Global Information Assurance Certification Paper

Nessus - A Very Capable Security Auditing Tool

Vernon Stark

August, 6 2000

One of the steps that can be taken to secure a computer or network is to periodically scan for vulnerabilities and fix any security problems identified by the scanner. Various scanners are available for this purpose including commercial scanners such as Internet Scanner™ from Internet Security Systems and open source scanners such as Security Administrator's Integrated Network Tool (SAINT™) and Nessus. This paper discusses one of those tools, Nessus (available at http://www.nessus.org/).

Why select Nessus? First, each tool has its strengths and weaknesses. The optimum approach may be to use a number of tools. If only a single tool is used to assess security, security holes that would have been uncovered by using multiple tools may be missed. Second, Nessus is free and provides an important alternative to pricey products such as Internet Scanner™. Third, can 1200 Nmap users be wrong? In May and June of 2000, 1200 Nmap users were asked to list five of their favorite security tools. Tools could be either open source or commercial and could run on any platform. With the votes tallied (not including votes for Nmap), Nessus came out on top (Reference 1). Finally, Nessus is flexible, extensible, relatively easy to use, and scans for a large number and variety of security holes. Nessus allows one to find security holes in network hubs, routers, computers running UNIX or Windows NT, and other devices (Reference 2).

The founder of the Nessus project, Renaud Deraison, released the first version of Nessus in April 1998. The current version of Nessus is version 1.0.4 which was released August 3, 2000. Nessus is released under the GNU General Public License (GPL) so everyone is free to read and modify the code.

Nessus uses client server architecture. The server daemon, nessusd, does the actual security scanning and must run on a UNIX machine (including Linux, *BSD, or Solaris). The client provides the user interface and can run on a much wider variety of computers including Windows 95/98/NT and any UNIX computer running GIMP (available at http://www.gimp.org/).

With Nessus, security checks are done entirely through external plug-ins (Reference 3). As of August 6, 2000, there's an impressive library of 479 plug-ins which fall into 17 families. The plug-in families are shown in Table 1 (Reference 4). Also listed in Table 1 are the number of plug-ins in the family and the names of a few of the plug-ins in the family. This list of plug-in families illustrates that Nessus is capable of testing for a wide variety of security holes. For example, in the "useless services" family, the "Echo port open" and "Chargen" plug-ins test to see if the host or hosts being scanned are vulnerable to the well-known echo-chargen attack. In the "backdoors" family, the "PC Anywhere" plug-in checks to see if the host is running PC Anywhere which may allow an attacker to take control of the system.

In addition to this wide variety of existing plug-ins, Nessus comes with its own scripting language that allows one to write additional security tests. The Nessus scripting language is called Nessus Attack Scripting Language (NASL). NASL provides the capability to quickly code security tests and to share those tests with others. In fact, new NASL scripts can be written and made available within hours of the announcement of a new exploit (Reference 5). Sharing plug-ins is safe (Reference 6) since no commands will be executed on the local host and Nessus will only send packets to the target host or hosts. NASL greatly facilitates the writing of security test scripts by providing support for sockets, packet forging, string manipulation, and the sharing of information gathered by other scripts. The ability to share information gathered by various scripts is done via a knowledge base. This knowledge base stores information gathered by the various plug-ins. For example, if Nessus is running multiple security tests that need information about the operating system version, that information can be gathered once and then shared among all the scripts that utilize that information. This sharing of information and cooperation between scripts helps minimize the time and bandwidth utilized to perform the security audit.

Family	Number of plug-ins	Sample Family Member(s)
Backdoors	25	Back Orifice, NetBus 2.x, PC Anywhere
CGI abuses	129	Finger.cgi, htimage.exe overflow
Denial of Service	72	Winnuke, cisco http DoS, SunKill
Finger abuses	5	in.fingerd |command@host bug
Firewalls	8	Proxy accepts CONNECT requests
FTP	26	Anonymous FTP enabled
Gain a shell remotely	11	SSH Overflow, rsh on finger output
Gain root remotely	34	Imap buffer overflow, BIND vulnerable
General	24	Predicable TCP Sequence number
Misc.	16	Services, Traceroute, Default accounts
NIS	2	NIS server, bootparamd service
Port scanners	5	TCP SYN scan, Nmap tcp connect() scan
Remote file access	24	NFS export, Insecure Napster clone
RPC	37	RPC portmapper, nlockmgr service
SMTP problems	18	EXPN and VRFY commands
Useless services	12	Telnet, Echo port open, Chargen
Windows	31	SMB shares access, SMB log in

Using the Nessus client, the user can specify the Nessus server to use, the port scanners to use, the vulnerabilities to test for, and the range of IPs to scan. Plug-in specific information can also be entered. Since Nessusd is multi-threaded, the user can also specify the parameter max_threads which determines the number of systems to test simultaneously. The user then initiates the test via the client. Once the security tests are complete, the results are passed from the server to the client and the client provides a report. The report generated provides information from each plug-in that identified a vulnerability. Moreover, each plug-in provides information about how to correct the

particular vulnerability located. For example, the SMB login plug-in attempts a null session login and also tries various user names and passwords. If a null session login is possible, Nessus reports that. If a user login was successful, Nessus reports the username and password combination that resulted in a successful login. Another example is the SMB shares access plug-in. If Nessus finds shares accessible, it lists the accessible shares. The SMB shares plug-in also provides the following message concerning plugging this security hole:

"To restrict their access under WindowsNT, open the explorer, do a right click on each, go to the 'sharing' tab, and click on 'permissions' Risk factor : High".

Clearly, the information passed between the client and server is very sensitive since it includes a list of system vulnerabilities. To protect this information and avoid session hijacking, Nessus uses encryption for client-server communications.

Clearly Nessus is a very capable security scanner that scans for a large variety of security holes. Nessus also exhibits a number of attractive features including flexibility, extensibility (via NASL), timely availability of new security tests, testing efficiency (resulting from information sharing via the knowledge base), encrypted communications, and open source policy. Nessus is well worth considering as an addition to the security professional's toolbox.

References

1. "Top 50 Security Tools." 20 July 2000, URL: http://www.insecure.org/tools.html, (6 August 2000)

2. beyondsecurity.com "Nessus the free, open-sourced and easy-to-use security auditing tool." (15 October 1998), URL: http://www.securiteam.com/securityreviews/Nessus_the_free__open-sourced_and_easy-to-use_security_auditing_tool.html, (4 August 2000)

3. "Scanning." 11 July 1999, URL: http://www.opensec.net/vulscan.html, (4 August 2000)

4. "Nessus Plugins families." URL: http://cgi.nessus.org/plugins/dump.php3?viewby=family, (6 August 2000)

5. Hrycaj, Jordan and Renaud Deraison "What is a security auditing tool?" "Nessus - the open sourced, up-to-date security scanner." 4 January 2000, URL: http://www.nessus.org/pres/workshop_12291999/2_2.html

6. Hrycaj, Jordan and Renaud Deraison "NASL." "Nessus - the open sourced, up-to-date security scanner." 4 January 2000, URL: http://www.nessus.org/pres/workshop_12291999/3_2_1.html, (5 August 2000)