

Network Security Fundamentals

Security Training Course

Dr. Charles J. Antonelli
The University of Michigan
2013



Network Security Fundamentals

Module 8 Scanning



Topics

- Scanning fundamentals
- Nessus installation & examination

Scanning Fundamentals



Scanning

- Purpose: Examine host(s) from the network
 - What ports are open
 - What services are running
 - What flaws exist in those services
 - What type of OS is running
 - What kind of filtering is in place

Scanning

- *Modus operandi:*
 - Phase 1: determine all hosts in specified range
 - Phase 2: interrogate open ports on each host identified in Phase 1
- Uses:
 - Attack tool
 - ▼ Reconnaissance
 - Defensive tool
 - ▼ Where are the security risks?

Scanners

- Commercial
 - eEye Retina
 - ISS
 - ...
- Open source
 - Nessus
 - Nmap
 - ...

Nessus Installation and Examination



Nessus

- Was open-source, GPL
 - ... Nessus 3.0 closed-source
 - ... Nessus 4.0 plugins not free
- Client/server architecture
 - Server placed on host(s) in network
 - ▼ UNIX/Linux, AIX, Mac OS X
 - Client connects to server(s), runs test
 - ▼ Web client
- Strong authentication
 - SSL

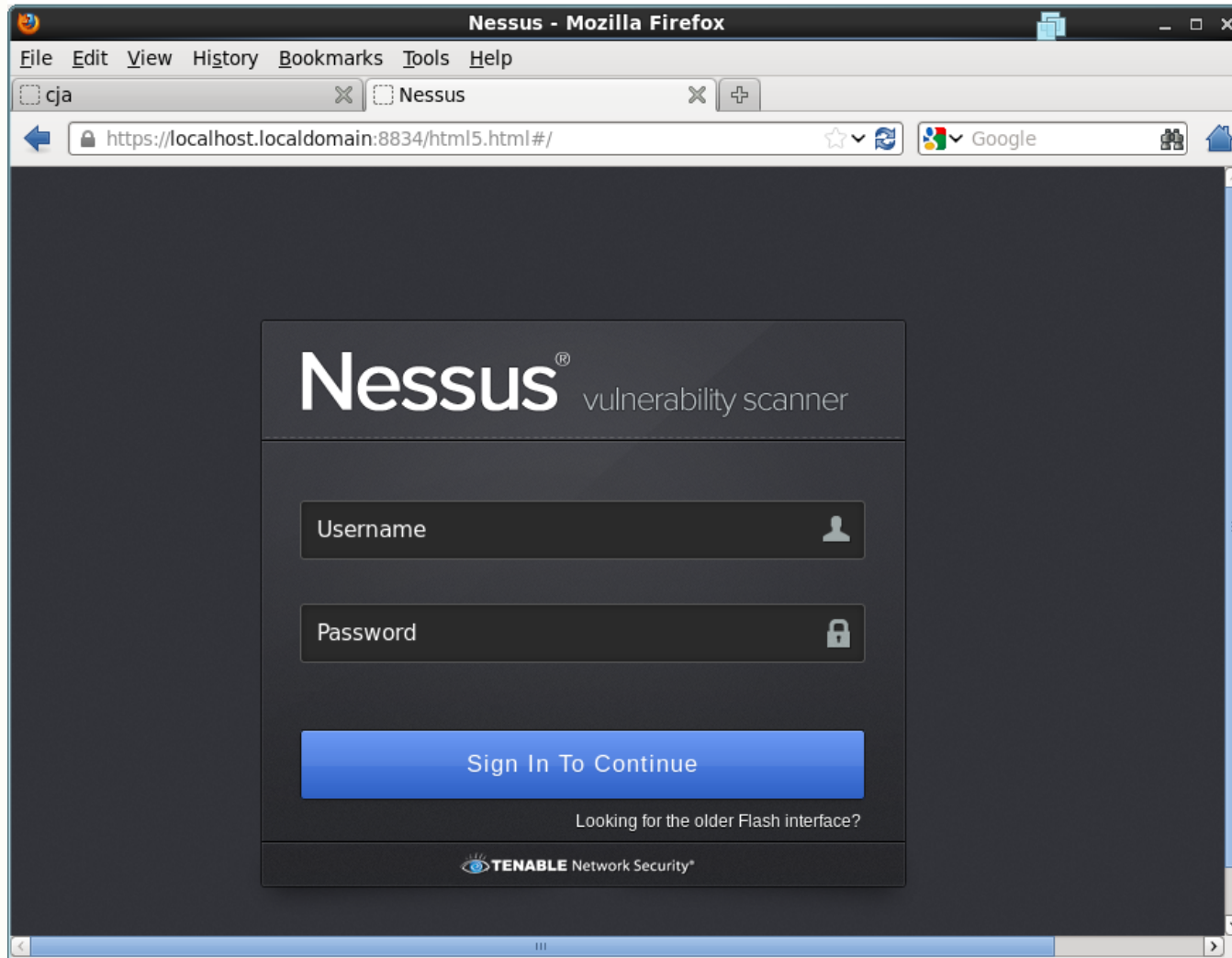
Install Nessus

- Download Nessus from <http://www.tenable.com/products/nessus>
- Register scanner
 - Nessus no longer ships with any plugins
 - HomeFeed vs. ProfessionalFeed
 - ▼ <http://www.nessus.org/register/>
- Start the nessusd server
- Browse to <https://localhost.localdomain:8834>
- Create nessusd account
- Get the plugins
 - This will consume about twenty minutes
- Nessus is pre-installed in the virtual lab environment

Run Nessus

- `sudo nessusd start`
- Browse to <https://localhost.localdomain:8834>
 - Port opened after plugins have been processed
- Understand certificate issues
- Login to nessusd account
- Add a policy: select plugins (checks to perform)
- Add a scan: select targets (networks)
- Start test!

Nessus login



Add a policy

The screenshot shows the Nessus web interface in a Mozilla Firefox browser window. The address bar displays the URL `https://localhost.localdomain:8834/html5.html#/policies`. The page title is "Listing Policies" and it includes navigation buttons for "New Policy", "Upload", "Options", and "Filter Policies".

<input type="checkbox"/>	Policy Title	Visibility	Created By
<input type="checkbox"/>	External Network Scan	shared	Tenable Policy Distribution Service
<input type="checkbox"/>	Internal Network Scan	shared	Tenable Policy Distribution Service
<input type="checkbox"/>	p1	private	nessus
<input type="checkbox"/>	Prepare for PCI-DSS audits (section 11.2.2)	shared	Tenable Policy Distribution Service
<input type="checkbox"/>	Web App Tests	shared	Tenable Policy Distribution Service

