RESEARCH ON SECURE VIRUS TROJAN IN CYBERSECURITY PLATFORM

Ahmad Fajar Sidiq, Rusydi umar, Anton Yudhana
Universitas Ahmad Dahlan, Yogyakarta, Indonesia
fajarmaneh082@gmail.com

ABSTRACT

Security is main issue of this generation of computing because many types of attacks are increasing day by day. Establishing a network is not a big issue for network administrators but protecting the entire network is a big issue. There are various methods and tools are available today for destroying the existing network. In this paper we mainly emphasize on the network security also we present some major issues that can affect our network, Trojan horse virus can give rise to the leakage of internal data.

Keywords:Security, Trojan Horse, System, Network.

1. INTRODUCTION

In security management, the invasion of the Trojan horse virus can give rise to the leakage of internal data. Aimed at the problems in security management computer network system, a series of targeted preventive measures are put forward to guarantee the reliability and stability of computer network operation[2].

Information systems have evolved in the last few decades from centralized and highly secure host-based systems to be decentralized. It is often said that in the enterprise model, “the network is the computer”. Ultimately, the systems so large that they were hard to manage effectively[3].

2. WHAT ARE THE THREATS?

Threats by floods and fires are easy to understand: the techniques for protecting against them area well known. But threats perpetrated by malicious users, disgruntled employees, and unknown hackers are a true nightmare. Every day some new technique for attacking systems is developed[3].

Definition of cybersecurity for daily life

If you must give the next definition of network security, network security is the information security on the net-work, and 'information security' have multiple understandings. All the deviation comes from the diff errant aspects of information security, so there have been 'computer security', 'network security', 'information content security'. There have been words associated as 'confidential', 'authenti-city' Integrity, " usability, 'and' non-repudiation, etc. The daily network security is of course the daily infor-mation security on the Internet.[1]

Definition of computer viruses

The history of computer viruses can be traced back to the 1980s. If you want to give it a definition, it can be said that it is a set of computer instructions in the computer

program to destroy the computer function or damage to the data, affecting the use of the computer and able to self-copy a set of computer instructions or program code. This is known as the computer virus. It is destructive, reproducible and infec-tious. In the end, the virus is a computer program. It's every activity is not as revered as mysterious by ordinary people, a little understanding can defend us from most of the virus program.[1]

Computer virus characteristics

Computer viruses do not come from sudden or contingent reasons. Occasionally a sudden power outage or occasional erroneous operation, some garbled characters or random commands will be disordered and chaotically generated in the computer's memory and disk. The virus on the other hand is a very strict, sophisti-cated, very orderly combination of a perfect code, and works with network system environment and adapt to each other to complete a certain instruction function. Computer viruses usually have the following main features:.[1]

1, Parasitic

Computer viruses, like parasites in the human body, are parasitic in the computer program. When someone executes the program, the virus will cause damage to the computer. But before poisoning the program, it is not easily detected. Just as the same reason when people do not get sick, you will never fi nd the body's parasite.[1]

2, Infectious

Infectivity is one of the basic characteristics of computer viruses. Computer viruses are not only very destructive, it has a very strong infectivity. The virus once the outbreak, copied or produce mutation, the speed is rapid and difficult to defend. It feels like a biochemical crisis in novels and films. For example, the most contagious virus in 2007 is AV Terminator, while AV Terminator also creates strong destruction.[1]

3, Latent

Hackers through timing, allow viruses work similarly as the timed bomb. Times of breaking out are pre-set. For example: Black Friday virus.[1]

4, Hidden

Some viruses can be checked by anti-virus software for effective killing, and some are simply cannot be found out. Some viruses sometime active and quiet and fickle. Dealing with this type of virus deal are generally very difficult, as this is a very strong type of hidden virus.[1]

5, Destructive

Sometimes a lot of Internet friends will find some of their own documents and information missing, or the computer will contain a lot of unknown documents, or click on an office file will find the contents of their own and the editor is not the same, or even garbled, or maybe that fi les on the D disk will be in E drive or desktop. It is likely that your computer suffered a devastating virus aggression. After the computer is attacked by such a virus, it will cause the normal program to run, and the fi les in the computer are damaged in varying degrees.[1]

6, Can be triggered

The triggering of a computer virus refers to the occurrence of an infection or attack by a computer virus, such as: opening of the antivirus software activates the outbreak of the 'AV Terminator'. Such similar features are called triggering.[1]

The problems of computer network system can be divided into two aspects: hardware and software. Hardware problems are mainly the aging of computers. Software problems involve several aspects. As for identity authentication risk, the host login and service system login of many libraries adopt fixed passwords. There may be storage records that can be repeatedly used in the database.[2] Once more aspect is a virus, there is three aspects problem in a computer network.

