

Evaluating Nessus

Abstract:

The key to securing assets is identifying them first and then find how vulnerable they are. If one does not realise the vulnerability found in a network in context to network security, it is highly likely that the network system is to crash at some point of exposure to either a malicious intruder or a person having no illicit intentions at first is tempted to play around in a vulnerable network. A lot of measures are taken to secure a network to bring to a level close to indivisible, however there can be holes and flaws found in even the most secure systems. In order to find flaws and openness in systems security tools are developed that expose the vulnerabilities in a system and make administrators aware of the dangers there system can face. In this report we will be taking a ride in the shallow waters with Nessus – a vulnerability scanner developed by the Tenable Network Security.

1.0 Introduction:

Network systems have grown so complex over the last decade with advancements in operating systems, applications, and network protocols that it is almost impossible for a dedicated security administrator to keep even a relatively small network shielded from attack by manually reviewing each networked system for security flaws as it is no longer feasible. Each development in the field of computing brings along with it a wave of security holes by bring in exploitable programming errors logic errors, vendor-installed back-doors, and default configurations plague that is accompanied in everything from modern operating systems to the simplest print server. New malicious programs come out when yesterday's viruses begin to seem to be positively tame.

Assessing Vulnerability:

Vulnerability assessments can explain by first defining what vulnerability is. For purposes of this report, vulnerability can be defined as any programming error or misconfiguration that could allow an intruder to gain unauthorised access. This may include anything from a weak password on data communication equipment, say a router to a programming flaw in an exposed network service which is not properly patched. Vulnerabilities are no longer just the area for system crackers and security consultants; it has now become the dominant factor behind most network worms, spyware applications, and e-mail viruses. Software vulnerabilities are being actively exploited by spammers to hide their tracks; open mail relays of the 1990s for example have been replaced by compromised "zombie" proxies today, that have been created through the mass exploitation of common vulnerabilities. The reason why systems are targeted lies in the answer that most exploited systems were not targeted intentionally, but they fell prey as there were simply one more address in a network range being scanned by an attacker, resulting in targets of opportunity, not choice. As long as spammers can install their relay software, to them it makes no difference which computer system is being attacked (1).

2.0 Choosing Nessus – the Vulnerability Scanner:

Nessus was chosen as the evaluation tool for this report with the chief goal of evaluating a vulnerability scanner. Nessus considered being the market leader in vulnerability scanners; therefore it is worth an effort to see what comes in the package that is used by over 75000 organizations worldwide even after being a closed source security tool.

A vulnerability scanner was chosen over other security tools like intrusion detection tools, port scanners and firewalls was that it is an administrators primary responsibility to know how weak the system is and what security holes are there that can be exploited and should be covered. Nessus is a vulnerability scanner that encompasses features of port scanners, detects what services and parts of devices can be accessed and what measures should be taken to harden the system. Therefore it is a one in all system for a network security administrator.

History of Nessus:

Renaud Deraison created the project known as Nessus in 1998. Being an open source it answered to the ever-increasing prices of commercial vulnerability scanners, and the relative stagnation of the SATAN project - the Security Administrator Tool for Analyzing Networks, the last remaining open-source scanner. Nessus was a framework; however it required a community of knowledgeable security researchers to work for free in order to bring Nessus up to the level of a full-fledged product. At that time network security was quickly rising in cost as the Internet was not only used by the National Science Foundation. As the growth of the Internet skyrocketed with dot-com financial trends a subsequent increase in cyber space became vulnerable. Vulnerability scanners were sold commercially for large sums of money in direct proportion to the number of devices being scanned by corporate giants (1).

With a free, powerful and up-to-date remote security scanner that was easy to use gain popularity of becoming rated among the top products of its type in the security industry. Today Tenable Network Security is the sole developer, owner and licensor of the Nessus source code. Even Nessus 3.0 is now closed source; however most of the plugins can be updated for free by simply registering with Nessus (2).

