Security Thinking

Magnus Mischel

Introduction

Today when most networks and many home computers are connected to the Internet 24 hours a day, 7 days a week, there is a need for new security thinking to protect the data on your machine and prevent crackers from gaining access to it. This paper is aimed at system administrators and home users alike. It attempts to point out some of the things that you must keep in mind when operating your computer and network, and why things can go wrong if you don't.

Are You at Risk?

Many users when first connected to the Internet are not aware of the dangers that come with being online. Of those who are, a great deal ignore basic security practices thinking "it won't happen to me". However, experience tells us that any computer connected to the Internet will be attacked or probed sooner or later. Most likely it will be sooner. The consequences can be devastating unless you are prepared.

The dangers that exist come not only from crackers or script kiddies. They also appear in the form of viruses, trojan horses and worms. Therefore, you need to protect yourself against these threats as well as against crackers.

Crackers and Script Kiddies

Crackers are people with a great amount of computer and network experience who use their knowledge to gain illicit access to other computers. (The term can also be used to refer to people who break the copy or shareware protection of software; however, in this paper it is not used in that context.)

The less advanced form of computer intrudes are often referred to as "script kiddies" and frowned upon by most crackers. Script kiddies take known exploits and use these ready-made programs (often created by a cracker) to gain access to computers which are vulnerable to the exploit. This requires little or no knowledge of computer security since the script kiddie is only executing a program. Nevertheless, these less-skilled individuals pose a threat to your network as much as the crackers do - not because of their skill, but because of their sheer number. There are far more script kiddies out there than there are skilled crackers. Someone has compared the script kiddies scanning for vulnerabilities to the million monkeys hammering away at type-writers to produce a Shakespeare play. Sooner or later, one of them is bound to find a vulnerable computer. And if you're not protected, it might be yours.

Defeating the Script Kiddie

The first thing you should keep in mind is that no networked computer should run more services than absolutely necessary. Every open port is a potential entry point for an attacker. This includes programs like ICQ or AIM that open ports to communicate with the outside world. For example, back in 1999 there was a vulnerability in ICQ where remote users could gain access to the entire drive where the program was installed through a flaw in the program's built-in web server. Having trimmed the number of programs that keep an open window to the Internet, you need to make sure you are informed when flaws are discovered so that you can install the proper updates.

Exploits surface almost on a daily basis. Usually when a vulnerability has been discovered by the security community, the vendor is first contacted so that he can provide a patch against the exploit. After that, the vulnerability is often made public, and that's the point when users can read about the vulnerability and protect themselves against it. Because there is no way to protect yourself against these dangers without knowledge, you need to stay on top of the security news. One good starting point is to subscribe to Bugtraq, a mailing list that discusses vulnerabilities. The list generates a lot of traffic, but is also available in a digest format. See *http://www.securityfocus.com* for details on how to subscribe.

Protecting Yourself From Crackers

Protecting yourself against crackers involves the same procedures as explained above for defeating script kiddies, but extends to more advanced techniques. A paper like this one cannot possible cover all the measures that need to be taken, but a few words on what you need to do are in order.

- Enable the logging features in your operating system, and install at least one third-party logging utility. If you are probed, attacked or even compromised, you need reliable logs. Make sure that the logs are written to an external computer, or to a media where the data can be written but not erased at a later time. Make sure that you take the time to read the log files so you can detect any suspicious activity.
- Install a file-integrity tool to detect changes to system files, and make sure you protect the signature-database in a proper way.
- Install a firewall, and learn how to properly configure it. The firewall policy should be to deny that which is not explicitly allowed. Enable logging, and check the logs from time to time. (More on firewalls in the next section.)
- Don't give users more access to the system than they need. Create an account for your daily use of the system, and use it instead of the administrator or root account. Never give accounts on your machines to people you don't know. It is infinitely much easier to gain leveraged access to a machine if you already have a legitimate account on it.

The ultimate tool you can have to efficiently protect yourself from crackers is knowledge. Know what methods crackers use to gain access to systems, and learn what counter-measures are available. Keep informed of the latest news in the security area, and make sure you properly understand the impact of new vulnerabilities.

Firewalls

A firewall controls who is allowed to access your network, and what they are allowed to access. Firewalls can also be used to control what people on a network are allowed access to on the Internet, but this section will focus on the former use of firewalls. A firewall can monitor packets travelling to and from your network and determine if they should be allowed through, or if they should be discarded. There are two basics stances a firewall can have when it comes to allowing and blocking connections. One is to allow all packets and connections that are not explicitly prohibited. The other is to block all packets and connections that are not explicitly permitted, and this is the one I recommend you implement. It is much better security practice to first say that everything should be prohibited, and then add rules for what should be allowed.

Firewalls should always be placed at the "edge" of your network so that all traffic travelling to and from the Internet passes through it. This way, you make sure that all data is inspected by the firewall. An commonly used example of how things might go wrong is if you are a business with a LAN, and an employee installs a modem and uses it to establish a connection to the Internet over the phone lines. This connection would not be protected by the firewall, and is thus a potential entry-point for a cracker or script kiddie.

Worms, Viruses and Trojan Horses

Worms, viruses and trojan horse programs all have one thing in common: they can contain malicious code. Worms are programs that automatically replicate over a network, viruses are programs that infect executables and need a user to run the infected files to propagate. Finally, trojans are programs that appear to perform some useful task, but covertly execute some malicious code. Many trojans open backdoors into a system.

What all of these (most often) malicious programs have in common is that they can be protected against rater easily. For viruses, you need to install a good virus scanner, keep the virus signatures updated, and run a resident scanner. Remote access trojans that open backdoors on a system can be subverted by a properly configured firewall. Worms can often be detected by antivirus programs, and their spreading and execution can many times be stopped by not opening e-mail attachments or running unknown executables.

Denial of Service Attacks

Denial of Service (DoS) attacks are attacks that prevent you from accessing the Internet, or prevent others from accessing you. This can be achieved in a number of ways. One way is to flood your Internet connection with massive amounts of data so that your link to the net is saturated. Another way is to exploit operating system or software flaws to lock up your machine or disable your services. However the Denial of Service is achieved, it rarely poses a risk to your data, but it can cost you lots of money if you run an e-Business.

For the sake of completeness, I should mention that DoS attacks can be used when spoofing connections. In this attack, forged packets are sent to the computer the cracker wants to establish a spoofed connection to. However, since the target host replies to these packets to the spoofed host, the cracker needs to prevent it from replying so as to not make the target tear down the connection. This is established through a DoS attack against the spoofed host. This is an advanced topic, but I wanted you to be aware of how DoS attacks can be used for more than inconveniencing a system administrator.

So what can be done to protect yourself? For the operating and software specific vulnerabilities, there are most likely patches available which you need to apply. As for the attacks that saturate your bandwidth, there is no final solution. If you have a firewall between your network and the Internet, you can probably configure it to start dropping packets if one single host suddenly starts sending you a large amount of data. However, this method isn't fool-proof. Firstly, because packets can be spoofed, and secondly because there is a DoS method called DDoS. DDoS stands for Distributed Denial of Service, and is an attack in which a large number of different computers work together to flood a single computer with packets, thus saturating its connection.

Final Words

Security can be divided into two big parts: Establishing a security plan and implementing it (locking down your system, creating security policies etc.), and keeping updated on new security issues. The first will give your network the basic security needed, and the second will assert you are aware of most new risks. Of course, you also need knowledge and practical experience. This paper, I hope, has given you some more knowledge in the area, but only you can make sure you get the practical experience needed to maintain good security. Read more documents like this one, implement the suggestions you come across and find might improve on your security, and stay on your toes.