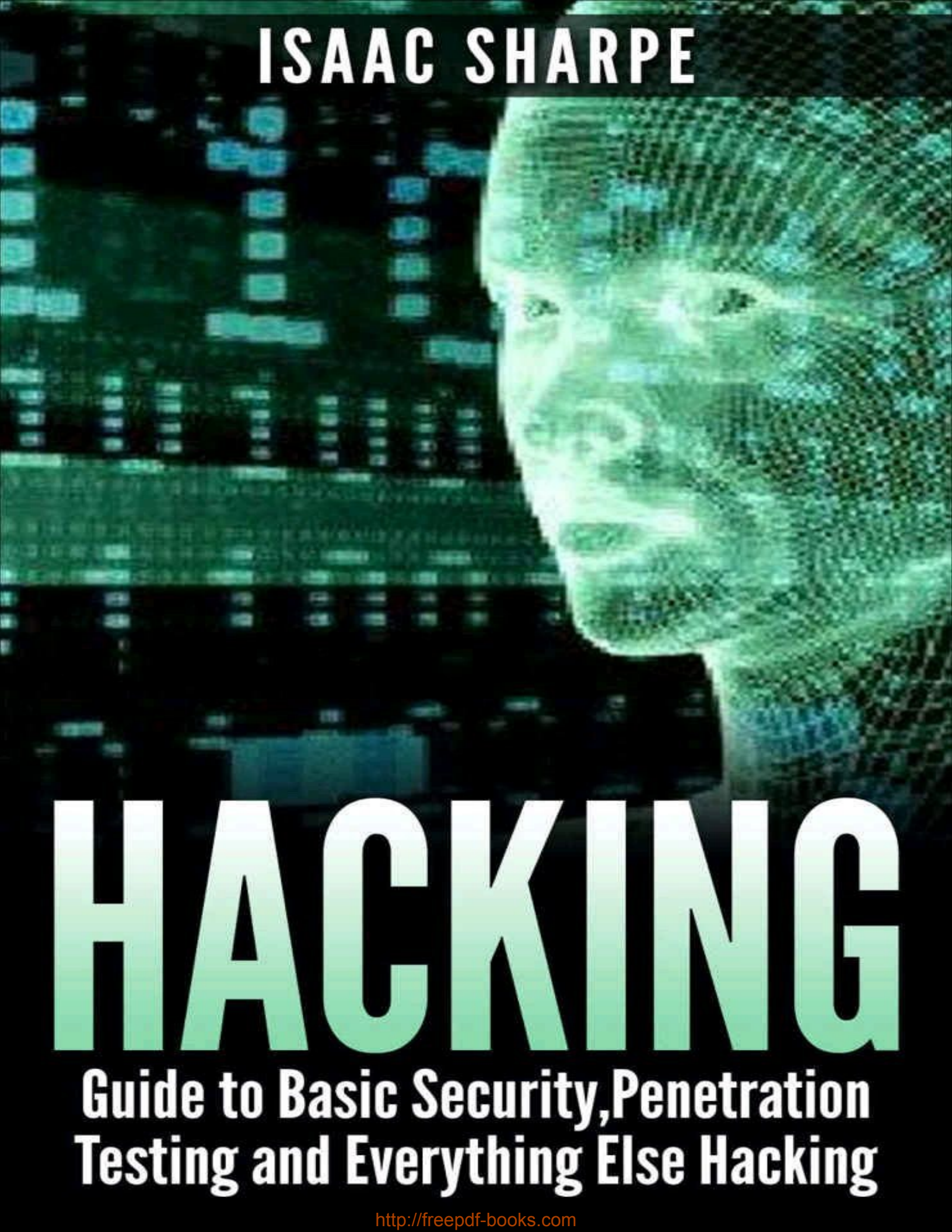

Hacking:

Guide To Basic Security, Penetration Testing And Everything Else Hacking

Table of Contents

Chapter 5: Few General Tips Of Computer Safety

Introduction

Intelligence agencies and security services of many nations consider hacking of their computer systems and networks as the biggest national threat. What was once considered as a harmless prank played by computer nerds has now evolved into a crime on par with any other in terms of its repercussions. It is viewed at with the same severity as terrorism by many countries and is condemned by the world governments at large.

