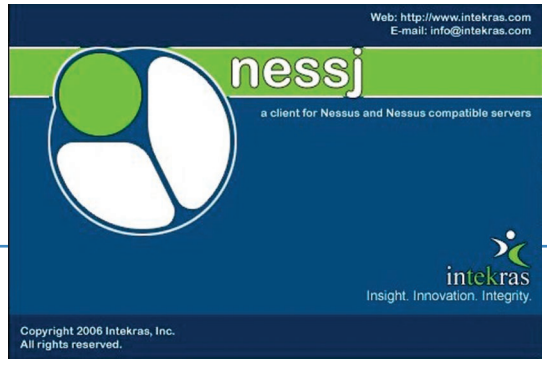
Nessj: Application/network security scanner client

By Russ McRee



Prerequisites

Java 1.5.0,

SWT 3.1 (if using the Java binary)

JFreeChart 1.0.1 (if using the Java binary)

Nessus

Introduction

It's unlikely that anyone reading this column hasn't heard of Nessus. What is likely is the premise that the same reader has taken issue with the performance of the Nessus client. Nessj to the rescue. Nessj, offered under the Clarified Artistic License, is free to download and use.

Janos Szatmary, Directory of Security Research at Intekras detailed the history of Nessj for *toolsmith*. In 2001/2002 Idealogica developed an application security assessment suite which was acquired by NetSec (now MCI/Verizon.) Just prior to the sale of the product, Arion Lawrence, Chris O'Ferrell and Janos joined the company and worked in the application assessment and reverse engineering space. After the merger of Netsec/MCI/Verizon, Verizon Business would not directly support their open source efforts, so they developed the product under an entity with which Verizon had a relationship - Idealogica. After a time they left Verizon and joined Intekras who was friendly to open source, and it seemed a good fit to move the project over during a feature enhancement.

The project evolved to its current state over several months and the current base code and features are fairly stable. Tasks to be completed shortly include bringing the application up-to-date with the latest Java/SWT releases, and to ensure some deployment issues fixes as there are some known Debian issues. There are also plans for an embedded DB instead of a serialized Java object (which tends to be slow and memory hungry.) The longer term goal is to make NessJ (after a rename) into a front end for several security related tools (nikto, metasploit, etc.) that would be able to share data between components; however, that is some time away. The developers are always open to suggestions, and welcome contributions to the product.

Preparing for Use

Nessj 0.7.0 is available in binary and source forms, and is packaged for Linux, OSX, and Windows. You'll note a heavy Java dependency, specifically, Java 1.5 or later. If you have issues with running Nessj on Linux due to SWT errors, refer to the FAQ.[1]

Download Nessj from SourceForge.[2]

Installation is straightforward and, after confirming the presence of a JRE on your system, install the appropriate binary.

Obviously, you'll need a Nessus server, and while we won't cover it's installation, there are a few notes. As of this writing, the current version of Nessus is 3.05 and is available for all major platforms and can be downloaded.[3]

Default installation includes the use of SSL for client connectivity.

When establishing your initial connection to a newly installed Nessus 3.0.5 server, select TLSv1 as the protocol.

