Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Anti-Hacking: The Protection of Computers

While the term Anti-Hacking may have different meanings to different people, one thing is certain. By definition, it means , "the opposite of hacking." If hacking is defined as an attack on a computer system, then Anti-Hacking is the protection of that system. The three aspects discussed in this paper: Education of the Security Adminis trator, Securing the Environment, and How to Fight Back are just one combined definition of how to protect a system.

Copyright SANS Institute
Author Retains Full Rights

AD

Anti-Hacking: The Protection of Computers
Chadd Schlotter

In the Computer Security industry, there are many solutions available to help combat cyber crime. Firewalls and Intrusion Detection systems are in place across the Internet to help protect more networks than ever before. Teams at software corporations work diligently on creating patches for known vulnerabilities, yet everyday the number of computers that are compromised increases. It seems like almost every week a big Internet or software company has a security incident, so what does this say about the Computer Security industry? Even with the software available to defend the networks of companies, it takes more than that. The education of the security administrators is the key to using those software packages correctly.

Anti-Hacking is a topic that should incorporate not only the tools to defend against black-hats but the knowledge to understand what the black-hat sees when he looks at a network. Anyone that connects to the Internet is at risk of having his or her machine compromised. And now, in the age of always on connections for even the home user, the threat to computer security is greater. It is each user's duty to ensure the integrity of their computer for everyone's sake, not just his own. While most topics in this paper will refer to security administrators in large networks, these common security practices should be applied in any scale; from major companies to home computer networks. Remember, the home user is the security administrator for his home network. This paper will cover three major topics of Anti-Hacking: Education of the Security Administrator, Securing the Environment, and How to Fight Back.

Education of the Security Administrator

Security Administrator positions in companies are being filled everyday by many classes of people. Some positions are filled with a seasoned security veteran with many years of firewall and operating systems experience. Then, there are some companies who will hire anybody that will take the job, whether they have security experience or not. Which company's network is more at risk? Do not be so quick to answer.

A person that is new to security will be sent to conferences, training, and seminars to be informed on the actual threat that is out there. Then, he could come back to his company and configure firewalls, intrusion detection devices, and alerting software to report any suspicious happenings on his network. Security policies for internal users are distributed and enforced. Scripts are set to run every hour to report abnormalities in the logs. Penetration testing is conducted on his network and patches are applied to software that is used on the Internet.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

By doing all of this, is his network secure? How many times will he get paged in the middle of the night with a false positive that he spends a couple of hours investigating? Can one person actually configure and install that kind of infrastructure or will the company need to hire another security person? These questions are usually associated with people that are new to security. New security people want to put up as many security tools as possible in the shortest amount of time. Without experience, a lot of valuable time is spent trying to protect a network without actually knowing what you are protecting it from.

The seasoned security veteran could implement the same security infrastructure. However, through his years of security experience he knows that every suspicious activity does not need investigation. Some are false-positives, which are caused by authorized users doing normal everyday activities. He tunes these events out and examines his network for targets that a common attacker would try to hit. After insuring that the most visible targets are secure, he goes about his other daily duties as an administrator. Is he missing real events because he is not thoroughly scanning the logs? Is his internal network secure? Do his users have modems in their computer or are they allowed to bring laptops into work? The more experienced security person could be a little lazy on applying patches and investigating his security policies for his own environment.

The education of security administrators goes past learning about security software and applying the software to one's network. Along with the topics in the examples above, the part of the education process that needs to be enforced is to understand the threat that exists. In the "Know Your Enemy" series of white papers on his website, Lance Spitzner, a well-known expert in the field of Information Security, describes the threat that is out there and the tools that the common black-hat uses. These papers are a good first resource for understanding the mindset of an individual who is trying to attack one's network. Spitzner talks about the importance of knowing who and what the threat is. These papers are a must for the education of security administrators. Without understanding what they are protecting their network from and what the attacker can do to their network, the network they protect is vulnerable. Spitzner goes on to discuss the tools and methodologies of one of the most common attackers, the 'script kiddie'.

Since the majority of attacks do come from the script kiddie, that should be an area of high concern for security administrators. The common black-hat has access to hundreds of scripts online that just requires an IP address to initiate some form of attack against a computer. Most of these scripts are attacks on vulnerabilities that have been documented for months. Patches are usually available within a few days after the vulnerability is announced. However, if the security administrator does not implement these patches, his network is vulnerable to such attacks.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

A honeypot is a computer system that is purposely put out onto the web to be attacked. Security professionals commonly use Honeypots as an educational tool to show how black-hats probe and exploit a system. All aspects of network defense lead back to education. Other uses for honeypots will be further discussed in the third topic of this paper.

