BCNET

Shared IT Services for Higher Education & Research

Conference 2018

# Nessus Vulnerability Scan for Institutions

Hugh Burley, George Jones, Ivor MacKay, and Rossilyne Tan

# Speakers:

George Jones, Director, Technology Services and Chief Information Officer

Justice Institute of British Columbia

Hugh Burley, Manager of Information Security/Information Security Officer

Thompson Rivers University/BCNET

Rossilyne Tan, Systems Analyst

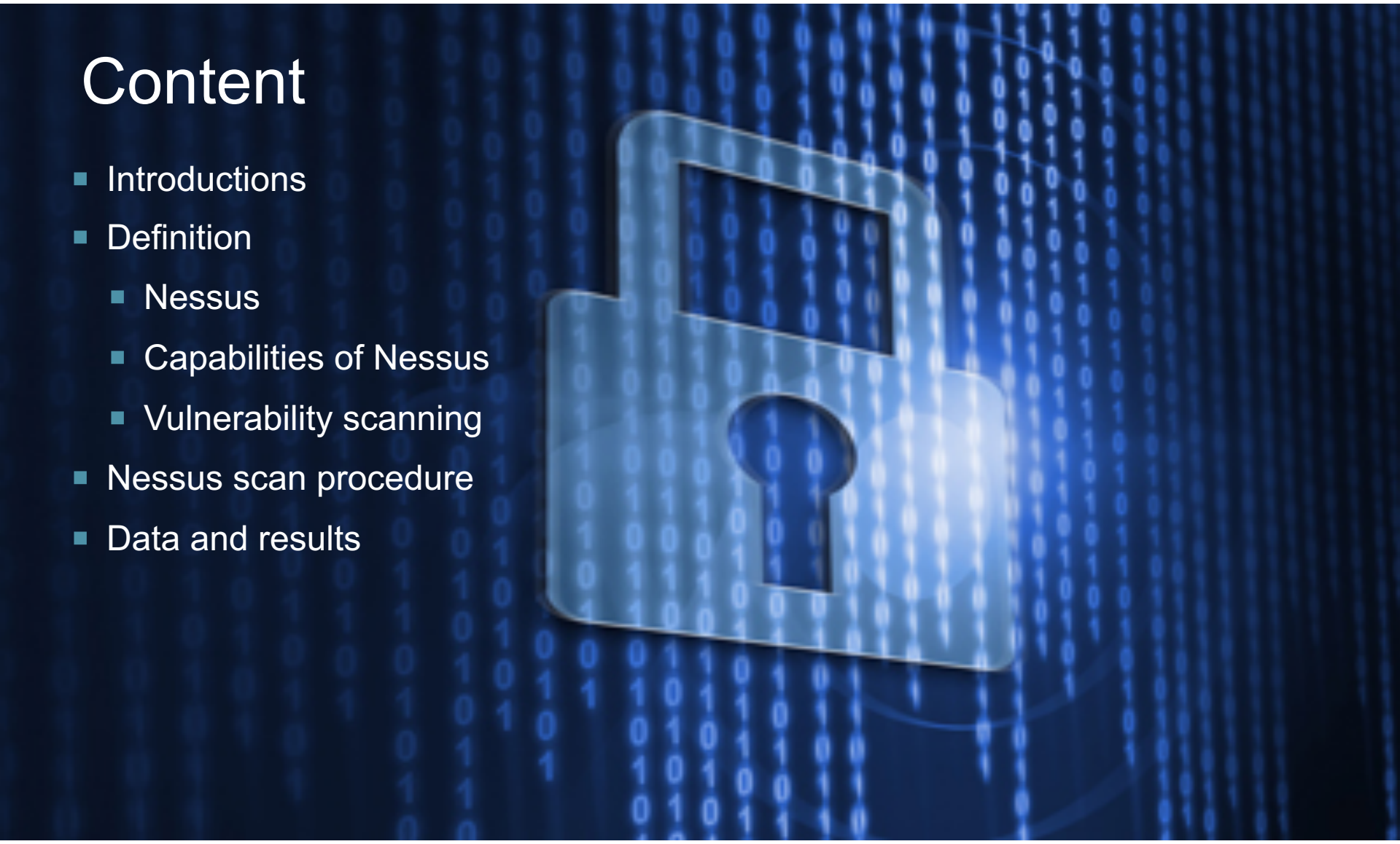
BCNET

Ivor MacKay, Manager, Information Technology

BCNET

# Content

- Introductions
- Definition
  - Nessus
  - Capabilities of Nessus
  - Vulnerability scanning
- Nessus scan procedure
- Data and results



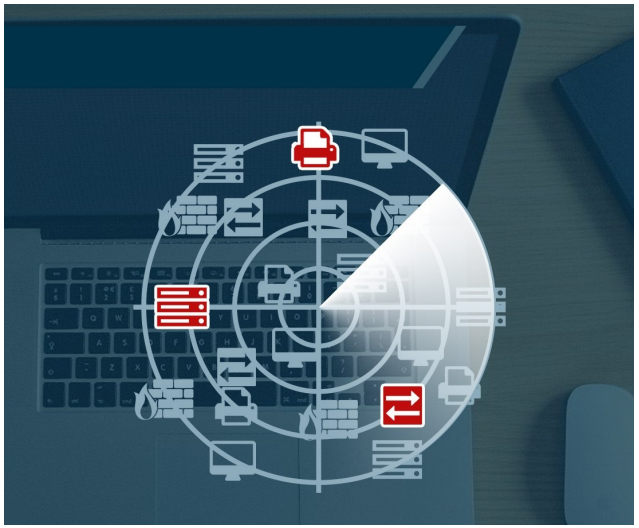
# What is Nessus?

