Use SPIKE and BURP for computer security

HTTP proxy is a tool widely used by computer security experts. However, not every expert understands all aspects of computer security. This article will introduce you how to use it

HTTP proxy is a tool widely used by computer security experts. However, not every expert understands all aspects of computer security. This article will show you how to use an HTTP proxy.

HTTP Proxy and friend

The world of computer security is a constantly changing world. There are always people exploiting vulnerabilities and people patching security holes in programs. Saying someone can understand all aspects of computer network security is unimaginable. Because of the nature of computer security and its multifaceted nature, any security expert needs to choose a specific area of ??his own. One of them is the field of web application security with its many forms. Why do we say that in many of its forms? That's because not all websites are written in the same language. They also do not share all the same configuration or support the same auxiliary programs.

Web application security is an area of ??concern in real life. Web applications are increasingly expanding on the Internet with a multitude of different applications. Those applications are designed for clients that can use and interact with it. Another thing is that the public front of a company on the Internet created by programmers does not mean there is no error. And one more thing is that it is impossible to write a perfect code regardless of the language used.

This leads to another aspect of web application security. Often a large number of coded web applications are in a state where they still do not guarantee good quality. Programmers were almost happy when they finished the project on time and spent very little time verifying the code was written. There are a number of external tools that can allow us to verify code but some of them are not really reliable. Good tools are very expensive.

All non-programmers can know that, which is a big problem in coding. It is also especially true when it comes to software programs for businesses with thousands of lines of code that make up such a program. Many times developers get a good grasp of the work in a software cycle, but they may not understand much about the protocol they are coding for.

So when a programmer ends up writing a web application that he is assigned to, it is also time we need to check it and find out if there are any holes or minor problems in it. or not. What is the best way to solve this test problem? This is really a good question. The question brings us back to the purpose of this series. Testing a brand new web application is best using an HTTP proxy. This is really a great tool, this tool will allow developers to interact with the web application in many ways that a typical web session will not re-create. Developers can block client requests and change most internal fields to emphasize web applications.

Approach the problem

Before we get into the issue, we will introduce you to some background for this topic, which is important when we approach a new issue. The two HTTP proxies that we will observe and use are **SPIKE** and **BURP** . The first one is written by Dave Aitel of Immunitysec, the latter is written by some others.

Now is the time to install the SPIKE proxy, do not assume that you will download it now from the link in the above paragraph because you will receive a message saying that a Python interpreter is required for SPIKE to work. So download Python here first. You need to give it an email address, but just that is enough. Once Python has been downloaded and installed, you need to place SPIKE at the root path of the C (c :) drive. From here you open the DOS command window, open the SPIKE folder. You need to read the README.txt file to properly configure your web browser.

