



JT-NM Security Vulnerability Scanning – Methods & Results

Brad Gilmer – Executive Director
IP Showcase

IP SHOWCASE THEATRE AT IBC – SEPT. 14-18, 2018



Overview

- JT-NM and vulnerability scanning goals
- IP Showcase Is A Unique Opportunity
- Describe rules, methodology, tooling
- Results summary
- Potential weaknesses of results



Joint Taskforce on Networked Media Goals With Respect to Security

- Produce security recommendations that make a difference
- Focus on low-hanging fruit
- Keep it simple
- Progress so far
 - Request to JT-NM Coordination Group with regard to PTP Security
 - Request to JT-NM Coordination Group with regard to API Security
 - Draft on vulnerability scanning in progress

3



IP Showcase Is A Unique Opportunity

- Pre-staging event August, 2018 in Wuppertal
- Largest variety of IP systems ever assembled
 - Over 50 systems
 - Hundreds of assigned IP addresses
 - Scan for security vulnerabilities



4



Enabling Others

- Key goal
 - To allow manufacturers and users to duplicate this testing on their own
- Would expect to see improvement over time

5



First Industry-wide Use Of Vulnerability Scanning

- Seeking to validate:
 - Methodology
 - Tooling
 - Overall approach
- Partnership between JT-NM vendors, users and system integrators

6



Vulnerability Scanning Goals

- Scan as many systems as possible in time available
 - Identify “howlers” – obvious security issues
 - NOT meant to be an exhaustive scan of a single system
 - Share detailed specific results with vendors privately
 - Share anonymized results publicly
-
- Validate tooling and methodology in partnership with vendors
 - Add to criteria for participating in future IP Showcase?

7



Tooling, Methodology & Testing

Tooling

- Hardware
 - Intel model NUC7i5BN
 - Intel i5 dual-core processor
 - 16 GB memory
 - 300 GB Flash drive
 - More processing, memory and drive space than necessary
- Operating System
 - Kali Linux rolling distribution
 - Automatic updates disabled
 - Manually updated on 22 Aug, 2018



8



Tooling, Methodology & Testing

Tooling

- Software

- NMAP (www.nmap.org)
 - Command line port scanner



- OpenVAS (www.openvas.org)
 - Menu-driven vulnerability scanner



9



OpenVAS

Why OpenVAS?

- Solid reputation
- Open Source
- Free
- Constantly updated
- Good coverage – over 45,000 tests as of IBC 2018
- Large community
- Recommended by AMWA/EBU Security Task Force security professionals



10



Tooling, Methodology & Testing

Workflow (for each vendor)

- Identify live IP addresses
- Set up scan targets
- Set up scan task
- Execute scan task
- Analyze results
- Send results to vendor

11

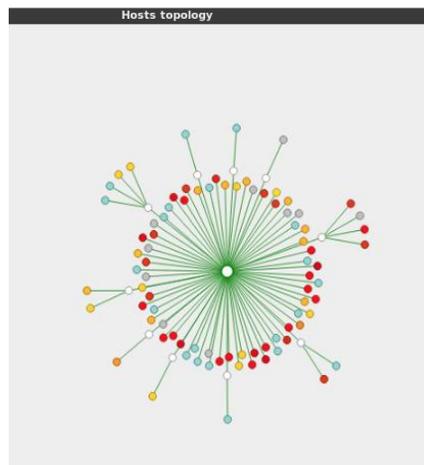


Tooling, Methodology & Testing

Identify live IP addresses

- Two networks – management & media
- Over 50 vendors
- Hundreds of assigned IP addresses
- Each vendor assigned multiple IP addresses
- But not all vendor addresses used
- How to quickly identify live addresses?

Very different from scanning a single device



12



Tooling, Methodology & Testing

Identify live IP addresses for each vendor

- nmap used to scan vendor address space

```
kali:$ nmap -sn -oG [filename] [addressRange]
Flags - ping scan (-sn), save "grepable" file (-oG)
```

- Results saved in a text file

- bash script takes in file and produces list of live IP addresses

```
kali:$ /bin/grep Up $1 |cut -d " " -f2 |tee $1.LiveHosts.txt
```