- Nessus is a security scanning tool that scans computers and raises an alert if it discovers security problems and any vulnerabilities that could allow malicious hackers to gain access to a computer connected to a network.

Source: http://www.cs.cmu.edu/~dwendlan/personal/nessus.html

# Capability of Nessus

- Detects security holes in local or remote hosts
- Detects missing security updates and patches
- Simulates attacks to pinpoint vulnerabilities
- Executes security tests in a contained environment
- Can be scheduled for security audits

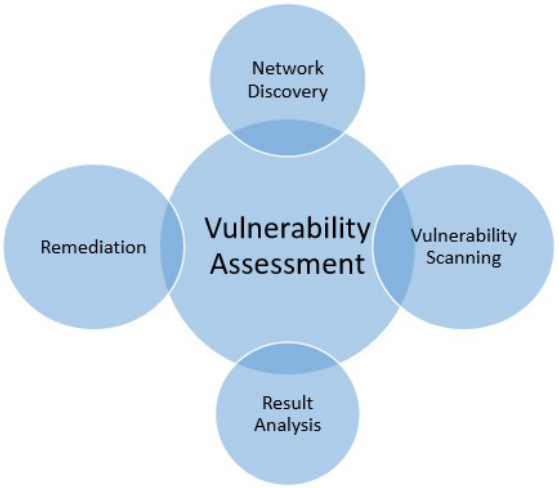


Source: http://searchnetworking.techtarget.com/definition/Nessus

# Vulnerability Scanning

An inspection of potential points of exploits on a computer or network to identify security holes.

Source: http://searchsecurity.techtarget.com/definition/vulnerability-scanning




Unlike penetration testing, which attempts to identify insecure business processes or other weaknesses that a threat actor could exploit, vulnerability scanning searches systems for known vulnerabilities.

Source: https://www.secureworks.com/blog/vulnerability-scanning-vs-penetration-testing

# What does Nessus offer?

1. **Remote and local security:** Capability to detect not only remote flaws of the hosts, but their missing patches and local flaws

2. **Up-to-date security vulnerability database:** By using the command Nessus-update-plugins, the Nessus security checks database (which is updated on a daily basis) can be retrieved

3. **NASL:** Nessus includes NASL (Nessus Attack Scripting Language): A language designed to rapidly write security test

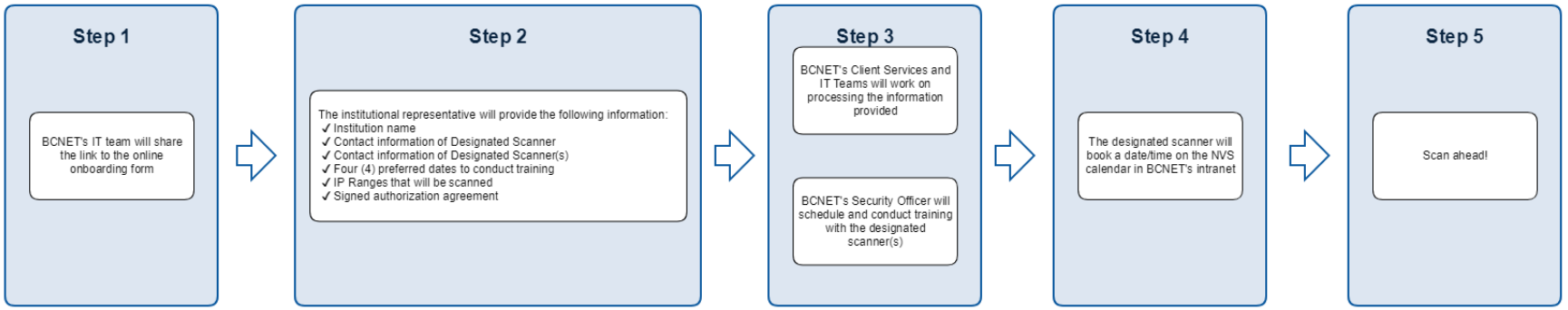
4. **Full SSL support:** Capability to test SSL-ized services such as https, smtps and imaps

5. **Non-destructive or thorough:** Nessus gives you the option to either perform a regular non-destructive security audit on a daily basis, or to throw everything you can at a remote host to test its mettle, and see how it will withstand attacks from intruders.

6. **Multiple services:** Nessus will test all of the services that are run twice or more by a host run

Source: https://www.uniassignment.com/essay-samples/information-technology/what-are-the-main-features-of-nessus-information-technology-essay.php

# NVS Onboarding Process



BCNET's IT team will share the link to the online onboarding form

http://surveys.bc.net/s/nvs/

# STEP 1

The institutional representative will provide the following information:

- ✓ Institution name
- ✓ Contact information of Designated Scanner
- ✓ Contact information of Designated Scanner(s)
- ✓ Four (4) preferred dates to conduct training
- ✓ Public IP Address of computer
- ✓ IP Ranges that will be scanned
- ✓ Signed authorization agreement

# STEP 2

http://surveys.bc.net/s/nvs/

BCNET



# Nessus Vulnerability Scanning

## 1. Name of your Institution

---

## 2. Information of **Contract Administrator**

This is the person who will be responsible for the Nessus Vulnerability Scanning agreement.

Name: Type here

E-mail Address: Type here

Phone Number: Type here

## 3. Information of **Designated Scanner**

This is the person who will conduct the scan. If there is more than one, then please place a comma to separate each person's information.

