



A method in finding out user's original IP of proxy server on IE using external program

by Beist Security Study Group
(<http://beist.org>)

ABSTRACT:

The objective of this paper is to present a method about finding out user's original IP of proxy server on IE. We will study direct network connection method by executing external program without using proxy server.

PROPOSED METHOD:

Lately, the original aim of proxy server is to degenerate. So proxy server is usually used for hiding user's IP. If user configures proxy server on IE, IE could communicate with the server through proxy a server.

There are some few public methods in finding a user's original IP. Proxy server provides HTTP_X_FORWARDED_FOR to your server. So, your server can check the identification of user's original IP using HTTP_X_FORWARDED_FOR. But, proxy of high anonymity mode doesn't provide HTTP_X_FORWARDED_FOR, so your server can't check the user's original IP.

There comes another method for solving the High anonymity mode's problem. This method is to get the user's PC information by installing ActiveX or Java Applet program. But, this way is not a good method either because it can't be installed without user's agreement.

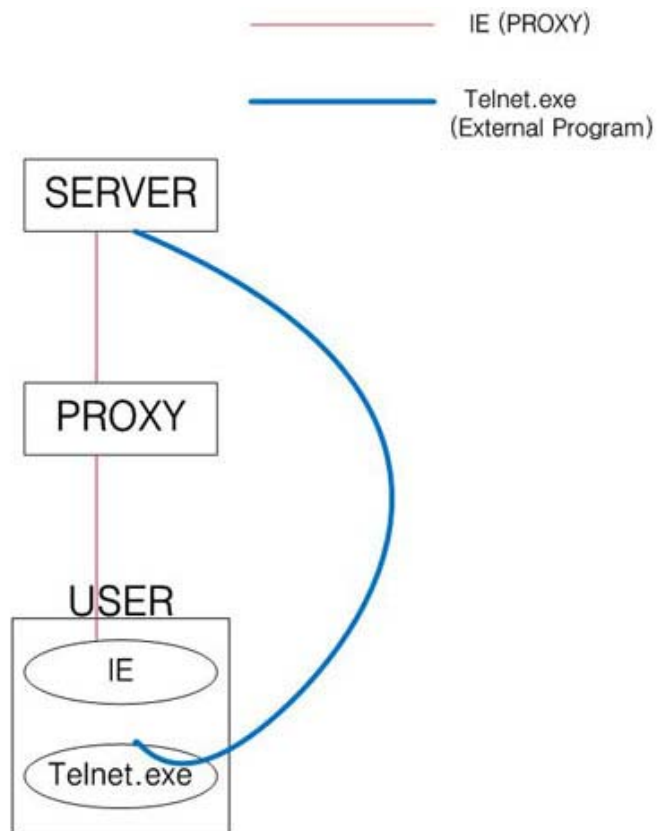
One more method is by using Flash. Flash can send user's original IP to server. But, we can't execute Flash without the user's agreement. However, recently PC, Flash has been already installed because it is one of the most popular programs.

The methods mentioned above are to find user's original IP using external program that is not controlled by IE (exactly, proxy policy.) The point of this discussion is not about the difference of principle. In IE, if it can execute a few external programs, we discuss telnet.exe.

For example

```
<iframe src="telnet://beist.org:destport" width=0 height=0>
```

If the upper tag exists in html file, IE executes the telnet.exe (IE doesn't directly executes the telnet.exe, but calling a TelnetProtocolHandler method in url.dll by executes the rundll32.exe.) At this time, telnet.exe is not controlled by IE. On the other hand, if user configures proxy server on IE, it can't connect through a proxy, because telnet.exe is an external program.



[FIGURE1] The difference network path between IE and telnet.exe

We can find out the user's original IP by using a simple method like this.

RESULT:

In fact, this paper's method is difficult to apply on cyber world because when IE executes telnet.exe, the user can see telnet.exe's window. Of course, you can disconnect at just established. But it is not a good idea. Also, Firefox browser shows a warning message to user 'Firefox is going to execute external program, do you agree?' I just want you to know methods like this.