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

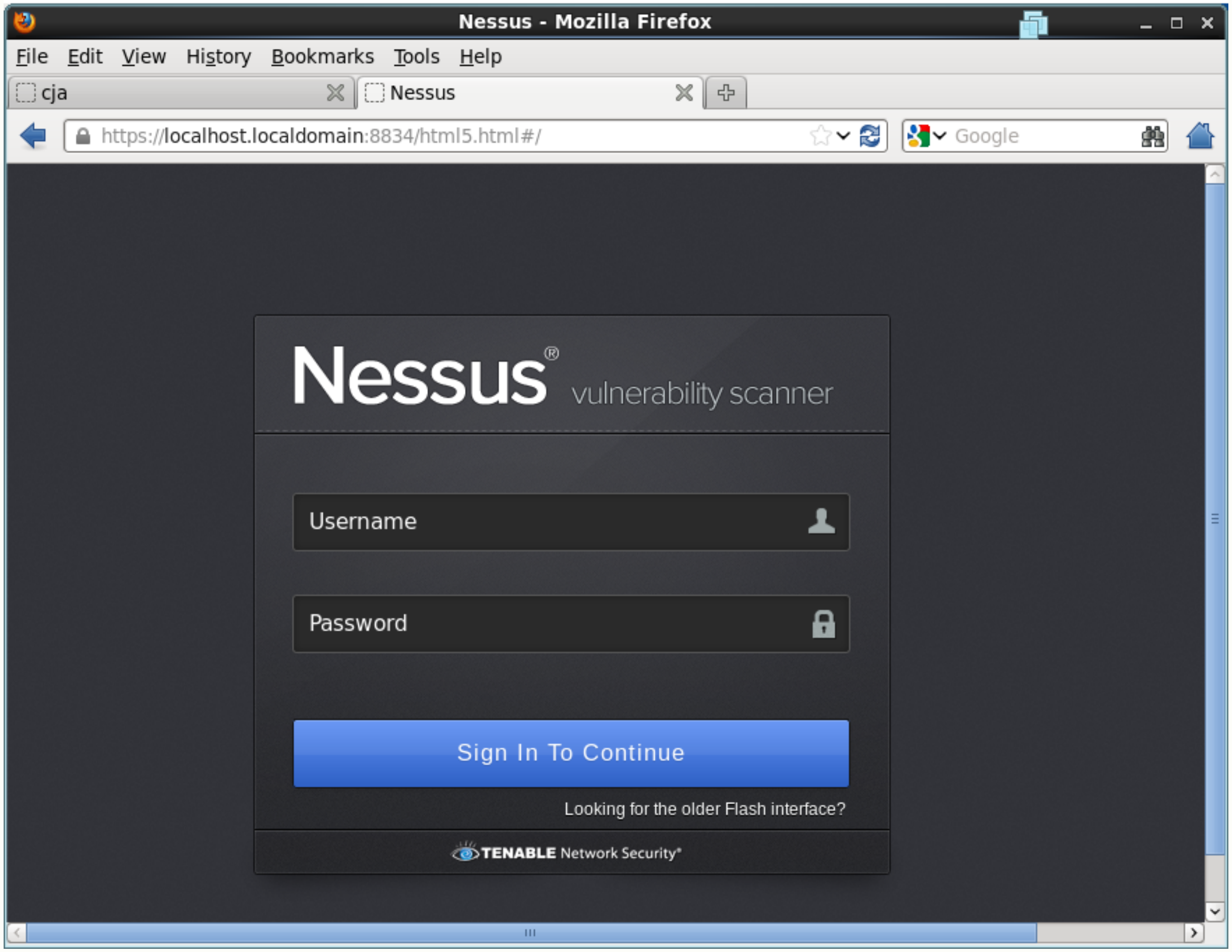
Install Nessus

- 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

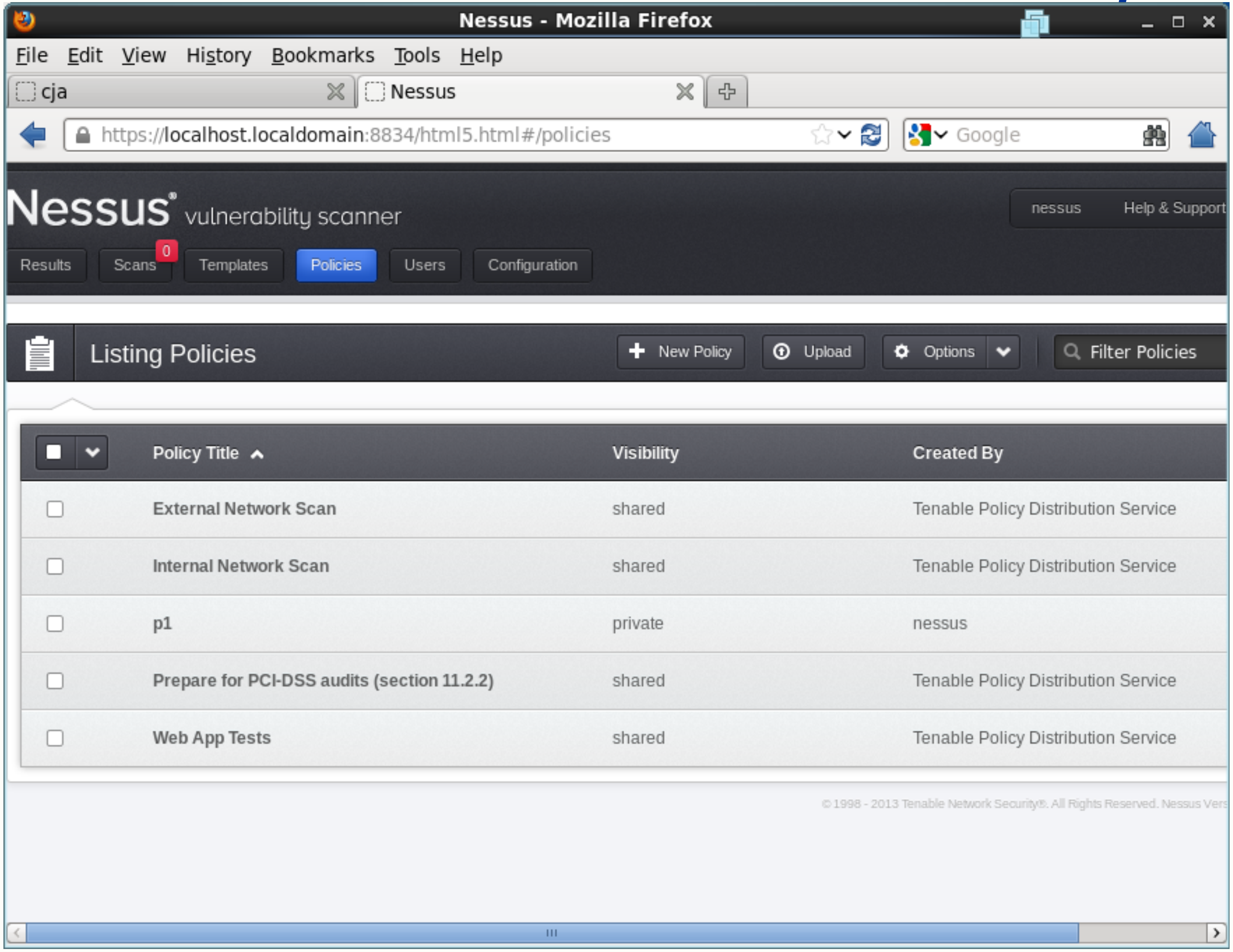
- `sudo nessusd start`
- Browse to https://localhost.localdomain:8834
  - Port opened after plugins have been processed
- Understand certificate issues
- Login to nessusd account
- Add a policy: select plugins (checks to perform)
- Add a scan: select targets (networks)
- Start test!

