of the key. Another example would be where one person is able to print checks while another person is able to sign them. In either case, neither of the individuals would be able to take advantage of a position without help from a co-worker.

Rotation of assignments limits an individual to a given role for a particular period of time. This method may have too many downsides for some businesses to implement but it may prove effective for others. Doing this can prevent an individual from becoming indispensable or prevent the individual from learning a system so well that they are able to find faults that would allow fraud or abuse to go undetected. An example would be an accounts payable clerk who discovers a way to write checks to himself in such a way that it looks like a legitimate expense to the company.

A System is Compromised

The stakes will be raised considerably if any or all of the measures discussed up to now fail and a system is compromised; regardless if it is done by a script kiddie, a

skilled attacker or a trusted user. Gaining control of just a single machine on the network is a big first step for an attacker to gain control of the entire network. No firewall, policy, procedure or physical security plan in the world is going to stop the intruder from doing greater harm. Systems need to be hardened, intrusion detection systems need to be in place, access control measures need to be strong, anti-virus software needs to be running with current definitions and users and system administrators need to be on the look out for unusual activities on their systems. But all of this is not enough. There need to be still more layers of defense in place to protect the network.

The attacker who has free access to the network may do more intelligence gathering. For instance, the attacker may sniff the network for data or passwords or the attacker might probe other machines for vulnerabilities. With this information, the attacker may mount attacks on other machines.

The attacker who has gained access to the network has gained a significant edge, but there are still measures that can be taken to protect the network. Sniffing and hijacking can be prevented or made much more difficult by using a switched Ethernet network where collision domains are broken up and the threat created by a network interface card in promiscuous mode is greatly diminished. Implementing a secure authentication and transmission method such as Kerberos can prevent the theft of passwords and data on the network.

Backups are also a critical defense that need to be in place in the event that a system is compromised. If all other layers of defense have not been adequate and a system is compromised, it is likely that the system will need to be rebuilt and restored. Without a proper backup strategy, data may be lost.

Conclusions

No single security measure can adequately protect a network; there are simply too many methods available to an attacker for this to work. The script kiddie, a skilled attacker and trusted user have some methods in common, but each presents unique problems to a secure network. For instance, a firewall does not provide any protection from an insider but should be a significant hurdle for an attacker from the outside. Likewise, policies and procedures do not mean anything to an attacker from the outside but should be part of the plan to protect a network from insiders.

Implementing a strategy of defense in depth will hopefully defeat or discourage all kinds of attackers. Firewalls, intrusion detection systems, well trained users, policies and procedures, switched networks, strong password and good physical security are examples of some of the things that go into an effective security plan. Each of these mechanisms by themselves are of little value but when implemented together become much more valuable as part of an overall security plan.

References

1. The Honeynet Project. Know Your Enemy: III. March 27, 2000. http://project.honeynet.org/papers/enemy3/.

2. Security Gurus Study Hackers With 'Honeypot' Computers. MSNBC, July 29, 2001. http://www.msnbc.com/local/wfla/mgadlrs6qpc.asp.

3. Thieme, Richard, "Q&A With Stephen Northcutt A Mentor's Mantra." Information Security, May, 2001. http://www.infosecuritymag.com/articles/may01/features_q&a.shtml.

4. The 7 Top Management Errors that Lead to Computer Security Vulnerabilities. The SANS Institute, May, 1999. http://www.sans.org/newlook/resources/errors.htm.

5. Northcutt, Stephen. Network Intrusion Detection An Analyst's Handbook. Indianapolis: New Riders, 1999.

6. The Honeynet Project. Know Your Enemy. July 21, 2000. http://project.honeynet.org/papers/enemy/.

7. CERT Incident Note, Carnegie Mellon Software Engineering Institute CERT Coordination Center, October 29, 2001. http://www.cert.org/incident_notes/IN-2001-08.html.

8. Microsoft Security Bulletin MS01-033, Microsoft Corporation, October 29, 2001. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp.

9. CERT Incident Note, Carnegie Mellon Software Engineering Institute CERT Coordination Center, October 29, 2001. http://www.cert.org/advisories/CA-2001-26.html.

10. Microsoft Security Bulletin MS00-057, Microsoft Corporation, October 29, 2001. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-057.asp.

11. Microsoft Security Bulletin MS01-020, Microsoft Corporation, October 29, 2001. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp

12. Unix Security Checklist v2.0. Australian Computer Emergency Response Team, October 29, 2001. http://www.auscert.org.au/Information/Auscert_info/Papers/usc20.html.

