SensePost: Wikto, Scully, and CrowBar

By Russ McRee

Prerequisites

.NET Framework 1.1 (Scully)
.NET Framework 2.0 (Wikto 2.0)
Paros Proxy or similar (CrowBar)

The team at SensePost recently released Wikto 2.0, so, to that end, *toolsmith* is pleased to bring you freely available tools from this South African information security specialist. As is evident in their "Hacking by Numbers" training offerings at Black Hat and other conferences recently, you will find that the SensePost team is often looking to capitalize on exploit opportunities. Their tools[1] are exemplary in this cause, and will make excellent additions in your toolkit as you remediate vulnerabilities in your workplace environments. SensePost offers some commercial tools that we will not cover here, but you may wish to explore them on your own, specifically BiDiBlah, an assessment/attack console, and Suru, a man-in-the-middle proxy.

Our coverage this month will explore free tools, including the latest version of Wikto, as well as Scully and Crowbar. *In my best Mafioso impression: "Hey Boss, you want me to call in Scully and CrowBar?"* All of the tools require a quick registration with SensePost, but registration is easily rendered SPAM-free if you wish. You will be sent an email with a key that will then allow you to download all the tools we will discuss here. Remember, as with many of the offerings discussed in *toolsmith*, you are well advised to point these tools only at sites and systems that you own or maintain.

Aura

One of the significant gains in Wikto is its inclusion of Aura. You may recall from June's *toolsmith* on Search Engine Security Auditing, in December 2006 Google discontinued use of their SOAP API, instead pushing development towards their AJAX API. If you did not have a valid Google API key by then you were out of luck using a number of great assessment tools. Wikto was victimized by this frustrating Google decision as well, but SensePost jumped on the opportunity and created Aura (API Usable / Re-Usable Again). Wikto 2.0 integrates Aura, eliminating the need for a Google API key. Before running Wikto with Aura you will need to download and install it, as the Wikto installer does not include it. Look for Aura enhancements in the immediate future as the SensePost team is moving it to Java and has Aura-J out in beta.

Wikto 2.0

Wikto, cleverly named a Nikto for Windows, is much more than just a Nikto GUI. Nikto, if you are not aware, is an open source Perl-based web server scanner built on Lib Whisker.[2] Wikto 2.0 offers some significant changes from it predecessors including:

- Built on the Dot-Net 2 Framework
- Reworked GUI
- Updated content compare algorithm
- Updated Nikto scanning to reduce false positives
- No longer requires HTTrack / HTTPrint
- Web Spider for directory discovery
- Wizard-based scanning
- SSL via proxy server CONNECT
- Pause / Resume functionality
- Trigger-based sorting of Nikto results.

Getting started

After the GUI loads, proceed to the *System Config* tab and update the database files under *Database Locations*. The Nikto database will update itself cleanly, but I found the updating of the Google Hacking Database required manual intervention. I am not sure if it is a function of the URL under the *Update Sites* (it points to a PHP page that redirects to the XML database file), simply a bug, or a failure in the fuzzy neural network behind the keyboard, but clicking *Update Now* under Database location makes a request to the local file system rather than an HTTP request as it does for the Nikto database update. I used the recommended URL, saved the `GHDB.xml` to the local file system, ensured that it was placed in the default directory for Wikto databases, and then ran *Update Now*. The update will take almost 60 seconds, so be patient. If you have a Google API key, load it under Google API. If you do not, no problem; start Aura. Once you have completed these steps remember to save your configuration file. This will create a `.wkt` config file, name and location of your choosing. The documentation for Wikto at the time of this writing was

1 http://www.sensepost.com/research_tools.html.

2 http://www.cirt.net/code/nikto.shtml.

for version 1.61, now two versions old; likely there will be an updated version for 2.0 soon.

Your GUI menu selection will read as follows: *Spider* | *Googler* | *BackEnd* | *Wikto* | *GoogleHacks* | *SystemConfig* | *Scan Wizard*.

Spider

Spidering a site is always a recommended first step in order to better understand the directory structure. Click the *Spider* tab, enter your target, a port if not the default 80, check SSL if applicable, and a starting directory if you wish.