Name: Type here

E-mail Address: Type here

Phone Number: Type here

# Specify dates for training

## 4a. First Choice

Date YYYY/MM/DD

## 4b. Second Choice

Date YYYY/MM/DD

## 4c. Third Choice

Date YYYY/MM/DD

## 4d. Fourth Choice

Date YYYY/MM/DD

# Provide Public IP Address of computer, IP Ranges and Signed Agreement Form

## 5. Specify Public IP of Computer

*Example: 199.166.1.0*

Type here

## 6. Specify IP Ranges

*Example: 199.166.1.0/23*

Type here

## 7. Additional Notes (Optional)

Type here

## 8. Upload signed Nessus Vulneraibility Scanning Agreement

**NOTE**: Hold CTRL or Command before clicking **here** to download the PDF form to avoid losing the information you've filled out above.

Choose a file to upload

Choose File No file chosen

Submit

# AGREEMENT FORM

Date:

This letter is to confirm that BCNET authorizes [the designated BCNET member] _____ to perform network vulnerability tests on [Institution name] _____ institutional networks using the BCNET Nessus vulnerability scanning service hosted at coho.bc.net.

The following information will be supplied via email to BCNET before beginning a scheduled scan:

* Institutional contact information, including email addresses for all those who should be alerted on completion of scans,

* The dates and times for scheduled scans,

* The target network ranges at the institution.

The BCNET member will execute all vulnerability and penetration tests against their institutional network with the written approval of the institutional CIO or Director of IT, use industry best practice, and take reasonable measures to avoid damaging networks, systems, and any data that might be contained within such networks and systems. A copy of the letter will be provided to BCNET. BCNET will not be held responsible should damages or any other unforeseen consequences arise as the result of using this service. When the institutional resources changes, a new letter of authorization will need to be provided.

Each institution will be restricted to scanning only their institutional IP address ranges. These IPs will be used only for the specific purposes of assisting to configure network scans. BCNET will take appropriate measures to protect all confidential information regarding this project. All vulnerability scans where more than 10 systems will be scanned at one time, will be performed only at specific date(s) to be mutually agreed upon and communicated by email. Scans of 10 or fewer systems may be run in an ad hoc manner. The institution is responsible for; supplying correct information for scanning, internal monitoring, escalation if a problem is noted during scanning, and any needed internal communications of the activity.

If the BCNET member is notified of a problem during the scan, the member will interrupt all tests, and advise the BCNET Operations Centre. The testing shall be suspended until the BCNET Operations Centre and the institutional representative authorizes testing to continue.

Sincerely,

_____

{Institution's Contact}

Date: _____

**BCNET**
Suite 750 – BCIT Downtown Campus
555 Seymour Street, Vancouver, BC, Canada V6B 3H6
Phone: 604.822.1348 Fax: 604.822.9887
www.bc.net ~ info@bc.net

BCNET's Client Services and IT Teams will work on processing the information provided

BCNET's Security Officer will schedule and conduct training with the designated scanner(s)

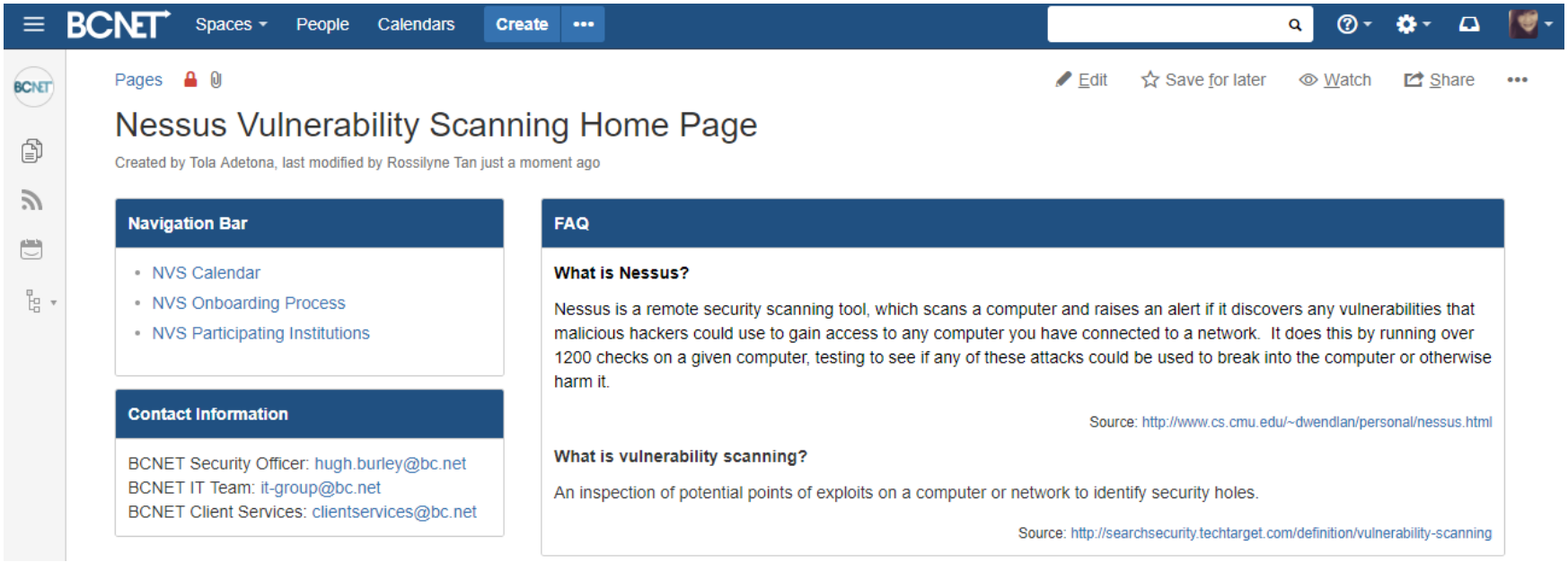
# STEP 3A

BCNET's Security Officer will schedule and conduct training with the designated scanner(s)