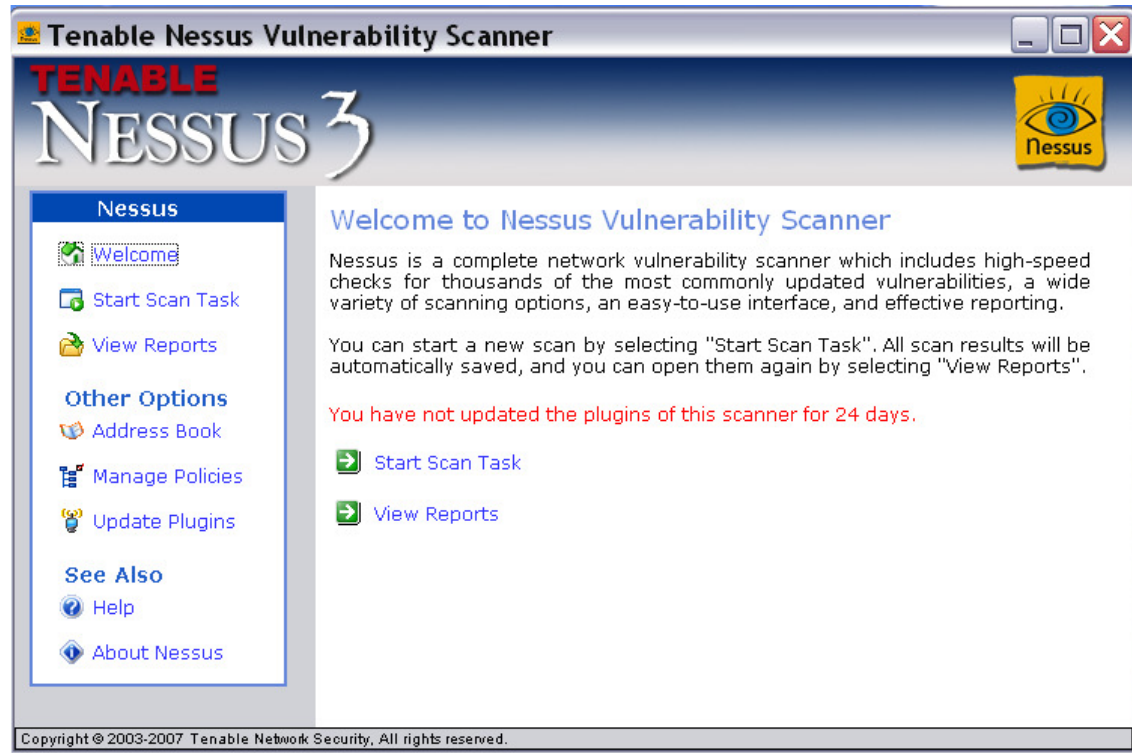
3.0 Nessus at Work:

Nessus can be used to scan for vulnerabilities on either a localhost or a remote host on a network. It uses the Network Attack Scripting Language or .nasl extension checks or plugins that are written in C language for security tests.

Using Nessus:

Nessus 3.0 can easily be downloaded from Tenable Network Security's website. Although it is now closed source, however most of the plug-ins can be used that function as port scanners and service scanners. In order to use Nessus registration is required to get the activation code for the software. Nessus comes in different flavours for UNIX, Mac and Windows systems. We will be looking at Nessus 3.0 for Windows systems in this report.

Figure 3.1: Start-up Interface for Nessus 3.0 Windows Edition.



Updating Plugins: Nessus notifies the number of days past since last update. There is a built-in feature that runs a wizard to update plugins from the Tenable website.

Managing Policies: before a scan is run policies can be added that control the ability of running checks. These policies can be edited and even deleted. This is an extra option if one wants to customize from the default configurations.

There are different tabs in the Manage Policies menu that help customize to personal requirements. The sub tabular menus that include configuration settings for restrictions are:
General: managing the number of hosts and security checks, timeout for checks and plugins in seconds, defining port range and reporting verbosity and paranoia.

Ping: the type of pings like ARP, TCP and ICMP

Services: To define specific parameters like number of connections, connection and network read/write timeout settings for detecting services that are running on ports.

