Hacking Techniques

Leroy N. Papke

Table of Contents

Abstract

This paper examines the more popular techniques employed by hackers to gain unauthorized access to computers and networks around the world. Types of defenses against these attacks are also discussed, as well as the economic impact on business and consumers. Hacking is a growing problem that must be dealt with at all levels of computer usage; it has advanced to the level where no computer is safe, even ones that are not connected to a network of any kind. These can still be infected by means of software, and so all machines must be inspected on a regular basis. At the end of this paper, conclusions are drawn for the most logical manner in which to proceed and the overall costs involved.

Introduction

Hacking techniques are as varied as the hackers that create them. Every person that decides to become a hacker builds on the results of the hackers that came before, and adding their own style of hacking to the mix, create new techniques for the hacking community along with new problems for network administrators.

This paper will describe some of the more popular hacking techniques that are available, and then examine them in greater detail, showing why they are a problem and what some of the solutions to stopping them are. At the end, there will be recommendations for possible ways to stop future attacks, as well as a conclusion over the material that has been discussed.

A complete section on why a person decides to become a hacker is beyond the scope of this paper; however the reasons why people become hackers are numerous. Some of them do it for fun, others for profit, and some just to see if they can do it. One aspect that is still being wrestled with is that of how much punishment does a hacker deserve if they are caught and convicted? Do the old styles of ‘let the punishment fit the crime’ apply?

If a hacker causes millions of dollars worth of damage to a system, or compromises hundreds of thousands of consumers personal data files, what should be done? Would a prison term of hundreds of years be appropriate? Or should we say one year in jail for every file that is involved? In some cases, that would mean a sentence of say 200,000 years, which of course is unrealistic.

The answers to these questions are still not found, and so society needs to decide what will be done with hackers who are caught. As in other crimes, just because it is illegal does not mean that someone will not do it. As one can see, this area is complicated and so a complete discussion must be made at another time.

The more popular hacking techniques to hack into a network include port scanning, in which a hacker “pings” an ip address to see if there is a live system residing there. If there is a response, then they can continue with other methods to hack into the computer. Alternatively, by using a text file or some other means, large amounts of ip addresses can be used to ping many systems a day.

This allows the hacker to scan thousands of ports a day, and so it more desirable than one at a time. Another popular method is that of reverse engineering, in which an attempt is made to take compiled code and return it to the un-compiled state so that the hacker can manipulate it.

Some other methods belong to a group known as “wet-ware”, and this differs in that the programming is that of the brain, rather than software. One part of this is “social engineering”, where the hacker subverts trust relationships or relies on predictable behavior; another is bribery, such as giving a night guard some money so that the hacker can gain entrance to an office that has something of value in it. Impersonation is part of wet-ware, it seems that it is surprisingly easy to call someone and get a password by stating the hacker is from the company IT department.

There is also “shoulder surfing”, standing behind someone while they type at the keyboard and memorizing the keystrokes, and a rather messy one is what is known as “dumpster diving”, since many companies carelessly toss valuable information in the trash every night without shredding it. And, of course if all else fails there is the art of deception, outright bald faced lying to someone to gain access to the network. The next section will go into greater detail on hacking techniques

Techniques

Some of the techniques that hackers employ to gain entry to a network were stated in the previous section, more will be listed here with greater detail. These techniques can include physical as well as software. To start with, hackers will attempt to gain entry by posing as a guest or with a tour group, then heading off at an opportune time to see what areas of the building can be accessed or broken into without detection. If found, they can simply claim that they are “lost”, or thought that this was an area that anyone could use.

Another method is that of “social engineering”, where the hacker will try to lull the employee into a false sense of security that the person on the other end of the telephone has a legitimate reason to ask for information such as passwords or user id’s, and so give them to the hacker. Hackers will also go through the trash of companies, looking to find any bits and pieces of documents that will give them the information that they need to enter the network and commit their nefarious crimes.

Programs have been developed that allow one to use a computer and by way of “brute force”, attempt to “crack” a password on a system. This has allowed the hackers the ability to attack more that one computer at a time, and to carry on the attacks continuously, thus giving them more opportunity to gain entry to a computer system.

By launching large numbers of attacks against a single computer or group of computers, hackers are able to create DOS, or denial of service attacks. This ties the attacked computer resources up for varying amounts of time, but the end result is that the legitimate traffic is not able to be processed, thus the attack is successful in crippling the business for the amount of time it lasts. Hackers can also use a Trojan horse to gain entry to a computer and then by logging the keystrokes, gain the information to allow access to higher level security.

Another technique that has gained notice lately is that of “zombie” computers, which lay dormant for a specified period of time and then awake, launching a coordinated attack on a computer or group of computers. The problem with these types is that one never knows when the computer will attack, or how many are infected that will comprise the attacking force. Usually these are found in the homes of consumers, and small businesses, who do not take the proper steps to ensure that they are not infected by the hackers.

Defenses

Hardware

Physical defenses against the hacker include greater scrutiny of the visitors and employees of a company, the access to sensitive areas, computers, and other network components. Policy must be created as to what information will be given out over the telephone, strict adherence to allowing employees to bring guests at parties and other functions, and what will be done with the daily trash that a company generates, no matter what the trash is.

By implementing id badges, coded to allow access only in specific areas, the company can start to eliminate the hacker gaining entrance to certain areas easily. Having specific policies about the telephone and the disposition of the trash will also eliminate the ability of the hacker to have an easy access to these common means of getting information.