BCNET's Client Services and IT Teams will work on processing the information provided

# STEP 3B

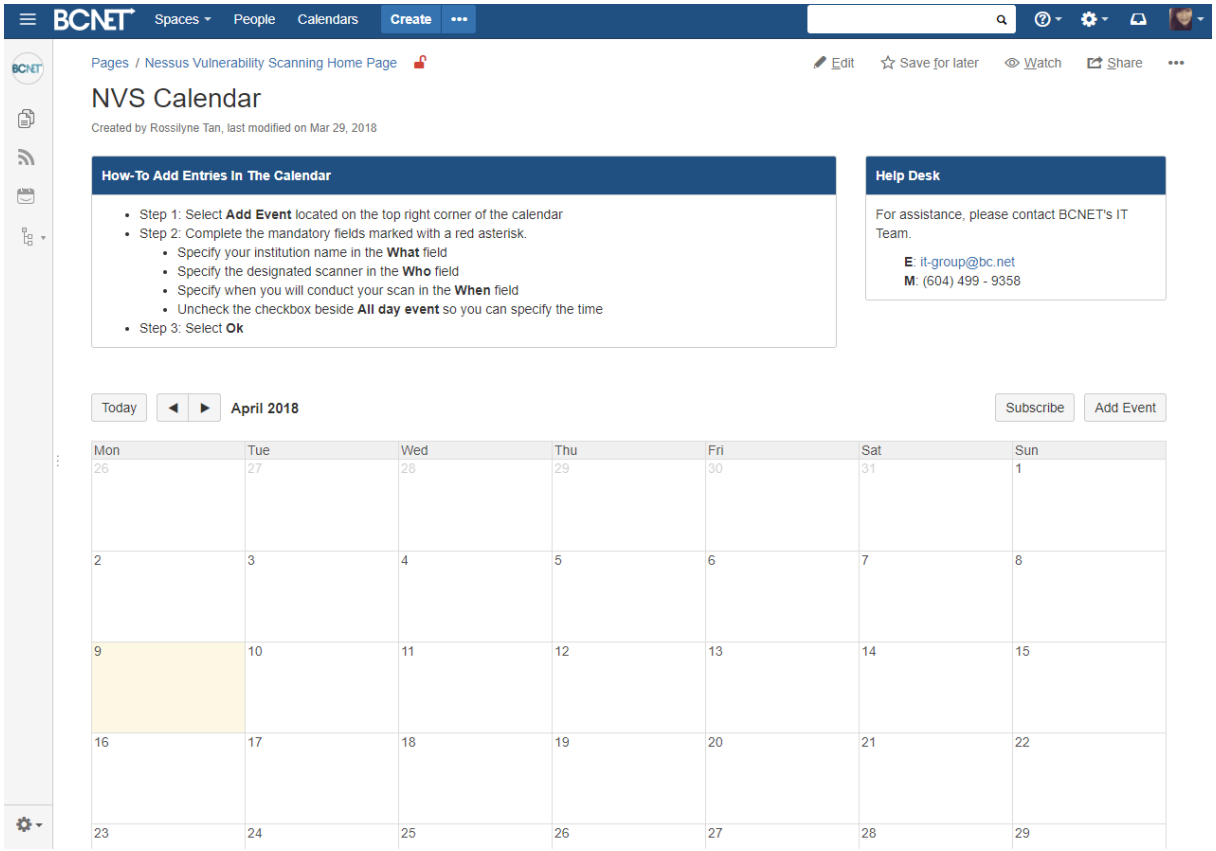
# Nessus Vulnerability Scanning Space

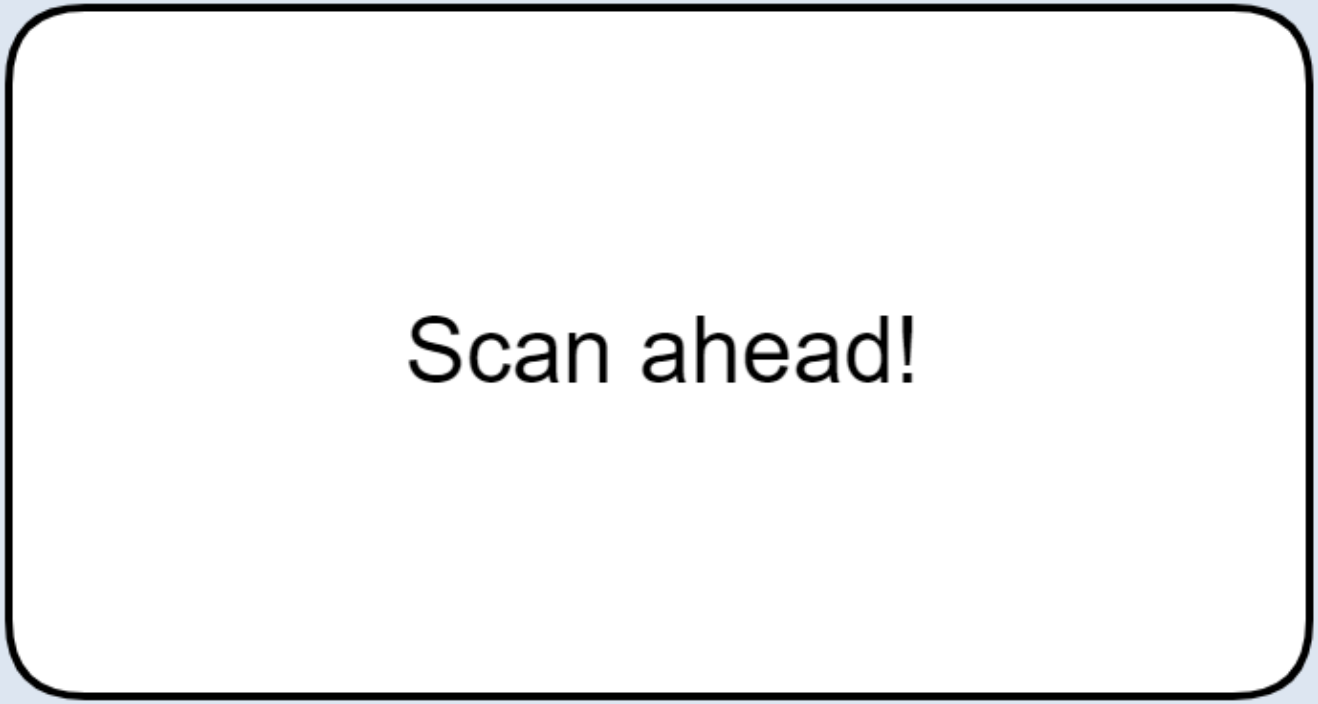