Credentials: This determines if critical security patches have been applied enabling Nessus to scan remote hosts as if locally connected. It includes settings to run Kerberos, SSH and SMB.

Web: this enables to scan for web services using HTTP, CGI and Web mirroring.

Compliance: a feature available to Nessus Direct Feed customers that performs compliance checks with different Windows and UNIX policies, these can be added, changed and reset.

Others: account information can be saved about FTP, SMTP, IMAP, POP2 and numbers for SID host and domain to enumerate local users.

Address Book: Nessus maintains an Address book containing IP address of the hosts that have either been scanned, or have simply been added for scans in the future. These addresses can be both added and delete from the address book. A short description about the host can be entered as well. Entries in the address book are available in the drop down menu when imitating a scan task.

Starting Scan Task:

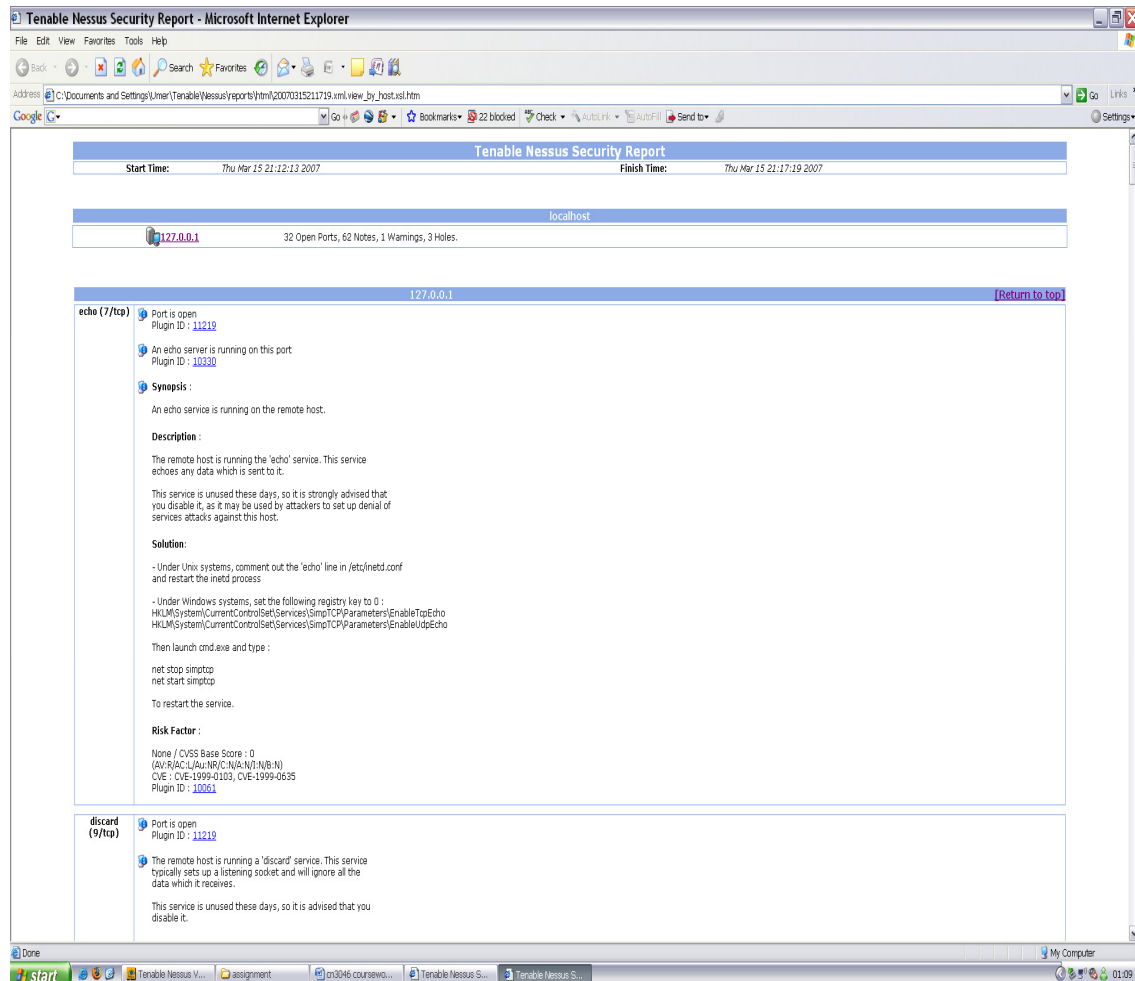
- Upon initiating a scan task a drop down menu appears containing a localhost and other addresses on a network. If an address does not appear, it can be added to the address book or typed in the field shown. IP addresses added to this field can be of a single host, a list of hosts separated by a comma, an IP range or even a network address.
- Once the host is chosen, a set of plugins can chosen, these can be enabling all plugins either including dangerous plugins or leaving them. A set of predefined policies can be used too or a new policy can be defined as well. Dangerous plugins may cause denial of service to the hosts being scanned.
- If scanning a remote host the port number can be specified and if it requires a login, username and password can be input for connectivity.
- As the scan completes, a report is generated that can be viewed later on as well.