Viruses and Trojan Horses

Viruses are small programs that mimic the activities of real-life viruses. They get into computer systems by being copied from contained disks or downloaded from online services by unsuspecting users. Once a system is contaminated, the virus executes some immediate action, or waits until a specified time or for a specific command executed by the user. Viruses may display harmless messages or destroy the information stored on entire hard disks. A Trojan horse is similar to a virus, but contaminates a system by posing as some other type of program[3].

Viruses are created by authors who are fascinated by how quickly their virus may spread through computer systems. Terrorists and industrial spies create viruses that cause damage in order to seek revenge on an opponent or to viruses that cause damage in order to seek revenge on opponent or tom damage the operations of a competitor. Some viruses are intended targets[3].

3. METHODS OF ATTACK

A. Phone Attacks

A preacher is a person who takes advantage of the telecommunications system to make free lone-distance telephone calls, listen to private conversations, access internal systems, or hack into other systems via the system broken into. Preachers are familiar with telephone switches, networks, and other equipment, and often have manuals from the manufacturers of telecom equipment that describe exactly how to operate and repair that equipment. Experienced preachers can manipulate telephone billing, access codes, and call routing. Preachers can make free long-distance phone calls by gaining "dial-in / dial out" capabilities.[3]

B. Hackers User Accounts and Passwords Attack

An attacker's first priority is to obtain user account names and passwords since this provides easy access to a system. Once inside, the hacker will find away to elevate his privileges. The attacker can obtain a list of user account names from a number of likely sources. Once a user account list is obtained, the hacker will try to determine which account will give the most access if broken into the pc support staff may inadvertently provide this information in the form of list of uses to contact in case of problems. Once a hacker obtains alginate user account name, cracking the password is the next step. Hackers take advantage of common passwords: if they know the user of an account, they may try various combinations of the user's kids and pets' names. Many people use the same password to log on to other systems, such as ATM machines. If a hacker obtains a user account name, but not a password, he can try brute force methods of breaking into the account. A program is set up to try thousands or millions of different passwords until the account opens. This method is ineffectively if logon restrictions that limit the number of attempted.[3]

C. Electronic Eavesdropping and Cable Sniffing

A packet snifter is a device or software that can read transmitted packets. Packet sniffing is a passive eves dropping technique that is hard to detect. The packet-sniffing devices may be installed on internal or external networks. Although packet sniffing an internet transition line is not necessarily informative, sniffing a cable that runs into your facilities who are armed with packet snifters, or from hackers who have penetrated your building and planted listening devices.[3]

D. Viruses and Trojan Horses

Viruses are small programs that mimic the activities of real-life viruses. They get into computer systems by being copied from contained disks or downloaded from online services by unsuspecting users. Once a system is contaminated, the virus executes some immediate action, or waits until a specified time or for a specific command executed by the user. Viruses may display harmless messages or destroy the information stored on entire hard disks. A Trojan horse is similar to a virus, but contaminates a system by posing as some other type of program. [3]

Viruses are created by authors who are fascinated by how quickly their virus may spread through computer systems. Terrorists and industrial spies create viruses that cause damage in order to seek revenge on an opponent or to viruses that cause damage in order to seek revenge on opponent or tom damage the operations of a competitor. Some viruses are intended targets.[3]

E. Natural Threats

Obviously, not all threats to the integrity of your network come from people. Power surges, failing components, and other problems may bring down systems and cost your organization thousands or millions of dollars in down time. In some cases, continuous access to information is critical to the operation of the entire business[3].

4. SECURITY MANAGEMENT OF COMPUTER SYSTEM

A. Network system

For program BUG, technical personnel are required to monitor the possible BUG in a program at any time. In normal operation of the system, any possible BUG should be prevented and corrected in time. If cannot handle the BUG independently, it needs to contact with the developer to solve it as soon as possible. For computer viruses, management personnel should deeply understand virus and the progress of the anti-virus field to improve the virus database. In view of the management factors of the service system, the monitoring of server running state should be strengthened so as to avoid the external malicious intrusion. In the meantime, it is necessary to repair the antivirus software and system bug at regular intervals.[2]

B. LAN

At present, LANs of many libraries realize network management through use Windows NT and some other management systems. The security management of these LANs can be divided into three aspects: (1) Login: A variety of verification methods should be adopted to complete the verification. Network security mana-gers should set corresponding accounts and passwords combined with their job category. Meanwhile, a public account should be set for readers and temporary network users. The specific use of authority should be in accordance with relevant regulations. (2) File servers: File servers occupy an important position in network system. The

management of file servers should be enhanced, and each operation server should be encrypted. The personnel should operate according to safety management regulations. (3) Per-mission and attribute: In view of the different reading ranges, the picture and file directory should be strictly controlled to prevent from leaking confidential documents or tampering important data[2].