13. SANS Institute Bookstore. The SANS Institute, October 29, 2001. http://www.sansstore.org/.

14. Incidents.org. The SANS Institute, October 29, 2001. http://www.incidents.org/.

15. Bugtraq Archive. Security Focus, October 29, 2001. http://www.securityfocus.com/archive/1.

16. CERT/CC Vulnerabilities Notes Database. Carnegie Mellon Software Engineering Institute CERT Coordination Center, October 29, 2001. http://www.kb.cert.org/vuls.

17. Peltier, Tom. "Security Awareness Program." Information Security Management Handbook 4th Edition. Ed. Harold F. Tipton and Micki Krause. Boca Raton: Auerbach, 1999.

18. Mr. Kevin Mitnick. Committee on Governmental Affairs, The United States Senate, 1997. http://www.senate.gov/~gov_affairs/030200_mitnick.htm.

19. McClure, Stuart, Joel Scambray and George Kurtz. Hacking Exposed Network Security Secrets & Solutions. Berkeley: Osborne/McGraw-Hill, 1999.

20. Cole, Eric. Hackers Beware Defending Your Network From The Wiley Hacker. Indianapolis: New Riders, 2001.

21. Wood, Charles Cresson. Information Security Policies Made Easy 8th Edition. Houston: Pentasafe, 2001.

Last Updated: February 19th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Reno Tahoe 2019	Reno, NVUS	Feb 25, 2019 - Mar 02, 2019	Live Event
SANS Brussels February 2019	Brussels, BE	Feb 25, 2019 - Mar 02, 2019	Live Event
Open-Source Intelligence Summit & Training 2019	Alexandria, VAUS	Feb 25, 2019 - Mar 03, 2019	Live Event
SANS Baltimore Spring 2019	Baltimore, MDUS	Mar 02, 2019 - Mar 09, 2019	Live Event
SANS Training at RSA Conference 2019	San Francisco, CAUS	Mar 03, 2019 - Mar 04, 2019	Live Event
SANS Secure India 2019	Bangalore, IN	Mar 04, 2019 - Mar 09, 2019	Live Event
SANS St. Louis 2019	St. Louis, MOUS	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS San Francisco Spring 2019	San Francisco, CAUS	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS London March 2019	London, GB	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS Secure Singapore 2019	Singapore, SG	Mar 11, 2019 - Mar 23, 2019	Live Event
SANS Secure Canberra 2019	Canberra, AU	Mar 18, 2019 - Mar 29, 2019	Live Event
SANS SEC504 Paris March 2019 (in French)	Paris, FR	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Munich March 2019	Munich, DE	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Norfolk 2019	Norfolk, VAUS	Mar 18, 2019 - Mar 23, 2019	Live Event
ICS Security Summit & Training 2019	Orlando, FLUS	Mar 18, 2019 - Mar 25, 2019	Live Event
SANS Doha March 2019	Doha, QA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS Jeddah March 2019	Jeddah, SA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS SEC560 Paris March 2019 (in French)	Paris, FR	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS Madrid March 2019	Madrid, ES	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS 2019	Orlando, FLUS	Apr 01, 2019 - Apr 08, 2019	Live Event
SANS Cyber Security Middle East Summit	Abu Dhabi, AE	Apr 04, 2019 - Apr 11, 2019	Live Event
SANS London April 2019	London, GB	Apr 08, 2019 - Apr 13, 2019	Live Event
Blue Team Summit & Training 2019	Louisville, KYUS	Apr 11, 2019 - Apr 18, 2019	Live Event
SANS Riyadh April 2019	Riyadh, SA	Apr 13, 2019 - Apr 18, 2019	Live Event
SANS Seattle Spring 2019	Seattle, WAUS	Apr 14, 2019 - Apr 19, 2019	Live Event
SANS Boston Spring 2019	Boston, MAUS	Apr 14, 2019 - Apr 19, 2019	Live Event
FOR498 Battlefield Forensics Beta 1	Arlington, VAUS	Apr 15, 2019 - Apr 20, 2019	Live Event
SANS FOR585 Madrid April 2019 (in Spanish)	Madrid, ES	Apr 22, 2019 - Apr 27, 2019	Live Event
SANS Northern Virginia- Alexandria 2019	Alexandria, VAUS	Apr 23, 2019 - Apr 28, 2019	Live Event
SANS Muscat April 2019	Muscat, OM	Apr 27, 2019 - May 02, 2019	Live Event
SANS Pen Test Austin 2019	Austin, TXUS	Apr 29, 2019 - May 04, 2019	Live Event
Cloud Security Summit & Training 2019	San Jose, CAUS	Apr 29, 2019 - May 06, 2019	Live Event
SANS Riyadh February 2019	OnlineSA	Feb 23, 2019 - Feb 28, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced