Network Intrusion Progress and its Countermeasure

JUN-JIN Kim

Version 1.3

March 25, 2002

Summary

A classic kind of system attack through Network and its principle/programs are explained in this part and also the appropriate countermeasure is recommended so that the basic measures for hackers' attack can be proposed. On the basis of the programs which hackers use for collecting information of target system and its principal, this paper explains the program and buffer overflow being used for system intrusion. On the last stage, it explains the stage that executes to attack other system based on the occupied system. In addition, it will introduce DoS and malicious agent including various kinds of ways of attack and its principals. The appropriate countermeasures of each attack are explained and also it describes the proper measure when UNIX system is attacked.

All kinds of attack in this paper might be already known but some of them are not usual ways of attack. The existing Intrusion Detection System contains the function of detecting attack and provides the appropriate measure for protection. As security technology develops, the hackers' technology has been developing together and newly developed ways of attack, such as DoS or malicious agent, are showing up. Therefore, thorough analysis of the attack and immediate countermeasure should follow after new attack shows up.

Introduction

Internet, the greatest invention in the 21st centuries, brought a huge change to our contemporary lives.

We can see a person's face using Internet on the opposite side of planet and send / receive mail without any additional payment or distance.

Along with this convenience, the concept of Information Security is emerging as a new issue.

Through the convenience of Internet, a great number of companies and people exchange any kind of economically valuable information with each other so that the critical information are being created all the time and they should depend on their information technology in order to prevent attacker. The concept of 'Information Security' emerged as an essential issue in safety and reliability of information exchange in cyber space, such as activities in e-commerce, e-government and etc.

-

-

Attackers attack the weak point of current security system and when it makes up for the weak points in security system, attacker find another weak point and starts to attack the point again.

Attackers are likely to change into being more cruel and more intelligent information criminals in information-oriented society.

This article is intended to promote the understanding of people about security system and its basis by reviewing intrusion patterns and appropriate countermeasures.

Intrusion Progressive and its Countermeasure

Step 1: After searching their attack tool or DNS server by *'ping'* and finding what kind of system exists in the target network, attackers use the automatic attack tool, Vulnerable Scanner or Port Scanner such as Sscan, Mscan, Nessus, Vanillascan, Nmap, SARA and etc., so search service type and open port that each system provides.

Countermeasure: When operating system is selected, you had better choose the system which doesn't contain weak points as less as possible and which its resource is opened. Also, the newest version of application or OS should be deemed to be chosen because new weak point can be found. When stable version is used, all kinds of vendor patch should be applied and updated.

All ports currently not being used should be closed and information on network would rather be hidden, therefore it doesn't become attacker's target.

Step 2: After finishing collecting information on step 1 system existence and services, attackers use tools featuring with 'IP stack finger printing', such as queso, nmap and etc., so collect OS information of target system.

Countermeasure: Every system implements different 'IP stack' and sends a specific packet so distinguishes the system according to its response. Through each server's setting, systems shows the fake version information and also modifies the kernel, so gets ready for attacker's OS detection attack. [4]

Step 3: attackers uses attack tool applying trace route program and collects Fire walk, hping, nmap and etc. (Network system information, firewall filtering rule information).

Countermeasure: Network topology can be found by *'hop count'*, distance between hosts and they use attack tool applying trace-route program. Also, they can collect system information that is protected by firewall and firewall filtering rule information itself. The attack with this method uses a specific ICMP packet which most of firewalls don't filter or trace-route using packet. Furthermore, they collect network system information through the documents, such as DNS, SNMP, Sendmail, NetBIOS and etc., which network server provides. In case of DNS, the registered host information can be known by means of *'zone transfer'* or a query. Wrongfully preset SNMP notifies network topology and various kinds of network information. At the same time, they collect the critical information through a router. For the appropriate countermeasure, there is a method to block DNS zone transfer.

Remote controlling function can be restricted if the important network equipments, such as a switch or a router, are controlled only in console.

