What is New in Nessus® v5.0?

For network security practitioners who routinely assess complex, enterprise networks for security and compliance issues, Nessus® v5.0 is the latest release of the industry's most widely-deployed vulnerability and configuration assessment product. Nessus reports are the industry's de facto standard, recognized by security professionals, network penetration testing teams, and auditors alike. Powered by Nessus' continuously-updated library of nearly 50,000 individual vulnerability and configuration checks, Nessus delivers the highest possible accuracy in the marketplace.

Nessus 5.0 introduces many important features and improvements that streamline and optimize each of the four major phases of the vulnerability scanning process.

- Enhanced report customization and creation for improved communication with all parts of the organization
- New data visualization provides immediate insight into scan results for improved efficiency
- Improved scan policy creation and design for more targeted scans
- Simplified installation and management for enhanced usability

Nessus 5.0 key features and improvements are described below. View a video overview of the new features. Log into the Tenable Support Portal to upgrade to Nessus 5.0 today.

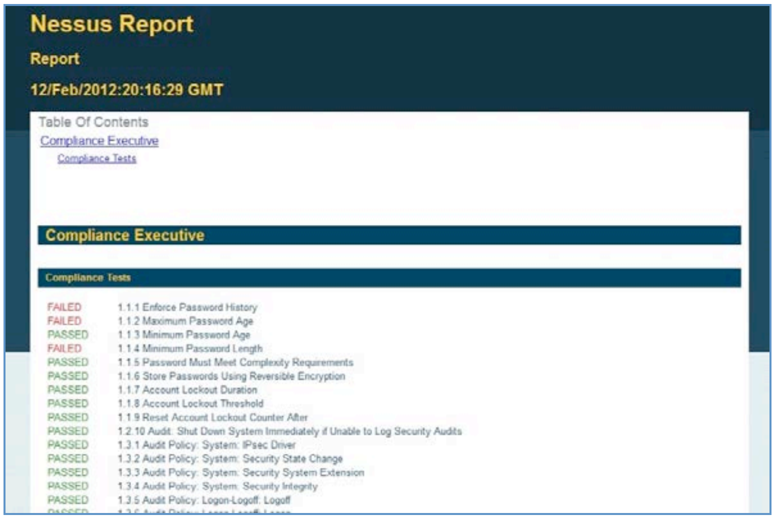
Report Customization and Creation

Multiple results filters, results management, and new pre-configured reports allow Nessus 5.0 users to produce targeted reports tailored to fit the needs/interests of their specific audience. Nessus 5.0 also gives users the ability to combine multiple report templates into a single, comprehensive report, which can be delivered in a variety of formats, including PDF.

- Results filtering and report creation: Results filtering and report creation is more flexible than ever before. Users can apply multiple result filtering criteria, and targeted reports can be generated against the filtered results.
  - Create reports that contain only exploitable vulnerabilities, multiple risk levels (e.g., only show critical and high risk findings), filter on CVE or Bugtraq ID, plugin name, and more!

- Reports customized by audience: Reports can be customized for executives, systems administrators, or auditors. A user can exclude particular vulnerabilities from a report before it is generated, allowing delivery of results targeted to specific audiences.
  - Example: During an internal scan, Nessus will report that a DNS server allows recursive queries, which is its function on the internal network. As this is a known condition, a user can suppress this result in the generated report to keep focus on true vulnerabilities.
  - With four new pre-configured report formats — Compliance Check, Compliance Check (Executive), Vulnerabilities by Host, and Vulnerabilities by Plugin — users can quickly create reports by chapters.
    - Example: The company's compliance policy dictates that passwords be greater than ten characters in length. Nessus v5.0 runs a scan against the baseline, and the Compliance Check (Executive) report shows a pass/fail result to indicate if all hosts on the network are compliant with the minimum password length. With

pass/fail results, the Compliance Check (Executive) report provides a quick snapshot of the company’s compliance checklist status.



