

Jeanne Security Demo: Whisker Before and After

by Chris Brenton
November 21, 2001

Introduction:

This document demonstrates what Jeanne (modified reverse proxy for squid) can do to protect a Web server.

We started by doing a vulnerability scan against an NT 4.0 server running Microsoft IIS 4 with service pack 6a installed, but no other security patches. This webserver is vulnerable to a large number of exploits, including Unicode attacks, Code Red/Nimda, and others.

We then checked the server again, after Jeanne had been installed as a reverse proxy.

Demonstration Details:

The tool of choice for performing this vulnerability scan is Whisker. Whisker was written by Rain Forest Puppy (RFP) and is the first adaptive CGI vulnerability scanner. Adaptive means that Whisker will identify the server it is probing and automatically customize the scanning it performs. Whisker is considered by many people to be the most advanced CGI scanner available.

Below you can see a small portion of the output produced by Whisker. Note that it had no problem identifying a plethora of vulnerabilities in our NT 4.0 Web server:

```
= Server: Microsoft-IIS/4.0
- Appending ::\, %2E, or 0x81 to URLs may give script source
- Also try +.httr and %20%20.htw tricks
- Security settings on directories can be bypassed if you use 8.3 names
+ 404 Object Not Found: GET /cfdocs/
+ 403 Access Forbidden: GET /scripts/
+ 200 OK: GET /msadc/Samples/selector/showcode.asp
+ 200 OK: GET /msadc/samples/adctest.asp
+ 200 OK: GET /iisadmpwd/aexp4b.httr
+ 200 OK: HEAD /msadc/msadcs.dll
+ 200 OK: HEAD /_vti_inf.html
+ 401 Access Denied: POST /_vti_bin/_vti_aut/author.dll
```

We then installed Squid as a reverse proxy and loaded Jeanne as the redirector. The Squid server is now advertised as the "www" host address, so all HTTP communications (including our vulnerability scan) are directed at this server. Jeanne then provides access control through a simple text file specifying which pages can be requested from the webserver and which ones cannot. Note that this setup is identical to a standard Squid reverse proxy setup, except that we are also using Jeanne to control which pages and scripts may be accessed.

Note the difference in the output from Whisker, below. The "Scripts" directory is listed as "not found," so Whisker skips checking for any vulnerabilities in this directory. Also note that `_vti_inf.html` is now listed as forbidden, since it was not specified for access through Jeanne:

```
= Server: Microsoft-IIS/4.0
- Appending ::\, %2E, or 0x81 to URLs may give script source
- Also try +.htr and %20%20.htw tricks
- Security settings on directories can be bypassed if you use 8.3 names
+ 404 Not Found: GET /cfdocs/
+ 404 Not Found: GET /scripts/
+ 403 Forbidden: HEAD /_vti_inf.html
+ 403 Forbidden: HEAD /_vti_pvt/
+ 403 Forbidden: HEAD /_vti_pvt/service.pwd
```

So, while our NT 4.0 server is still technically vulnerable, Whisker is incapable of finding any vulnerabilities. Whisker is fooled into thinking that the server is fully secured. Also note that if an attacker actually attempted to exploit any of the vulnerabilities, Jeanne would filter them out, thus maintaining the integrity of the server. Attacks such as Code Red or Nimda would fail.

Psychological warfare:

Jeanne also has some advanced configuration options that allow you to throw an attacker off the trail even further. For example, below you can now see that the Web server is identified as being Squid. We could just as easily change the banner to read "Apache" or "Bob's Way Cool Server":

```
= Server: Squid/2.4.DEVEL4
+ 200 OK: GET /cfdocs/cfcache.map
+ 200 OK: GET /scripts/cfcache.map
+ 200 OK: GET /cfcache.map
+ 200 OK: GET /cfdocs/cfmlsyntaxcheck.cfm
+ 200 OK: GET /cfide/Administrator/startstop.html
+ 200 OK: GET /cfdocs/snippets/evaluate.cfm
+ 200 OK: GET /cfdocs/snippets/fileexists.cfm
+ 200 OK: GET /cfdocs/snippets/gettempdirectory.cfm
+ 200 OK: GET /cfdocs/snippets/viewexample.cfm
+ 200 OK: GET /cfdocs/exampleapp/docs/sourcewindow.cfm
```

Also note the remaining output produced by Whisker. Whisker thinks it is successfully downloading every file it tries to read. The result is that it will report multiple vulnerabilities that do not exist as well as spend a lot of time checking for non-existent files. For example, remember that in the initial Whisker scan, the `cfdocs` directory was listed as "not found." Since Whisker could not find the directory, it skipped all file checks within that directory structure. Since it now thinks this directory exists, it wastes its time looking for vulnerabilities it will never find.

The result is an attacker has no more useful information than when he started. Also, since so many different probes were made, our IDS has probably lit up like a Christmas tree, thus

warning us that some trickery is afoot. We can now go through and ban this IP address from making further attack attempts against any part of the network.

Conclusion:

While it's never advisable to run a vulnerable Web server, Jeanne can provide you with some breathing room to patch your servers before the bad guys come along and take over the box. As an additional plus, you also get the speed benefits of running a reverse proxy.