# Summary of popular network attacks today

For attacks by exploiting vulnerabilities, hackers must be aware of security issues on the operating system or software and take advantage of this knowledge to exploit vulnerabilities.

For attacks by exploiting vulnerabilities, hackers must be aware of security issues on the operating system or software and take advantage of this knowledge to exploit vulnerabilities.

## 1. Passive attack (Passive attack)

In a passive attack, hackers control unencrypted traffic and search for unencrypted passwords, sensitive information that can be used in other types of attacks. Passive attacks include traffic analysis, unprotected communications monitoring, decoding weak encrypted traffic, and collecting authentication information such as passwords.

Attacks block network system information so that an attacker can consider the next action. The result of passive attacks is that information or data files will fall into the hands of an attacker without the user's knowledge.

## 2. Scattered attack (Distributed attack)

For scattered attacks, an attacker must introduce code, such as a Trojan horse program or a back-door program, with a "trusted" component or software distributed to many other companies attack users by focusing on modifying the hardware or software malware in the distribution process, etc. Attacks introducing malicious code such as back door on a product for the purpose of unauthorized access to information or unauthorized access to functions on the system.

## 3. Internal attack (Insider attack)

Insider attacks involve insiders, such as an employee who is "dissatisfied" with his company, . attacks on the intranet system can be harmful. or harmless.

Insiders intentionally eavesdrop, steal or undermine information, use fraudulent information or gain unauthorized access to information.


## 4. Phishing attack

In phishing attacks, hackers will create a fake website that looks 'identical' to popular websites. During phishing attacks, hackers will send an email to the user to click on it and navigate to the fake website. When users log into their account information, the hacker will save the username and password again.

## 5. Hijack attacks (Hijack attack)

During hijacking attacks, hackers will gain control and disconnect the conversation between you and another person.

## 6. Password attack (Password attack)

For password attacks, hackers will try to "break" the password stored on the network account database or password protected files.

Password attacks include three main types: dictionary attack, brute-force attack and hybrid attack.

Dictionary attack uses a list of files that contain potential passwords.

## 7. Exploiting the attack vulnerability (Exploit attack)

For attacks by exploiting vulnerabilities, hackers must be aware of security issues on the operating system or software and take advantage of this knowledge to exploit vulnerabilities.

## 8. Buffer overflow (buffer overflow)

A buffer attack occurs when hackers send data to an application more than expected. And the result of the attack attack is that hackers attack the system administrator on the Command Prompt or Shell.

# 9. Denial of service attack

Unlike password attacks (Password attack), denial of service attacks prevent the use of your computer or the network system in the usual way by valid users.

After attacking, accessing your network, hackers can:

- Block traffic.

- Sending irrational data to network applications or services, resulting in notice of termination or unusual behavior on these applications or services.

- Buffer overflow error.

# 10. Man-in-the-Middle Attack attack

As its name suggests, a Man-in-the-Middle Attack attack occurs when a conversation between you and someone is monitored, captured and controlled by an attacker. your in a transparent way.

The Man-in-the-Middle Attack styled attacks are like someone faking identity to read your messages. And the other person believes that it is you, because the attacker can respond positively to exchange and gather more information.

# 11. Cracking attack (Compromised-Key Attack)

The key code here is the secret code or key numbers to 'decode' the confidential information. Although it is difficult to break a key, this is possible for hackers. After the hacker has a key, this key will be called a malicious key.

Hackers use this malicious key to gain access to contact information without having to send or receive attack protocols. With malicious codes, hackers can decrypt or modify data.

# 12. Attack directly

Common direct attacks are used in the early stages to gain internal access. A classic attack method is to detect user names and passwords. This is a simple, easy to implement method and does not require any special conditions to get started. An attacker can use information such as user name, date of birth, address, house number, etc. to guess a password. In the case of a user list and information about the work environment, there is an automated program for detecting this password.

A program can be easily obtained from the Internet to solve the encrypted passwords of the unix system called crack, capable of testing combinations of words in a large dictionary, according to user-defined rules. Self-definition. In some cases, the success of this method can be up to 30%.

The method of using application program errors and the operating system itself has been used since the first attacks and still continues to gain access. In some cases this method allows an attacker to gain the rights of a system administrator (root or administrator).

Two examples are often given to illustrate this method, for example with the sendmail program and the rlogin program of the UNIX operating system.

Sendmail is a complex program, with source code that includes thousands of C language commands. Sendmail is run with the priority of the system administrator, because the program must have permission to write to users' mailboxes. use the machine. And Sendmail directly receives requests for mail on the outside network. These are the factors that make sendmail a source of security vulnerabilities to access the system.

Rlogin allows users from one machine on the remote access network to another machine to use this machine's resources. In the process of receiving the user's name and password, rlogin does not check the length of the input line, so an attacker can include a pre-computed string to override the program code of rlogin, via that gain access.

# 13. eavesdropping

Internet eavesdropping can provide useful information such as user name, password, and online information. The eavesdropping is usually done as soon as the attacker has gained access to the system, through programs that allow the Network Interface Card (NIC) to be in full receive mode. circulated on the network. This information can also be easily obtained on the Internet.

# 14. Forging address

IP address spoofing can be done through the use of source-routing capability. With this attack, the attacker sends IP packets to the internal network with a fake IP address (usually the address of a network or a machine that is considered safe for the internal network), copper Time specifies the path that IP packets must send.

# 15. Disable the functions of the system

This is the type of attack to paralyze the system, not allowing it to perform the function it designed. This type of attack cannot be prevented, because the organized media attacks are also the means to work and access

information on the network.

For example, using the ping command with the highest possible speed, forcing a system to consume the entire computational speed and capabilities of the network to respond to these commands, there are no resources available to perform the tasks. Other benefits.

## 16. System administrator error

This is not an intruder attack, but system administrator errors often create vulnerabilities that allow attackers to access the local network.

## 17. Attack on human element

An attacker can contact a system administrator, pretend to be a user to request a password change, change his or her access to the system, or even change some configuration. of the system to perform other attack methods.

With this type of attack, no device can effectively prevent it, and there is only one way to educate internal network users about security requirements to raise awareness of suspicious phenomena.

In general, human factor is a weakness in any protection system, and only education plus the spirit of cooperation from users can enhance the safety of the protection system. .

Refer to some of the following articles:

1. How to know if your computer is being "attacked" by a hacker?

1. How to set super strong iPhone password to hackers also "give up"

1. 50 Registry tricks to help you become a true Windows 7 / Vista "hacker" (Part 1)

Wish you have moments of fun!