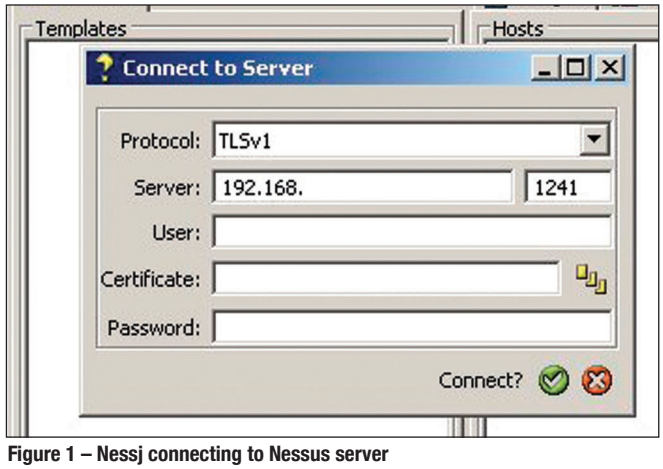


Figure 1 – Nessj connecting to Nessus server

1 http://sourceforge.net/docman/display_doc.php?docid=33221&group_id=157279

2 http://sourceforge.net/project/showfiles.php?group_id=157279

3 http://www.nessus.org/download/

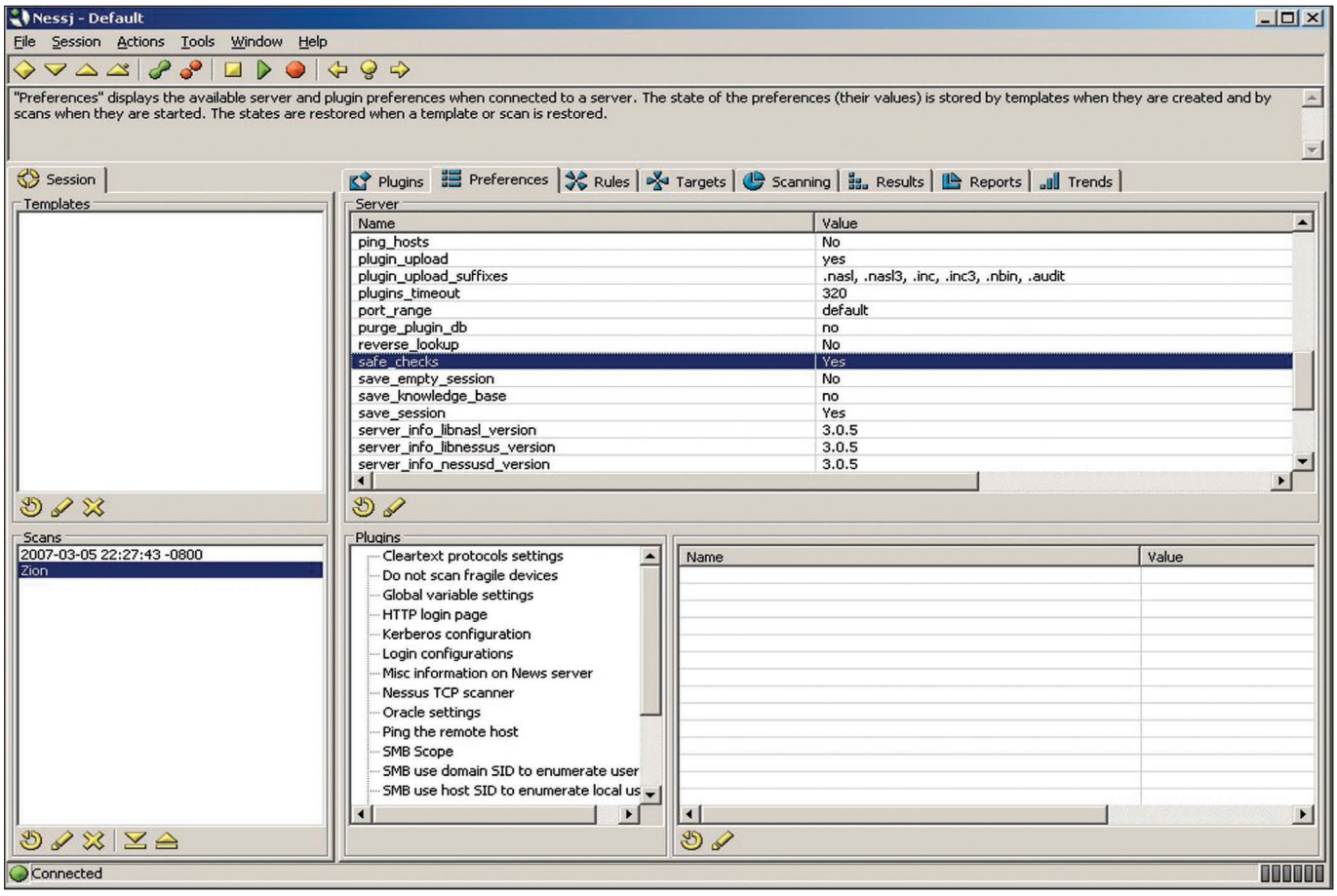


Figure 2 – Establishing Nessus scan preferences

Nessj works equally well on Windows, Mac, and Linux systems, as I tested it on all three.

Using Nessj

You'll find the Nessj UI unique, and perhaps a bit cryptic at first, but realize that every icon offers a description if you hover over it.

In order, I prefer to select my Targets first, check my Preferences, enable my Plugins based on the system I'm scanning, then engage the scan.

The Preferences tab is important if, for no other reason, than to ensure that *safe_checks* is enabled (set to yes), unless you want to risk bringing a system down (trust me, Nessus can bring a system down).