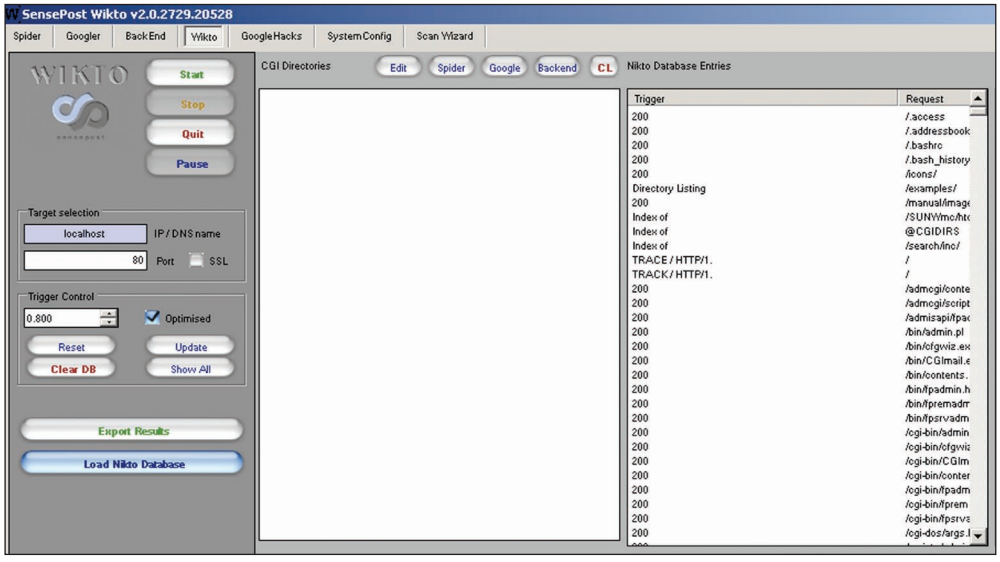

Figure 1 – Wikto

Googler

This tab is extremely useful for extracting interesting file types from your site of interest, including htm, html, asp, pl, php, cgi, aspx, wsdl, xml, xls, sh, csv, txt, doc, pdf, mdb, and zip. I always add jsp, so feel free to enhance the list as you see fit.

BackEnd

The BackEnd feature attempts to find interesting files and directories on your target by assuming that a web server might have certain directories that are not linked from any page on the server that a Spidering/mirroring effort would have missed. This includes administrative backend interfaces, which is why the module is called BackEnd. SensePost extends this concept to files as well: with a list of directories on the web server you can also start looking for interesting files in those directories.[3]

BackEnd will load directories found in your Spider step and file types found in your Googler effort. You can also load directories, file names, and file types from preconfigured lists you may have already configured. Finally, you can update Suru-default, Standard, Quick, or Full lists directly. Wikto 2.0 also features scanning AI to reduce false positives, which you can configure and enable under Trigger Control. Results can also be preserved and exported.

Wikto

The namesake tab takes you into the land of more aggressive testing and will load results from the Spider, Googler, and BackEnd tabs to aid you in your cause. Before you begin, click *Load Nikto Database*. This will take advantage of the Nikto db you updated in *Getting Started* and offer you 2795 "tests" (as of this writing). As you run it, results will populate the lower half of the GUI and weigh them according to severity. Results can again be exported.

GoogleHacks

As you did in your Wikto effort, click *Load Google Hack Database* to take advantage of 1467 different queries (as of this writing) to execute against your target. This module automates the same attempt you might make manually at the Google search URL, such as *site:<your target> "Index of /backup."* This can be particularly handy when conducting your monthly audit of the sites in your care for disclosure of information that has no business being visible to a search engine. You are doing this, right? You can further customize this effort by loading queries that might be applicable to your sites but not in the GHDB. Imagine internally hosted web-based Oracle administration tools. The GHDB has 15 Oracle entries currently, but may not include some relevant to your environment. You can build your own `ghdb.xml` for these relevant queries and point Wikto to it for your specific monthly audit requirements. Regardless, you want no such URL publically available and Wikto 2.0 can help you ensure it is not.