Nessus login



Nessus - Mozilla Firefox
File Edit View History Bookmarks Tools Help
cja
Nessus
https://localhost.localdomain:8834/html5.html#/
Google
Nessus® vulnerability scanner
Username
Password
Sign In To Continue
Looking for the older Flash interface?
TENABLE Network Security®

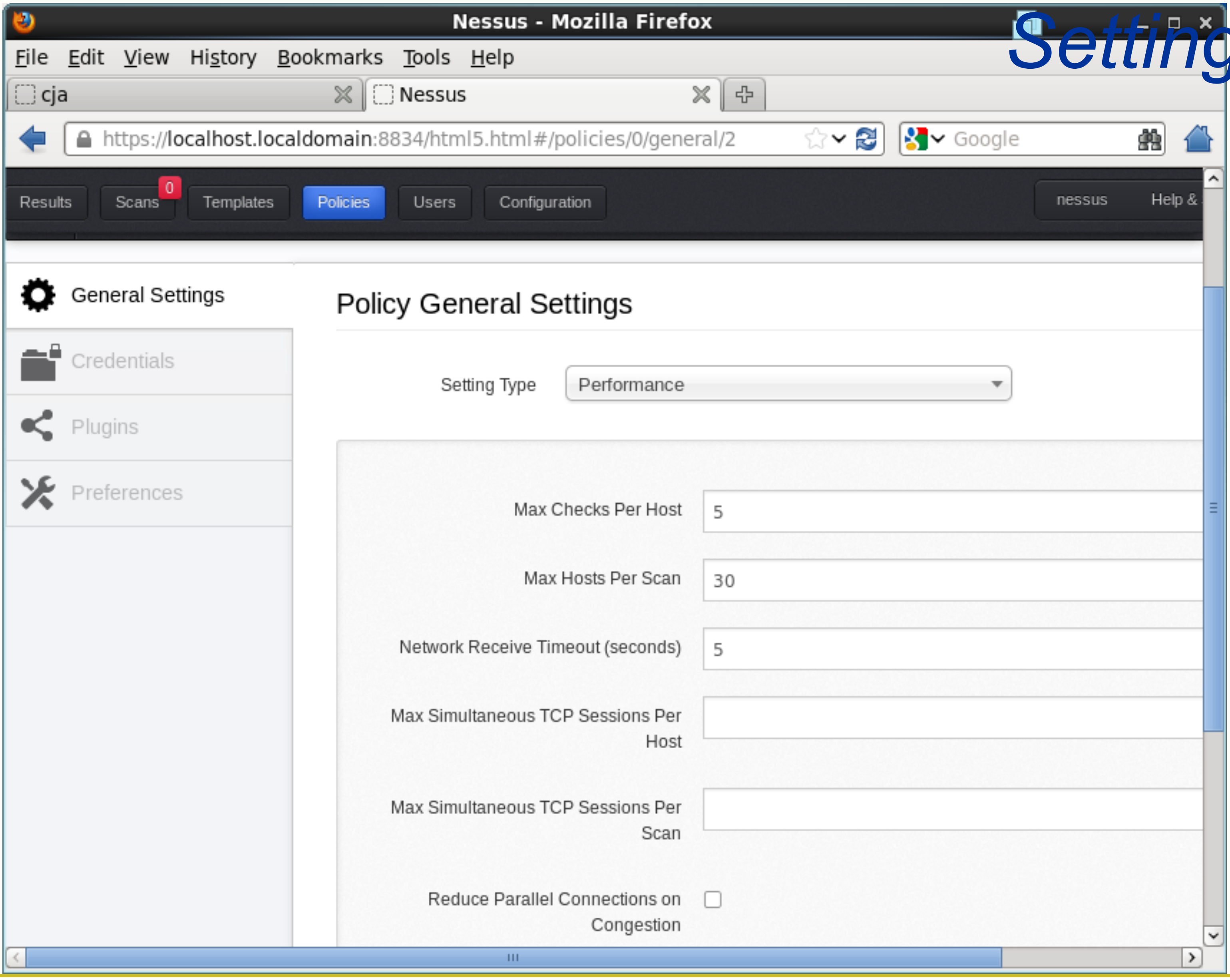
Add a policy



□	Policy Title	Visibility	Created By
□	External Network Scan	shared	Tenable Policy Distribution Service
□	Internal Network Scan	shared	Tenable Policy Distribution Service
□	p1	private	nessus
□	Prepare for PCI-DSS audits (section 11.2.2)	shared	Tenable Policy Distribution Service
□	Web App Tests	shared	Tenable Policy Distribution Service

