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

2

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

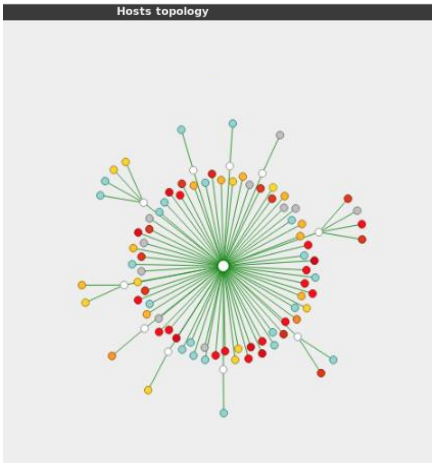
11

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

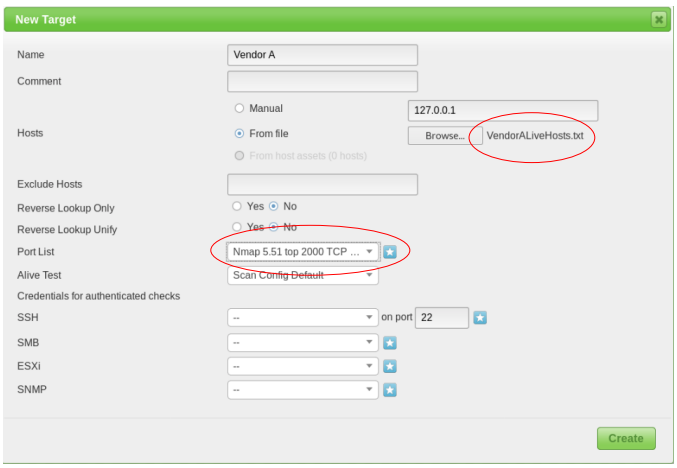
```
192.168.1.6
192.168.94.193
192.168.251.32
```

13

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`”



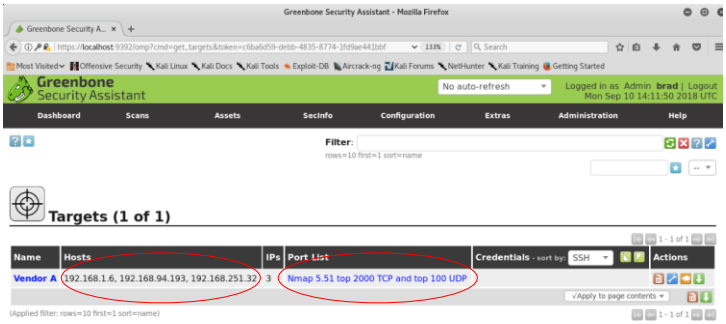
OpenVAS

14

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`"