I've picked a Linux-based firewall to scan, in particular the inside interface, so we'll likely see SSH access and perhaps a browser console. I enable more plugins than likely necessary, but given that we're testing a firewall for vulnerabilities, I selected plugin families like Backdoors, Denial of Service, Firewalls, Port Scanners, Gain a Shell Remotely and Gain Root Remotely. You can always opt to throw the kitchen sink at your target, but keep in mind relevance and the fact that your scan will take significantly longer with more plugins enabled. Nessj really begins to shine when it comes to reporting results. Not only are they attractive and legible, they are often built with hyperlinks to additional information.

Again, as we scanned the inside interface of the firewall we found it had some ports open to the internal LAN as seen in Figure 3.

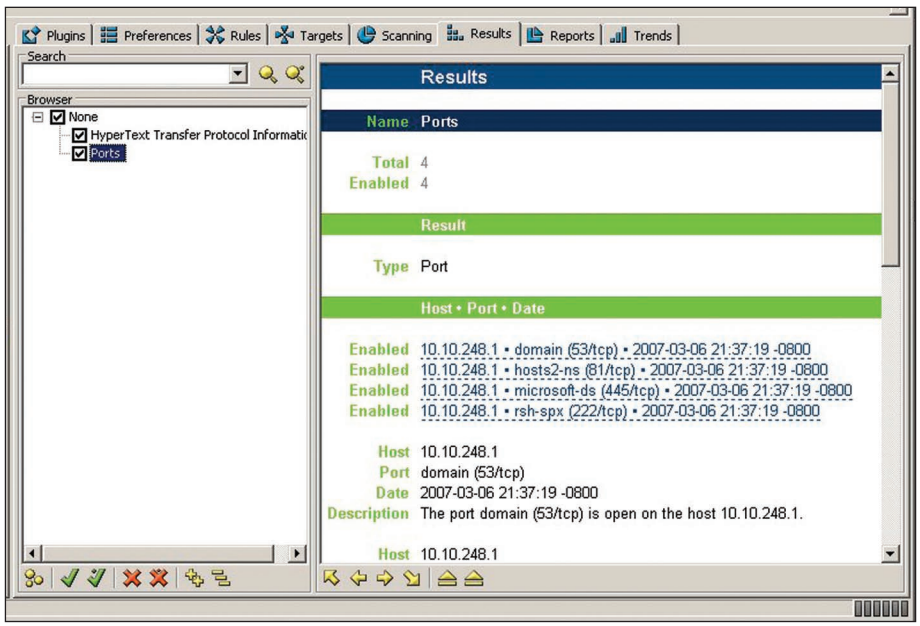


Figure 3 – Nessj scan results

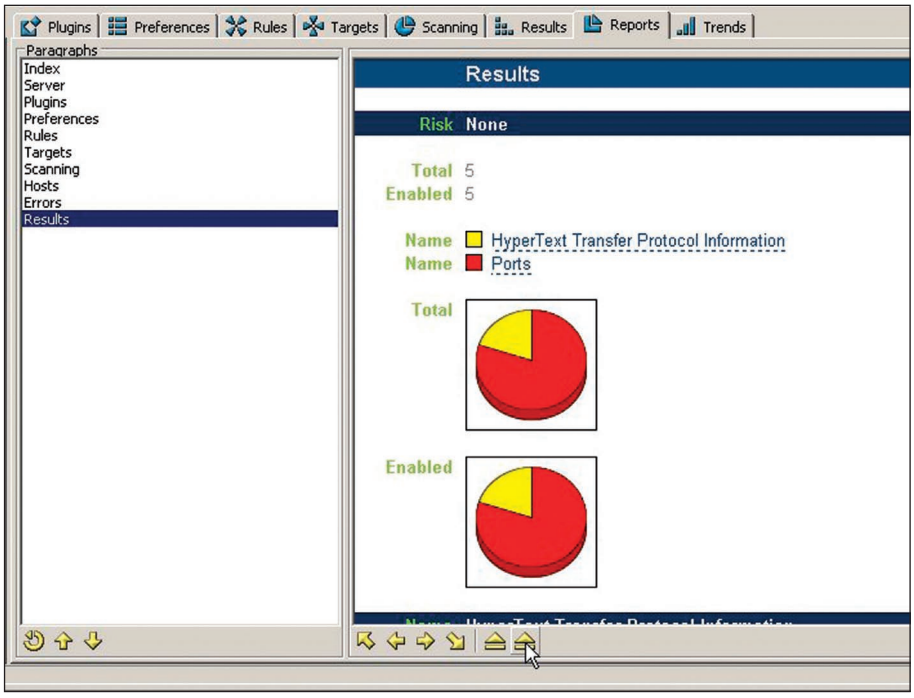


Figure 4 – Nessj reporting

As with any decent tool, a major feature enhancement is certainly a strong reporting engine, and Nessj comes through here as well. We all report to someone, right? In the reports tab, you'll note that you can view a plethora of information, including your server information, plugins selected, preferences, rules, targets, etc. The last option is results which offers attractive graphs, as well as risk level. Best of all, reports are easily exported for dissemination. At the bottom of the primary reports frame you'll see two up arrows, one to export HTML, the other, XML.