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

Settings



Policy General Settings

Setting Type: Performance

Max Checks Per Host: 5

Max Hosts Per Scan: 30

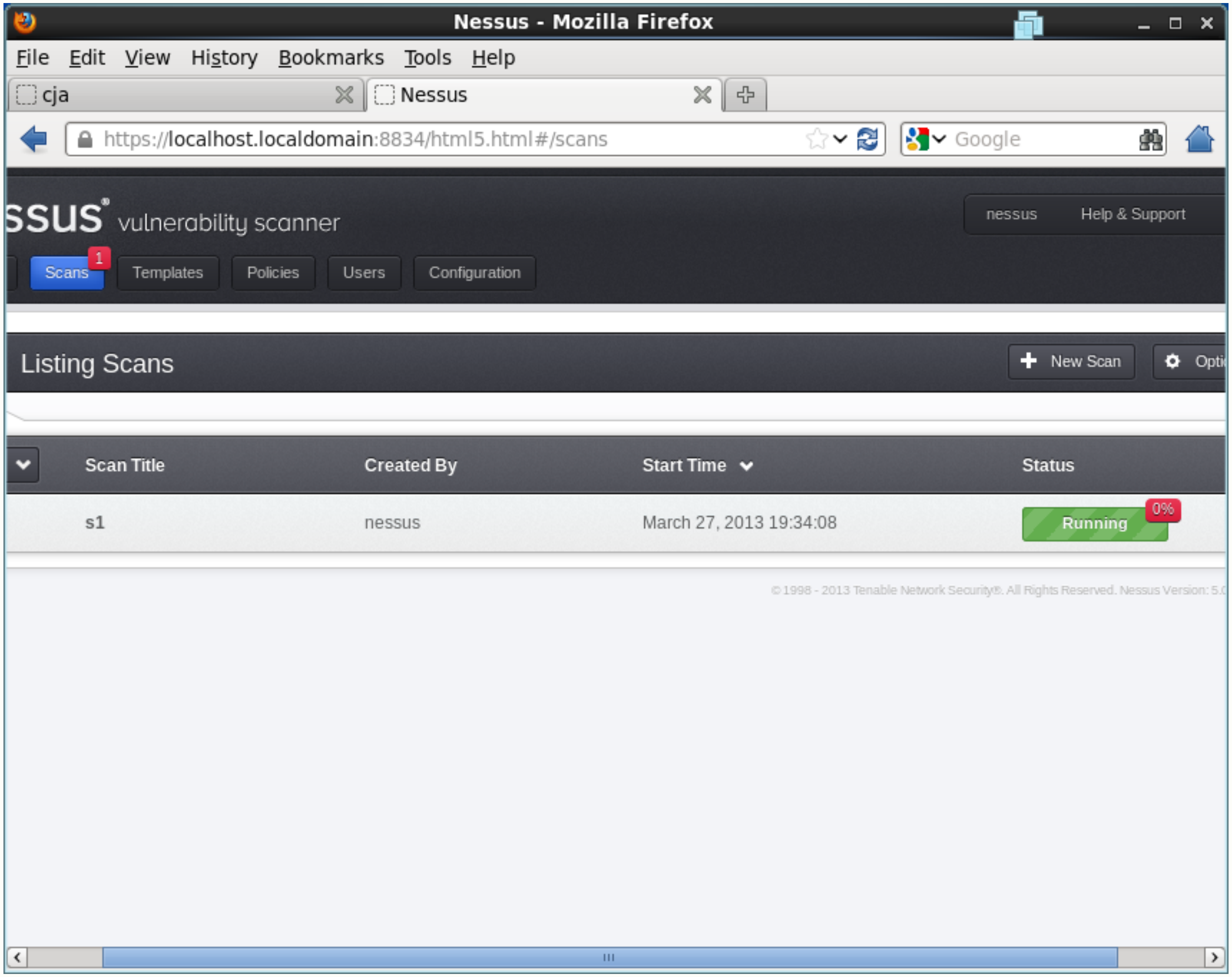
Network Receive Timeout (seconds): 5

Max Simultaneous TCP Sessions Per Host:

Max Simultaneous TCP Sessions Per Scan:

Reduce Parallel Connections on Congestion ☐

Add a scan

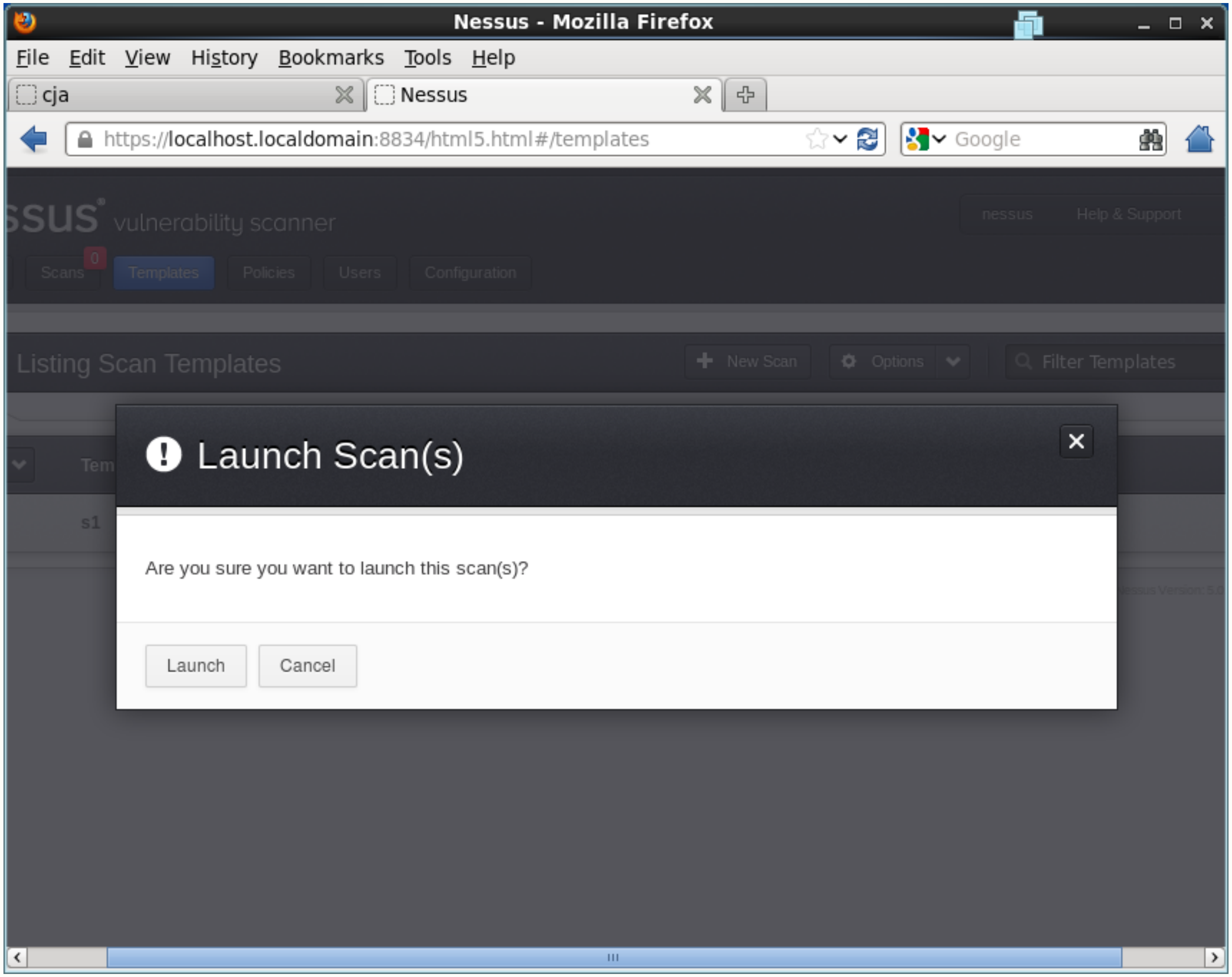

Nessus - Mozilla Firefox
File Edit View History Bookmarks Tools Help
cja
Nessus
https://localhost.localdomain:8834/html5.html#/scans
Google
ssus® vulnerability scanner
nessus
Help & Support
Scans 1
Templates
Policies
Users
Configuration
New Scan
Opti