Nessus Report

Report

12/Feb/2012:20:16:29 GMT

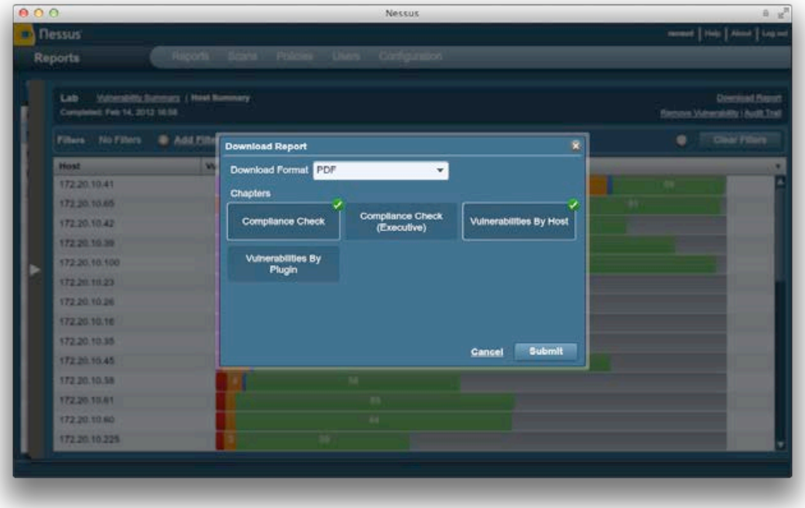
Compliance Executive

Compliance Tests

FAILED	1.1.1 Enforce Password History
FAILED	1.1.2 Maximum Password Age
PASSED	1.1.3 Minimum Password Age
FAILED	1.1.4 Minimum Password Length
PASSED	1.1.5 Password Must Meet Complexity Requirements
PASSED	1.1.6 Store Passwords Using Reversible Encryption
PASSED	1.1.7 Account Lockout Duration
PASSED	1.1.8 Account Lockout Threshold
PASSED	1.1.9 Reset Account Lockout Counter After
PASSED	1.2.10 Audit: Shut Down System Immediately if Unable to Log Security Audits
PASSED	1.3.1 Audit Policy: System: IPsec Driver
PASSED	1.3.2 Audit Policy: System: Security State Change
PASSED	1.3.3 Audit Policy: System: Security System Extension
PASSED	1.3.4 Audit Policy: System: Security Integrity
PASSED	1.3.5 Audit Policy: Logon-Logoff: Logoff
PASSED	1.3.6 Audit Policy: Logon-Logoff: Logon

Nessus 5.0 Compliance Check (Executive) Report

- Report formats: Reports can be generated in native Nessus formats, HTML, and now PDF formats (requires Oracle Java be installed on the Nessus server).
  - The new PDF report format makes it easier to share reports.



Download Report

Download Format: PDF

Chapters

☑ Compliance Check
□ Compliance Check (Executive)
☑ Vulnerabilities By Host
□ Vulnerabilities By Plugin

Nessus 5.0 PDF Report Format

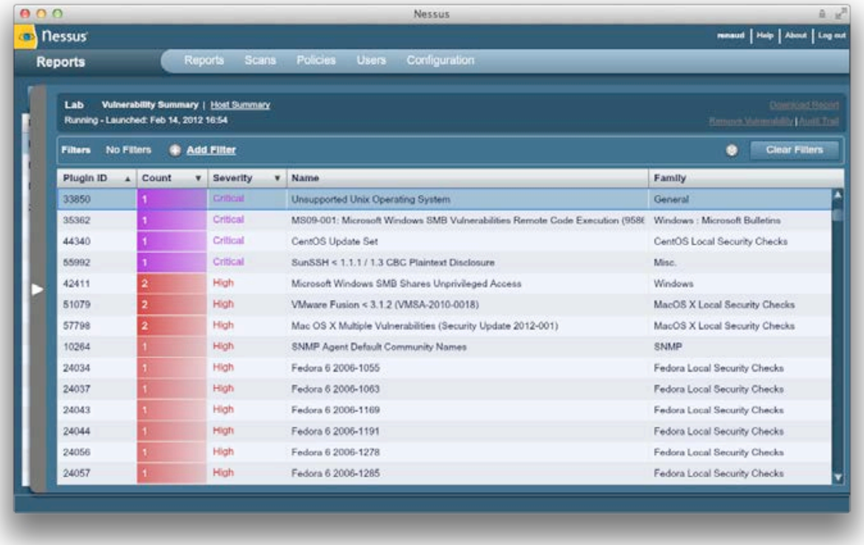
- Combined reports: Multiple report templates can be combined into one report.
  - A single report can now contain vulnerabilities sorted by host and by IP address/hostname.