Finally, Nessj offers Trends, a feature I am most fond of. We'll consider different scan results than our first effort against the firewall.

Let's instead consider a Windows XP host, conceptually intended to be a gold image for deployment to entire company-wide rollout. Our first scan of the host found that Windows Firewall had not been utilized and that File and Print services were available. Not the end of the world, but with a hardened desktop system in mind, these services needn't be made available to all hosts. After receiving the results of our first scan, the image building team enabled the firewall, allowing unrequited access to only the WSUS server for patching. We then diligently rescanned to confirm and sure enough, the second scan found no signs of our first scan's concerns.

Additional features, found under *Tools… Settings* in the main menu, include the ability to modify path and behavior of all options, such as graph type and report/results style sheets. You can also establish scan templates, manage your sessions, and view both network and debug logs.

Conclusion

Nessj is a fine offering from Intekras and offers much promise beyond it's initially impressive functionality. I look forward the prospect of it becoming more BiDi-Blah-like, or even Core Impact, mentioned by John and his team as a goal for the future.

One note on Intekras: they're a minority-owned infosec and defense systems contracting company with a penchant for work that contributes to a greater good, in addition to their support for open source work like Nessj. Their site is enjoyable read while grabbing Nessj for your vulnerability assessment work. Cheers…until next month.

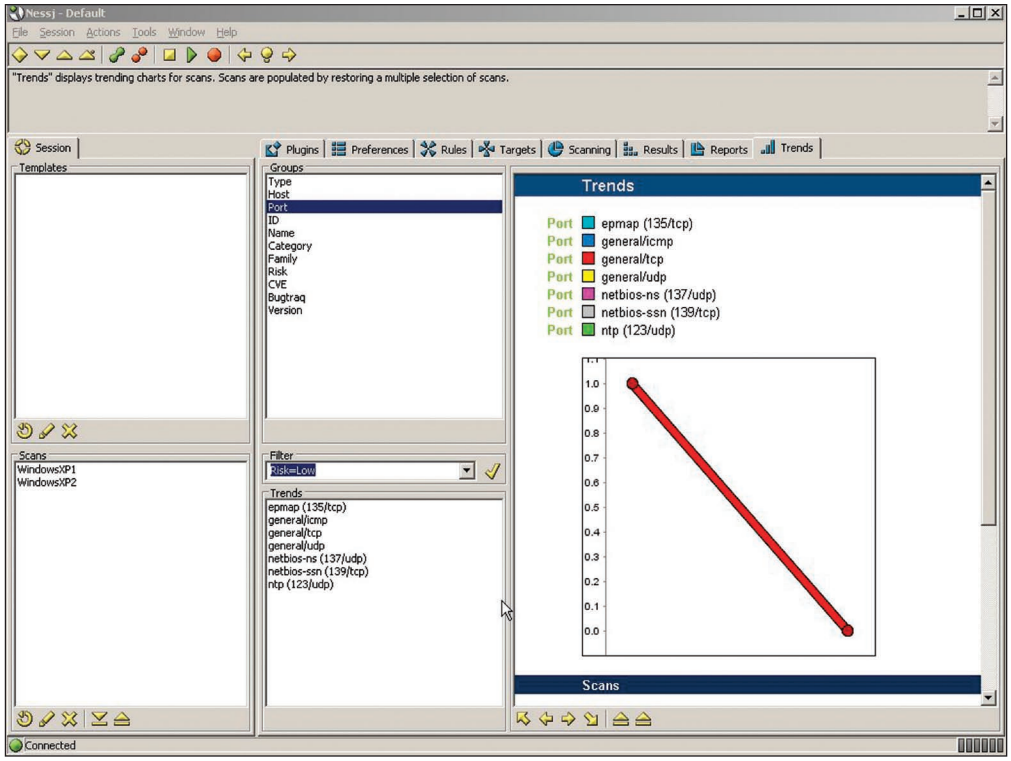


Figure 5 – Nessj trends

About the Author

Russ McRee, GCIH, is a security analyst working in the Seattle area. He is a member of ISSA, Pacciso, InfraGard, and CCSA (Cyber Conflict Studies Association). Russ maintains holisticinfosec.org. Contact him at russ@holisticinfosec.org.