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

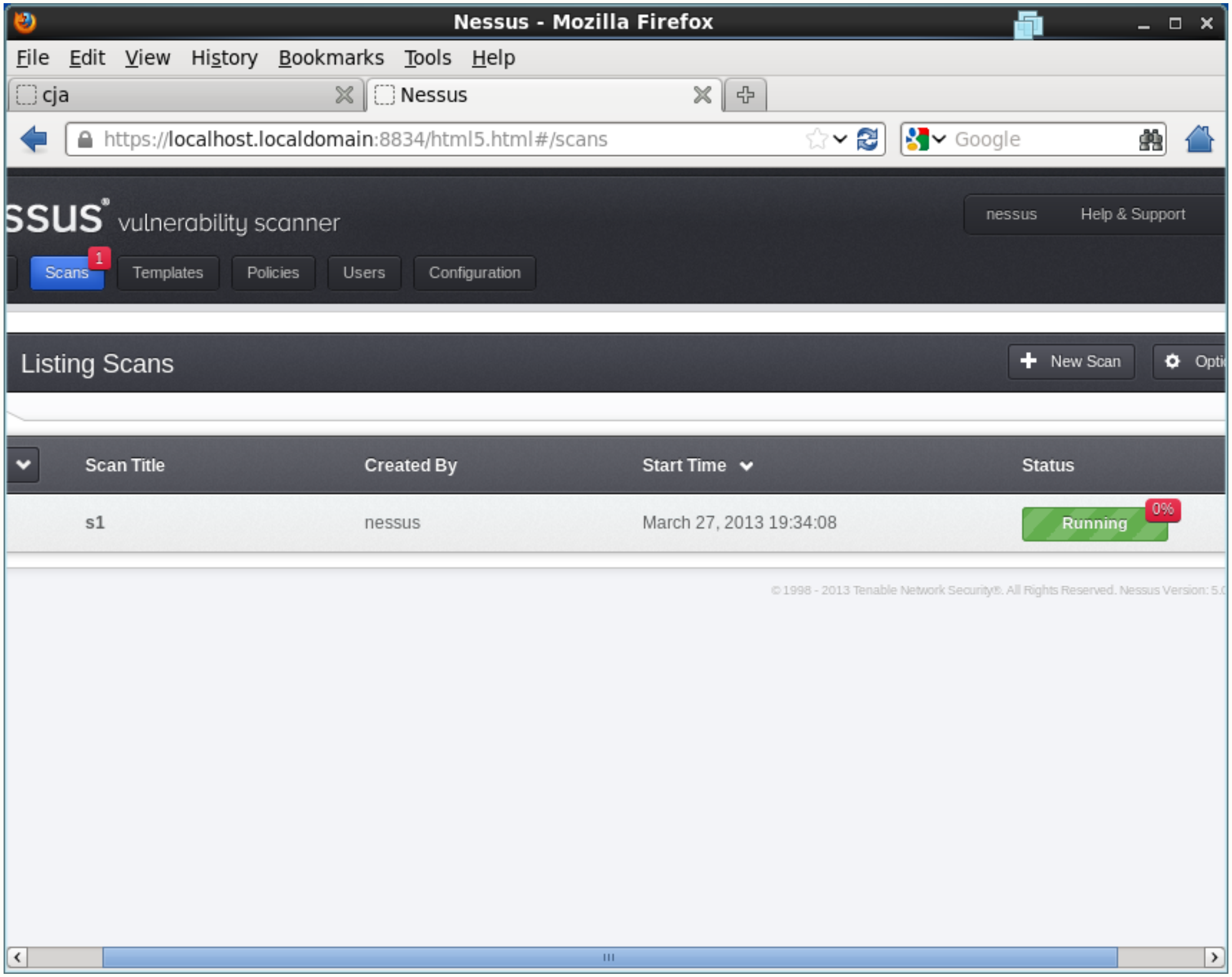
Launch a scan



https://localhost.localdomain:8834/html5.html#/templates

Are you sure you want to launch this scan(s)?