In simple terms hacking is nothing but breaking into someone else's computer or system by circumventing the safety measures and stealing the information contained within, or worse, sabotaging the entire system.

The roots of hacking can be traced back to the 1960's and 70's when the "Yippies" movement was at its peak. Yippies were the members and followers of Youth International Party, which was nothing but a product of the anti-war movements of that time. The group was comprised mainly of youths and was counter-cultural at its very basic level. They engaged in carrying out elaborate street pranks and taught its member the technique of tapping telephone lines.

This gradually developed into what is now called hacking, except that the phone lines and pliers were replaced by state of the art mega core processors and multi function plasma screens.

But over time, the goofy nature of the whole activity has taken a back seat and the more evil face has materialized, hugely due to the fact that, what was once started by peace loving activists to pull pranks on the authorities, is now being increasingly used by terrorist organizations for a multitude of reasons such as spreading their propaganda, obtaining funding, gathering intelligence about troop movements, to even launching missiles.

In this eBook we shall look into various aspects of hacking and provide you with detailed instructions for protecting your home computer or laptop of office systems from this vile menace of the World Wide Web. I want to thank you for downloading this eBook and I hope you find the contents useful and easy to put into practice.

Chapter 1: Hacking - An Overview

In this chapter we will give you a general idea about what hacking really is and then move on to look into the classification of different kinds of hackers.

In its most elemental form, hacking can be defined as the process of ascertaining and the subsequent exploitation of the various shortfalls and weaknesses in a computer system or a network of such computer systems. This exploitation may take the form of accessing and stealing of information, altering the configuration, changing the structural picture of the computer system and so on.

The whole spectrum of hacking is not something that is found only in the developed countries. In fact, with the kind of advancement that has been witnessed in the field of information technology during the last two decades, it should not come as a surprise that many of the most tenacious communities of hackers are based in the developing countries of South and South-East Asia.

There is so much of smoke screen and ambiguity in the world of hackers that it is extremely difficult to pinpoint a particular activity as hacking or not. This ambiguity is so much that the very term “hacker” is subject to a lot of controversies. In some contexts, the term is used to refer to any person who has a command over computer systems and networks. In other contexts it is used to refer to a computer security specialist who strives to find and plug the loopholes in the system. They are sometimes called crackers. But more on the classification of hackers shall be dealt with in detail in the later part of this chapter.

A plethora of reasons may be behind hacking. Some do it with the very predictable reason of making money. They may steal and retrieve information from a computer system, or plant incorrect information in return for monetary gains. Some others do it simply for the challenge of the whole activity. The rush of doing something that is prohibited, accessing what is forbidden. And yet others are computer world equivalents of social miscreants who may access a network or system and scramble, thereby rendering it utterly useless for the users of such network.

There are people who hack a system as a sign of protest against the authority. Instead of being vocal against the policies which they consider unreasonable, they burrow into the technological network systems employed by the authority and wreak havoc.

Classification – Various kinds

Based on their modus operandi and the intention behind their actions, hackers can be classified into the following types;

White hat hackers

The term white hat is used to refer to someone who hacks into a computer system or network for intentions that are not malafide. They may do as a part of a series of tests performed to check the efficacy of their security systems or as a part of research and development that is carried out by companies that manufacture computer security software.

Also known as ethical hackers, they carry out vulnerability assessments and penetration tests (which shall be explained in detail in subsequent chapters).

Black hat hackers

A black hat hacker, as the name suggests is the polar opposite of a white hat hacker in terms of both intention as well as methodology. They violate a network for malafide intentions for monetary and personal gains. They are the illegal communities who fit the commonly perceived stereotype of computer criminals.

They gain access into a system and steal or destroy the information or modify the same. They may tweak the program in such a way that it is rendered useless for the intended users. When they notice a weak spot or vulnerable area in the system, they take control of the system by way of such weak spot. They keep the proprietors, authorities and the general public in the blind regarding such vulnerability. They do not make any attempts to fix the lacunae unless their reign faces a threat from a third party.

Grey hat hackers

A grey hat hacker has a curious mix of both black hat and white hat characteristics. He trawls the internet and sniffs out network faults and hacks into the system. He does so with the sole intention of demonstrating to the system administrators that their network has a defect in terms of security. Once hacked into the system, they may offer to diagnose and rectify the defect for a suitable consideration.