Step 4: On the basis of collected information through the previous steps, attackers attack the weakest part of system. To attack the system, attackers attack the network server with bugs. At the moment, attackers attack the weak point of server's remote buffer overflow, such as s*admind, amd, amountd, statd, POP, Imap* and etc. [5] Otherwise, they can use system server error. In case of acquiring password file, they decode the password and go through crack process and intrude. Usually, the type of step 4 is systematic and used widely.

Countermeasure: For the currently used bug, patch versions are distributed so appropriate patch program can be chosen and installed.

Unnecessary accounts should be deleted when mail or ftp servers are constructed and the access should be restricted according to the authorization. In multi-user environment, appropriate access restriction (quota, permission check) should be done over the local data access.

Buffer overflow can be acquired in remote or local system without any authentication and there are numberless exploit codes to be acquired so that it is exposed to danger. The reasons of buffer overflow can be classified by the operational system performing data writing and execution in the field of stack or hip and compiling error which doesn't examine buffer boundary and programmer's carelessness on appropriate function selection. For the appropriate countermeasure of each reason, authorization of user's stack or writing in hip area should be deleted. Also, supporting buffer boundary examination, thorough buffer examination and appropriate function / tool selection can be answers, too.

In order to make up for weakness caused by the complicated application, security tool notifies the process access to special file, memory page segment, kernel and etc. so this tool can be used. Furthermore, stackguard and some UNIX kernel patch protects stack segments and internal register and provides the protection tool against buffer overflow attack. This can be used, too.

For buffer overflow attack, SETUID route program or server program is executed by route authorization so that its execution should be minimized and its program should be patched when there is any possibility, even though there is no concrete way of buffer overflow attack. In order to preventing buffer overflow attack, many OS companies also provide the patch that disables execution in stack field. By using this, buffer overflow attack can be prevented to some extent. In addition, you can use compiler that examines the possibility of buffer overflow.

Step 5: When attackers succeeded in intruding through the previous 4 steps, they acquire the system information and use it as an intermediate point. In this case, intrusion step starts all over again. Attackers use intermediate points because it's very hard to track attacker's record and sometimes, attackers use at least 2 ~ 5 intermediate points. All system intrusion are for this reason.

Countermeasure: If attackers succeeded in intruding the system through 5 of steps and the attackers deletes his trace of intrusion and records of information collection. Then, they construct backdoor program that allows the unauthorized access in order to make next intrusion much easier. This kind of backdoor opens a specific port by means of demon service type or abnormal service setting and makes re-intrusion much easier. Rootkit makes the work easier and there are various tools for each system type. But the recent backdoor doesn't need to open a specific port or to connect to the network. Tunneling technique opens Raw socket and waits for a specific packet so if the suitable packet comes over, it works properly. Tunneling technique can be implemented in various kinds of protocols, such as ICMP, UDP, IP, TCP and etc. so that it provides a mean of intrusion through evading firewall. Moreover, it provides password and function for evading intrusion detection system.

The attacker monitors traffics in Telnet, POP, FTP on target network by *'packet sniffer'* in the system and collects user name and password [6]. For the countermeasure, password application, such as ssf, sftp, SSL, kerboros, VPN and etc., can be used. Especially, when there is a trial to access to the internal site from the distant point, it is essential to have data security, such as IPSEC, IPv6, VPN and etc.

Attacker can find out the other system's information that has a trusts with the target system so that they can attack another system as an authorized user without additional attack. The most popular case is to use 'r' series of commands and besides it. There are some ways to access to database.

Others: DoS(Denial of Service)

DoS attack can be executed in OS supporting Multi-tasking. Technically speaking, it means that a certain process occupies all the resource or uses up or destroys all of them so that the system cannot provide proper service to other processes. Therefore, all of activities that bring about problem on normal execution can be called '*DoS attack*'. DoS attack looks different from other attacks. DoS attack doesn't acquire an authorization of system route and doesn't modify or steal the data. Even when attack is executed, it is very hard to find out the reason or identity of attack and difficult to fix up the trouble. There are many kind of way of attack and they can occur by operator's mistake.