Besides the series of papers mentioned earlier, many books have been written on the methodologies of hacking. One of the more famous books is Hacking Exposed by McClure, Scambray, and Kurtz. This book, and the second edition of the book, has opened the eyes of security administrators everywhere. These books describe in plain English many common black-hat attacks that are used on computers and networks. Understanding how these attacks take place and knowing what the common attacks are help security administrators defend their networks. The Anti-Hacking effort can benefit enormously just by educating security administrators as to the threats that are out there.

Securing the Environment

This topic is the most obvious form of Anti-Hacking, yet it is not fully utilized in most cases. Security Administrators design network diagrams placing firewalls and intrusion detection systems at the perimeters of their network and implement these designs. However, the most neglected parts are actually the most important:

- **Checking the logs of the firewall (Both FW and System)**
- **Fully utilizing intrusion detection software**

First of all, the firewall logs can collect as much or as little information as the administrator wants. If this information is never examined, then the firewall should not be logging it at all. The configuration of firewalls to log the correct data without logging too much information is an ongoing battle that changes with the topology of the network. The key to successful logging is planning. Before the implementation of the firewall is complete, the administrator should plan out what events he wants to be logged and what information associated with those events should be logged. This is where the education of an administrator really helps out. The security administrator knows what activity should and should not be going on through his firewall. Most firewalls offer user-defined alerts that can send emails or alert pagers to any suspicious activity. However, what if the attacker does not set off any alerts? What if the traffic is legitimate traffic to the firewall, but a box is exploited? The third challenge after logging the information is putting it into a form that can be understood. The faster these events can be brought to the administrator's attention, the less time an intruder has to do his damage. There are many products available that arrange firewall logs in a simple, easy to read, report.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

In addition to the firewall logs, the system logs of key boxes should be examined on a routine basis. In another paper written by Lance Spitzner, he describes the logs as being, "extremely copious, quickly overwhelming us with information." The paper titled, "Watching Your Logs", goes into detail on how to filter your system logs for the correct information and how to put this information in an easy to read form. Once again, the education of the security administrator is needed to know exactly what logs need to be examined and what triggers should be set up in order to catch illegal activity.

The second topic under securing the environment is understanding the intrusion detection alerts. By default, many intrusion detection software packages spawn alerts on almost everything. Many of the alerts are bogus and the administrator wastes time trying to sort through the alerts to find the real ones. The recurring theme of education comes up again here when the administrator needs to know what alerts are real and what alerts are not. This has some to do with the specific software he is using, but for the most part it has to do with understanding the attacks. For example, if the software is only configured to monitor traffic coming from the outside, one key facet of security breaches will be missed. Many Trojan or backdoor programs initiate specific traffic to the outside. The intrusion detection software can spot this traffic and spawn an alert. However, without knowing how some of these attacker programs work, these alerts can be easily mistaken for false positives.

In addition to understanding the alerts, security administrators need to understand the purpose of using both firewalls and intrusion detection software. Firewalls are vulnerable to attacks that are allowed to pass through from the outside because of protocol and traffic that never has to hit the firewall. Some examples of this include the hacking of public viewable boxes (DMZ servers) and internal attacks. In the example of DMZ servers, web servers are the number one target. Since the firewall should allow web traffic to your public web servers, the firewall cannot do anything. However, intrusion detection software can examine the packets traveling to the server for what are called signatures. Signatures are packets that can be identified as having a specific purpose, such as a specific exploit on a web server. The software can then block the packet and in some cases send packets back to the attacker dropping the connection completely.

Through the proper implementation and use of firewalls and intrusion detection systems, many black-hat attempts can be over before they start. However, if one happens to slip by the defenses, the logs of the systems can be used to determine who invaded the network and what kind of damage was done. These two tools, when used effectively, have the most impact on computer security and the Anti-Hacking effort.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

How to Fight Back

The third aspect of Anti-Hacking is a mixture of two things: what to do during or after the hack and some deception methods to lure black-hats toward a network. In the event that a computer is hacked or probed, the number one thing that an administrator does not need to do is retaliate. This solves absolutely nothing and puts the administrator in the same category as the attacker. This also reveals that there are actually computer systems out there and someone is monitoring them. This could prompt the attacker to try some different types of attacks. The best thing to do is to gather up enough information about the attack to where the facts can be put together to determine exactly what the attacker did or was trying to do and proceed from there. If it is just a script kiddie scanning a network for possible targets, there is not much that you can do. If an administrator tried to track down every person that scanned their network, he would not get very much done.

If a computer is hacked, the main thing to determine is whether the black-hat is done or he is still on the box. The one thing that needs to happen first is to try and determine where the black-hat is coming from. An IP address can go a long way in tracking down a black-hat. Do not start deleting files off the system. If a black-hat sees files magically disappearing, he may decide to get off the computer or delete valuable logs before the administrator can get the information needed to prosecute the black-hat. Once an administrator has identified the black-hat and has enough information to prosecute the black-hat, the box should be removed from the network. Granted, there are some exceptions to this. If the box has been compromised and is being used as a weapon against other computers (i.e. DDOS), the box should be removed immediately.

