

RAIN FOREST PUPPY




CANSECWEST 2002



Assessing the web:
finally tools that
don't suck



- 
- Whisker 1.4 is getting quite old and outdated...
 - Last year @ CanSecWest I discussed the limitations of CGI scanning, and introduced RFProxy
 - There weren't many public or open source tools available for use



In the meantime:

- Yet more web technology has been released
- .NET, SOAP, and XML-RPC is started to rear it's ugly head all over the Internet
- Sites use javascript because that's all the HTML wizards generate nowadays
- Easier to write client-side javascript than server-side CGI code (or so it seems)




To date...

- RFPProxy hasn't been touched
- Where is whisker 2.0?
- Libwhisker thingy...



Finally: good tools
to the rescue!





Some interesting free (as in beer) tools as of late:

- Nikto CGI scanner
- WhiteHat Security WHArsenal
- @stake WebProxy
- Nessus (well, new web plugins)

Nikto

- CGI scanner, similar to whisker 1.4
- Checks for CGIs, common dirs, and old versions
- Database frequently updated

<http://www.cirt.net/>



WHArsenal

- Set of CGI's that plug into existing Apache install
- Allows you to do all kinds of requests, while controlling/modifying request particulars
- Similar in function to RFProxy, but not an actual proxy

<http://community.whitehatsec.com/>



@stake WebProxy

- Assessment proxy with full fuzzer/rewriting capabilities
- Actually does what RFProxy meant to do
- Implemented in Java; supports Linux, Solaris, and Windows right now
- Tool is free, but source is closed

<http://www.atstake.com/>



Nessus

- Has a few new interesting web assessment plugins which do site crawling/mirroring and other fun stuff

<http://www.nessus.org/>



Whisker 2.0



Whisker 2.0

- Written for Perl 5.004 or later
- Built on libwhisker
- Complete rebuild of whisker 1.x, from scratch
- Tests written in raw Perl
- Finally implements a few lacking features



Now natively supports:

- SSL
- Proxies
- Authentication
- Transfer encodings and other funkiness
- HTTP 1.1 keep-alives



Big changes/additions:

- Integrated web crawler
- Better custom 404 error handling
- Server identification beyond HTTP banner
- Completely modular design, catering to the 'plugin' craze that is sweeping the industry



Whisker 2.0
in action






Planned future additions:

- Output plugins
- Updated tests, including CVE mappings
- More server fingerprinting
- Automatic auth brute forcing



Planned libwhisker additions:

- NTLM auth support
- SSL client-side session caching
- LW::Bin
- More anti-IDS modes



Where can you get whisker 2.0?

It's available on the CanSecWest CD!*

Version 2.1 will be the first publicly available version, and will be released in a few weeks

* Make sure to download the latest libwhisker from www.wiretrip.net/rfp/p/doc.asp/d21.htm



Whisker resources:

Wiretrip library document #21

<http://www.wiretrip.net/rfp/p/doc.asp/d21.htm>

General site, news, etc:

<http://www.wiretrip.net/rfp/>

Questions?





By the way...

The demo target IIS 5.0 server is not really IIS, but an emulation of a default IIS 5.0 server.

It's a Perl script written by HD Moore and myself, for use with Neils Provos' honeyd.

The IIS emulator is a full web server allowing you to serve custom content in the same manner as IIS, and even has emulated support for .NET and ActiveState Perl.

The script itself will be bundled with honeyd.



Thanks!

rfp@wiretrip.net