Countermeasure: DoS attack is divided by the type of disk resource exhaustion and the type of SYN Flooding and creates temporary files and keeps increasing the file size and fills disk with trash data or connects numberless half-open tcp, so fills the listen queue of partner host fully and makes the partner host deny the other tcp connection. Therefore, the process that fills data in disk should be found and deleted or the quota restriction can be released so independent partition can be composed over common directory (*/tmp, /var/tmp*). For SYN Flooding attack, the size of backlog queue should be enlarged and Half-Open Time should be lessened.

Anyone can make a DoS attack nowadays and network availability is considered very importantly. In the first place, system unit should take a basic security measure. Currently in many operating systems, it provides the measure for lessening DoS attack. In terms of network, it is recommended that all the different system provide all the different services.

In a large-sized network, network can be divided by each segment and it can be used in emergency by using more than one uplink. In case of Mission Critical Site, it is recommended that Site Distribute, such as construction of back-up site, can be executed so you can prepare for the emergency. Attacker might need more time to find out backup site of the target system and in this case, administrator can save time for protecting the system.

Since counterfeit IP addresses are used in DoS attack, it is basically recommended that they should be filtered in each site to alleviate DoS attack. There are numberless ways of attack over routing protocol so it can be also a useful security measure, which uncertified routing protocols are restricted.

> In DoS attacks, it is probable that the source address is spoofed. Pleased report them to your CIRT anyway. Many of the DoS attacks are old and well understood, but this does not mean they aren't effective. There is nothing impressive about *echo* or *chargen*, but I was just talking with a major Internet service provider who lost a T-3 circuit for three hours to an oscillation. [8]

Others: Malicious Agent

The number of Windows-based attack tool is increasing nowadays. This type of attack is aiming at average users who don't have any security concept and therefore, hackers don't have to pay attention to security system. Furthermore, windows system upgrade can also inspire hackers to think it is an attractive target.

An agent type of program is the most effective means to utilize window client system. Agent receives attacker's order and executes intrusion and even transmits the result in various kinds of ways. This one lets attacker operate system without logging in the system so minimizes the danger of disclosure. Therefore, backdoor or attack tools currently being used in UNIX system are changing into the agent type.

Each malicious agent contains various kinds of functions, such as diffusion of virus, spy function, remote controlling, system intrusion and etc., and there is a malicious agent that contains all of the functions. The number of attack tools like back orifice is already countless and Internet worm virus using E-mail as a medium can be a good means of spreading all of these attack tools. Even, it can use not also E-mail, but browser and spread the bug through the web so it becomes more dangerous way of attack.

Countermeasure: Malicious programs, such as virus, Internet worm and Trojan horse, are the biggest threat on the Internet. Especially, there are many kind of virus or Internet worm and it spreads out in diverse way so it's very difficult to detect.

The current anti-virus technology detect base on learned virus pattern so, it is very difficult to correspond upon new virus. This is why virus related accident is continuously happening even though anti-virus software is broadly used. This is a succession of battle between the virus-producer and vaccine producer. And vaccine producer is always late. It is not a correct way to prevent a vicious program only with the vaccine products. However, vaccine companies' recognition about security which is –Everything would be jus OK if vaccine product is periodically upgraded- is definitely wrong and in addition make the situation even worse.

There must be a more restricted guideline for better solution. An application must be down loaded only from trusted site, and all source codes must undergo an authentication process. If not, the program could not possible used at any circumstances. This only would be possible with general trainings of users.

After Intrusion occurs:

Prevention is the most important part of the security process. Looking series of process such as preventative activity (security policy settlement and realization, implementation of security system, trainings, etc.), hacking prevention (monitoring, intrusion detection and prevention) and feedback (preventive activity restructuring), the hacking preventative activity executes the role of up-grading enterprise's security. If there is no such activity, it means there is no way to protect from hacking. That is same as to construct a single round system with high cost.

