Web Server vandalism activities (Part 1)

Learning from the word 'urban art', the online world also has many destructive ways to lose the beauty of the web server. Last year, a debate about web server defragmentation took place, creating a major shift. Vandals carry out their behavior

Learning the word "urban art", the online world also has many destructive ways to lose the beauty of the web server. How do vandals perform their behavior? Reading the next article will know and understand more about how to do it. Since then, building a safety protection class before these dangerous activities.

Destroying a company's website is no longer strange in the technology world. People call these implementers the "bottom layer" of the internet community. People have made an assessment of the situation of placing an index.html file on a web server being hacked to invade, destroying the website is no longer special. Real talent is the source of the code, discovered the vulnerability to attack the first web server and create momentum for others to develop. When these people open up the flaw, many others, "sabotage children" begin to do it again and again.

These types of attacks become quite normal, like a network security expert who doesn't know how to break his website himself!

To protect you must learn to attack

If you want to protect your computer network from attacks in many different ways, you must first know how they attack. Not all colleagues agree with me on this idea, but the truth is we can't comprehend the problem without starting to do it ourselves. In the specific case here, we will learn how to break a website. If you are studying packages on the intrusion detection system, you will see that they are like someone uploading an index.html page. If not, you will have to write and submit as a person requesting the site.
If you want to perform electronic destructive activities, you have certain conditions. First of all, you need to know how the web server, IIS or Apache type. The condition of firewalls for companies that provide web servers as a service for clients is easy to break down, whether clients are easily accessible. For these clients, there must be an open port in the firewall that allows them to access the web server. You may have an appropriate application-layer firewall that helps protect your service, but that's quite another issue we haven't considered here.

Review the whole scene

As we know, it is necessary to meet certain standards to exploit the system to destroy. You can call it a series of problems. Whether the service is vulnerable or not, is it revealed on the web, and whether . You will have to draw a specific picture for yourself. The actual operations we will do with all the steps required to invade a web server, then upload the individual index.html version to the server. We will have to list the activities that need to be done corresponding to the operating system and web server type.

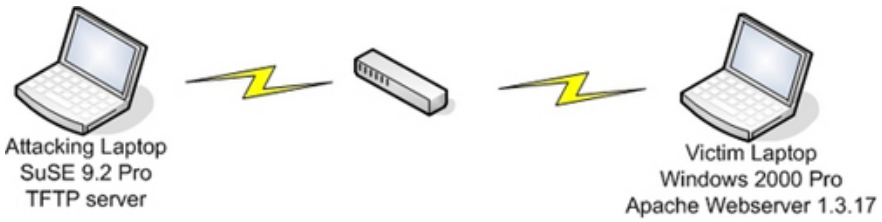
I did this vandalism in the home office with two laptops. One machine installed SuSE Linux, the other installed Windows 2000 Professional. In W2K laptop I installed Apache open source web server version 1.3.17. There are several versions of the vulnerability that came out after 1.3.17 but we will use this version as an example because it has a strong encryption hole.

details

It all seems to be fine, but have you only identified the source location to exploit? Not only can you know for sure that there are no "additional value" components in the exploit code? To simplify me use the Metasploit Framework. This framework is put together with HDM and spoonm. It is also a free version for everyone. The advanced feature of using this tool is that you can safely exploit all the attached vulnerabilities without fear of any backdoors. This framework can be used in either Linux or win32 environments. You can have your own choice, but in this example I use Linux because the tftp server is running on it. This server will be used in experimental illustration activities of the whole lesson.

The requirements for attacking a site mentioned above include:

Metasploit Framework to start the extraction process.
Windows 2000 Professional installs Apache 1.3.17.
Two laptops connected to each other via a switch.



Metasploit

In part one we will take a look at Metasploit. In part two, you will be given detailed instructions on how to use each step. We will provide some information to help you get an initial idea about it. In this article, I use Metasploit in Linux.

Below are all folders and files created once in the Framework without compression.

```
don @ linux: ~ / framework-2.2> dir
total 107
drwxr-xr-x 2 500 10000 112 2004-08-07 17:50 data
drwxr-xr-x 2 500 10000 744 2004-08-07 17:50 docs
drwxr-xr-x 2 500 10000 280 2004-08-07 17:50 encoders
drwxr-xr-x 2 500 10000 1288 2004-08-07 17:50 exploits
drwxr-xr-x 2 500 10000 144 2004-08-07 17:50 extras
drwxr-xr-x 6 500 10000 208 2004-08-07 17:50 lib
-rwxr-xr-x 1 500 10000 4687 2004-07-29 23:41 msfcli
-rwxr-xr-x 1 500 10000 22975 2004-07-29 23:41 msfconsole
-rwxr-xr-x 1 500 10000 5744 2004-07-05 06:52 msfdldebug
-rwxr-xr-x 1 500 10000 5639 2004-07-29 23:41 msfencode
```

```
-rwxr-xr-x 1 500 10000 1538 2004-08-07 17:58 msflogdump
-rwxr-xr-x 1 500 10000 2104 2004-07-29 23:41 msfpayload
-rwxr-xr-x 1 500 10000 9361 2004-07-27 03:38 msfpayload.cgi
-rwxr-xr-x 1 500 10000 6952 2004-07-29 23:41 msfpescan
-rwxr-xr-x 1 500 10000 12096 2004-08-08 04:37 msfupdate
-rwxr-xr-x 1 500 10000 16116 2004-08-07 18:31 msfweb
drwxr-xr-x 2 500 10000 120 2004-08-07 18:17 nops
drwxr-xr-x 3 500 10000 1664 2004-08-07 17:50 payloads
drwxr-xr-x 3 500 10000 168 2004-08-07 17:50 sdk
drwxr-xr-x 3 500 10000 80 2004-08-07 17:50 src
drwxr-xr-x 2 500 10000 216 2004-06-07 04:21 tools
don @ linux: ~ / framework-2.2>
```

The following is how to recover specific Framework and msfconsole.

```
don @ linux: ~ / framework-2.2> ./msfconsole


__. .__. .__. __.
_____ _____ / | _____ _____________ | | ____ | __ | / | _
/ _ / __ _____ / ___ / _____ | | / _ | __
| YY ___ / | | / __ _____ | | _>> | _ () || |
| __ | _ | / ___> __ | (____ / ____> | __ / | ____ / ____ / | __ || __ |
/ / v2.2 / / | __ |

+ - - = [msfconsole v2.2 [30 exploits - 33 payloads]
```

We can see that the Metasploit Framework actually has 30 vulnerabilities and 33 payloads that can be exploited. Very impressive! Not only that, it is also free in use, unlike other similar commercial versions. This difficult problem will continue to be done later. We will go deeper into how to use Metaspoit to serve the ultimate goal and knowledge of your computer security. Please continue to see part two.