The designated scanner will book a date/time on the NVS calendar in BCNET's intranet

# STEP 4

# NVS Scheduling Calendar






# STEP 5

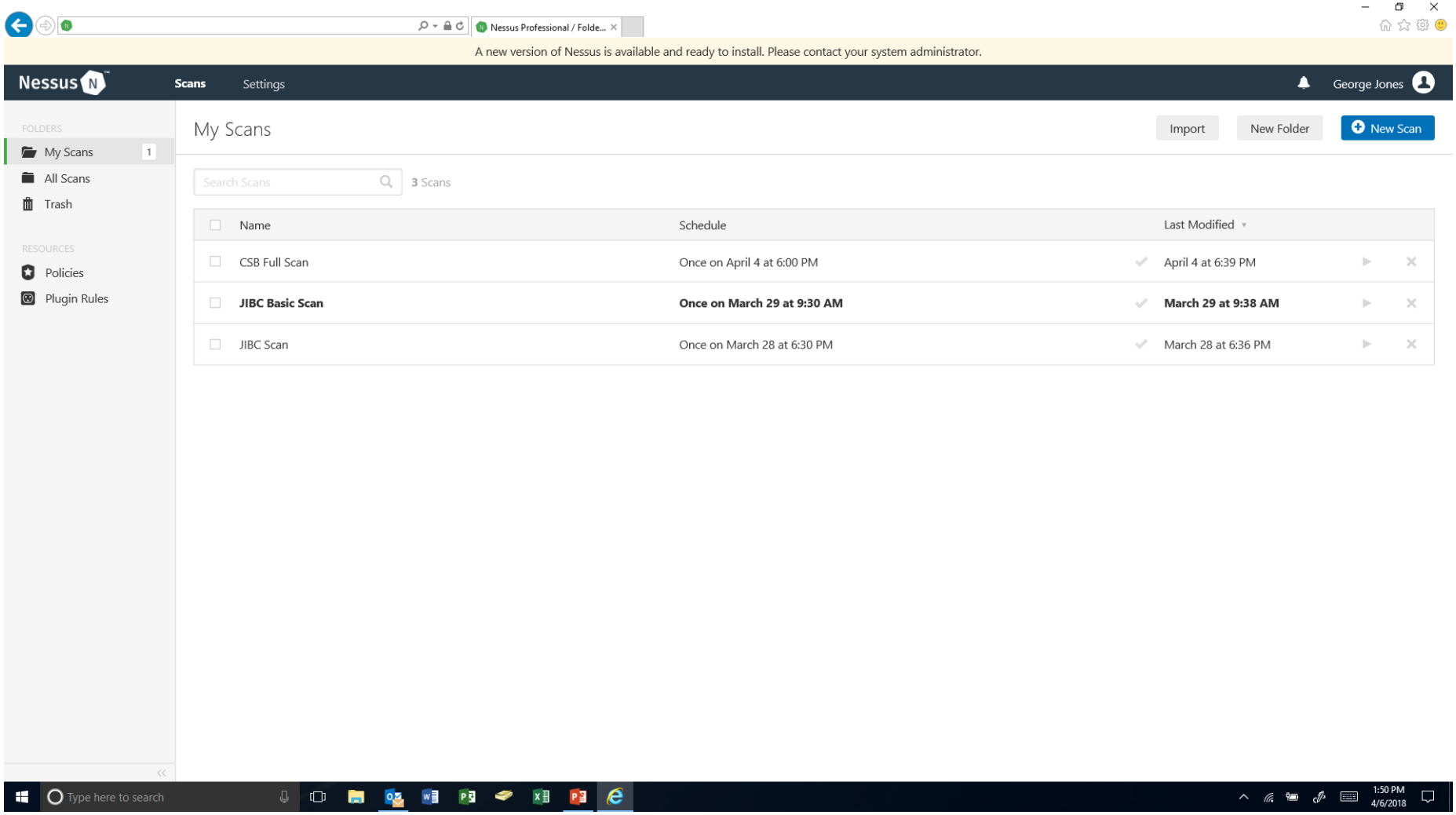
George Jones: CIO Justice Institute of British Columbia