When attackers intruded system using many kinds of OS, basic emergency service should follow immediately or a great deal of financial loss and institute's image will be caused. Therefore, immediate examination and treatment will minimize the damage. [9]

Countermeasure:

▲ Check User, Commands in use, Process record, Network connection and analyze log contents and trace.

▼ In order that attacker cannot modify or delete logs, move log contents onto other system.

◄ To prevent attacker's access, disconnecting the network.

► Check modification record of system execution file, especially all program called from backdoor, */bin/login*, */usr/etc/in.** files, */libc.so.** inetd, and modification record of checksum, netstat, ps, ls, inconfig. Modification record of other file should be compared with the original CD or checksum of tape.

⮜ For better and more secured password management, *'npasswd'* or *'passwd+'* are to be installed and operated. The crack is periodically executed to change those passwords, which are easily verified.

⮞ Check every users' rhosts, forward. It automatically checks whether rhosts possess '+' using the corps and modifies the shell of the news, sundiag.sync password into */bin/false*.

⮝ Check the NFS's settlement. Collect the NFS transaction logs using the NFS Watch program and checking whether the order is appropriately constructed with *'showmount –e'* order. And use *'nosuid'* flag as much as possible.

⮟ Install the latest sendmail and latest patch version program.

← Apply the list to check the system's weakness.

Operate the system with firewall to prevent attackers invasion. Delete source routing and IP-FORWARDING function except DNS and NTP port to block up the NFS (2049/UDP), prtmap(111/UDP).

Send e-mails to every organization where attackers have passed through. Whenever a request for attackers prevention advance is needed, ask for cooperation to CERT-CC.

Conclusion

As already you have given a glimpse at the above, illegal intrusion method and techniques have been developing rapidly these days. It has been changing from finding out the bug at legacy system for static attack into the active attack as Internet worm or Trojan horse.

As the general understanding about the security and the importance of the system increases, the need for system security is getting popularized. And as the means for dealing with attackers develops, attackers are also improving their attacking technology for the financial profits, knowledge acquirement and social terrors. Furthermore, the trend of changes is currently shown in the actual attacks. Therefore, in order to cope with the current situation, all the possible protective means should be devised.

Together with the development of the information technology, information security is on the rise as the enterprise's life and death depends on the information security. However perfect information security is very difficult. So, to cope with the active attack, which is momentarily changing, basically every enterprise must strictly apply their security regulations and construct an efficient security system. However security system, as per now, after invasion accident occurs then the corresponding device is settled. So, system operator or administrator need continuous education and monitor about information security.

References

1. Lee Hyunwoo, "Network Attack Paradigm Shift and Its Countermeasure", Ver 1.0, 2000. 11
URL: http://www.certcc.or.kr/paper/attack-shift-part1v1.0.html

2. http://www.robertgraham.com/pubs/network-intrusion-detection.html#2.1

3. Ofir Arkin, "Trace-Back –A Concept for Tracing and Profiling Malicious Computer Attackers-", Version 1.0, Published: January 31st, 2002
URL: http://www.sys-security.com/html/papers.html

4. Fyodor, "Remote OS detection via TCP/IP Stack Fingerprinting", October 18, 1998
URL: http://phrack.org/show.php?p=54&a=9

5. http://www.securitymap.net/stm/stm_system.html

6. http://www.robertgraham.com/pubs/sniffing-faq.html

7. Lance Spitzner, "Armoring Solaris", August 19, 2001
URL: http://www.enteract.com/~lspitz/armoring.html

8. Stephen Northcutt, “Network Intrusion Detection An Analyst’s Handbook”, New Riders, 1999.

9. Lee Gwangmin, “Information Security System State and Countermeasure”

10. Steve Schupp, “Limitations of Network Intrusion Detection”, December 1, 2000
URL: http://rr.sans.org/intrusion/net_id.php