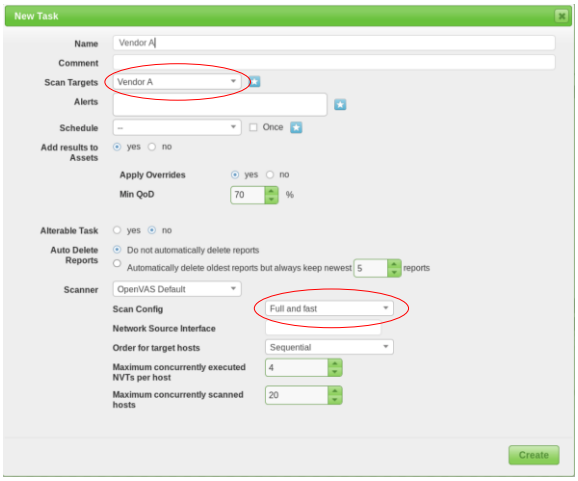
OpenVAS

15

Tooling, Methodology & Testing

Complete scan task

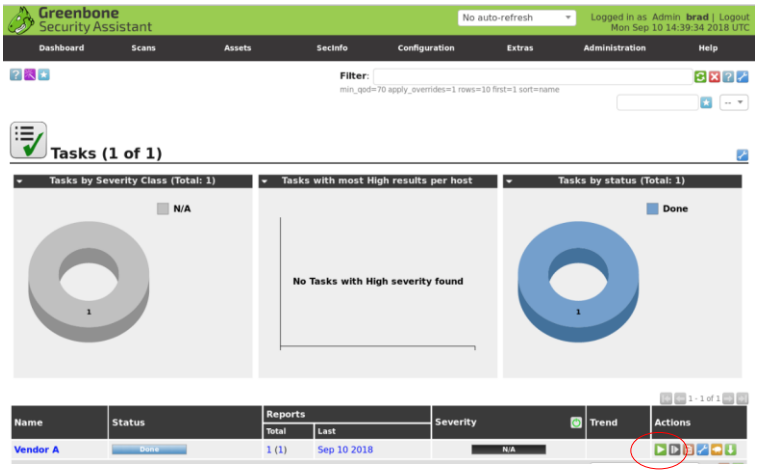
- Set scan targets to "`Vendor A`"
- Select Scan Config "`Full and Fast`"



16

Tooling, Methodology & Testing

Run task



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

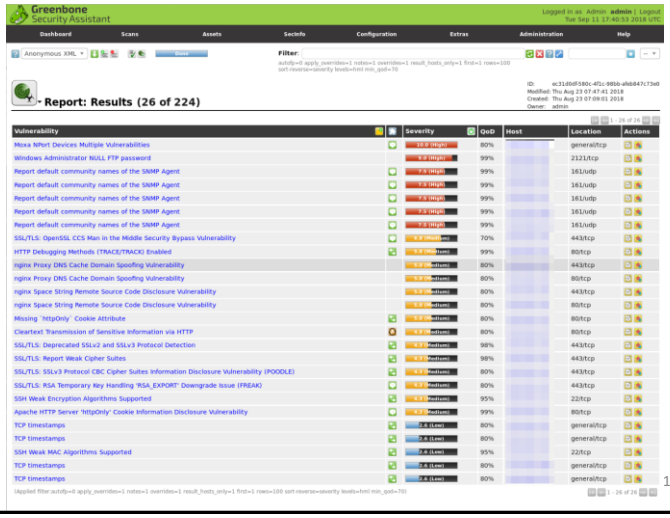
Approximate total number of NVTs executed during testing period – 427,800

- Number of IPs scanned concurrently – 4
- Number of NVTs run concurrently - 20

18

Anonymized Actual Vendor Result

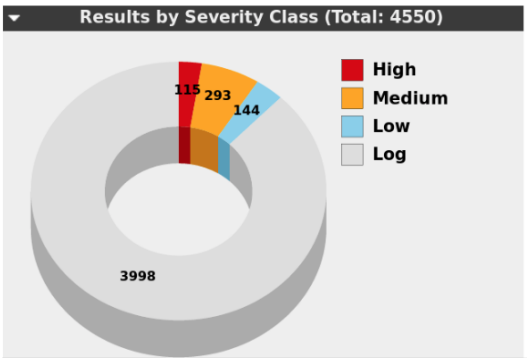
- Actual anonymized vendor result
- Severity
  - High, Medium & Low
- Results by IP address
- Specific NVT Identified
- Click-through NVT for more info



19

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)



20

Summary Results

Some top vulnerabilities found

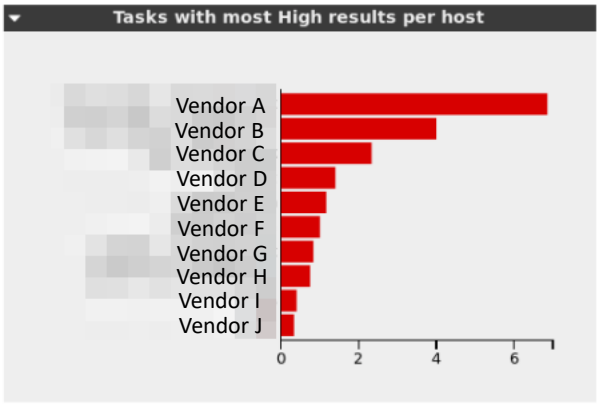
- OS End Of Life
  - Older OS, more vulnerable
- HTTP Directory Traversal
  - Allows download of files, e.g. /etc/passwd
- SSH login with default credentials
  - Default login credentials have not been changed
- Windows Administrator account 'NULL' FTP password
  - Allows upload of malicious code
- PHP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

21

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