Scan Execution

Powerful new Nessus 5.0 features allow customers to take advantage of real-time scan results, with on-the-fly filtering and sorting, and streamlined results navigation.

- New criticality level: Nessus v5.0 now has five severity levels — Informational, Low Risk, Medium Risk, High Risk, and Critical Risk. The Informational level quickly identifies non-vulnerability information (“nice to know”) and separates it from the vulnerability detail (“need to know”).
    - Example: A user may want to run a query against all hosts running web servers not on the normal http or https ports, port 80 or port 443. The Informational level allows a user to quickly identify information that may be useful, but does not require immediate attention — keeping the focus on the actionable results.

- New vulnerability summary: A new vulnerability summary and redesigned host summary make it easy to see risk level without even running a report.

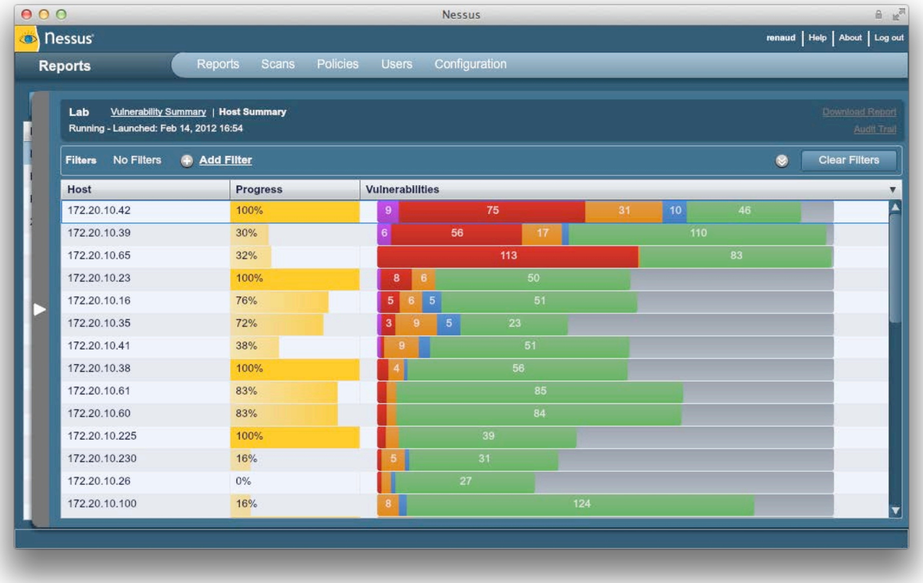

Nessus
Nessus
renaud | Help | About | Log out
Reports
Reports Scans Policies Users Configuration
Download Report
Remove Vulnerability | Audit Trail
Clear Filters

Lab Vulnerability Summary | Host Summary
Running - Launched: Feb 14, 2012 16:54

Filters No Filters Add Filter

Plugin ID ▲	Count ▼	Severity ▼	Name	Family
33850	1	Critical	Unsupported Unix Operating System	General
35362	1	Critical	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958(	Windows : Microsoft Bulletins
44340	1	Critical	CentOS Update Set	CentOS Local Security Checks
55992	1	Critical	SunSSH < 1.1.1 / 1.3 CBC Plaintext Disclosure	Misc.
42411	2	High	Microsoft Windows SMB Shares Unprivileged Access	Windows
51079	2	High	VMware Fusion < 3.1.2 (VMSA-2010-0018)	MacOS X Local Security Checks
57798	2	High	Mac OS X Multiple Vulnerabilities (Security Update 2012-001)	MacOS X Local Security Checks
10264	1	High	SNMP Agent Default Community Names	SNMP
24034	1	High	Fedora 6 2006-1055	Fedora Local Security Checks
24037	1	High	Fedora 6 2006-1063	Fedora Local Security Checks
24043	1	High	Fedora 6 2006-1169	Fedora Local Security Checks
24044	1	High	Fedora 6 2006-1191	Fedora Local Security Checks
24056	1	High	Fedora 6 2006-1278	Fedora Local Security Checks
24057	1	High	Fedora 6 2006-1285	Fedora Local Security Checks

