



North West Chicagoland Linux User Group
Nessus Vulnerability Scanner
Presented by: Dan Tesch
May 06, 2003

NWCLUG

**some content has been plagiarized from the Nessus website.*

- The Nessus Project aims to provide to the internet community a free, powerful, up-to-date and easy to use remote security scanner.
- A security scanner is software which will audit remotely a given network or host and determine whether vulnerabilities exist so that they may be patched. This differs from a simple port scanner because not only does Nessus show whether a service is running on a host but also determines whether a found service is configured properly or running at a current patch level.
- Nessus functions as a client / server, the server performs the testing and the client controls the server. The server is available only for *nix, the client is also available for Windows and Java.
- Nessus uses a plug-in architecture, plug-ins can be enabled or disabled to perform tests of different types of hosts, why look for Windows vulnerabilities on a Unix mail server?

Plug-ins can be updated automatically by typing the command `update-nessus-plugins` at the server. Plug-ins can also be updated manually at the server or uploaded via the client. Nessus also gives you the ability to write your own plug-ins using NASL (Nessus Attack Scripting Language) or C.

- The session between the client and server can be encrypted or not, you can log in using a certificate or simple username / password.
- 2.0.4 is the current version of Nessus and it will compile under redhat 9
- Additional information and downloads are available at www.nessus.org.

Setup as demonstrated this evening

redhat 7.0 server running Nessus Server (PII400 / 256Mb RAM)
W2K Professional running Nessus Client (PIII500 / 500Mb RAM)
Target machine: default install of W2K Server IIS, FTP, SMTP, DNS

Installation & running

- Download and compile the server. There are some dependencies but installation is pretty straightforward.
- Create a user account by using the command `nessus-adduser`, answer some simple questions like username, password and what targets the user has rights to scan.
- Modify the `nessusd.conf` file at the server, I used the supplied one and made only slight simple modifications like making my username the `admin_user` and allowing users to upload plug-ins into the global Nessus directory.
- Start the Nessus daemon, `nessusd -D`.
- Log in to the server with your client.

** I have been unable to get the authentication via certificate to work correctly.

Configure a test with the client

- Choose Session > New and give it a name (you can change it later).
- In the Targets tab, click Add or Edit and enter your hosts.
- Generally, the default options have worked for me. Safe Checks is advisable for live hosts.
- Set your port range to scan and select the port scanner you would like to use.
- The Plugins tab is where you can select host specific tests.
- After saving your session set up, you can right click on it and select Execute.

View test results

- Live demo

I have used Nessus to:

- Test my web, e-mail, FTP servers and routers as seen from inside my network and from the internet.
- Test my home network as seen from work
- Test the router supplied configured and maintained by my ISP.
- Test an installation of Snort

Some other security scanners and services:

ISS Internet Scanner - Managed Service - www.iss.net

eEye Retina Network Security Scanner - www.eeye.com

Qualys QualysGuard Service - www.qualys.com

Foundstone Enterprise Risk Solutions - www.foundstone.com