Settings

Nessus - Mozilla Firefox

File Edit View History Bookmarks Tools Help

cja x Nessus x +

https://localhost.localdomain:8834/html5.html#/policies/0/general/2

Results Scans 0 Templates Policies Users Configuration nessus Help &

General Settings

Credentials

Plugins

Preferences

Policy General Settings

Setting Type Performance

Max Checks Per Host 5

Max Hosts Per Scan 30

Network Receive Timeout (seconds) 5

Max Simultaneous TCP Sessions Per Host

Max Simultaneous TCP Sessions Per Scan

Reduce Parallel Connections on Congestion

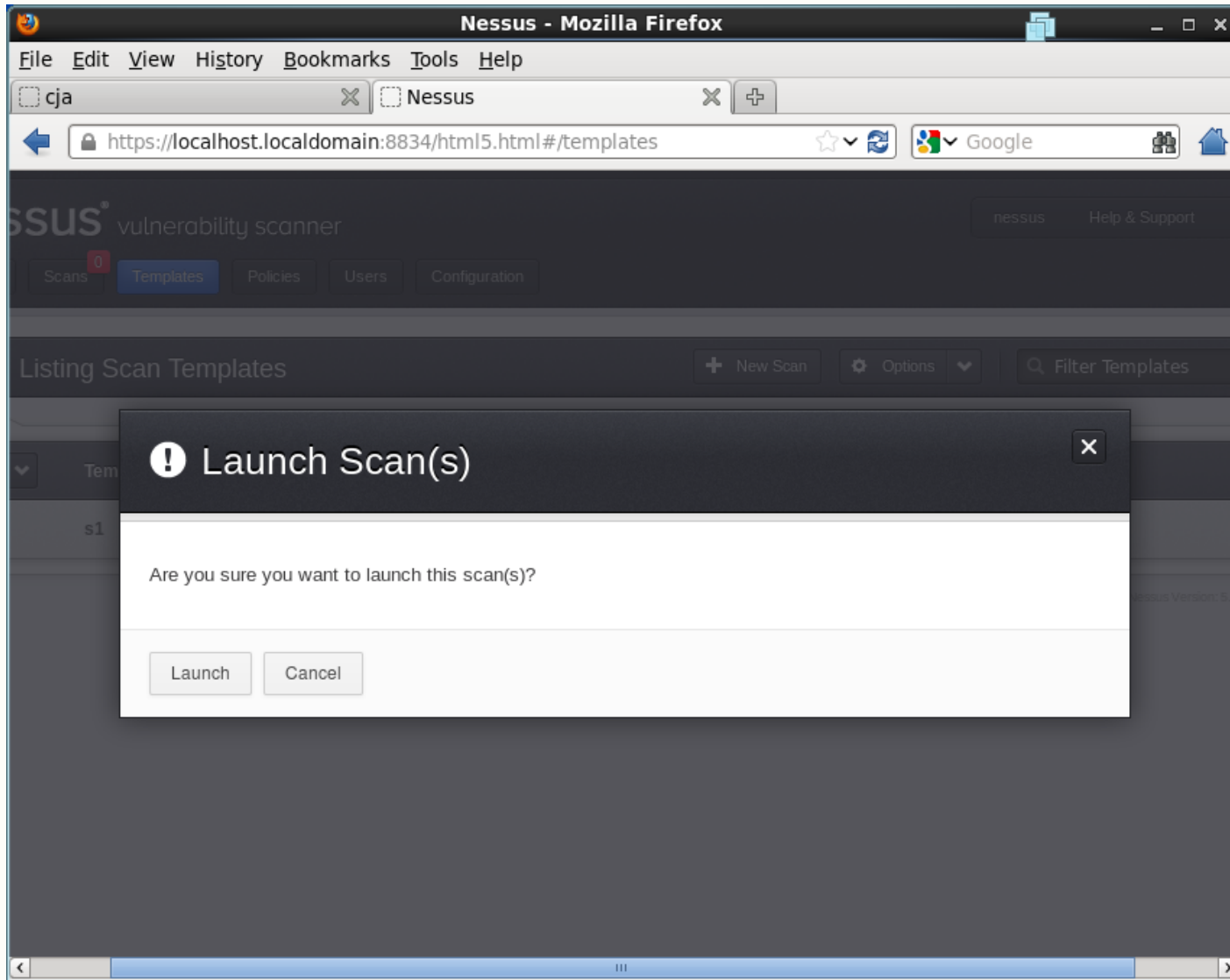
Add a scan

Listing Scans

Scan Title	Created By	Start Time	Status
s1	nessus	March 27, 2013 19:34:08	Running 0%

© 1998 - 2013 Tenable Network Security®. All Rights Reserved. Nessus Version: 5.0

Launch a scan



Running a scan

The screenshot shows the Nessus web interface in Mozilla Firefox. The browser address bar displays `https://localhost.localdomain:8834/html5.html#/scans`. The page title is "Nessus - Mozilla Firefox". The interface includes a navigation menu with "Scans" (highlighted with a red notification badge), "Templates", "Policies", "Users", and "Configuration". The main content area is titled "Listing Scans" and features a table with the following data:

Scan Title	Created By	Start Time	Status
s1	nessus	March 27, 2013 19:34:08	Running 0%

At the bottom of the page, there is a copyright notice: "© 1998 - 2013 Tenable Network Security®. All Rights Reserved. Nessus Version: 5.0".

Scan finished