Scully

Scully is a SQL database interface and brute forcer useful against MSSQL and MySQL databases. Where, in the past, you may have needed database-specific client libraries, ODBC connections management interfaces to make connection attempts, Scully does all the heavy lifting for you. You are presented with a clean, simple GUI that will serve you brilliantly in testing blank or weak SA and root passwords. There is nothing like slapping down that know-it-all DBA with a text dump of a table laden with PII. Of course, management permission is in order before conducting such an audit. Start with the Brute Force option, and ensure that you have a `dictionary.lst` file available to point it at. Ensure the `.lst` contains well known weak passwords as well as any others you feel may work in your environment. Figure 2 shows a scenario where the `dictionary.lst` found a match, and after populating it in the Scully password field was able to issue

3 Wikto documentation, http://www.sensepost.com/research/wikto/using_wikto.pdf.

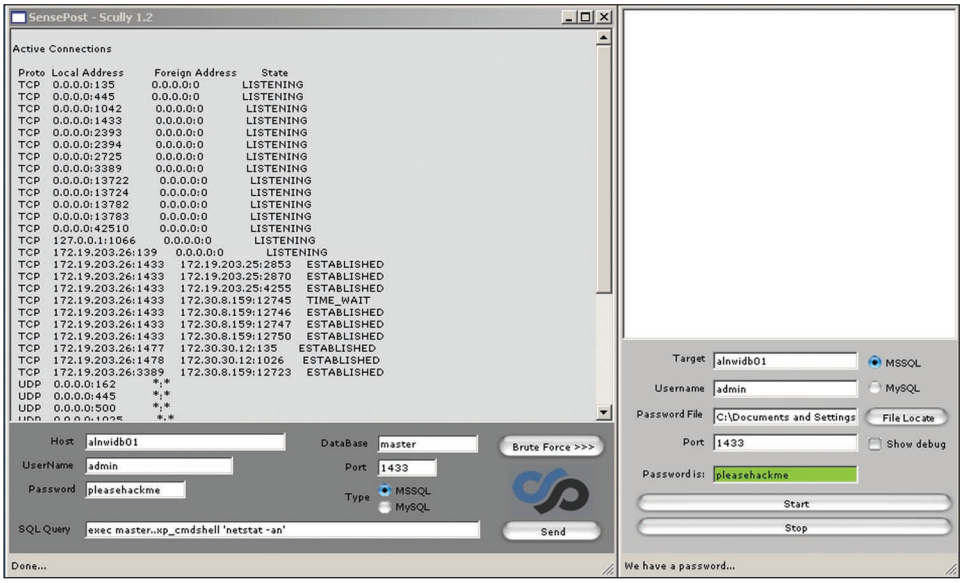

Figure 2 – Scully=scary

exec master..xp_cmdshell 'ipconfig.' Suffice it to say that if you can let loose with *xp_cmdshell*, you basically own the server.

CrowBar

CrowBar is a self-described "new generation web application brute force attack tool." I am not often a proponent for brute force attack tools as they are often inelegant and crude, but CrowBar distinguishes itself by trying to keep you in control of the session through the use of a content comparison algorithm, the same algorithm offered in Wikto. That said, I did not find this a very successful tool in test. I have also learned that CrowBar is no longer under active development as it has been superseded by the fuzzing capabilities innate in the Suru product. The documentation is not current so it is unclear if I missed a step. Even with a test site configured with simple four digit numeric usernames and passwords, CrowBar was not particularly successful in differentiating responses. Give the existing documentation a close read and consider this a learning tool. If nothing else, it is excellent for seeing responses on the fly while conducting input manipulation. However, I am by no means a web application security expert, so this little app may be far better suited to more skilled auditors. As described in the documentation, "Crowbar does not try to be a particularly sexy tool – it's rather ugly. It's also not a point and click brute force tool – it rather gives the analyst as much as possible control of the process." This is a fair statement, so the transition to Suru indicates the likelihood that you will find improvements on this theme in that offering.

For my test session, I used Paros Proxy, and lifted a POST session and response for cut and paste into CrowBar. I found best results when providing the IP address of the target, then executing Base Response. Thereafter, you should be able to see responses after running Start and waiting a bit. Assuming you are successful, you should see numeric differences in responses in the bottom window.