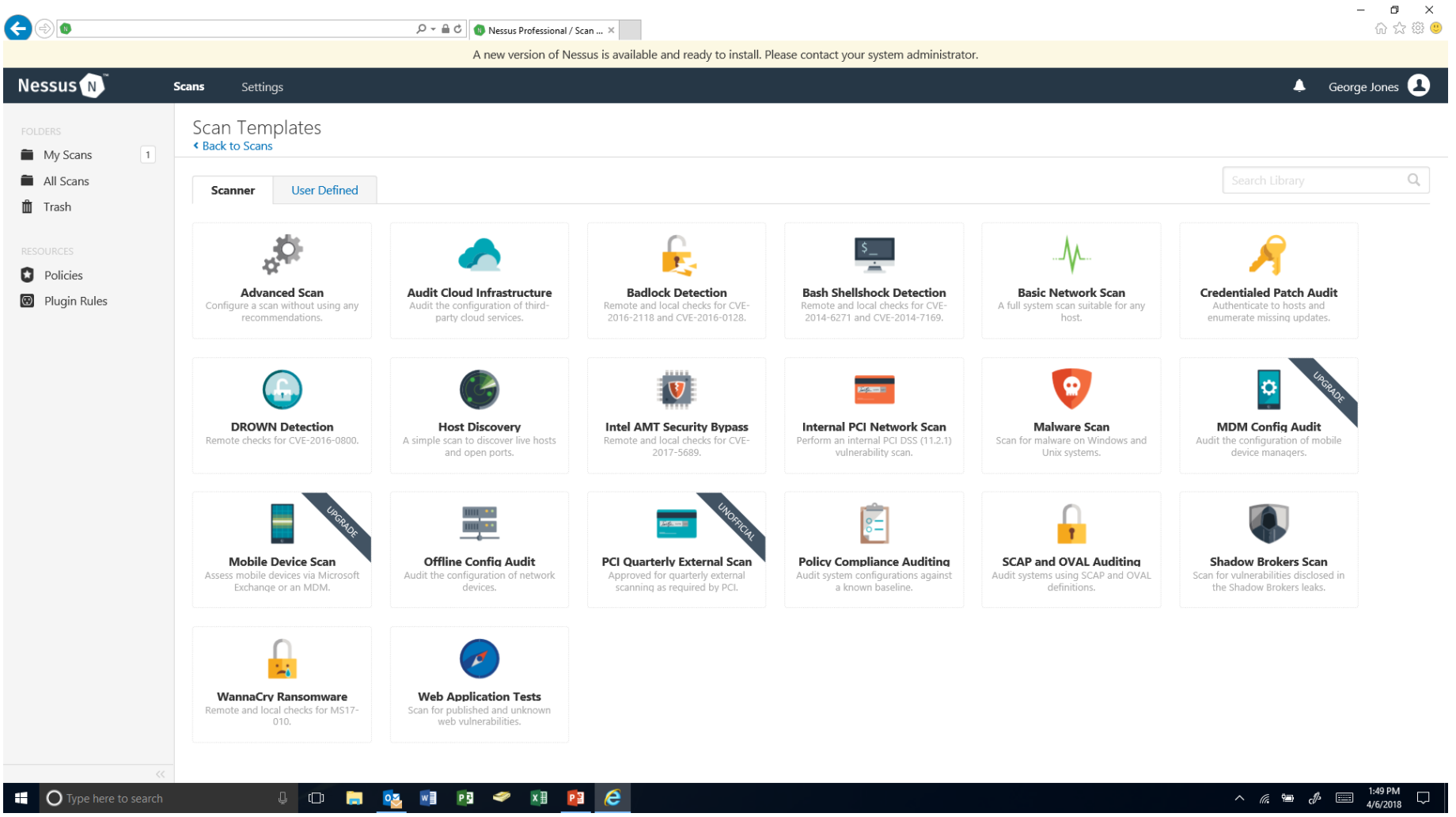
The Justice Institute is a Public Institution that focuses on Public Safety Education
Police Academy for BC Municipal Police Forces, Fire Academy, Paramedic Academy, Sheriff Academy, Corrections, Leadership Training, Certifications – Security, Taxi, others

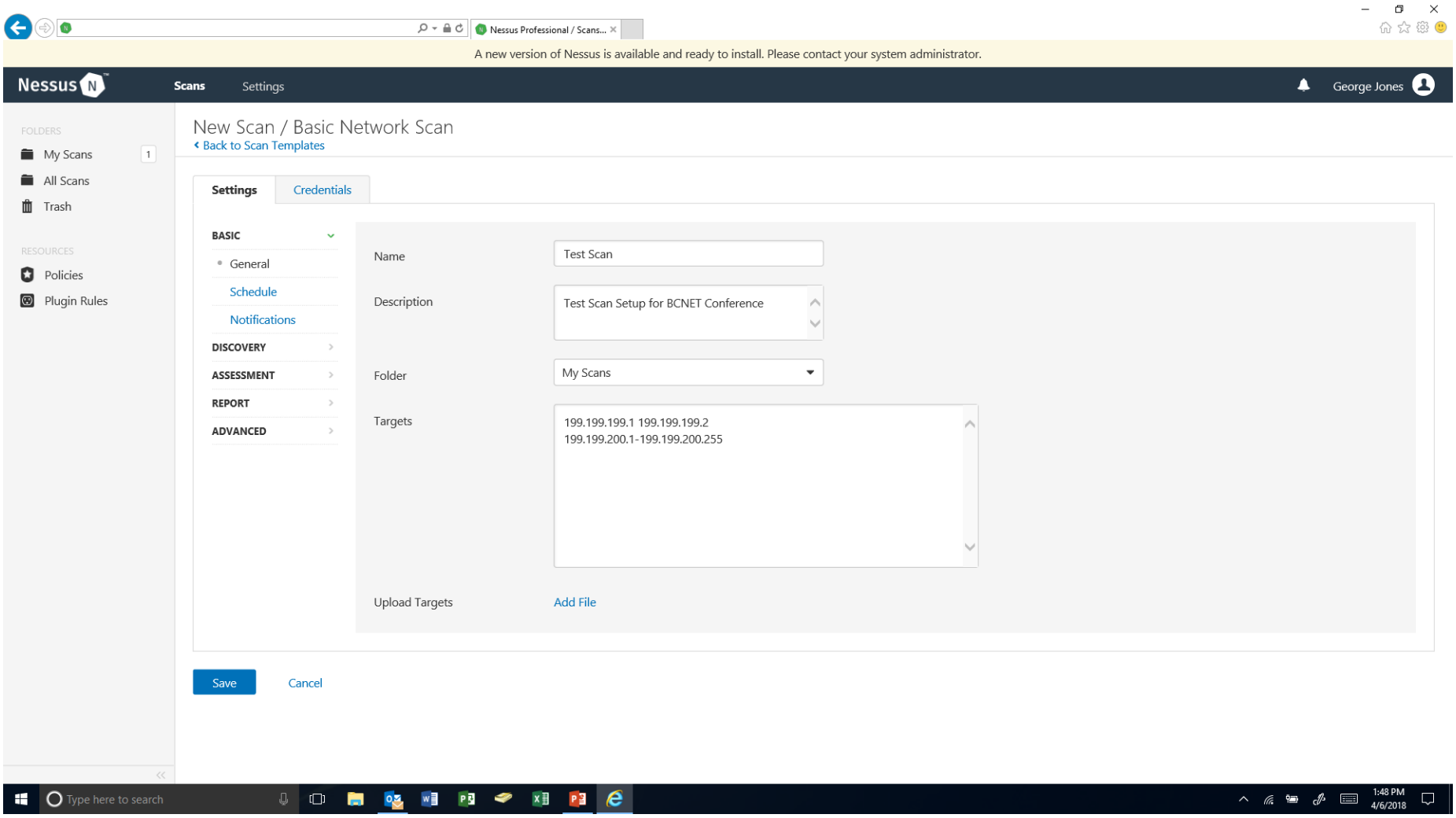
230 Full Time Staff, 15 IT Staff, 6 Campuses, 2300 FTE Students