The screenshot displays the Nessus web interface in a Mozilla Firefox browser window. The browser's address bar shows the URL: `https://localhost.localdomain:8834/html5.html#/results/e389811f-d1ad-f31`. The Nessus logo and navigation menu are visible at the top. The main content area is titled "s1 Hosts Summary" and shows a progress bar for "localhost" at 100% completion. A secondary progress bar below it indicates 47 items. The left sidebar contains navigation options: "Hosts" (1), "Vulnerabilities" (20), and "Export Results".

Host	Progress
localhost	100%

47

© 1998 - 2013 Tenable Network Security®. All Rights Reserved. Nessus

Examine results

- Browse report
- Three severity levels
 - Low - informational
 - Medium - possible vulnerability
 - High - verified vulnerability
- Detail pane gives descriptions, suggested fixes, CVE numbers, references and links

Scan results

The screenshot shows the Nessus web interface in a Mozilla Firefox browser. The browser address bar displays the URL: `https://localhost.localdomain:8834/html5.html#/results/e389811f-d1ad-f31`. The Nessus logo and navigation menu are visible at the top. The main content area is titled "s1 Vulnerability Summary" and features a sidebar with "Hosts" (1) and "Vulnerabilities" (20). The central panel lists several detected vulnerabilities, each with an "info" button and a category label.

Category	Vulnerability Name
Port scanners	netstat portscanner (SSH)
Service detection	Service Detection
Web Servers	HyperText Transfer Protocol (HTTP) Information
Web Servers	HTTP Server Type and Version
Web Servers	Apache Banner Linux Distribution Disclosure
General	Backported Security Patch Detection (WWW)
General	BIOS version (SSH)

Additional Features

- **Filter**
 - Select which vulnerabilities to show
 - Select by plugin, vulnerability text, host, port, protocol, severity