Blue hat hackers

These are freelancers who offer their expertise for hire to computer security firms. Before a new system is introduced in the market, the services of blue hats are called for, to check the system for any potential weaknesses.

Elite hackers

These are the crème de la crème of the hacking community. This is a marker of social status used to demote the most proficient hackers. They are the first ones to break into a seemingly impenetrable system and write programs to do so. The elite status is usually conferred on them by the hacking community to which they belong.

Skiddie

The term "skiddie" is short for "Script Kiddie". These are the amateur level hackers who manage to break into and access systems by making use of programs written by other expert level hackers. They have little or no grasp on the intricacies of the program which they use.

Newbie

Newbies, as the name suggests, are hackers who are beginners in the world of hacking, with no prior experience or knowledge behind them. They hang around at the fringe of the community with the object of learning the ropes of the trade from their peers.

Hacktivism

This is another version of hacking, in which the individual or the community makes use of their skills to promulgate any religious or social message through the systems they hack into. Hacktivism can broadly be classified into two kinds- Cyber terrorism and Right to information. Cyber terrorism refers to activities that involve breaking into a system with the sole intention of damaging or destroying it. Such hackers sabotage the operations of the system and render it useless.

The hackers who belong to the "Right to information" category operate with the intention of gathering confidential information from private and public sources and disseminate the same on the public domain.

Intelligence agencies

Intelligence agencies and anti-cyber terrorism departments of various countries also engage in hacking in order to protect the state interests and to safeguard their national systems against any foreign threats. Though this cannot be considered as hacking in the true sense of the term, such agencies engage the services of blue hat hackers as a sort of defense strategy.

Organized crime

This can be construed as a kind of conglomerate of black hat hackers working for a common goal or under a leadership. They access the systems of government authorities and private organizations to aid the criminal objectives of the gang to which they belong to.

Chapter 2: Penetration Testing

When the world became aware of the magnitude of the threat posed by hacking, various security measures were invented by computer experts and security specialists. One of the most prominent among such measures is the process called penetration testing. In this chapter we shall look into this concept in detail and the various reasons for undertaking this testing.

What is it?

Penetration testing is the process whereby a deliberate attack is mounted on a computer system, in which its weak spots are noted, and the data stored in it is accessed. The intention is to demonstrate and thereby ascertain the efficiency of the security safeguards installed in the system.

The primary objective of penetration testing is to find out the vulnerable areas in a system and fix them before any external threat compromises them. The key areas to be tested in any penetration testing are the software, hardware, computer network and the process.

The testing can be done both in an automated way as well as manually. The automated method makes use of software and programs that the penetration tester has composed, which are then run through the system and network. However it is not possible to find out all vulnerabilities solely through penetration testing.

This is when the manual testing comes in. For instance the vulnerabilities in a system due to human errors, lack of employee security standards, design flaws or faulty employee privileges can be diagnosed better by way of manual penetration testing.

Besides the automated and manual methods of penetration testing, there is a third variety which is basically a combination of both automated and manual systems. This form of testing is more

comprehensive in terms of area of coverage and hence it is used commonly to identify all possibilities of security breaches.

This is in many ways similar to the concept called "business process re-engineering" and is used as a management planning and decision making tool. The process of penetration testing involves execution of the following steps:-

- Identification of the network and in particular, the system on which the testing is to be carried out.

- Fixing of targets and goal. Here, a clear demarcation is made between breaking into a system to prove its faults as against breaking into and retrieving information contained in the system.

- Gathering information pertaining to the structure of the system or network.

- Reviewing the information that has been collected and based on such data, charting out a plan of action to be adopted. Multiple courses of action may be outlined and the most suitable one is selected.

- Implementation of the most appropriate course of action.

There are two broad kinds of penetration tests. It may be in the form of a "White Box" test or a "Black Box" test. In case of a white box test, the company or organization enlists the services of an agency or individual to carry out the penetration tests, and provides them with all information with respect to the structure of the system and its background.

The party carrying out the tests need not do any groundwork for collection of information. On the other hand, where the penetration test is of the black box variety, very little or in most cases, no background information is provided to the agency except the name of the organization for which the test is being done.

Once the penetration test is successfully completed, the system administrator or owner is briefed about the weaknesses in the system that has come to fore as a result of the test. The test report should list out in detail the weak spots as observed in the test, the severity of such flaws, the short term and long term impact on the system and its contents and finally the methods to fix such shortcomings.