Viewing Reports:

Reports generated can be viewed in the View Reports menu. These reports can be deleted and any two reports can be compared. Reports can be imported as well by giving the target address of the host and browsing for the file extension. See Appendix A.1.0 to see an example of the reports generated.

Figure 3.2: Generated Report appearing in Internet Explorer.

Nessus - the Vulnerability Scanner Evaluation



Interpreting Reports:

The report displays:

- The start/end time and date of the scan.
- The IP address and the Computer Name of the scanned host.
- The number of open ports, warnings and holes if any during the scan.
- Every plugin that is used brings an individual report about its security check. This may display the service or protocol it scanned, the port it used, whether it used TCP or UDP, Synopsis (brief introduction of the particular scan), Description of what the current status is, how it can be misused and what prevention can be made. It also displays the risk factor of having the particular service in its current state; high, medium or low.

4.0 Characteristics of Tenable Nessus:

Network vulnerability scanners are set to have a certain criteria, these can be encompassed within their characteristics. The following characteristics can be outlined when looking at Nessus (3):

Accuracy:

The key goal of the security tool was accuracy to measure up to the effectiveness. The features it contains to bring this effectiveness are:

1. *“Smart” receive function recv()*: the scanner caps the input at a user-specified amount rather than allow a scanned host to return data of nearly any length. This feature or function restricts the remote admin or user to interfere with the scanner by intentionally flooding the scanning machine with bogus reply data. For example when the `recv ()` function is called to read only 512bytes of data it will only read 512bytes from the scanned host.
2. *UDP and recv ()*: the same `recv ()` function is used during a time out period of the UDP session. The scanner resends the original UDP packet every second until a response is received from either ICMP unreachable or UDP response.
3. *Intrusiveness*: the scanner comes along with a Knowledge Base (KB) system that can be updated by any plugin. The scanner looks in the KB to see whether if any other plugin has found and recorded a session earlier. This helps a scanned machine from not crashing.
4. *Service Port Diffing*: the `check_port.nasl` is a dedicated plugin that examines all known open ports to notify the scan administrator if a service port is closed at the end of the scan.
5. *Safe Mode*: the `safe_check()` function, when enabled does not attempt any overflow tests that defer to a port banner check.

Speed:

Accuracy usually comes at the expense of speed; however Nessus uses protocol-specific speed enhancement. Most protocols advertise the amount of data they send, like HTTP has a Content-length field and SMB has a two byte packet length field. There is a non exhaustive list of protocols in NASL. When more NASL scripts use the same protocol the scanner almost always creates a separate protocol API.

Encapsulation: not only increases the speed of the scanner but also reduces the traffic to the remote scanned machine. The Nessus scanner achieves results from a TCP socket many times with a single session.