Nessus 5.0 Vulnerability Summary Showing Critical and High Risks


Nessus
Nessus
renaud | Help | About | Log out
Reports
Reports Scans Policies Users Configuration
Download Report
Audit Trail
Clear Filters

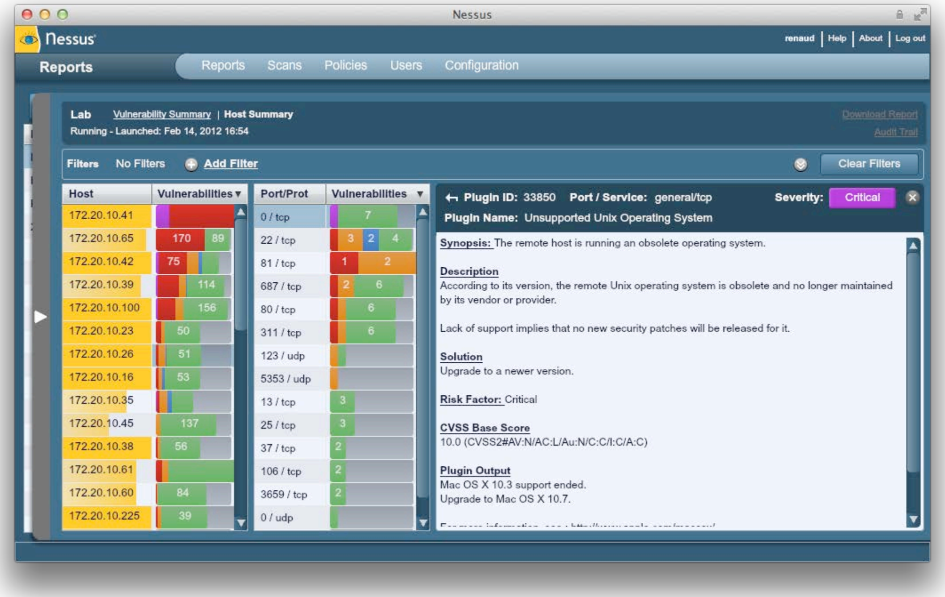
Lab Vulnerability Summary | Host Summary
Running - Launched: Feb 14, 2012 16:54

Filters No Filters Add Filter

Host	Progress	Vulnerabilities
172.20.10.42	100%	9 75 31 10 46
172.20.10.39	30%	6 56 17 110
172.20.10.65	32%	113 83
172.20.10.23	100%	8 6 50
172.20.10.16	76%	5 6 5 51
172.20.10.35	72%	3 9 5 23
172.20.10.41	38%	9 51
172.20.10.38	100%	4 56
172.20.10.61	83%	85
172.20.10.60	83%	84
172.20.10.225	100%	39
172.20.10.230	16%	5 31
172.20.10.26	0%	27
172.20.10.100	16%	8 124

Nessus 5.0 Host Summary with 5 Levels of Risk Severity

- Streamlined results navigation: One click to jump from a critical vulnerability to see the host(s) that is vulnerable to the details of the vulnerability.



Lab Vulnerability Summary | **Host Summary**
Running - Launched: Feb 14, 2012 16:54

Filters No Filters

Host	Vulnerabilities
172.20.10.41	
172.20.10.65	170 89
172.20.10.42	75
172.20.10.39	114
172.20.10.100	156
172.20.10.23	50
172.20.10.26	51
172.20.10.16	53
172.20.10.35	
172.20.10.45	137
172.20.10.38	56
172.20.10.61	
172.20.10.60	84
172.20.10.225	39

Port/Prot	Vulnerabilities
0 / tcp	7
22 / tcp	3 2 4
81 / tcp	1 2
687 / tcp	2 6
80 / tcp	6
311 / tcp	6
123 / udp	
5353 / udp	
13 / tcp	3
25 / tcp	3
37 / tcp	2
106 / tcp	2
3659 / tcp	2
0 / udp	

Plugin ID: 33850 **Port / Service:** general/tcp **Severity:** Critical
Plugin Name: Unsupported Unix Operating System

Synopsis: The remote host is running an obsolete operating system.

Description
According to its version, the remote Unix operating system is obsolete and no longer maintained by its vendor or provider.