VendorA.LiveHosts.txt

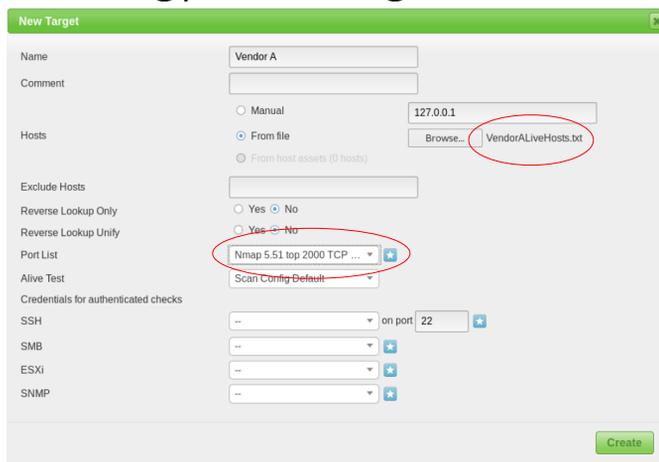
```
192.168.1.6
192.168.94.193
192.168.251.32
```



Tooling, Methodology & Testing

Set up scan target

- Import hosts file list
- Set Port List to "Nmap 5.51 top 2000 TCP and top 100 UDP ports"

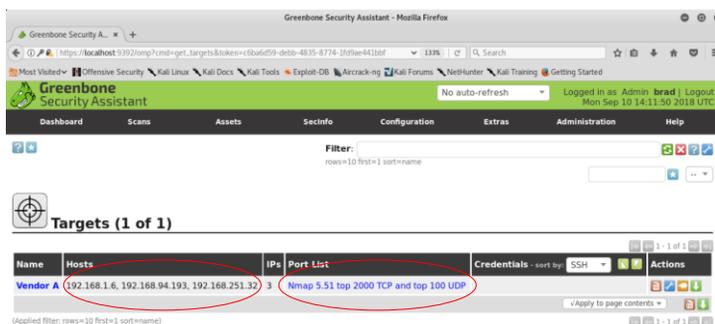




Tooling, Methodology & Testing

Set up scan target

- Import hosts file list
- Set Port List to “Nmap 5.51 top 2000 TCP and top 100 UDP ports”



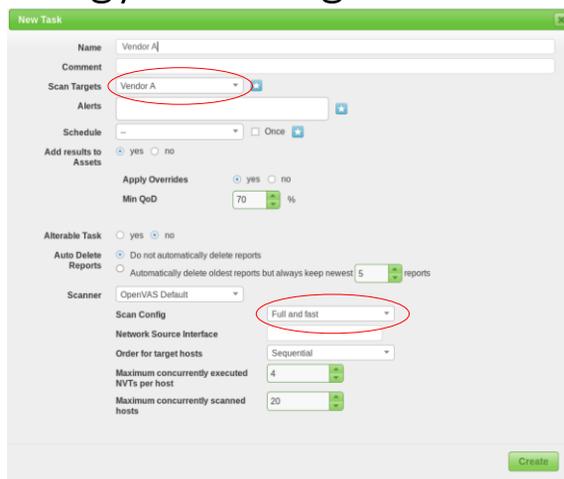
15



Tooling, Methodology & Testing

Complete scan task

- Set scan targets to “Vendor A”
- Select Scan Config “Full and Fast”



16



Tooling, Methodology & Testing

Run task

The screenshot shows the Greenbone Security Assistant interface. At the top, it says 'Greenbone Security Assistant' and 'Logged in as Admin brad | Logout Mon Sep 10 14:39:34 2018 UTC'. Below the navigation bar, there's a filter section and a 'Tasks (1 of 1)' section. The 'Tasks (1 of 1)' section contains three charts: 'Tasks by Severity Class (Total: 1)' showing a donut chart with 'N/A', 'Tasks with most High results per host' showing 'No Tasks with High severity found', and 'Tasks by status (Total: 1)' showing a donut chart with 'Done'. Below the charts is a table with columns: Name, Status, Reports (Total, Last), Severity, Trend, and Actions. The table has one row for 'Vendor A' with status 'Done', 1 report, and a date of 'Sep 10 2018'. The 'Actions' column for 'Vendor A' contains several icons, with the 'Run' icon circled in red.

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Vendor A	Done	1 (1)	Sep 10 2018	N/A		Run, Stop, Refresh, etc.

17



A few facts...

- Scanning period – about 20 hours
 - Number of IPs scanned – 124
 - Number of ports scanned per IP address – 2,098
- Total number of ports scanned – 260,152
- Total number of Network Vulnerability Tests (NVTs) available – 46,663
 - Average number of NVTs executed per host – 3,450
- Approximate total number of NVTs executed during testing period – 427,800
- Number of IPs scanned concurrently – 4
 - Number of NVTs run concurrently - 20

18



Anonymized Actual Vendor Result

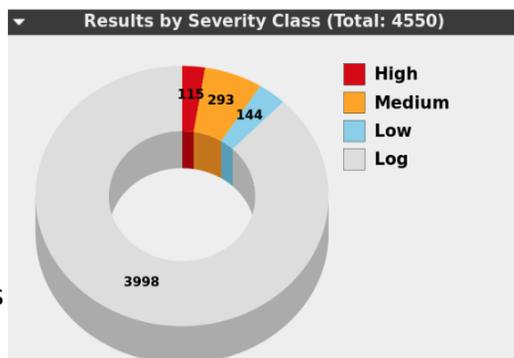
- Actual anonymized vendor result
- Severity
 - High, Medium & Low
- Results by IP address
- Specific NVT Identified
- Click-through NVT for more info

Vulnerability	Severity	QoS	Host	Location	Actions
Mixxx NVT Devices Multiple Vulnerabilities	High (9.0)	80%		generatortcp	[Info] [Close]
Windows Administrator NtLm_PFP password	High (9.0)	99%		2121tcp	[Info] [Close]
Report default community names of the SNMP Agent	High (9.0)	99%		161udp	[Info] [Close]
Report default community names of the SNMP Agent	High (9.0)	99%		161udp	[Info] [Close]
Report default community names of the SNMP Agent	High (9.0)	99%		161udp	[Info] [Close]
Report default community names of the SNMP Agent	High (9.0)	99%		161udp	[Info] [Close]
SQL/TLDS OpenSQL CCS Man in the Middle Security Bypass Vulnerability	High (9.0)	70%		443tcp	[Info] [Close]
HTTP Debugging Methods (TRACE/TRACE2) Enabled	High (9.0)	99%		80tcp	[Info] [Close]
nginx Proxy DNS Cache Domain Spoofing Vulnerability	High (9.0)	80%		443tcp	[Info] [Close]
nginx Proxy DNS Cache Domain Spoofing Vulnerability	High (9.0)	80%		80tcp	[Info] [Close]
nginx Space String Remote Source Code Disclosure Vulnerability	High (9.0)	80%		443tcp	[Info] [Close]
nginx Space String Remote Source Code Disclosure Vulnerability	High (9.0)	80%		80tcp	[Info] [Close]
Missing 'HttpOnly' Cookie Attribute	High (9.0)	80%		80tcp	[Info] [Close]
ClearText Transmission of Sensitive Information via HTTP	High (9.0)	80%		80tcp	[Info] [Close]
SSL/TLS: Degraded SSLv2 and SSLv3 Protocol Detection	High (9.0)	98%		443tcp	[Info] [Close]
SSL/TLS: Report Weak Cipher Suites	High (9.0)	98%		443tcp	[Info] [Close]
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	High (9.0)	80%		443tcp	[Info] [Close]
SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)	High (9.0)	80%		443tcp	[Info] [Close]
SSH Weak Encryption Algorithms Supported	High (9.0)	95%		22tcp	[Info] [Close]
Apache HTTP Server 'HttpOnly' Cookie Information Disclosure Vulnerability	High (9.0)	99%		80tcp	[Info] [Close]
TCP timestamps	High (9.0)	80%		generatortcp	[Info] [Close]
SSH Weak MAC Algorithms Supported	High (9.0)	95%		22tcp	[Info] [Close]
TCP timestamps	High (9.0)	80%		generatortcp	[Info] [Close]
TCP timestamps	High (9.0)	80%		generatortcp	[Info] [Close]



Summary Results

- Total # of IPs checked – 124
- Total # of vulnerabilities found
 - 115 High
 - 293 Medium
 - 144 Low
- Log events
 - Items of note, but not vulnerabilities (e.g. scan info)





Summary Results

Some top vulnerabilities found

- OS End Of Life
 - Older OS, more vulnerable
- HTTP Directory Traversal
 - Allows download of files, e.g. /etc/passwd
- SSH login with default credentials
 - Default login credentials have not been changed
- Windows Administrator account 'NULL' FTP password
 - Allows upload of malicious code
- PHP Denial of Service
 - Crash heap memory
- Eclipse Jetty Server Pipeline Request
 - Bypass credential checking