Various strategies employed

The following are the most commonly adopted strategies of penetration testing:

Targeted test

In this form of penetration testing, the procedure is performed by the organization's in-house security department. They may call for the help of external agencies but the decision making and implementation powers rest with the organization itself. One of the most characteristic features of this form of penetration testing is that employees in the organization are kept in the loop and are aware of the tests.

External approach

This form of penetration testing is carried out exclusively on those devices and servers of the

organization that are visible to outsiders, for instance the e-mail servers, domain name servers etc. The intention of performing a penetration test with the external approach is to ascertain whether any outsider can attack the abovementioned devices and in case of such an attack, the repercussions of the same.

Internal approach

This is the exact opposite of a test as per the external approach. Here the intention is to mimic the situation where the system is under attack from inside by someone who has high level access and privileges. The test can establish the extent of damages that can be causes in the event of such an attack.

Black box test

The basic principle behind a black box test has been mentioned in the earlier part of this chapter. The agency or individual carrying out the penetration test is given very little information about the organization or its system safeguards. This form of testing is very time and resource intensive because the agency has to start from scratch and undertake the complete process of gathering information, planning and execution.

Advanced black box test

As is obvious from the name, this is a higher level of black box test. The major differentiating factor is the quantum of people inside the organization who are aware of the penetration test being carried out. In case of a normal black box test, although only a limited amount of information is provided to the testing agency, almost all the managerial level employees of the organization are aware of the tests being carried out. However in case of an advanced black box test, only a few people in the top management of the company will be aware of the tests being conducted.

Chapter 3: Basic Security Guidelines

Now that you have had a look at what exactly hacking is, we shall go ahead and line out some basic guidelines for you to protect your system and the information contained in it from an external threat. This is compilation of the most practical methods devised by computer security specialists that you can follow to avoid your machine from being attacked and ravaged by the omnipresent threat of hacking.

Update your Operating System

The simple truth is that all the different versions of even the best of the operating systems have succumbed to hacking. Having said that, the simplest way to protect your system would be to keep updating your operating system on a weekly or monthly basis or as and when a new and improved version comes along. This drastically brings down the risk of your system playing host to viruses.

Update your software

Please understand that there is a reason why software developers bring out newer versions of their product every once in a while. Besides providing better efficiency and convenience, they also have better in-built security features. Therefore it is highly imperative for you to make sure that your applications, browsers and programs all stay updated.

Anti-Virus

The importance of having good and effective anti-virus software in your system can never be stressed enough. This is more so when your system is always connected to the internet. There are many anti-virus software available in the market with varying degrees of efficiency. They may be both free as well as paid and we would always recommend you to go for the latter. And if you think that just installing one in your system is good enough, then you are mistaken. The anti-virus software, like any other software requires frequent updating for its definitions to remain effective.

Anti-Spyware

Anti -spyware software are as important as anti-virus for the very same reasons. And here too, you have a lot of options to choose from. So make sure that you pick one that is rated high enough.

Go for Macintosh

Now this is a tricky one. You may have read it in countless comparisons and on numerous blogs that Macintosh operating systems are the least secure ones out there, especially when pitted against the vastly more popular Windows operating systems. But here, the very popularity of Windows works against it. Don't get it? Well here is the thing, Very few hackers target Macintosh systems because of the fact that a large majority of people do not use it. Take advantage of this and switch to Macintosh operating systems. And do not forget the fact that there is no operating system in the world which is completely hack-proof.

Avoid shady sites

Would you walk into a dark alley on the secluded part of the street at night, wearing expensive jewelry? You wouldn't. Similarly, be wary of dubious websites that parade as reputed ones. Also avoid visiting porn sites, gaming websites and sites promising free music and movie downloads. These websites are frequently tracked by hackers and anything you view or download from these sites may contain malware that may harm your computer and compromise its security.

Firewall

If there are more than one computer systems operating under one network, it is highly advisable to install software that provides a security firewall. Otherwise make sure that the in-built firewall in your Windows is activated. This feature is comes in all versions of Windows starting from the XP to the latest version.

Spam

Never ever open mails that look suspicious. Especially the ones that have attachments. All the mainstream e-mail websites provide a certain amount of protection against such spurious mails by straightaway moving them to the spam box when you receive them. However there may be mails that get past the filters of your e-mail server and that is when you have to exercise caution. Do not attempt to read such mails or download the contents.