C. Service management

In service management, information channels and network exports should be encrypted to ensure that the network information transmission process is encrypted. The security state of transmission channel needs to be checked in advance. Network infor-mation monitoring devices, firewalls and security proxy servers can play a role in this aspect. In order to prevent the illegal external supply and the possible theft of the internal staffs, two different encryption methods should be adopted, such as FIP and e-mail [2].

D. Back recovery

The three aspects System recovery, Application recovery, Data recovery should reasonably set to guarantee the rapid recovery of information system after being attacked [2].

E. Improvement of security manage-ment organization

Security management organization is mainly improved in two aspects are Reader and staff management and Security management personnel management in terms of reader and staff management, relevant personnel can be organized to participate in training classes, so that all staff members can have high moral quality, technological level, safety awareness and political awareness. As for professional assessment, the qualified or unqualified personnel should be rewarded or criticized. For the personnel in charge of hardware facility safety, we need to divide the management and configuration planning of computer equipment, the planning and design of the computer room, and the installation and integration of the server operation system. As for the job responsibilities of software system and network, the normal startup work of network system, system authority, equipment and adjustment work should be divided [2].

Information security is the practice of protecting resources and data on computer systems and networks, including information on storage devices and in transmission. Make it your business to control and monitor the security of your systems and to implement security policies and procedures that people can follow[3].

- Identification and authentication
- Access control
- Accountability and auditing
- Accuracy
- Reliability
- Data exchange

F. Virus Protection

Viruses are a real threat to your network. They are easily contracted form unknown disks or by downloading files form online services, bulletin boards, and the Internet. Any of your network users can contract a virus at any time and spread it to the network. A virus is often hard to detect. It may wait on your system before it executes. Vigilant users or network administrators may detect unusual activity or notice an increase in the size of files (indicating potential infection)[3].

Even after detecting and cleaning up a virus infection, there is still a good chance that the

virus is lurking somewhere in your organization, ready to re-infect systems. It may even have infected the backup sets. You may need to implement a plan to detect and remove the virus throughout your organization. Check all workstations, disks, and other data sources for infections[3].

G. Advantages

These advantages can be lined up simply as[3].

1. Protects personal data of clients on the network.
2. Protects information been shared between computers on the network.
3. Protects the physical computers from harm based from possible attacks on the network from the outside
4. Provides levels of access if the network has many computers attached so some computers may have more access to information than others. (Account system)
5. Private networks can be closed off from the internet making them protected from most outside attacks. Which makes them secure from Virus attacks.
6. protects computer from internet with firewall.

5. CONCLUSIONS

The main problems of computer network system interconnected equipment from Trojan Horse can be solved through a series of measures such as authentication, access control, firewalls, passwords, BUG patches, and intrusion detection. In the mean time, the safety management system should be perfected to improve the stability and reliability computer network system and enhance the quality of service provided.

REFERENCES

[1] Jinliang Shen,Shiming Gong,Wencong Bao, Analysis of Network Security in Daily Life, School of Computer Science and Technology, Shiyan University of Science and Technology, Hubei, China, Information and Computer Security (2018).

[2] Zhang Jing, Research on Security Management and Preventive Measures of Library Computer Network System, Wuhan University of Technology Library, Wuhan 430070, China 694593@qq.com 2018 International Conference on Computer, Civil Engineering and Management Science (ICCEMS 2018)

[3] R.Sakthi Uma1, Prof. R. Angelin Preethi2, Cryptography Techniques, 12 Department of Computer Science, Kamban College Of Arts and Science for Women, Tiruvannamalai, Tamil Nadu, India, International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2018 IJSRCSEIT | Volume 4 | Issue 3| ISSN : 2456-3307

[4] Yi Cao,Hao Tang,Jiangang Zhou, Research on Secure Communication Based on QQ Chat Platform, *Software Research and Development Center, College of Computer Science, Ningde University, Fujian, China, Journal of Secure Communication and System (2017)*