In a perfect world every administrator would be able to catch the intruder in the act. Unfortunately, it does not work this way most of the time. Usually the box is hacked and the administrator discovers this after the fact. There are many papers online about recovering from attacks. The main things to remember are to remove the box from the network and to not change or delete any files on the disk. Some files may contain certain clues about the identity of the intruder and how long he has been on your box.

The second topic under fighting back is common deception methods. Some of these methods, although not new to the information security world, are not publicized as much as firewalls and NIDS. However, these methods can be just as effective. The first of these methods is called a honeypot or honeynet. While these boxes can be used to educate administrators as to the ways of black-hats, they can also be used to catch black-hats. In the article mentioned earlier, "To Build a Honeypot", Spitzner says that he does not use honeypots as a way to catch black-hats. However, a well-configured honeypot can be a warning of activity to come. Since honeypots are usually the least secure, these boxes are likely to be the first ones attacked. Alerts spawned by the attacking of these boxes can keep an attacker from moving on to any of the real boxes in a network.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Before setting up a honeypot, an administrator needs to protect his network from the box being compromised. A few rules to remember are as follows:

- Confine the honeypot to its own network. If the box is compromised, ensure that the hacker does not have access to the rest of the production network.
- As an extension of the first point, do not block all outgoing access on the honeypot. If an attacker compromises the box and then cannot get anywhere else, he will get suspicious and leave. This may lead to not gaining enough information about the attacker.
- If NIDS is being utilized on the network, make sure there are special alerts sent out for any honeypot. These alerts, as mentioned above, can be early warning signs that an attacker is looking at your network.
- Store logs that could be used as evidence off of the honeypot. If a skilled attacker does compromise the box, the first thing that he will do is look to delete or change the logs.
- Keep the honeypot up to date. Do not think that if you are running Windows 2000 SP 1 and IIS 5.0 on all your boxes and your honeypot is running Windows NT 4.0 SP3 with IIS 4.0 that a black-hat will not be suspicious and may not attack the box at all.

There are many types of honeypots and up until now this paper has talked about full systems. However, one of the more amusing ways to fight back against attackers is with deception systems. One of the more famous ones is Fred Cohen's Deception Toolkit. This is a combination of the most commonly hacked protocols in one kit. This kit interacts with the attacker so the attacker thinks he is on a real system. One of the most notable amusing deception systems is the "00[Sub]7", the Ultimate SubSeven Logging Tool by Jeff Capes. One of the most common port scans on a system nowadays is for port 27374, or the SubSeven port. SubSeven is a very powerful Trojan that can do any number of things to a victim's computer. This deception tool looks like a SubSeven server listening on the standard port. It logs all activity that goes on between the client and the fake server. The user can send the attacker a message with the attacker's IP saying that he is being logged as well as some other goodies. This is more of a tool geared toward the home user instead of a corporate environment. Tools such as honeypots turn the tables on the black-hat world. The administrator can collect IP addresses fairly easily and report these addresses to the proper authorities.

While honeypots are a good educating tool and a good way to catch some beginner black-hats in the act, these boxes should be monitored very closely and should only be implemented on networks by experienced security administrators.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Conclusion

While the term Anti-Hacking may have different meanings to different people, one thing is certain. By definition, it means, "the opposite of hacking." If hacking is defined as an attack on a computer system, then Anti-Hacking is the protection of that system. The three aspects discussed in this paper: Education of the Security Administrator, Securing the Environment, and How to Fight Back are just one combined definition of how to protect a system.

References

Capes, Jeff. "00[Sub]7 – The Ultimate SubSeven Logging Tool." 20 August 2000. URL: http://www.rendo.dekooi.nl/~jeff/Sub7.htm (3 March 2001).

Graham, Robert. "FAQ: Network Intrusion Detection Systems." Vesion 0.8.3. 21 March 2000. URL: http://www.ticm.com/kb/faq/idsfaq.html (3 March 2001).

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

Schwartau, Winn. "Honeypots Wreak Sweet Revenge Against Cyber Intruders." 4 December 2000. URL: http://www.nwfusion.com/columnists/2000/00173866.html (2 February 2001).

Spitzner, Lance. "Know Your Enemy." 18 August 1999. URL: http://www.netclimb.com/lspitz/enemy.htm (26 July 2000).

Spitzner, Lance. "To Build A Honeypot." 7 June 2000. URL: http://www.project.honeynet.org/papers/honeypot/ (3 March 2001).

Spitzner, Lance. "Watching Your Logs." 19 July 2000. URL: http://www.enteract.com/~lspitz/swatch.html (3 March 2001).

Spitzner, Lance. "Welcome to Logger." URL: http://www.enteract.com/~lspitz/logger.html (3 March 2001).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 23rd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced