



# BCNET<sup>→</sup>2019

## Making dealing with Nessus vulnerability scans more manageable

Anna Machaj  
Douglas College



# About Douglas College



- Revenue: 148 M
- Student FTE: 10,716
- Students: 24,801
- Employees: 1,800 (approximately & including temporary employees)
  - 100 Administrative
  - 470 Staff
  - 560 Regular Faculty
  - 350 Contract Faculty
- Information Security practice started approx. 5 years ago.

# Vulnerability Scanners

- Number of good vulnerability scanners on the market
  - Some scanners are specialized
    - [Netsparker](#) – web application security scanner
  - Some scanner are generic
    - [Nexpose](#) – aims to support the entire vulnerability management lifecycle
- [Nessus](#) Professional is the de-facto industry standard for vulnerability assessment for:
  - Software flaws
  - Missing patches
  - Misconfigurations



Metasploit Project



Nessus



OpenVAS



Nikto



Nmap



Netsparker



URPS  
Enterprise

Burp suite

# No such Thing as a Perfect Scanner

Someone scanned a sample set of devices with these results:

<b>Nessus 5</b> External Network Profile	Critical 3 High 6 Medium 22 Low 8 Info 137
<b>OpenVAS 5</b> Full Audit Scan Profile	High 38 Medium 24 Low 36 Log 44
<b>Nexpose</b> Full Audit Scan Profile	Critical 49 Severe 103 Moderate 18

- Out of a sample of 15 security holes each of the scanners identified 7
- One of the significant vulnerabilities was classified by Nessus as medium and by Nexpose as low

# Sample Nessus Scan

The screenshot displays the Nessus Professional web interface. The browser address bar shows the URL <https://coho.bc.net:8834/#/scans/reports/962/hosts>. A notification banner at the top states: "A new version of Nessus is available and ready to install. Please contact your system administrator." The interface includes a sidebar with navigation options like "My Scans", "All Scans", and "Trash". The main content area is titled "Douglas External" and shows a summary of the scan results: 59 Hosts, 55 Vulnerabilities, 1 Note, and 6 History items. A table lists individual hosts with their respective vulnerability counts, represented by horizontal bar charts. The "Scan Details" section on the right provides metadata: Name (Douglas External), Status (Completed), Policy (Basic Network Scan), Scanner (Local Scanner), Start (March 15 at 5:00 PM), End (March 15 at 5:32 PM), and Elapsed (32 minutes). A "Vulnerabilities" donut chart shows the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Host	Vulnerabilities
[Redacted]	60
[Redacted]	49
[Redacted]	56
[Redacted]	36
[Redacted]	42
[Redacted]	38
[Redacted]	39
[Redacted]	35
[Redacted]	30
[Redacted]	31
[Redacted]	27
[Redacted]	29

# Drill-down into one of the Servers

The screenshot shows the Nessus web interface. The top navigation bar includes 'Nessus N', 'Scans', and 'Settings'. The user 'douglas2' is logged in. The main content area displays the scan results for 'Douglas External / [redacted].douglascollege.ca / SS...'. A 'Vulnerabilities' tab shows 20 total vulnerabilities, with 7 displayed in the table below. The table columns are 'Sev', 'Name', 'Family', and 'Count'. The vulnerabilities listed are:

Sev	Name	Family	Count
MEDIUM	SSL Medium Strength Cip...	General	1
LOW	SSL RC4 Cipher Suites Sup...	General	1
INFO	SSL Certificate Information	General	1
INFO	SSL Cipher Block Chaining...	General	1
INFO	SSL Cipher Suites Support...	General	1
INFO	SSL Perfect Forward Secre...	General	1
INFO	SSL Session Resume Supp...	General	1



On the right, the 'Scan Details' section provides the following information:

- Name: Douglas External
- Status: Completed
- Policy: Basic Network Scan
- Scanner: Local Scanner
- Start: March 15 at 5:00 PM
- End: March 15 at 5:32 PM
- Elapsed: 32 minutes

Below the scan details is a 'Vulnerabilities' donut chart showing the distribution of severity levels:

- Critical: 0 (0%)
- High: 0 (0%)
- Medium: 1 (14.3%)
- Low: 1 (14.3%)
- Info: 5 (71.4%)

# Understanding Exported Nessus Scans

- **Plugin ID** – Plugin is a program written in the Nessus Attack Scripting Language. It is checking for a set of vulnerabilities. [E.g. 65821](#)
- **CVE** – Common Vulnerability and Exposure ID (may not be populated) [E.g. CVE-2013-2566](#) 
- **CVSS** – Common Vulnerability Scoring System (may not be populated) [E.g. 2.6](#) 
- **Risk** – None, Low, Medium, High, Critical. [E.g. Low](#)
- **Host** – DNS Name or IP address. [E.g. myServer.ad.douglascollege.ca](#)
- **Protocol** – TCP/ UDP. [E.g. TCP](#)
- **Port** – Port number. [E.g. 5071](#)

# Understanding Exported Nessus Scans

- Name
  - Short description of a vulnerability. Always populated.  
E.g. [SSL RC4 Cipher Suites Supported \(Bar Mitzvah\)](#)
- Synopsis
  - Short clarification why this is a vulnerability.  
E.g. [The remote service supports the use of the RC4 cipher.](#)
- Description
  - Detailed description of a vulnerability
- Solution
  - Recommended action to remediate a vulnerability.  
E.g. [Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 ...](#)
- See Also
  - Usually set of links to more information
- Plugin Output
  - Output generated by the plugin



# Understanding Exported Nessus Scans

- Observations:
  - **CVE** and **CVSS** are not always populated
  - **Risk** is always populated but expressed in words and therefore it does not sort well
  - Vulnerability **name** and **name/host** combinations are de-facto unique identifiers of vulnerabilities
  - Number of different plugins report on the same vulnerability therefore reports contain “duplicates”
  - Same vulnerability may be exploitable from different ports and this will result in “duplicates”

# Challenges for Nessus Scans

- If you are not running authenticated scans:
  - Number of false positives will be higher
  - Critical vulnerabilities may not be uncovered
- For authenticated scans, you will need sensitive credentials
- There is no such thing as a single expert for all vulnerability scan results

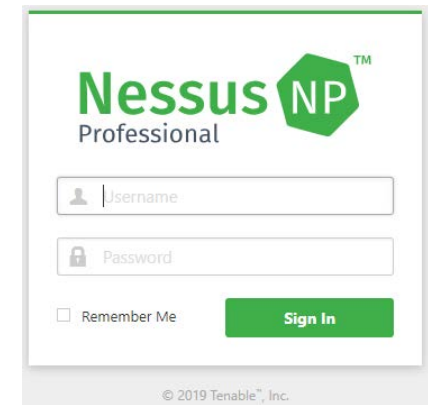


# Challenges for Nessus Scans

- To make it manageable you want to **group your scans in a meaningful way**
  - You want them reviewed by subject matter experts
  - You want them prioritized by severity of vulnerabilities and criticality of devices and/or systems
- Your subject matter experts don't want to be reviewing same vulnerabilities more than once
- Sometimes you **can't remediate a vulnerability** (e.g. legacy system scheduled to be sunset on unsupported OS)

