Network Attacks

電機二 徐子旻
B00901168

***"Know thy self, know thy enemy. A thousand battles, a thousand victories."* - Sun Tzu.**

Introduction

Internet has been growing explosively and attacks across the network hit the headlines so frequently that we cannot omit the importance of Internet security. In this essay, we will go through the possible attacks a network administrator would encounter.

Definition

"Hacker": someone skilled and finds weakness in computer.

"Cracker": someone who attempts to access computer systems without authorization.

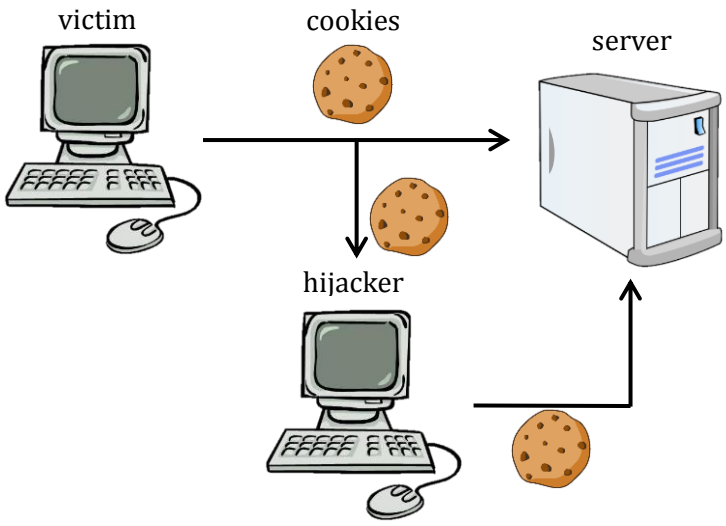
"Script kiddie": someone who use scripts or programs developed by others to attack computer systems without knowing its principle.

In general, network attacks can be categorized into three stages, and they will be introduced in the following paragraph.

Preparation

This kind of attacks usually refers to the scouting and setting up before real infiltration. It mainly consists of sniffing, snooping, and spoofing. "Sniffing" indicates the interception of packets, which can be achieved by accessing unencrypted networks. A famous Firefox extension "Firesheep" stormed the world in 2010 since users could log in with victims' Facebook account within a few clicks. It basically sniffs the cookies sent over the air, intercepts them, and if they are unencrypted, the hijackers can log in the victims' account using their cookies.

The logo of Firesheep



By “snooping” we mean running a background program keeping track of the memory of the computer, or the keys pressed by the user in order to obtain the password. “Spoofing” is the act of setting up a fake website (phishing) or disguising the network addresses.

