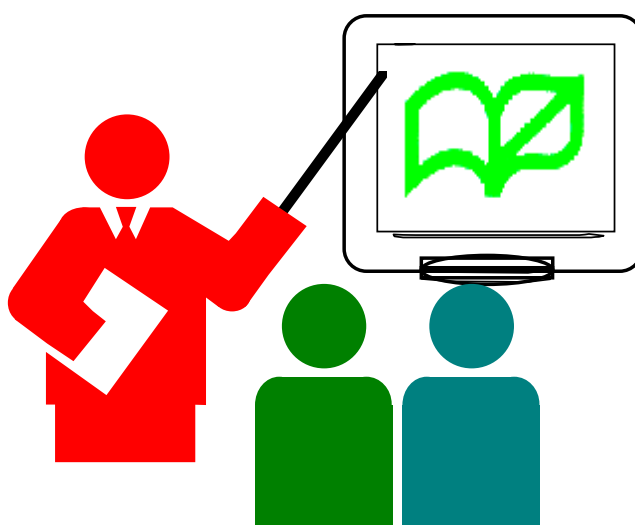


Information Technology in Education Project

Server Hacking

(RM07/2002)



**Quality Education Division
Education and Manpower Bureau
The Government of the HKSAR**

www.emb.gov.hk/ited/

revised in Nov 2005

For enquiry on this document, please direct to the Information Technology in Education Section, Education and Manpower Bureau at (852) 3123 8228 or write to the Principal Inspector, Information Technology in Education Section, Quality Education Division, Shop 28-37, UG/F, Phase I, Waterside Plaza, 38 Wing Shun St., Tsuen Wan, N.T.

The full text of this publication is available at the Information Technology in Education website at <http://www.emb.gov.hk/ited/>

Server Hacking

The exponential growth in the use of information technology in the past years has made a tremendous impact on the society and our daily lives. Nowadays, the Internet is becoming an increasingly indispensable tool in our "information society". Globally, more and more people are now going online to engage in most routine activities such as education, business transactions, personal correspondence, research and information gathering.

We have gained benefits from using IT and Internet, however, you may hear the news like "Websites, corporations and even governments 'hacked' into, websites defaced, or Denial of Services (DoS) attacks, perpetrated by some 'hacker'" from the media everyday. Computer hacking is one of the most widely publicized computer crime around the world today.

About this document:

Before reading this document, reader may have the following questions in mind:

- Who are the hackers?*
- Why do hackers hack?*
- What are their targets?*
- What are the Intrusion Techniques?*
- How do they exploit the vulnerabilities?*
- How to prevent the Intrusion? ... etc.*

This document will give you the answers.

The Targets

Servers are the core items in a network and are always the most interesting place to most people, especially the hackers. It is common for servers to store valuable resources and confidential information. In Hong Kong, we have installed:

- ♦ a SAMS (School Administration & Management System) server in each school to store administrative data and performs most of the administrative tasks;

- ♦ teaching & learning servers to store school's teaching materials or even examination/test papers;
- ♦ school web and mail servers to be accessed by the public.

Security breaches on any server mentioned above can result in the disclosure of critical information or the loss of server's capability that will affect the operation and management of the entire school.

Who are the Hackers?

A hacker is someone who gains access to a computer without permission. Usually, there are two types of hackers:

Outsiders are hackers from outside. They may access the network or computer through the Internet, or actually through physical break-ins. These people may be the former employees, students, vendors or some real unknown outsiders.

Insiders are the users within the network. They have the user rights to access the resources in the network. "Insiders" refer to users who misuse privileges or impersonate higher privileged users. In fact, most of the hacking activities come from the "insiders".

The Hackers Motives

Apart from criminal and political motives, the reasons that lead hackers to hack could range from malice and revenge to simple boredom. Some hackers' intention are just to having fun, trying to cause a little mischief, wishing to be noticed, expecting recognition for his/her knowledge. However, some hackers intend to crash systems, as a result of causing the system to malfunction, stealing data/information for profit, infringing intellectual property, etc.