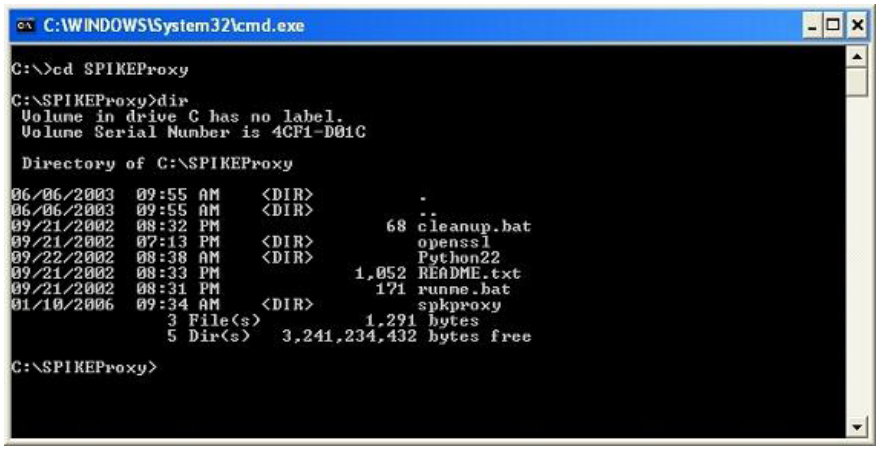

Figure 1

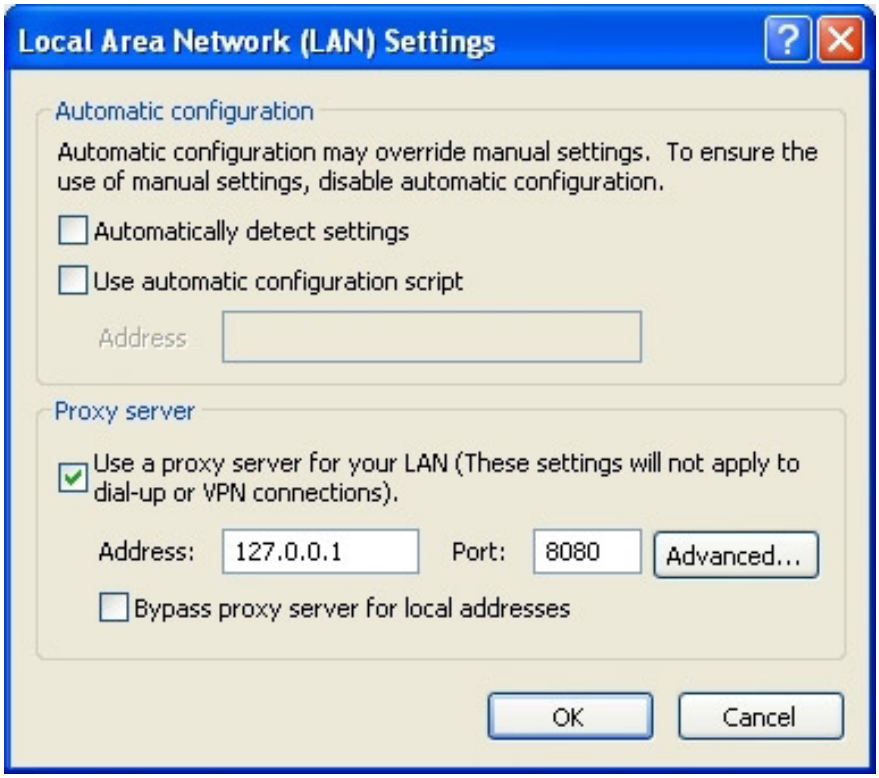

Figure 2

The last step is to type in ' **runme.bat** '. Once you've done that, type in the url bar of your web browser *http:///spike /* and you'll see SPIKE. Congratulations on installing and configuring an HTTP proxy. What needs to be done with now? The answer is very easy. Let's have a little relaxation with the web server. In case I installed Apache web server on another VMware for our testing purposes. This will allow us to play with SPIKE in a controlled testing environment. Nothing has been done with the web server and I installed a website on it.

Check time

Whenever you do any work, you should have some form of packet sniffer running in the background. The thing to be able to verify the output of the tool you are running in a different situation and with strange results. It is no different for our case. I was thinking of **tcpdump** from MicroOLAP, which will work well with Windows XP SP2. It is also completely free for home users.

After installing this tool, we already have the packet sniffer running in the background. Now it will prompt it to write only packets between the computer that SPIKE is running and the computer on which the Apache web server is running. That will reduce the number of packages that the attacking computer can observe. You can also further refine that by instructing tcpdump to write packets with port 80 in it. For example, this tcpdump can be seen in the picture below.

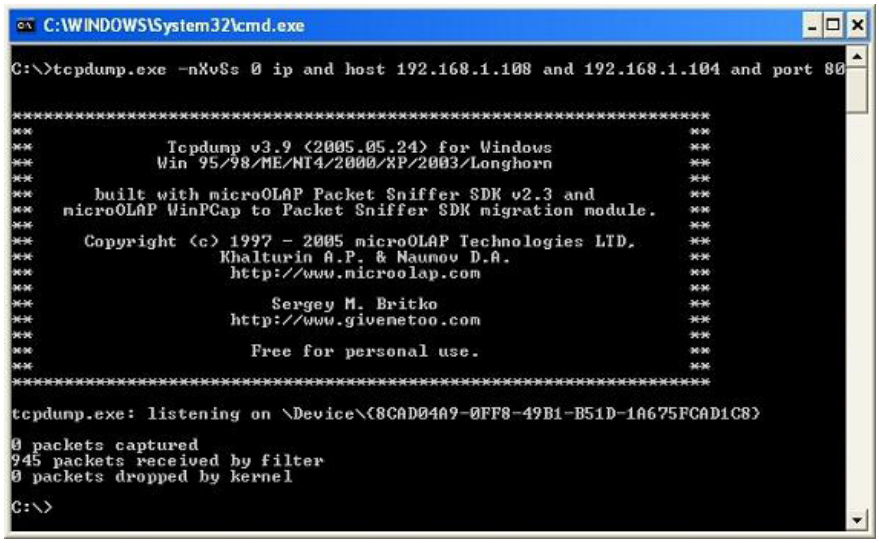

Figure 3

You can see in the picture that 945 packages were obtained before canceling the tcpdump session. This is the action of running another background mode that I am running on my computer. That shows why you want a relatively narrow selection filter when running experimental tests or performing real tasks. We can see many things, here are some parts to consider before moving on to learn how to use an HTTP proxy. This may also be a homework exercise before moving on to the new issue in the following sections.