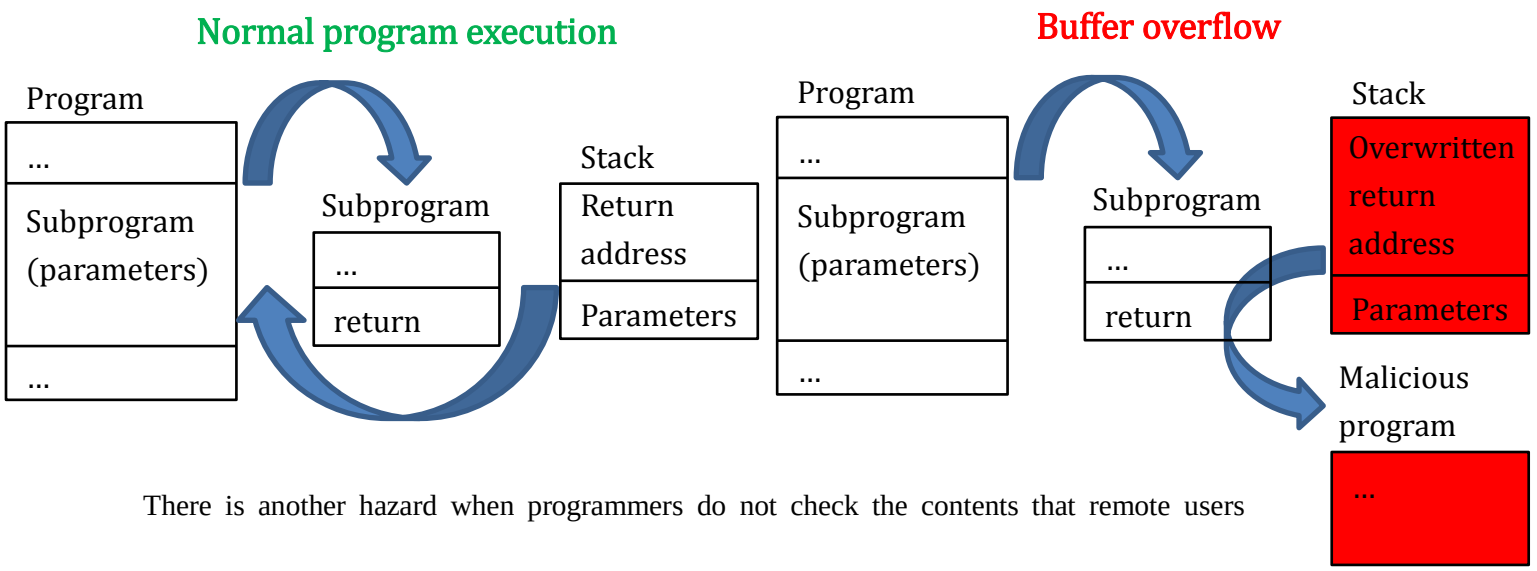
Attack

Attacking is the main spirit of hacking and requires the most knowledge to complete. There are several ways of attacking a remote host, including password cracking, exploiting, and some other ways. Password cracking can be achieved either by brute-force cracking or utilizing a dictionary file. This kind of attack mainly aims to Unix-like systems which validate users by password. Instead of directly connecting to the host and trying the password, it is more preferable to fetch encrypted password files in the system to guess. It is because of the host may track the client when they try and only limited attempts are offered. A renowned operating system, Backtrack, packs all the tools required for infiltration together including password-cracking utilities. Below is a simple illustration of how it cracks Windows admin password.


```
1 bt ~ # cd /mnt/hda1/WINDOWS/system32
2 bt system32 # cp -R config /tmp
3 bt system32 # cd /tmp/config/
4 bt config # bkhive system syskey
5 bt config # samdump2 sam syskey > hash.txt
6 bt config # john hash.txt -w:dic.txt
7 bt config # john hash.txt -i:all
```

Line 1 shows the directory of system boot key and in line 2 and 3 they are copied to a temporary workspace to process. It is the principle mentioned above that one fetches the critical files out. The command `bkhive` simply extracts system key out of the file `system`, and in the next line, the command `samdump2` takes the `sam` file and the system key to generate the password hash. Finally `john` compares the hash with existed password hashes in `dic.txt`. If there is no match, one can consult to brute force cracking in line 7.

Exploit of the bugs is another powerful weapon that hackers hold. An example is the “buffer overflow” which results from the absence of input length check. The input overflows to the memory that does not belong to the buffer and hence make the system execute the injected programs. Buffer overflow is illustrated below.



There is another hazard when programmers do not check the contents that remote users return. "SQL injection" is often called the hackers fill-in-the-blank and primarily attacks the websites with forms to "post" to the server and a server-side SQL database. A typical SQL query is:

```
Select id, password from users;
```

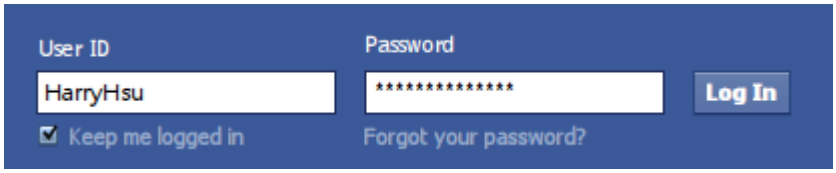
This query will have all rows of `id` and `password` in `users` to be returned. In order to specify a single row, we use:

```
Select id, password from users where id='HarryHsu' and password='ILoveIntroToCN';
```

Thus only the row with id "`HarryHsu`" and password "`ILoveIntroToCN`" will be returned. If we make a little modification and let online users log in with this database, we would write the code as:

```
Select id, password from users where id='$ID' and password='$PWD';
```

The `$ID` and `$PWD` are the strings sent by users. What will happen if a user enter ID as "`' OR 1;--`"?