White hat

"White hats" hack systems for intellectual curiosity. Generally, they do not want to damage the target systems, steal data, or interrupt services. Their activities are illegal if they explore systems which they are unauthorized to enter. During the hacking, "White hats" may unintentionally damage or delete data. Nowadays, many "white hat" hackers work as well-paid security consultants, programmers, and network administrators.

Black hat

"Black hats" break into a computer system usually with bad intent. They will take advantage of the break-in, perhaps destroying files or stealing data for other purpose. The "black hat" may also make known the exploit to other hackers and/or the public. This gives others the opportunity to further exploit the vulnerability of the system/network before the organization is able to secure it.

According to their motives, hackers can be classified into "white hat" and "black hat". No matter which hat a hacker is wearing, when a hacker enters a computer he/she does not have permission to do so, it is illegal.

Steps in hacking

A hacker may go through the following steps in his/her hacking:

1. Gather target information and identify the services offered by the target to the public (e.g. Web, FTP, DNS and e-mail services).
2. Research the services available from the target for known vulnerabilities (e.g. discover exploits, default configuration, vendor announcement).
3. Attempt to exploit the services (to gain access). Utilize exploited services to gain additional privileges from the target (e.g. administrator account, backdoor).

Common techniques for server hacking

Hackers are usually computer experts who are knowledgeable to find out any possible vulnerability of servers and exploit them. The following are some common ways or techniques used by the hackers.

Sniffing

Sniffing refers to capturing information traveling along a network. Hackers may run sniffing software in their workstations to listen in to the network traffic and resemble the message. Information like usernames, passwords, addresses, ports, or contents of emails can be obtained. Sniffing is commonly used in system with unsecured network design, poor managed network and server, or clear-text network protocol.

Port Scanning

The "port" here refers to the TCP/IP ports, which are the doors for information to go into and out of a computer. Port scanning identifies the open door(s) in a computer by systematically scanning all the ports.

Port scanning itself is not a crime. It does no make harm to the scanned computers. There is no way to stop someone from scanning the ports of your computer while you are on the Internet. The really important question rests on the intention of the person who is performing port scanning.

Denial of Service (DoS)

DoS aims to stop the computer system offering service to other users by overloading it. This is usually done by sending numerous network requests, messages or processes to occupy all the computing resources of that computer system. Software bugs in a system are the common door for DoS attack which could hang up the system.

Exploit software bugs and system mis-configuration

Software always has bugs. Software bugs are often exploited in the server, client applications, operating systems, and the network operating systems. At present, all operating systems have their specific vulnerabilities and bugs that can be exploited. The vulnerabilities of a particular operating system can be easily found on the mailing lists. Software companies usually release service packs or patches trying to fix these security holes. However, as long as these updates are not installed on time in the user's machine, the said software is vulnerable to the attacks.

System mis-configurations are common mistakes made by system administrators. Hackers have their standard ways to discover these mis-configurations. Though, most of the situations are due to carelessness of the system administrators, sometimes the problems evolved from the system administrators being not alert of the possible system vulnerability.

Password cracking

Getting a valid user account and password is the easiest and most efficient way to gain access to a system.

Guessing

Guessing password is usually the first attempt carried out by the hacker to crack a system. People may use easy-to-remember passwords such as their phone number, birth date, and the names of their children/spouse/pet as their passwords. Also some users may even use the word "password" for the password or simply null password.

Dictionary attacks

With this attack, the hacker will use a program that will try to guess the password using every possible word in a dictionary. Hackers will make use of the English dictionary or even foreign language dictionaries for the purpose. Some of them will also use additional dictionary-like

Common mis-configuration

Default configurations

Most systems are shipped to customers with default, easy-to-use configurations. Unfortunately, "easy-to-use" implies "easy-to-break-in". Hence, nearly any WinNT machine that shipped to you can be hacked easily by the hacker.