Back-up options

Whether it is your home computer or the system at work, always create a back-up of the data that you store in it. You may be having all sorts of important and confidential information such as financial information, personal files and work related documents saved in your system. In that case, make sure that you transfer a copy of everything into an external source such as a standalone hard disk or some other similar device or server. Remember single potent malicious software may completely scramble your data and make it irretrievable. And merely having a back-up option is not good enough if you do not utilize it. Perform a back-up transfer as often as possible, at least once in 4 to 5 days.

Passwords

We have kept the most important aspect to the last. The significance of having a secure password can never be undermined enough. Be it for your documents, for e-mail or even your secure server, a good enough password is the first and quite often the last line of defense against any external threats. There are some golden rules when picking a password. Do not make your bank account number, telephone number or car registration number as your password. Similarly it is a big no when it comes to the names of your family members.

Do not adopt any dates such as birthdays and anniversaries as passwords. In short, when it comes to adopting a password do not take predictable words or numerals. As far as possible, make it a combination of jumbled alphabets and numbers that do not bear any importance to you on a personal or professional front. And a golden rule when it comes to password security is that, never write down your password anywhere, be it your personal diary or at the back of the telephone index. The same goes for saving it in your cell phone.

Chapter 4: Security Guidelines For Offices And Organizations

The threat of hacking is an all pervasive one and the big scale corporations and organizations are equally affected by it. This is especially so in the case of banks and financial institutions where a huge quantum of personal and financial information of the clientele is stored. An attack on such networks can wreak havoc of scale beyond imagination. In this chapter we shall deal with how offices and organizations can take precautionary measures to avoid such instances and neutralize an external threat to their computer network.

Safeguard the points of entry

The first and foremost step is to identify and mark out the points of entry between the internet and organization's network. This is not as easy as it sounds. There will be numerous interfaces where the internal network is exposed to the internet and these need to be monitored because any external attack on the network can only originate from these points. Once these entry points are identified, steps should be taken to ensure that these are well protected.

Diagnostic tests

Various diagnostic tests can be run on the network to ascertain the points of weakness. These tests must be run keeping in consideration the fact that the threat can emanate from both external as well as internal sources. The results of the tests will provide a clear picture as to where the organization is lacking in terms network security. The faulty lines can then be addressed by patching up the lacunae or by adding an extra layer of security or by eliminating such faulty areas completely. The diagnostic tests should be run on regular intervals based on the level of exposure to external sources.

Firewall configuration

Merely having a firewall system installed in your network is not enough. The firewall should be configured in such a way that it is aware of the nature of threat that your network can face. It should be able to let through such communication which is relevant and conducive and block traffic that appears to be having malafide intentions. The configuration must be in tandem with the security requirement of the network and should complement its functionality.

Password policies

As mentioned in the earlier chapter, passwords are an integral part of any network of computer systems. They are one of the main areas of human-machine interface. In case of a large corporation or organization, where are a large number of employees, the risks of the network coming under attack also increasing manifold. In such large scale operations, the network administrator should devise properly outlined policies for generation, alteration and periodical change of passwords. The passwords should mandatorily consist of alphabets, characters and numbers. They should have a minimum length of seven to eight characters and should be in a jumbled fashion.

Strict guidelines should be introduced with respect to sharing of passwords or providing authentication to a person other than to whom the password is issued. In the higher levels of the organization, the nature of data accessible is of a more confidential variety, both qualitatively and quantitatively. In such situations non-disclosure agreements may be put in place binding the higher level managerial staff.

Another key step to be taken is to introduce a system where the passwords are automatically changed every two weeks and fresh ones are generated in its place.

Bio-metric scanners

It is a given fact that no matter how many safety measures you install in place, when it comes to passwords, the threats can never be completely ruled out. Many computer security specialists believe that the best way to deal with this situation is to minimize the use of the passwords and in their place, establish other forms of employee specific security measures such as smart cards to access individual computer systems and finger print scanners and retinal scanners to gain entry into server rooms, data storage rooms etc. These devices are not as prone to breaches as passwords due to the simple fact that a second party cannot impersonate the actual user and enter the system.