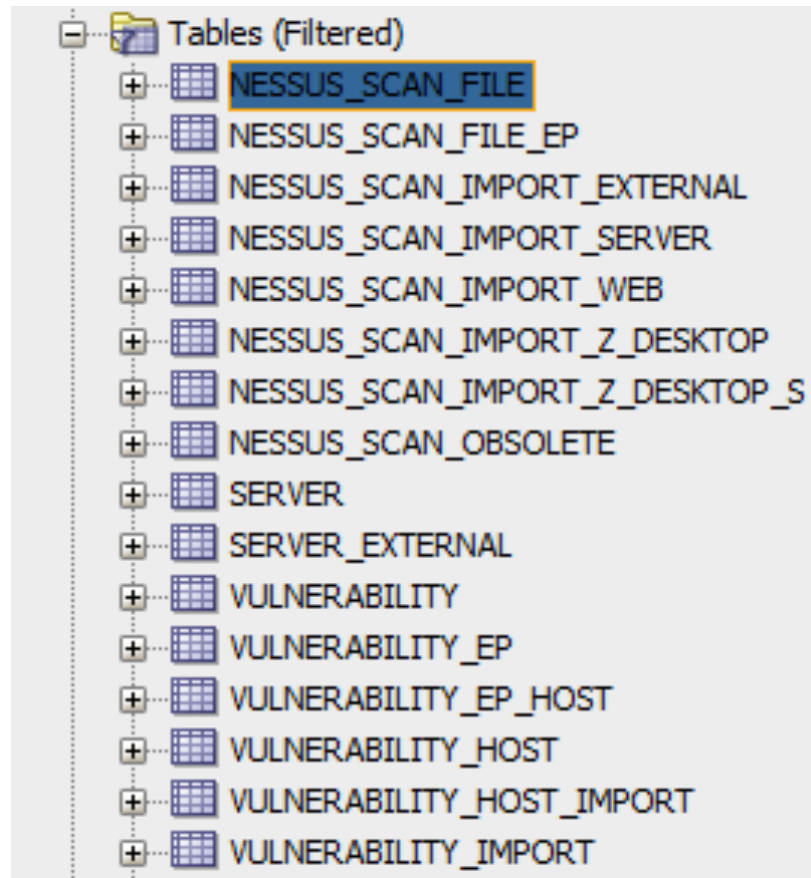
# How we Grouped our Nessus Scans

- **External Scans** – unauthenticated via BCNET Nessus instance
- **Desktop Scans** – authenticated
  - Employee Desktop Scans
  - Student Desktop Scans
- **Server Scans** – authenticated
  - Security Devices
  - Key Infrastructure Servers
  - Application System Server (including Web vulnerability)
  - Other Servers



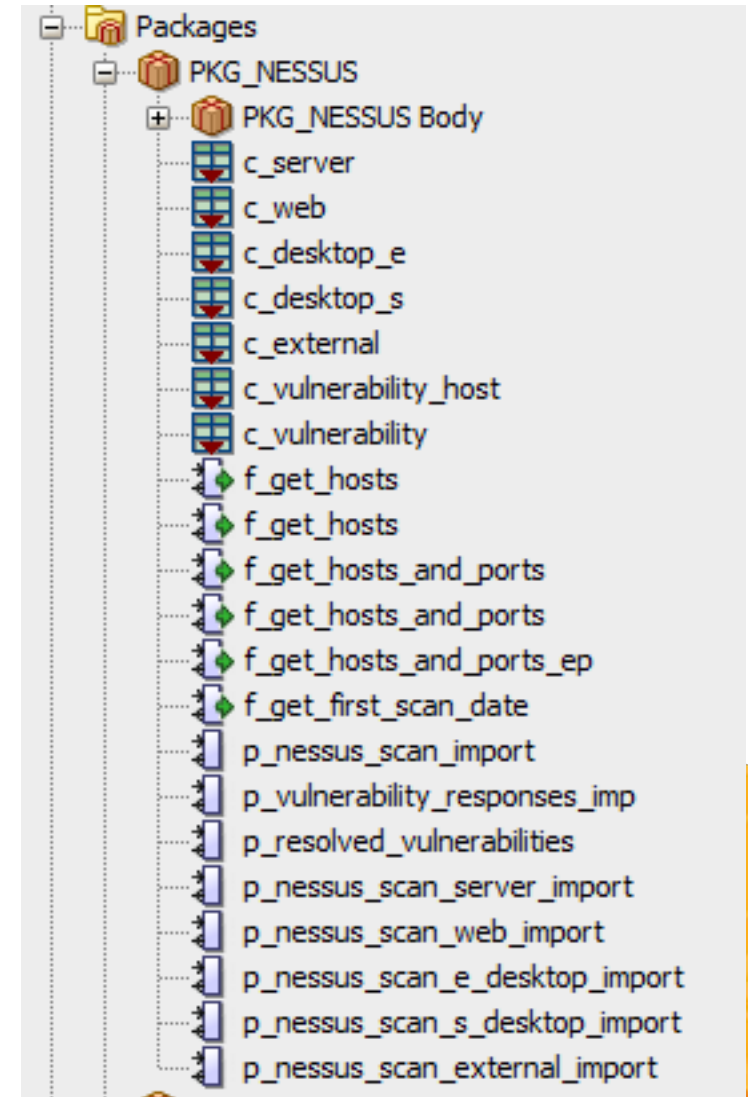
# Our Solution – Functionality in Oracle

1. We import the scans into relevant Oracle tables



# Our Solution – Functionality in Oracle

2. We execute a stored procedure that does the following:
  - Loads unique vulnerabilities by host (**name + host**) into **vulnerability\_host** table
  - Loads unique vulnerabilities (**name**) into **vulnerability** table
  - Vulnerabilities which were identified in previous scans but no longer exist in new scans, are marked as resolved



# Our Solution – Functionality in Oracle

3. Managers receive extract of outstanding vulnerabilities.  
Some of the columns are:
  - Priority Rank (1 – critical, 2 – high, 3 – medium, 4 – low)
  - Scan Type (Security, Infra, App\_Server or Web, Server\_Other, External, Desktop, Desktop\_Stu)
  - Name
  - ....
4. Managers are asked to populate columns:
  - Status
  - Comments