Empty administrator password

A surprising number of machines have been configured with an empty administrator password. This is because most of the administrators consider such arrangement is more convenient to get the machine up and running quickly with minimal fuss. Unfortunately, they never get around to fixing the password later, allowing hackers easy access the system. One of the first things a hacker will do on a network is to scan for empty passwords.

Running unnecessary service

Virtually all programs can be configured to run in a non-secure mode. The administrators will then inadvertently open a hole on their machines. In order to avoid accidental hole, most administration guides have suggested that administrators should turn off everything that doesn't absolutely need to run on a machine.

databases, such as names and lists of common passwords in their guessing.

Brute force attacks

Brute force attack is a trial and error method in password cracking. Programs are used to try all possible combinations of characters. Comparing with the dictionary attack, this is an exhaustive method not adopting any intellectual strategies. It is both time and resources consuming. If we use a longer the password, the hacker using brute force attack will need more time to break the code.

Observation

Secure password is usually long in length. It is difficult to guess as well as difficult to remember. Some users may write his/her password down in his/her working area (e.g. a piece of paper under the keyboard). It is easy for the hackers to find the passwords. Also, some hackers may even stand behind a user's back watching him/her to key in the password.

Social Engineering

Social engineering is a common technique adopted by hackers, especially outsider hackers. For example, the hacker may simply call the school and say:

"Hello, Miss/Mr Chan, this is David from BBB Company. Your principal, Mr Leung, is having an important meeting with my boss. He now needs a file that is available in the school server. However, Mr. LEUNG does not have a computer with him in the room. Hence, he wants me to login the school server to get the file and print for him. Would you please tell me his user name and password for double checking?"

Many users will simply give the hacker the answer.

Trojan horse

"Trojan horses" are executable programs which are often spread via e-mail as attachments. However, it was also found that a number of freeware, trial-ware or even homepages had "Trojan horses" embedded.

Secret codes are contained inside the programs in such a way that they can later get control over victims' computers with chosen form of damages. Unlike viruses, "Trojan horses" do not replicate themselves. "Trojan horse" actually acts as a client agent that sits inside the victims' computers to which a remote computer can get control and cause damages to the host.

Common Hacking Scenarios

There are three primary ways a hacker can get into a system:

1. Physical Intrusion;
2. System Intrusion;
3. Remote Intrusion;

Physical Intrusion involves a physical access to a machine, i.e. hacker may use the keyboard directly accessing the system, or take apart the system/hard disk to access the information. **System Intrusion** assumes that the attacker has a low-privileged user account on the system

and is trying to gain additional administrative privileges. **Remote Intrusion** involves a hacker who attempts to penetrate and access a system remotely through the network. The attacker may begin with no special privilege.

The following are some hacking examples:

Example 1

Students may use various password-cracking skills to uncover teacher's password in order to access a teacher's account. The skill can be as simple as to remember the teacher's keystroke pattern. Of course, there are many automated software that makes hacker's life easier. After logon to the server, students may retrieve the coming examination papers stored in the server.

Or students may deliver a "Trojan horse" software into a teacher's workstation from a floppy disk while it is left unattended. The software will remember every keystroke made by the teachers and will be logged to a file. Using this method, students may even uncover a teacher's bank account and password in case the teacher performed an Internet bank transaction afterward.

Example 2

Hackers may run software to test for vulnerability of a server's services. It is commonly known as "port scanning" because most servers' services are implemented through network ports.

There are plenty of software packages available in the Internet that help novices to do the job. They are easy to use and some of them can even interpret the testing results and suggest further action. Thus it is easy to find some teenagers to perform hacking at home.

Sniffing unsecured traffic**Shared Medium**

On a traditional Ethernet, all you have to do is to put a sniffer on the wire to see all the traffic on the segment. This is getting more difficult now as most corporations are transitioning to a switched Ethernet.

Server Sniffing

On switched networks, if you can install a sniffing program on a server (especially the one that act as a router), you can probably use that information to break into the client machines and the trusted machines as well. For example, you might not know a user's password. However, by sniffing a Telnet session during the user logs in the system, you will get the user's password.

