Global Information Assurance Certification Paper

Nessus – Get on Board
Greg Brooks
February 15, 2001

Introduction

The purpose of this document is to describe my real world experiences with the Nessus Security Scanner, hereafter referred to as simply Nessus. Nessus is a software tool that provides host-based vulnerability scanning. The biggest difference between Nessus and the majority of its competitors is the price tag – Nessus is free. According to the developers, the "Nessus" Project aims to provide to the internet community a free, powerful, up-to-date and easy to use remote security scanner.

Whoever coined the phrase, “You can’t get something for nothing”, never used Nessus. Just because you don’t need to spend thousands of dollars on Nessus, doesn’t mean that it is a poor man’s security scanner. The features of the product compare very favorably with others in the market, such as ISS Internet Scanner and NAI CyberCop Scanner. In fact, it was an e-mail news bite that came out from The Systems Administration, Networking, and Security (SANS) Institute that turned me on to Nessus.

Our company was about to purchase a consulting license for eEye Digital Security’s Retina to do vulnerability scans for our clients. We were pleased with its reporting capabilities and user interface and it detected a wide range of security vulnerabilities. In addition to Retina, we had tested other products such as the ISS and Network Associates’ scanners. The week that we were going to make our purchase of Retina, the report came out from SANS that Network Computing magazine had done laboratory tests on several vulnerability scanners. Out of the eight scanners tested, including eEye, ISS and NAI’s product, Nessus was the tool that detected the greatest number of security holes that they had planted.

Let me be clear that the point of this paper is not to knock any of the other vendor’s products. All of the scanners that we’ve tested have had their strengths and will help identify areas where a company can tighten security. A host of benefits can be gained by running vulnerability scanners with the only drawback being that a company can gain a false sense of confidence if the results show that there are no security holes. Each of the scanners tested by Network Computing failed to identify at least one critical security hole. I would strongly recommend running more than one scanner to cover all the bases. For companies that don’t have a scanning product already, Nessus is a great choice to start out with. And for companies that have already invested in a security scanner, Nessus is the ideal choice to bolster their security architecture inexpensively.

The Network Computing study was compelling enough to make me want to take Nessus out for a test drive. Following is a more detailed description of what Nessus offers and why I believe Nessus is valuable for everyone in the information security field.

Nessus Security Scanner

Nessus follows a client-server architecture. The server portion, an executable named nessusd, actually performs the attacks and the client portion is simply the front-end that connects to the server. The server portion must run on a POSIX system (such as Solaris or Linux). I ran the server on Mandrake Linux version 7.2. I used two different versions of the software – the first was 1.07 and had binaries packed up into a nice downloadable RPM that was easily to install. Shortly after I installed this version, 1.07a, came out but an RPM was not immediately available. Since there were enhancements that I wanted to get a hold of, I downloaded the freely available source code and compiled it for my machine. There are Nessus clients available for Unix, Windows, and one written in Java.

One of the great things the inventors of Nessus did is leverage the strengths of other good network security products out there instead of reinventing the wheel. NMAP, the best-in-breed port scanner, is used to determine which services are active on a given target. In addition, Queso, a remote OS identification tool is used by Nessus along with NMAP to determine (quite effectively) what operating systems are running on scanned targets.

A unique feature of Nessus is that it does not trust that services will be running on their proper IANA-assigned port. For example, just because the NMAP scan of a host revealed that port 23 was open, Nessus would not assume that the host was running telnet. If a web server happened to be running on this port, Nessus would detect this and run the appropriate vulnerability tests against web servers. Additionally, if a web server were also running on port 80 and 8080 of the same host, all three would be checked for web-specific vulnerabilities. This kind of untrusting behavior makes both for a good security professional and a good security scanner.

Plug-in Architecture

The greatest strength of Nessus is definitely the plug-in architecture. Each and every security test that Nessus performs is written as an external plug-in. This means that new security tests can be added without having to recompile Nessus. New plug-ins are added to the Nessus web site as soon as they are written, very often on a daily basis. I was paying special attention when I noticed a recent security alert that came out about BIND vulnerabilities. Covert Labs issued this security advisory on January 29th, 2001. The very same day, a

plug-in was available for download from Nessus and it's mirror sites. That is what is called response.

Getting the latest plug-ins is trivial. The command, nessus-update-plugins, will go out to the Nessus Internet site, verify which plug-ins are already installed and grab any new ones. As of February 13th, 2001, there were 593 plug-ins available. That means 593 different security flaws that Nessus is capable of detecting out of the box.

The plug-ins are arranged into groups to keep them manageable. The following are the list of groups:

- Backdoors
- CGI abuses
- Denial of Service
- Finger abuses
- Firewalls
- FTP
- Gain a shell remotely
- Gain root remotely
- General
- Misc.
- NIS
- Port scanners
- Remote file access
- RPC
- SMTP problems
- SNMP
- Useless services
- Windows

The last thing that I want to mention about the plug-ins is that the source code for all of the tests is all out in the open. You can view what commands the plug-ins actually issue by clicking on the plug-in on the Nessus web page or by looking in the plug-in directory on your Nessus server. The plug-ins are written in a scripting language called NASL. This is a C-like programming language that is fairly easy to learn if you have some programming experience. Nessus allows you to develop your own scanning scripts. In a utopian security world, when flaws were discovered a NASL script would be available for download with the report of the security flaw. By writing this document, I would like to urge the white hat community to download and use Nessus and start developing these scripts. Any new scripts that are developed can be contributed on the Nessus web site and they be considered for posting on the web site for all to download.