# Vulnerability Risks Analysis – By Vulnerability

- For any given vulnerability all hosts and ports affected by this vulnerability are listed
- Suitable for desktops where number of machines will have the same vulnerability
- Suitable for some servers

PRIORITY_RANK	SCAN_TYPE	NAME	FIRST_SCAN_DATE	Description	Status	COMMENTS	HOSTS_LIST
2	Server_Other	MS16-033: Security Update for Windows USB Mass Storage Class Driver to Address Elevation of Privilege (3143142)	2018-11-16	The remote Windows host is missing a security update. It is, therefore, affected by a flaw in the Windows USB Mass Storage Class driver due to improper validation of objects in memory. A local attacker can exploit this, via a specially crafted USB device, to elevate privileges, allowing the execution of arbitrary code.	Scheduled	Will update by March 1, 2019	xxxxxidow1.ad.douglascollege.ca (445) * xxxxxidow2.ad.douglascollege.ca (445) * xxxxxsvr.ad.douglascollege.ca (445) * xxxxxapp.ad.douglascollege.ca (445) * xxxxxorkdb.ad.douglascollege.ca (445) * xxxxx1k1.ad.douglascollege.ca (445) * xxxxx1k2.ad.douglascollege.ca (445) * xxxxxan1.ad.douglascollege.ca (445) * xxxxxan2.ad.douglascollege.ca (445) * xxxxxclu1.ad.douglascollege.ca (445) * xxxxxsql.ad.douglascollege.ca (445) * xxxxxrd1.ad.douglascollege.ca (445) * xxxxxord2.ad.douglascollege.ca (445)



# Vulnerability Risks Analysis – By Vulnerability and Host

- Useful when similar vulnerabilities have different action plans

PRIORITY	SCAN_TYP	NAME	HOST	HOST_NAME	FIRST_SC	DESCRIPTION	Status	COMMENTS
RANK	E				AN_DA			
1	Web	RHEL 6 / 7 : libxml2 (RHSA-2016:1292)	xxxxxo1.douglascollege.ca	xxxxxo1.douglascollege.ca	2018-11-16	<p>An update for libxml2 is now available for Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7.</p> <p>Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.</p> <p>[Updated 18 July 2016] This advisory has been updated to push packages into the Red Hat Enterprise Linux 6 Desktop channels. The packages included in this revised update have not been changed in any way from the packages included in the original advisory.</p> <p>The libxml2 library is a development toolbox providing the implementation of various XML standards.</p> <p>Security Fix(es) :</p> <p>A heap-based buffer overflow flaw was found in the way libxml2 parsed certain crafted XML input. A remote attacker could provide a specially crafted XML file that, when opened in an application linked against libxml2, would cause the application to crash or execute arbitrary code with the permissions of the user running the application. (CVE-2016-1834, CVE-2016-1840)</p> <p>Multiple denial of service flaws were found in libxml2. A remote attacker could provide a specially crafted XML file that, when</p>	Reviewed	Plan to patch by Feb end, dependent on availability with App Services

# Vulnerability Status can be

- **Identified** – when vulnerability is first identified by a Nessus scan.
- **Risk Accepted** – when management decides to accept the risk coming from a vulnerability, at least for a time being. Justification for risk acceptance is required.
- **Scheduled** – when work on remediation of a vulnerability is scheduled.
- **In Progress** – when work on a resolution of a vulnerability is in progress.
- **Reviewed** – when we analyze a vulnerability but other statuses can't be assigned to it at the moment.
- **Resolved** – this status will be automatically assigned by the system, when vulnerability is resolved.
- **Reemerged** – this status will be populated automatically if previously resolved issue reemerged.

# Our Solution – Functionality in Oracle

5. Analyzed vulnerabilities imported into respective `vulnerability_import` and `vulnerability_host_import`
6. Vulnerabilities processed by an Oracle procedure (status and comments applied to `vulnerability` and `vulnerability_host` tables)
7. Oracle SQL scripts can be run to create following reports:
  - Vulnerabilities resolved in a set date range
  - Vulnerabilities identified in a set period of time
  - Vulnerabilities in a given status



# What does it get us?

- Managers and their teams have more manageable amount of vulnerabilities to review
- No need to review same vulnerability over and over again once an action is planned for it
- All vulnerabilities were reviewed

Thank you

**DOUGLAS**

Anna Machaj

Assoc. Director, Information Security

Douglas College

[machaja@douglascollege.ca](mailto:machaja@douglascollege.ca)