Clear-text sniffing

A number of protocols (Telnet, FTP, HTTP Basic) are using clear-text passwords, i.e. the passwords are not encrypted as they go over the wire between the client and the server. An attacker with a protocol analyzer can watch the wire to look for such passwords. No further effort is needed.

Encrypted sniffing

Most protocols use some sort of encryption on the passwords. In these cases, the attacker will need to carry out a Dictionary or Brute Force attack to decrypt the code of the password. Please note that the user still doesn't know about the presence of the hacker, as the hacker has been completely passive and has not transmitted anything onto the wire. Password cracking does not require anything to be sent onto the wire as hacker is using his/her own machine to authenticate the user's password.

Example 3

After downloading some packet sniffer tools from the Internet, a student can run the software in one of the workstations in school LAN. Since the school LAN is built on a shared medium (e.g. Ethernet hubs) and most of the current Intranet applications are using clear-text password (e.g. HTTP server), the student can then easily get the passwords of his classmates, and use them, instead of his/her own one to log on the School Intranet.

To improve the security, the school can consider using Ethernet Switches instead of Ethernet Hubs and re-configure the

Intranet Server by enabling Secure Sockets Layer (SSL) protocol.

How to prevent server hacking?

For details on IT security, please refer to the document "IT Security in Schools", which is available at [http://202.64.213.147/ited/Support_Servic/TSS_Ref/IT_Security_in_Schools_\[Nov_05\].pdf](http://202.64.213.147/ited/Support_Servic/TSS_Ref/IT_Security_in_Schools_[Nov_05].pdf). Here are some basic precautions to be noted.

Physical security

This is the fundamental step in protecting the servers. Servers should be kept in a locked server room and entry to the room is restricted to authorized person only.

Server logging

The activity of server(s) and Internet gateway, if any, should be logged. It is important to determine what kind of events for logging. In general, for security incidence handling, the log should provide adequate information including the log-in attempts, changes of user access rights and the activities carried out by the privileged users.

Apply updated patches frequently

Software patches, especially security fixes, in server operating system and applications from vendors should be updated and applied frequently.

Disable unnecessary services in server

Unnecessary services not only add burden to server, but also provide loopholes for the hacker to break in. All services that is not essential for server operation should be disabled.

Password Management

The disclosure of passwords including the administrator and all privileged users should be avoided. Practices such as using hard-to-guess passwords or setting password expiry date will improve the security.

Backup

Server backup is an essential task in server administration. The backup can help restore the server operation after compromise.

Use of Internet Access Gateway

When the school LAN is connected to the Internet, the use of gateway can control the traffic flow between the school LAN and the Internet. Logging of the gateway should be activated for tracing the traffic flow between the school LAN and the Internet.

User education

We should through education let our students understand the obligation and responsibility in using the computer systems. As most of the hacking activities are originated from the insiders, prevention of hacking from insiders would put the server in a safer position.

What do we need to do when the system is hacked?

For details of incidence handling, please refer to the document "IT Security in Schools", which is available at [http://202.64.213.147/ited/Support_Service/TSS_Ref/IT_Security_in_Schools_\[Nov_05\].pdf](http://202.64.213.147/ited/Support_Service/TSS_Ref/IT_Security_in_Schools_[Nov_05].pdf). The following are the highlights of the procedures in handling the compromised system:

1. Identify the compromised server(s) – check log and all computers.

Some signs of hacked system

Corruption/Loss of Data

Unexplained User Accounts

Alerts from Security Monitoring Tools

Denial of service (Hackers may disable some of the services for changing administrator passwords)

2. Remove the hacked system from the network (Containment) – while a successfully compromised system remains on the network, it is vulnerable to further attacks.
3. Contact the appropriate parties for assistance. (e.g. CERT, Police).
4. Copy your users' data files to another media.
5. Reinstall the system or restore system from backup.
6. Restore services, back to normal.

Summary

Server can be hacked by both insider and outsider. An effective way to prevent outsider attack is to establish a firewall system that separates hackers from the server. To prevent insider attack, a well-managed server as well as good user education is needed.