Lack of support implies that no new security patches will be released for it.

Solution
Upgrade to a newer version.

Risk Factor: Critical

CVSS Base Score
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Output
Mac OS X 10.3 support ended.
Upgrade to Mac OS X 10.7.

For more information, see : http://www.apple.com/macosx/

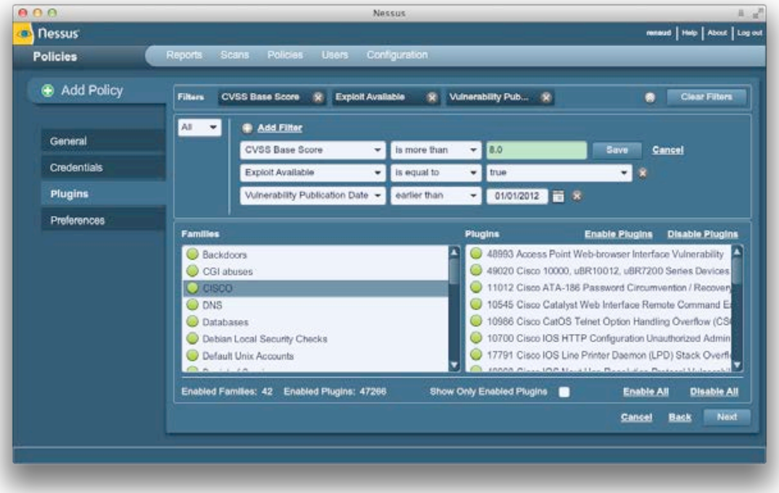
Nessus 5.0 One-click Navigation

- Take advantage of real-time results: As the scan is being run, not only can you see the results as they are being gathered, but navigate and filter on them as well. This allows you to easily act upon the vulnerability data while the scan is happening.

Scan Policy Creation and Design

Over two dozen new plugin filters make it fast and easy for security and compliance professionals to create policies for laser-focused scans. Users can easily select multiple filter criteria, such as, Vulnerability Publication Date, public vulnerability database ID (OSVDB, Bugtraq, CERT Advisory, and Secunia), Plugin type (local or remote), information assurance vulnerability alert (IAVA), and more, to quickly identify easily-exploitable vulnerabilities. For example,

- Scan for all easily remotely-exploitable vulnerabilities for which there is an exploit published in your favorite exploit framework.
- Scan for local third-party client software that is unpatched.
- Scan for systems that have been missing patches for more than a year.



All

CVSS Base Score	is more than	8.0
Exploit Available	is equal to	true
Vulnerability Publication Date	earlier than	01/01/2012

Families:
- Backdoors
- CGI abuses
- CISCO
- DNS
- Databases
- Debian Local Security Checks
- Default Unix Accounts

Plugins:
- 48993 Access Point Web-browser Interface Vulnerability
- 49020 Cisco 10000, uBR10012, uBR7200 Series Devices
- 11012 Cisco ATA-186 Password Circumvention / Recovery
- 10545 Cisco Catalyst Web Interface Remote Command E
- 10986 Cisco CatOS Telnet Option Handling Overflow (CS
- 10700 Cisco IOS HTTP Configuration Unauthorized Admin
- 17791 Cisco IOS Line Printer Daemon (LPD) Stack Overfl

Enabled Families: 42 Enabled Plugins: 47266 Show Only Enabled Plugins □

Nessus 5.0 Plugin Filtering

Policies can be configured to produce reports that are locked to prevent editing.

Installation and Management

Streamlined installation and the unified web interface with GUI configuration simplify Nessus 5.0 installation and administration.

- Installation: Nessus v5.0 has a browser-based installation wizard — no special knowledge required. Users on a wide variety of platforms — Windows, Mac, Linux, or UNIX — can have Nessus v5.0 installed within minutes.

- Configuration and management: Nessus v5.0 configuration and management is now done 100% through the GUI. No more command line text file editing, and no more Nessus Server Manager to install on Windows clients.
    - With all configuration and management now done through the web interface, the Nessus user experience is the same for all users, regardless of OS.
- With the touch of a button on the GUI, Nessus users can now quickly initiate plugin updates and see last update information.

TENABLE Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
410.872.0555
www.tenable.com