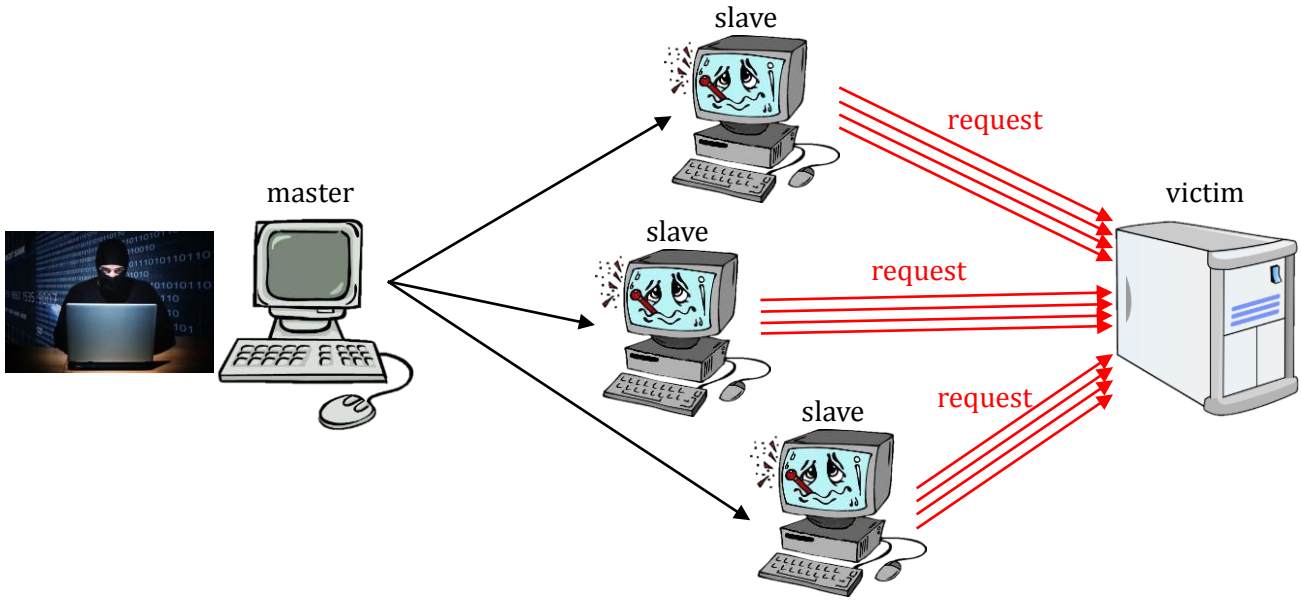

```
Select id, password from users where id=''' OR 1;--' and password='$PWD';
```

This single quote has turned a single-component `where` into a two-component one and that clause is guaranteed to be true because `id='' OR 1` is always true. Moreover, the dashes `--` makes everything behind it comment until the line is over. Therefore practically the database will return the first set of data in `users` chart and attackers can log in with that very user's account! This is only a simplest example of SQL injection. Higher level of SQL injection codes can even manipulate the data, insert malicious programs in the database, and infect any computer who is trying to access that database.

As a complete attack, a trained attacker would put a backdoor program inside the infiltrated target. The attackers are afraid that the administrator would discover the vulnerability and fix it, making them unable to hack in again. Therefore many attackers would put backdoor programs in order for themselves to gain future access.

Destruction

Some systems can be extremely hard to hack, and when attackers cannot attack on his own, he would resort to other computers. DDoS, or distributed denial of service is the act of gathering hacked computers as “zombies” and sending request to the targeted server at the same time. The requests can not only occupy the band width of the network but also the resources of the server, reaching the goal of suppressing regular internet services.



Conclusion

As a programmer, we will more or less develop programs or applications across the network in our career. In the era of information explosion, security has to be emphasized more than functionality. No user would feel comfort with the risk of exposing their personal information to the public. Therefore, we have to elevate our vision, and know our enemies more. That is how you can have a thousand victories out of a thousand battles.

References

1. Attacks over the Network and Countermeasures, Chi Ching Chang, Ying Da Lin: http://speed.cis.nctu.edu.tw/~ydlin/miscpub/hack_antihack.pdf
2. Hacker (computer security): http://en.wikipedia.org/wiki/Hacker_(computer_security)
3. Firesheep, Eric Butler: http://codebutler.com/
4. Backtrack Linux: http://www.backtrack-linux.org/
5. Backtrack password cracking http://recover.pixnet.net/blog/post/4535887-backtrack-%E7%A0%B4%E8%A7%A3administrator%E5%AF%86%E7%A2%BC%E5%AF%A6%E4%BD%9C
6. SQL injection how-to and prevention http://www.dotblogs.com.tw/hatelove/archive/2011/12/19/what-is-sql-injection-and-how-to-prevent.aspx