21



Greenbone Security Assistant Logged in as: admin | admin | Logout Tue Sep 11 19:05:33 2018 UTC

Dashboard Scans Assets Schedules Configuration Extras Administration Help

Result: Eclipse Jetty Server Fake Pipeline Request Security Bypass Vulnerability ID: c786e62-3c5-4861-096a-686e643f901
Created: Wed Aug 22 11:54:20 2018
Modified: Wed Aug 22 11:14:20 2018
Owner: admin

Vulnerability	Severity	CoD	Host	Location	Actions
Eclipse Jetty Server Fake Pipeline Request Security Bypass Vulnerability	CVSS:3.1/AV:N/AC:L/AT:N/AU:N/CA:C/CR:P/EA:U/PR:R/SC:N/TC:E/XX:N	80%	192.168.1.100	/tcp	Details

Summary
The host is installed with Eclipse Jetty Server and is prone to security bypass vulnerability.

Vulnerability Detection Result
Installed version: 9.4.
Fixed version: 9.4.11.v20180605
Installation path / port: /tcp

Impact
Successful exploitation will allow an attacker to bypass authorization.
Impact Level: Application

Solution
Solution type: Vendorfix
Upgrade to Eclipse Jetty Server version 9.2.25.v20180606 or 9.3.24.v20180605 or 9.4.11.v20180605 or later as per the series. For updates refer to Reference links.

Affected Software/OS
Eclipse Jetty Server versions 9.2.x before 9.2.25.v20180606, 9.3.x before 9.3.24.v20180605 and 9.4.x before 9.4.11.v20180605

Vulnerability Insight
The flaw exists due to an improper validation against pipelined requests.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details: Eclipse Jetty Server Fake Pipeline Request Security Bypass Vulnerability (OD: 1.3.6.1.4.1.25623.1.0.813551)
Version used: \$Revision: 10443 \$

Product Detection Result
Product: `spec/eclipse-jetty:9.4`
Method: `jetty-version-detection (OD: 1.3.6.1.4.1.25623.1.0.800953)`
Log: [View details of product detection](#)

References
CVE: [CVE-2017-7658](#)
CERT: [DPN CERT-2018-1285](#)
Other: https://bugs.eclipse.org/bugs/show_bug.cgi?id=535689
<https://www.eclipse.org/jetty/>

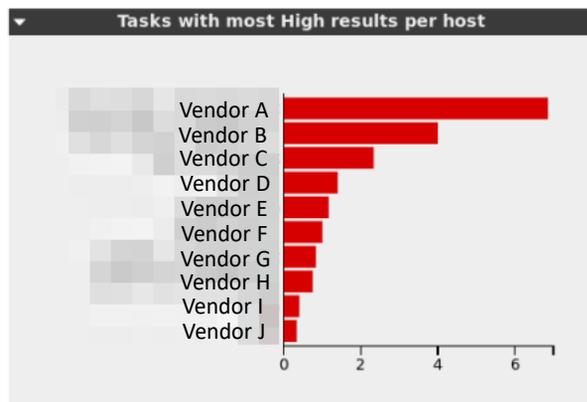
User Tags (none)

22



Summary Results

- Not all hosts were the same
 - Some hosts had many more issues than others
 - Could make significant improvement overall by addressing issues with two or three hosts



23



Potential Issues

- False Positives
 - Identifying vulnerabilities that do not exist
 - False Negatives
 - Failing to identify actual vulnerabilities
 - Not understanding what the tooling is doing
 - Incorrectly interpreting the results
 - Vulnerability issues that are there by design
 - Example: using HTTP instead of HTTPS
- No specific issues with OpenVAS identified so far

24



Closing Thoughts

- You (vendors, users, system integrators) can do this
- Possible to scan very large facilities in a reasonable amount of time
- Serious vulnerabilities with simple fixes were identified
- Results are tentative
- Plan to publish this information as a paper
- Vulnerability testing may be part of qualification for future events
- Goal is to see the industry improve over time
- This is a partnership – vendors and users need to work together

25



Thank You

Brad Gilmer – Executive Director, IP Showcase
brad@gilmer.tv

IP SHOWCASE THEATRE AT IBC – SEPT. 14-18, 2018