Doing a more through and complete background check on current and prospective employees and other persons who are allowed onto the company grounds for repeated or extended periods of time will tighten security where it has been known to be very lax in the past.

Upgrading the network hardware to routers, switches, and other components that have the ability to provide firewalls and other security measures is also very important, and should be high on the list of things to do. When one is able to have a hardware firewall in place in addition to that of software firewalls, then the level of protection is greatly increased for the network.

Routers must have all of their ports configured properly, and any ingoing and outgoing traffic should be logged to determine if there are any attacks taking place or improper usage of the network has happened.

Switches that have imbedded operating systems must also be checked to ensure that all of the proper channels are configured correctly, and monitored on a constant basis. Any computers that do not need to be connected to the Internet should be disconnected, and any gateways should be checked for the proper configuration. Too many times hardware is put in place with the default factory settings, which do no provide any more protection that tissue paper does for the network.

Administrators that do not take the time to configure their networks properly should be either reprimanded or terminated, for they do the company and the employees a great disservice.

Software

There are many software packages that can be installed to provide protection for a network. These range from very simple, such as what comes with the operating system, to the complex, packages designed to protect networks such as those found in the banking industry, or the defense of the country.

There are also many websites that offer various types of software, ranging in price from zero to several hundred dollars, and also provide patches and updates in a regular basis. Installing the software is only part of the solution, one must also configure it and then maintain it with regular patches and updates, or else it will become outmoded and thus may fail when a hacker launches some sort of new attack that the software has no defense against.

A popular package that is offered for free is Ad-Aware, by a company called Lavasoft. It is designed to scan the system and look for known programs that are used by hackers, and then can remove them if desired. Microsoft is bringing out a tool that will scan the computer for malicious code and then remove it if one wants. Most of the major anti-virus makers, such as CA and McAfee have software that will do this, and so there are numerous programs that one can download and install that will check the computer and clean it if infected.

It is important that after downloading and installing the software that the computer user also maintains regular checkups of patches and updates, else the software will become obsolete and then it is useless in protecting the computer from the hackers that are on the loose out there.

Costs to businesses and consumers

Due to the large numbers of DOS, viruses, worms, and unknown zombie computers that are in the world, the exact costs of hacking to businesses and consumers is incalculable, but the author of this paper estimates billions of dollars every year, with the figure rising rapidly all the time.

Add to this the unseen mental and psychological costs that people endure, from the knowledge that someone has broken into a personal computer or a company network, rummaged around at will, then who knows if they have left or are still lurking in some dark corner of a hard drive. It can be equated with the feeling of coming home and finding that the house has been burgled, or the automobile has been stolen.

The reputation of the business is something that the hacker can also destroy, because if a website is defaced or a database stolen and then opened publicly, the costs to the business rise dramatically. Many businesses that suffer this kind of loss close their doors, or have to reduce operations because of the lack of sales. This also has another effect of putting many people out of work, which then continues to spiral through the economy, causing ripples out to all sectors.

These unseen costs are part of the victory for the hacker, because then they can cause so much damage for such an extended period of time that even they did not imagine when they started the attack. This is part of the reason why laws need to be toughened when it comes to hacking, for there is much more at stake than just the monetary losses, and these side losses should be brought to light when punishment is considered for the hacker.

Once a business or consumer has been attacked by a hacker, they are never quite the same again. There is a loss of trust and security that may never be regained, or only after an expense of time and money, along with new equipment purchased and alarms installed but this may never totally repair the damage that the hacker has caused, and many times this is something that will not be known until years later.

Conclusion

In conclusion, hackers, like many other items, are here to stay. The ability of the hacker to operate with almost total anonymity for an unknown period of time before possible detection and apprehension is very large. The hacker has the luxury of being able to use the computer to enhance his or her ability to attack millions of computers simultaneously, and to invade many computers at once or have them act as his willing aides.

Perhaps the motivations that the hackers have should be examined as well, to see if there is any way that society can help to stop a hacker before they get started, or to channel their creativity into more lawful pursuits, that might benefit business as well.

Computer and network administrators must act to secure and protect their equipment, in order to harden the first line of defense against the hacker, and to limit the ability of them to infect machines. By doing this, when the number of computers that can be infected grows smaller and smaller, it will become easier to begin detecting the location of the hackers because the attacks will be against the small number of computers that are vulnerable.

Thus, the war against the hackers will continue as long as there are computers and people who wish to attack them for whatever reasons that they have, but if the rest of the world builds their defenses properly then there will be less for the hackers to break into.

As with most anything that is there, when common sense is invoked, the computers and the networks will be protected until the next invasion of the hackers occurs. But this time we had better be ready because there is no excuse for not protecting one’s computer and network in this day and age.

References

Briney, Andrew L. (2001, May). Retrieved April 17, 2005 from http://infosecuritymag.techtarget.com/articles/may01/columns_note.shtml

Collins, John (2004). Illegal Internet. Retrieved April 17, 2005, from http://www.akamarketing.com/illegal-internet-contents.html

Long, Johnny (2004, December 1). Google Hacking for Penetration Testers. Retrieved April 17, 2005, from http://www.securityfocus.com/excerpts/syngress

Blackcode <http://www.blackcode.com/>

Infosyssec <http://www.infosyssec.net/infosyssec/index.html>

ISS <http://www.iss.net/>

Phrack <http://www.phrack.org/>

Securemac <http://www.securemac.com/>

Windowsecurity <http://www.windowsecurity.com/>