Running a scan

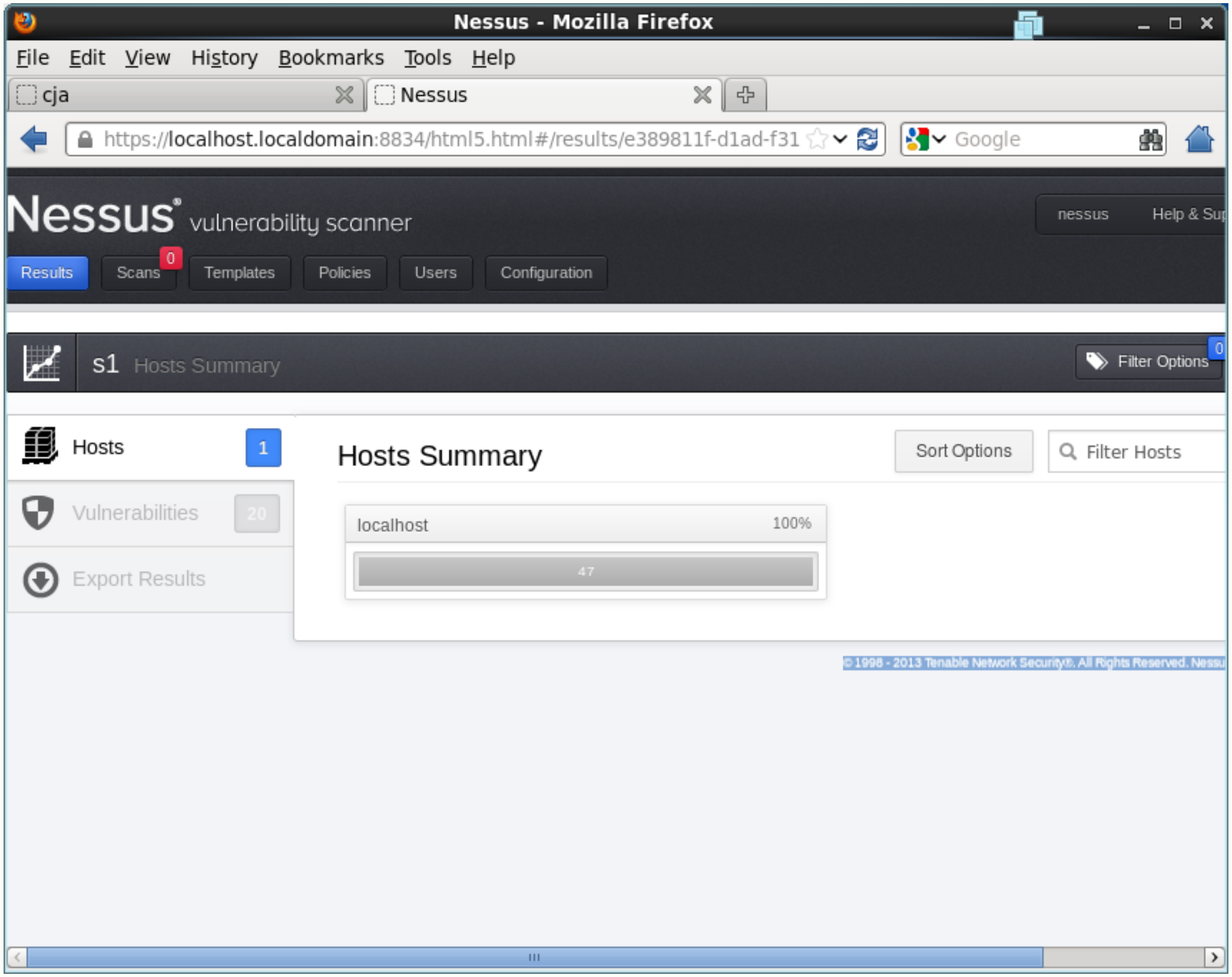


https://localhost.localdomain:8834/html5.html#/scans

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

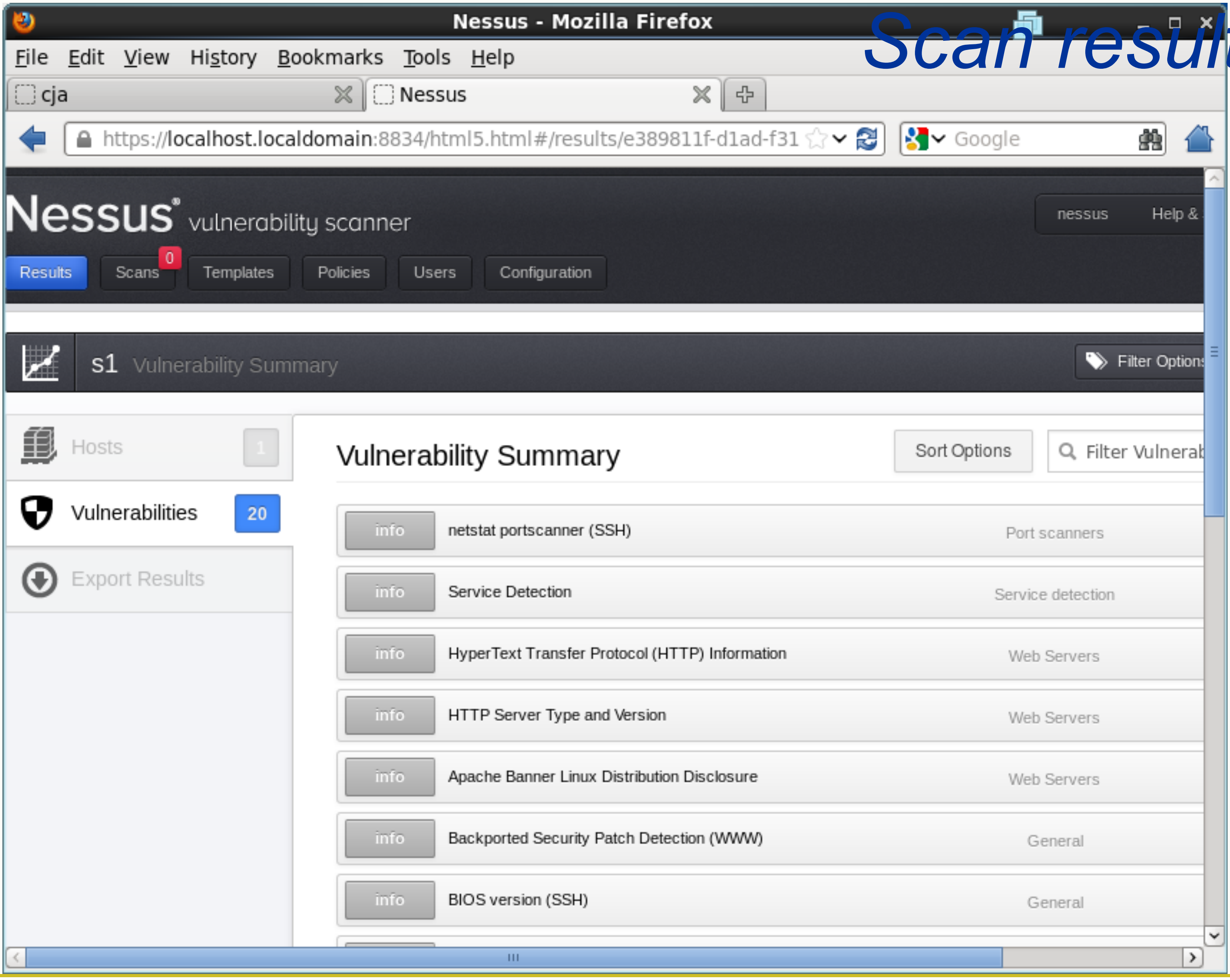
Scan finished



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



Vulnerability Summary

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

Additional Features

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