The Art of the Vulnerability Scan

This section covers some of the options available when doing scans with Nessus and the discoveries that I noted when using the product. The Nessus client has several options to consider before running a security scan. Obviously, the first thing I should cover is the target. Nessus is flexible in the fact that it can be used to scan a single host, a network subnet, or a group of hosts enumerated by a text file.

The second thing that should be done is to verify that the appropriate plug-ins are being used to scan the network. Handy buttons allow the user to enable all plug-ins or enable all but dangerous plug-ins. I would recommend the latter when doing tests on a live network environment, as it will skip the denial of service tests that could serious cripple a network or server. However, the most comprehensive scan can only be done by leaving these plug-ins enabled. Also, individual or families of plug-ins can be disabled. Suppose you are scanning your internal firewall-protected network, and you don't care if hosts respond to SNMP queries on the default community strings. You can easily disable this test.

In real-world testing, I noticed a few other points that I'd like to cover. First, if you are scanning a protected host that does not answer to pings, you have to disable all options with the word "Ping" in them. By default, if NMAP is unable to ping the remote host, it does not continue with a port scan, it just assumes that the host is not alive. The second point has to do with performance. One of the key performance concerns as far as scanning speed goes is the "checks_read_timeout" in the /etc/nessusd.conf file. This controls how long plug-ins wait for responses. While the default is set to 15 seconds, you get a big performance gain by lowering this if you are on a fast network connected to the hosts that you want to scan. I recommend toning this down to two or three seconds in this situation.

The Scanning Results

A security-scanning product would not be complete without the final report. Nessus provides very sharp-looking output that can be sorted both by host and by service port. The issues that are found are reported as either informational, security warning or security holes and the risk factor of the problem is also identified by words such as "Low" or "Serious". This is critical because oftentimes security scanners such as this reveal a huge number of security holes; sorting them according to risk gives the IT staff the ability to plug the gaping holes first.

Another nice feature of Nessus is that it documents CVE numbers of the problems it detects. CVE stands for Common Vulnerabilities and Exposures. CVE aims to standardize the names for all publicly known vulnerabilities and security exposures. A cooperative consortium of security-related organizations such as security tool vendors, academic institutions, and government as well as

other prominent security experts works together to do this. It's a great mechanism for sharing information on vulnerabilities – such as how to deal with them! Nessus reports provide a link to the appropriate web page on mitre.org's website when finding catalogued vulnerabilities.

The reports are exportable to different formats. They can be saved in the NSR format, which makes them readable to any Nessus client. If they are to be shared with someone who doesn't have Nessus, you can save the data in a variety of other ways. These formats include straight ASCI text, HTML, and XML. There are two options for HTML – one creates a single page document and the other creates several documents with some nice charts and graphs about the number and type of vulnerabilities. I was very impressed with this flexibility.

Conclusion

In conclusion, Nessus provides a lot of bang for the buck! Actually, if bang for the buck is defined by bang divided by buck, you'd get a division by zero error when measuring the value of Nessus. All weak computer humor aside, Nessus is a very capable tool, competitive with commercial scanners.

If you are a security professional that doesn't already have a vulnerability-scanning product in house, Nessus is a perfect choice for you. Once a colleague of mine went in to a potential customer to pitch security and said, "You can pay me to scan your network for you, or I can go home and see what I can find on my own free time." He was trying to show the customer that in this Internet age, you never know who is going to come knocking on your back door. The hackers and crackers of the world have access to this tool and are using it. It is never a good situation when they know more about your network than you.

Even if you are already using a different product to audit network security, Nessus will provide an additional level of detection. The more people that use this tool and contribute detection scripts and feedback to the authors, the better it will become. But I believe that Nessus is one of the best tools out there, already. With its up-to-date and comprehensive plug-in architecture, its wide range of supported platforms, and its well-organized reports, Nessus is truly an excellent software package. Get on board the Nessus security train and let's win back the war against the crackers.

References

The following are cited as references in this paper:

Securify Inc. Packetstorm. http://packetstorm.securify.com/. (14 Feb 2001)

The SANS Institute. "Vulnerability Scanners Fail To Find Common

Vulnerabilities." SANS NewsBites Vol. 3 Num. 01. (3 Jan 2001)

Deraison, Ranuad. "The Nessus Project : Introduction." http://www.nessus.org/intro.html. (14 Feb 2001)

Deraison, Ranuad. "Nessus : Features." http://www.nessus.org/features.html. (14 Feb 2001)

The MITRE Corporation. "Common Vulnerabilities and Exposures." February 7, 2001. http://cve.mitre.org/. (15 Feb 2001)

Forristal, Jeff and Shipley, Greg. "Vulnerability Assessment Scanners." Network Computing Magazine. January 8, 2001. URL: http://www.nwc.com/1201/1201f1b1.html. (15 Feb 2001)