George is a member of the Cybersecurity Committee of BCNET

The Justice Institute was a pilot user of the BCNET Nessus Scanning Service


Nessus Professional / Folde...
A new version of Nessus is available and ready to install. Please contact your system administrator.
Nessus
Scans
Settings
George Jones
FOLDERS
My Scans 1
All Scans
Trash
RESOURCES
Policies
Plugin Rules
My Scans
Import
New Folder
New Scan
Search Scans
3 Scans
Name
Schedule
Last Modified
CSB Full Scan
Once on April 4 at 6:00 PM
April 4 at 6:39 PM
JIBC Basic Scan
Once on March 29 at 9:30 AM
March 29 at 9:38 AM
JIBC Scan
Once on March 28 at 6:30 PM
March 28 at 6:36 PM
Type here to search
1:50 PM
4/6/2018


Nessus Professional / Scan ...
A new version of Nessus is available and ready to install. Please contact your system administrator.
Nessus
Scans
Settings
George Jones
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scan Templates
Back to Scans
Scanner
User Defined
Search Library
Advanced Scan
Configure a scan without using any recommendations.
Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.
Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.
Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.
Basic Network Scan
A full system scan suitable for any host.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
DROWN Detection
Remote checks for CVE-2016-0800.
Host Discovery
A simple scan to discover live hosts and open ports.
Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.
Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.
Malware Scan
Scan for malware on Windows and Unix systems.
UPGRADE
MDM Config Audit
Audit the configuration of mobile device managers.
UPGRADE
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
Offline Config Audit
Audit the configuration of network devices.
UNOFFICIAL
PCI Quarterly External Scan
Approved for quarterly external scanning as required by PCI.
Policy Compliance Auditing
Audit system configurations against a known baseline.
SCAP and OVAL Auditing
Audit systems using SCAP and OVAL definitions.
Shadow Brokers Scan
Scan for vulnerabilities disclosed in the Shadow Brokers leaks.
WannaCry Ransomware
Remote and local checks for MS17-010.
Web Application Tests
Scan for published and unknown web vulnerabilities.
Type here to search
1:49 PM
4/6/2018


Nessus Professional / Scans...
A new version of Nessus is available and ready to install. Please contact your system administrator.
Nessus
Scans
Settings
George Jones
FOLDERS
My Scans
1
All Scans
Trash
RESOURCES
Policies
Plugin Rules
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Test Scan
Description
Test Scan Setup for BCNET Conference
Folder
My Scans
Targets
199.199.199.1 199.199.199.2
199.199.200.1-199.199.200.255
Upload Targets
Add File
Save
Cancel
Type here to search
1:48 PM
4/6/2018


A new version of Nessus is available and ready to install. Please contact your system administrator.

Nessus | Scans | Settings

FOLDERS
- My Scans 1
- All Scans
- Trash

RESOURCES
- Policies
- Plugin Rules

# New Scan / Basic Network Scan

‹ Back to Scan Templates

**Settings** | Credentials

**BASIC**
- General
- Schedule
- Notifications

**DISCOVERY**

**ASSESSMENT**

**REPORT**

**ADVANCED**

Enabled: ON

Frequency: Once

Starts: 04/06/2018 14:00

Timezone: America/Vancouver

Summary: Once on Friday, April 6th, 2018 at 2:00 PM

Save | Cancel


# Nessus Scan Report

Wed, 04 Apr 2018 18:39:51 PDT

Nessus completed the scan **Full Scan**. Please click here to view and edit the scan results.