Anti-virus and anti-spyware software

The basics of safeguarding against malicious virus attacks and spyware are the same when it comes to a personal laptop or a large network of systems. It is only the scale of operations that differ. In case of large organizations, efficient anti-virus and anti-spyware software having a wide ambit of operations must be installed. The software must be able to tackle threats of a wide variety from simple reconnaissance bugs to all-out hacking codes. In addition to detection of viruses, it must also be capable of quarantining infected files and keeping them isolated from the other files.

Physical security of the premises

When it comes to computer security and protection against hacking, corporations tend to ignore the very simple fact that unless the office premises are properly guarded and secured at all times, all the internal software security measures shall be in vain. If the system is exposed to threats from inside due to lack of proper hardware security, the network can be easily breached.

There should be continuous monitoring of people who have access to computers anywhere in the organization. The inflow and outflow of people into the premises should be recorded and documented. Care should be taken to ensure that, visitors should not be allowed access to computer systems under any circumstances. And last, it should be ensured that the office premises are under round the clock security.

Awareness campaigns

All the precautions taken by the organization and the safety measures and procedures set in place shall not prove to be effective unless the employees, right from the high level ones to the low level maintenance are aware of the gravity of the threat posed by hacking, viruses and other malicious activities. Employees from all levels of security clearances must be aware of the importance of secured and breach free systems and their role in ensuring the same.

Awareness campaigns and drills must be held on a regular basis, where the employees are trained on the basic security measures to be observed and abided by them. They should be acquainted with the anti-virus and anti-spyware software installed by the organization. And more than everything, as a result of the campaigns, they should realize that they all play an important part in making sure that their systems and in turn the network does not come under the threat of being hacked.

Chapter 5: Few General Tips Of Computer Safety

By now you must be having a fair idea about the various facets of hacking and the guidelines for ensuring basic safety to your personal computers and also to large scale, computer networks. Given below are some general tips that you can keep in mind to avoid falling prey to the threat of hacking.

- Never open mails from unknown sources and more importantly, do not ever download the attachments to your system.

- Always engage in safe browsing. Avoid visiting websites that you suspect of having malware.

- When installing a new program, make sure that the old program is completely uninstalled before you begin installing the files pertaining to the new one.

- With respect to whatever programs and software you have in your system, ensure that they are

updated to the latest version possible.

- If you are one of those work-at-home professionals, do not hesitate to enlist the services of a professional firm of computer security experts to keep your system and network well guarded.

- Do not reply to chat room invitations and messages from people whom you don't know or whose authenticity you suspect.

- Always keep a back up of your files and information in a separate external source that is kept secure.

- Many computer security experts believe that while browsing the internet, it is better to use Mozilla Firefox browser than Internet Explorer. Firefox provides better inbuilt security features than other browsers.

- Deactivate features such as Java, Active X etc in your browser, when not in use.

- As mentioned earlier in this book, shift to operating systems like Macintosh or Linux if you are comfortable with their operation. The incidence of hacking in computers using these operating systems is very less compared to the vastly more popular Windows.

- The last and often overlooked tip - turn off your computer when not in use. Do not keep your computer in sleep mode and leave your workstation for more than twenty minutes. It is impossible to hack into a system which is not switched on.

Conclusion

By now you must having a good idea about what hacking is and what will be the consequences if your system is attacked by an external or internal party. But fear not, simply follow the instructions and guidelines provided in this book and you can be rest assured that your system is well protected.

Although we have explained all the concepts here in a very lucid and comprehensible fashion, putting them all into practice may sometimes be a bit tough. Do not think twice before seeking help from professional security specialists if you feel all this is a bit too technical for you.

And please note that the world of computers is an ever changing and advancing one. The more advanced the hackers become, the more effective should be your defensive mechanisms. Always keep your software and system updated.

Thank you again for downloading this eBook and I hope you enjoyed the information shared.

Free Bonus Video: Top Hacker Shoes Us How Its Done

Here is a great video, showing how almost every secure network is vulnerable from a top hacker.

Bonus Video: https://www.youtube.com/watch?v=hqKafI7Amd8

Checkout My Other Books

- **http://www.amazon.com/Apps-Design-Development-Made-Simple-ebook/dp/B00UEMM5X4/ref=sr_1_9?s=digital-text&ie=UTF8&qid=1427558209&sr=1-9&keywords=apps**