On the immediate horizon: Squeeza

Look forward to Squeeza,[4] coming soon to a pen testing platform near you.

Demoed at Blackhat/Defcon this year, it promises to be the SQL Injection tool to end all SQL injection tools, including full binary file transfers and database enumeration via a

4 http://www.sensepost.com/research/squeeza.

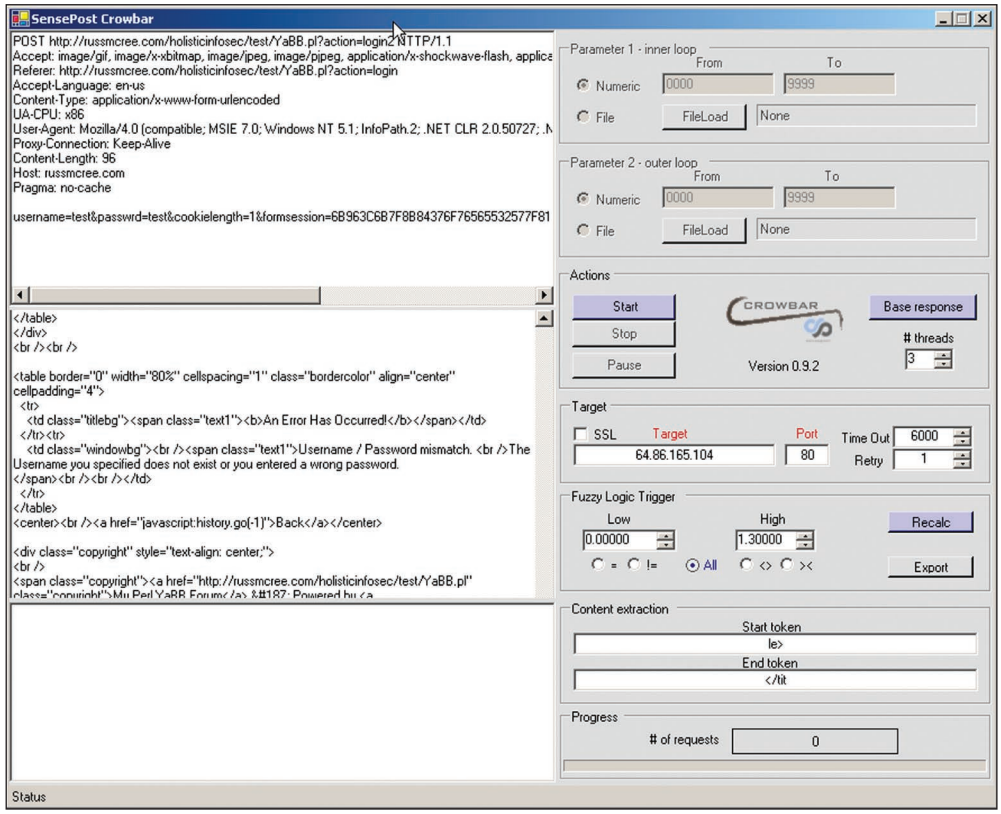

Figure 3 – CrowBar

number of channels including DNS, HTTP error messages, and timing. By the time you read this, it should be available.

Benefits and drawbacks

Obviously, there are no costs associated with these tools. Any security analyst or administrator should find Wikto and Scully quite useful in their regular auditing efforts. CrowBar is more a work in progress and should be watched for future releases. Neither Wikto nor Scully require much effort to get up and running, so you will not see much cost associated with time spent.

In conclusion

SensePost has committed a strong effort with these tools. While a bit behind in documentation, it keeps development moving along as noted in Wikto 2.0. They have indicated that documentation will be updated soon and send along their apologies. Keep an eye on their website for tool updates and enjoy these useful freebies. Cheers, until next month…

Acknowledgments

Ian de Villiers and Haroon Meer of SensePost, for their feedback and insight.

About the Author

Russ McRee, GCIH, CISSP, is a security analyst working for Expedia. He is a member of numerous security organizations and maintains holisticinfosec.org. Contact him at russ@holisticinfosec.org.