Examples of security checks used by NASL:

- FS/SMB: `mount()`, `umount()`, `opendir()`, `readdir()`, `read()` and `close()`
- FTP: `ftp_close()`, `ftp_recv_line()`, `ftp_get_pasv_port()`
- HTTP: `http_keepalive_send_recv()`, `http_get()`, `http_post()`, `http_recv()`
- SMTP: `smtp_send_socket()`, `smtp_send_port()`, `smtp_recv_banner()`

Stability:

The Nessus scanner has been made immune to attacks. It does this by:

- Running each script as separate process with a total time out.
- Memory share of maximum 80MB is limited to each script along with a dynamic memory allocation.
- Each host is tested in its own individual process
- Every network loop has a counter
- It utilizes cryptographic “signing” of scripts
- Protocol sanity checks for remote servers to check for header information.
- Decreasing False Positive: the scanner makes best guesses regarding the scanned operating system and relevant security data for network-based fingerprinting.

5.0 Vulnerability Assessment Techniques:

Nessus uses a combination of different assessment techniques to achieve the desired results. The following are the type of network assessment methods used (4):

- **Active Assessments:** any assessment invoking placing packets on the wire to interrogate a host for unknown services or vulnerabilities is known as an active assessment regardless the fact that the scan is sending one ICMP packet or a fully fledged DOS attack.
- **Passive Assessments:** are referred to as any activity that defines sniffing network traffic to deduce a list of active services, applications, or even vulnerabilities. For example knowing which IP address is active or not on a DHCP network.
- **Host-Based Assessments:** a patch level or configuration level check that can be performed by any type of a security check through a command line or API of a given system is considered to be form of host-based assessment.

Blended Assessment by Nessus: Nessus adopts to a combination of all three assessments techniques as each has advantages and disadvantages on its own.

6.0 Web Application Security Support:

Nessus allows scheduling and reporting on scans in an automated and distributed fashion by detecting the application layer flaws with the HTTP applications that use the web services. This is done through source code audits to find security holes.

It is important to find a security flaw as an attacker that has gained access to a web server may be able to modify or fabricate content over the web.

Nessus checks for flaws by going through all the web/CGI vulnerabilities. It uses the webmirror.nasl that stores in the KB with all known active scripts and forms.

Protecting against SQL Injection: Sql_injection.nasl takes the output from the webmirror.nasl and queries the web server using an invalid SQL statement. Nessus then waits from the reply from the web server and flags the errors.

Nessus can be set to scan every day to find the obvious flaws with an application as manual scan be tedious (5).

7.0 Nessus and Anti-viruses:

Nessus uses plugins dedicated to find and report on antivirus configurations on remote systems. It uses a GPL denoted plugin that is available to the general public.

There are different plugins for different antivirus companies like Symantec's Norton and McAfee's Antivirus. It uses "antivirus_installed.nasl" to check the Nessus KB to see if any of the common antivirus products have been installed, this plugin is however not available to general public.

If an organization likes to extend the functionality of its plugin it is trivial with NASL as Nessus KB allows companies to write custom plugins which only query the KB during a scan. There would be simple checks for this customisation (6):

- KB to be checked to see if the host resides in domain X

- KB to be checked to see if the Antivirus Y is installed
- KB to be checked to see the version of Antivirus Y
- Present report on hosts which are within the domain and are either not running antivirus or running an older version of antivirus signatures.

8.0 Detecting Wireless Access Points:

Nessus uses ID#11026 plugin for access point detection. The four techniques it uses for identifying the presence of a WAP are (7):

1. **NMAP TCP/IP fingerprinting:** it performs a wide variety of network discovery and service enumeration techniques along with determining the remote operating system based on specific responses from specific TCP/IP probes.
2. **HTTP fingerprinting:** there is a web based configuration screen with almost all WAP in market today. There are many items on the screen that can be used to look for a 'unique' fingerprint, the best search could be for the 'wireless' keyword while searching on a returned webpage.
3. **FTP fingerprinting:** some devices have FTP servers added by vendors for uploading new firmware images when upgrading the WAP device. The way it works is that a banner is returned by the FTP service running on the WAP determining the devices ID.
4. **SNMP fingerprinting:** it uses the plugin #11026 to attempt to probe the SNMP service for the "sysDesc" value if the SNMP port is open and the SNMP community string is known. The plugin contains a list of six common access points that can be recognized.