## Report Summary

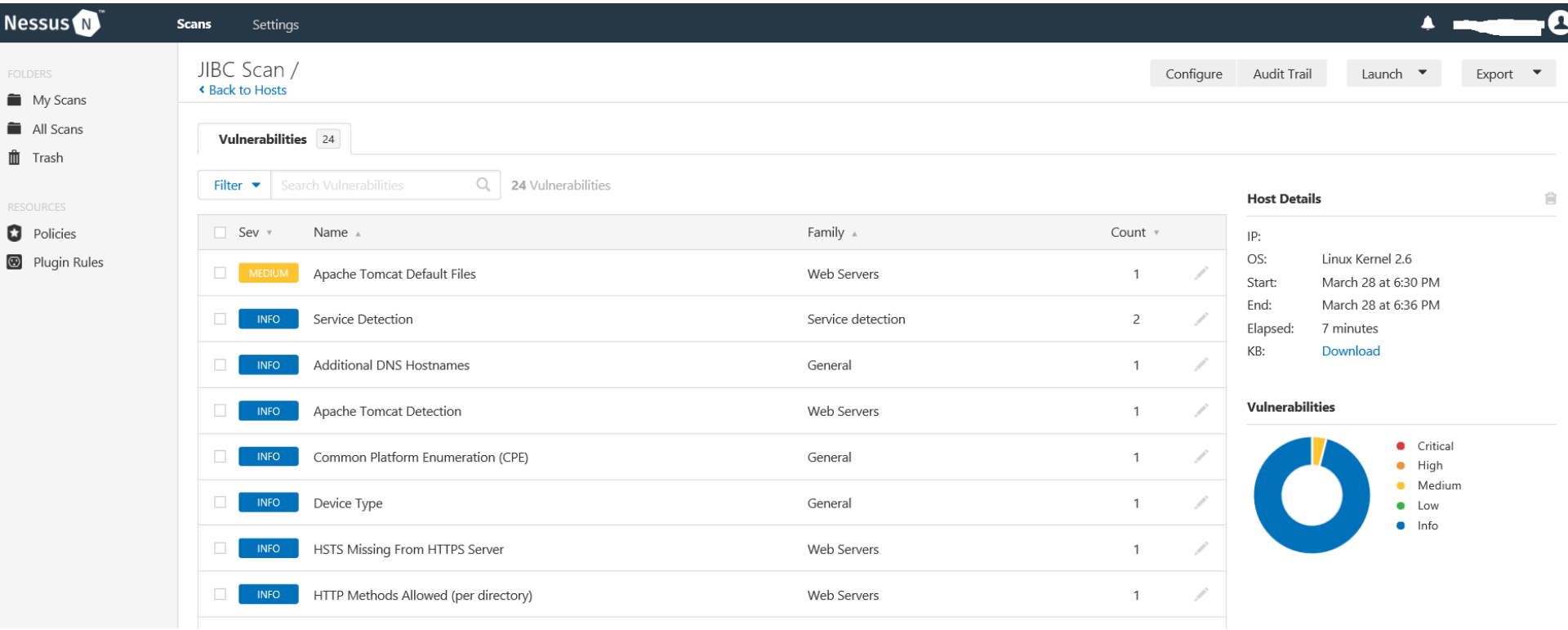
### Plugins: Top 5

| Severity | Plugin Id | Name |
|---|---|---|
| Medium | 42873 | SSL Medium Strength Cipher Suites Supported |
| Medium | 12085 | Apache Tomcat Default Files |
| Medium | 51192 | SSL Certificate Cannot Be Trusted |
| Medium | 20007 | SSL Version 2 and 3 Protocol Detection |
| Medium | 57582 | SSL Self-Signed Certificate |

### Hosts: Top 5

| Host | Critical | High | Medium | Low | Info | Total |
|---|---|---|---|---|---|---|
| | 0 | 0 | 3 | 2 | 26 | 31 |
| | 0 | 0 | 2 | 1 | 22 | 25 |
| | 0 | 0 | 2 | 0 | 21 | 23 |
| | 0 | 0 | 2 | 0 | 21 | 23 |
| | 0 | 0 | 2 | 0 | 15 | 17 |


Nessus
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Full Scan
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 17
Vulnerabilities 41
History 1
Filter
Search Hosts
17 Hosts
Host
Vulnerabilities
3 2 26
2 1 22
1 23
1 22
1 22
2 21
1 22
2 21
Scan Details
Name: ull Scan
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Start: at 6:00 PM
End: at 6:39 PM
Elapsed: 40 minutes
Vulnerabilities
Critical
High
Medium
Low
Info


Nessus
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
JIBC Scan /
Back to Hosts
Configure
Audit Trail
Launch
Export
Vulnerabilities 24
Filter
Search Vulnerabilities
24 Vulnerabilities
Sev
Name
Family
Count
MEDIUM
Apache Tomcat Default Files
Web Servers
1
INFO
Service Detection
Service detection
2
INFO
Additional DNS Hostnames
General
1
INFO
Apache Tomcat Detection
Web Servers
1
INFO
Common Platform Enumeration (CPE)
General
1
INFO
Device Type
General
1
INFO
HSTS Missing From HTTPS Server
Web Servers
1
INFO
HTTP Methods Allowed (per directory)
Web Servers
1
Host Details
IP:
OS:
Linux Kernel 2.6
Start:
March 28 at 6:30 PM
End:
March 28 at 6:36 PM
Elapsed:
7 minutes
KB:
Download
Vulnerabilities
Critical
High
Medium
Low
Info

MEDIUM

# Apache Tomcat Default Files

## Description

The default error page, default index page, example JSPs, and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself.

## Solution

Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.

## See Also

https://wiki.apache.org/tomcat/FAQ/Miscellaneous#Q6
https://www.owasp.org/index.php/Securing_tomcat

## Output

```
The following default files were found :
/nessus-check/default-404-error-page.html
```

| Port ▲ | Hosts |
| --- | --- |
| 443 / tcp / www | |

Questions?