These plugins or checks are attempted in series and if one succeeds the remaining checks do not execute.

9.0 Assessing Nessus:

After installing and running the scanner an evaluation can be made about its strengths, weaknesses, ease of use, installation, configuration, updates and support. In this section assessment will be based on Nessus 3.0 for Windows System. This scanner is a free download; therefore all plugins might not be tested. The assessment is based on the limited functionality of this scanner that might be reduced if compared to the Direct Feed or procured copy of the scanner.

Installation:

Nessus is very easy to install, its installation simplicity is like any other software wizard running on windows for installation. The activation code emailed after a simple registration before download. The server is not busy resulting in quick download from the Nessus download webpage.

Ease of Use and Configuration:

Any person with little knowledge of using and maintaining networks or computers can start the scans, view, interpret, compare and import reports. To manage and define policies, however I think the administrator should know how services run and can be controlled, when customizing configurations. It is easy to use the software even at intermediate complexity of giving port or IP address ranges but when it comes to managing FTP and SMTP accounts, credentials and Compliances with other Windows and UNIX policies an administrator must have some experienced know how of how these services run.

Strengths:

- The scanning does not involve network management tools therefore it bring accurate information about the services running and ports that are active.
- A report can be generated when ever requested.
- Customized policies can be set to match requirements.
- There is comparison available therefore a report generated earlier can be compared to a report generated after recommended protection has been applied. This makes an administrator confident about risk factors and holes.
- The new functions and plugins added make Nessus 3.0 more reliable and fast compared to old versions.

Weaknesses:

- Being closed source now, all updates cannot be received for free.
- Some plugins make the scanned host end up with a denial of service attack. This might be because of the algorithm used to work with the ICMP protocol to ping the scanned host.
- It uses harmful procedures to test like brute force in some cases to test the strength of the accounts in the scanned, a network or host not properly configured for scans might end up in loss resources.
- When used with VMWare on same machine, the scan is very slow on a virtual host compared to scan on remote machine.

Support:

There are blogs and forums both official and those maintained by professionals using the scanning tool. For this coursework, I did not find them as useful, however an administrator working with a larger network at a deeper level might find it very useful as people come up with queries, one can learn from. I think the feedback exchanged makes it worth visiting. Tenable Security provides help and support for all registered software as well.

Updates:




The scanner lets you know how many days have passed since the plugins were updated. The updates are received directly from the Tenable Network Security Server with very slight effort, rather a few clicks and a few minutes to spare, depending on how long the plugins have not been updated.


9.0 Conclusion:



Nessus has gained great popularity and even if it is now mostly closed source for the latest plugins it is not losing its ground by running on systems around the world. Most of the white papers and documentation about the tool is being updated regularly setting a very aggressive attitude towards progress by the Tenable and other professionals that have invested their skills and other resources in surviving this security tool. I think its ease of use and providing solution for vulnerabilities are one of the greatest factors for its popularity among the thousands of machines that are relying on its vulnerability checks.

Appendix:

A.1.0 Sample of a report generated by the Nessus Vulnerability Scanner:

Tenable Nessus Security Report	
Start Time: Thu Mar 15 21:12:13 2007	Finish Time: Thu Mar 15 21:17:19 2007
localhost	
 127.0.0.1	32 Open Ports, 62 Notes, 1 Warnings, 3 Holes.
127.0.0.1 [Return to top]	
echo (7/tcp)	 Port is open Plugin ID : 11219  An echo server is running on this port Plugin ID : 10330

	<p> Synopsis : An echo service is running on the remote host.</p> <p>Description : The remote host is running the 'echo' service. This service echoes any data which is sent to it.</p> <p>This service is unused these days, so it is strongly advised that you disable it, as it may be used by attackers to set up denial of services attacks against this host.</p> <p>Solution:</p> <ul style="list-style-type: none">- Under Unix systems, comment out the 'echo' line in /etc/inetd.conf and restart the inetd process- Under Windows systems, set the following registry key to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpEcho HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpEcho <p>Then launch cmd.exe and type :</p> <pre>net stop simptcp net start simptcp</pre> <p>To restart the service.</p> <p>Risk Factor : None / CVSS Base Score : 0 (AV:R/AC:L/Au:NR/C:N/A:N/I:N/B:N) CVE : CVE-1999-0103, CVE-1999-0635 Plugin ID : 10061</p>
--	---

discard (9/tcp)	<p> Port is open Plugin ID : 11219</p> <p> The remote host is running a 'discard' service. This service typically sets up a listening socket and will ignore all the data which it receives.</p> <p>This service is unused these days, so it is advised that you disable it.</p> <p>Solution:</p> <ul style="list-style-type: none">- Under Unix systems, comment out the 'discard' line in /etc/inetd.conf and restart the inetd process- Under Windows systems, set the following registry key to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDiscard <p>Then launch cmd.exe and type :</p> <pre>net stop simptcp net start simptcp</pre> <p>To restart the service.</p> <p>Risk Factor : Low CVE : CVE-1999-0636 Plugin ID : 11367</p>
------------------------	--

References:

1. Nessus Network Auditing: by Jay Beale, Renaud Deraison, Haroon Meer, Roelof Temmingh, Charl Van Der Walt. Publisher: Syngress, Publication Date: September 2004, ISBN: 1-931836-08-6.
2. About Nessus: <http://www.nessus.org/about/>
3. Reliability and uniqueness of Tenable Nessus Technology; White Paper. Publication Date: February 7, 2007, (original paper first released in 2002), proprietary Information of Tenable Networks Security, Inc.
4. Blended Security Assessments; Combining Active, Passive and Host Assessments Techniques; White Paper. By Renaud Deraison and Ron Gula. Publication Date: February 7, 2007 (Revision 8)

5. Web Application Security Testing with the security center and Nessus; White Paper. By Stephen Schwig and John Lampe. Publication Date: January 2, 2004 (Updated February 7, 2007).
6. Tenable tools for security compliance – the antivirus challenge; White Paper. By Nicolas Pouvesle and John Lampe. Publication Date: January 20, 2005 (updated February 7, 2007).
7. Using Nessus to Detect Wireless Access Points; White Paper. By Renaud Deraison and Ron Gula. Publication Date: May 5, 2003 (updated February, 2007)

Bibliography:

1. Top 100 Network Security Tools. <http://sectools.org/>.
2. Introduction to Nessus by Harry Anderson. Dated: 28-3-2003. <http://www.securityfocus.com/infocus/1741>
3. Nessus 3.0 Installation Guide, Dated: March, 30 2007 (Revision 32), by Tenable Network Security.
4. Nessus 3.0 Advanced User Guide, Dated: February, 5 2007 (Revision 8), by Tenable Network Security.
5. Nessus, Snort, & Ethereal Power Tools: Customizing Open Source Security Applications. Author: Brian Caswell, Gilbert Ramirez, Jay Beale, Noam Rathaus, Neil Archibald. ISBN: 1597490202.
6. Official Nessus Blog: <http://blog.tenablesecurity.com/>

Nessus - the Vulnerability Scanner Evaluation

7. Nessus Technical Guide:
http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1159345,00.html
8. Nessus Vulnerability Scanner: by Tony Bradley.
<http://netsecurity.about.com/cs/toolsutilities/p/aapf100403.htm>
9. Nessus closes source => How to help open source projects From: Fyodor. Date: Wed, 5 Oct 2005. <http://seclists.org/nmap-hackers/2005/0015.html>
10. Sensitive data discovery capabilities for Nessus 3, Posted on 29 March 2007.
<http://www.net-security.org/secworld.php?id=4950>
11. Nessus Tutorial: Using the open source vulnerability scanning tool, by Mike Chapple. Dated: 04.05.2007.
http://searchsecuritychannel.techtarget.com/tip/0,289483,sid97_gci1236162,00.html