

An aerial photograph of a road intersection. A road curves from the bottom towards the top, meeting a horizontal road. To the right of the intersection is a parking lot with several cars. Bare trees line the roads and the parking lot. The image is in grayscale with a dark overlay.

Know Thyself

Identifying Your Own Weaknesses

(Through Effective Infrastructure
Vulnerability Scanning)

~# whoami

Joe Tegg

- Husband
- Father
- Security guy
- Recovering BOFH



Infra Vulnerability Discovery - Identifying your own 'errors'

"Therefore, whoever wishes to be good and noble must consider that he cannot but fail to recognize many of his own errors. I can tell him how he might discover them all (*or most*), just as I have discovered them." - Aelius Galenus (Galen) AD 129 - 216

Ironic fact:

Galen had his own errors... he used animals instead of humans for his research and made impactful mistakes because of it.



Deploying Effective Infra Vulnerability Scanning Processes

1. What is an infrastructure vulnerability scan?
2. Why is it important?
3. What should we scan?
4. What tool(s) should we use?
5. Important configuration settings / knowledge
6. How often should we run the vulnerability scans?
7. We ran the scan, now what?
8. Upleveling the vulnerability scanning processes
9. Questions / Comments



Infrastructure Vulnerability Scan

NIST: “A technique used to identify hosts/host attributes and associated vulnerabilities.”

1. Datacenter Networks (Internal / External / Agents)
2. Office Networks (Internal / External* / Agents)
3. Cloud Networks* (Internal* / External / Agents)
4. Endpoints* (Agents)

Why Is Vulnerability Scanning Important?

Hackers do it.

Leadership wants it.

Auditors require it.

You need it.

Johari Window



What should we scan?

Use the standard process of an attacker to start.

1. External Assets

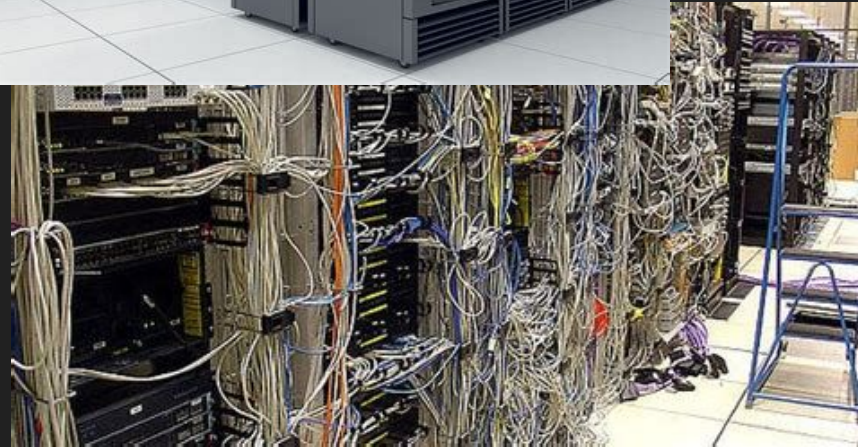
- a. AMDB*
- b. OSINT - (lots of things here)
- c. Infrastructure SORs - Eng Management, Cloud, Network tools
- d. Third party mafia (BitSight, Security Scorecard, UpGuard, etc)



What should we scan? (con't)

2. Internal Assets

- a. AMDB / Internal Network Ranges (Agents)
- b. Network Segmentation areas
- c. Infrastructure SORs
- d. OT networks*



What should we scan? (con't)

3. All the things!

- a. Databases?
- b. Unknown Applications
- c. Unknown IT (Shadow IT)
- d. Unknown Unknowns*



What tool(s) can we use?

1. NMAP - Seriously. NMAP.
2. OTB Vulnerability Scanners
 - a. Rapid7, Tenable, Qualys - Seen most often
 - b. OpenVAS - Free
 - c. Others (Agent based tools, rebrands, free specific tools)



Important configuration settings / knowledge

Some types of infrastructure scans (templates)

- a. Discovery
 - i. IP Scans
 - ii. Port Scans
 - iii. Service Scans
- b. Full*
 - i. Discovery+
 - ii. Vulnerability Checks (auth / no auth)
 - iii. Configuration Checks (auth)
- c. Compliance
 - i. Discovery
 - ii. Configuration Checks (auth)
 - iii. Limited Vulnerability Checks

When the auditor asks to see the vulnerability scan templates that we use



Important configuration settings / knowledge

Customize the templates!!!

Canned templates have limitations.

TCP SCANNING

Select target ports to scan with TCP packets.

Method

Stealth scan (SYN)

Ports to scan

Well-known port numbers (default)

Additional ports

1-1040

CHECK CONFIGURATION

- ☐ Perform unsafe checks
- ☐ Include potential vulnerability checks
- ☒ Correlate reliable checks with regular checks
- ☐ Skip checks performed by the Insight Agent ?
- ☒ Use the Metasploit Remote Check Service when available (Beta) ?
- ☐ Enable Scanning Diagnostic checks ?
- ☐ Store invulnerable results ?

SELECTED CHECKS

- > By Category (294 of 295 enabled)
- > By Check Type (11 of 12 enabled)
- > By Individual Check (905854 of 905854 enabled)

Important configuration settings / knowledge

Detailed scan logs can provide a wealth of information!

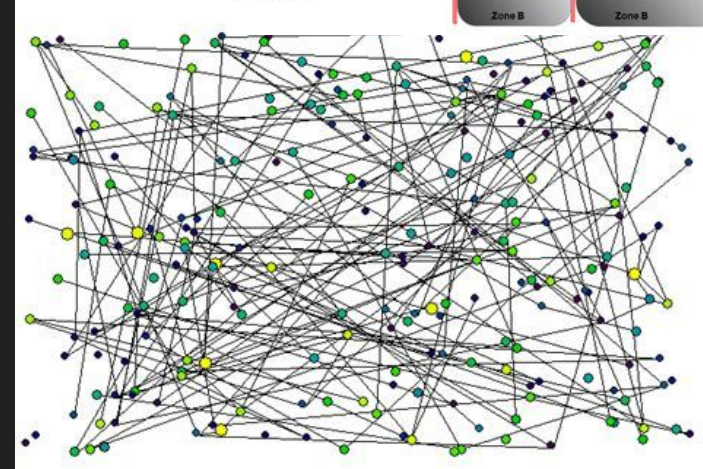
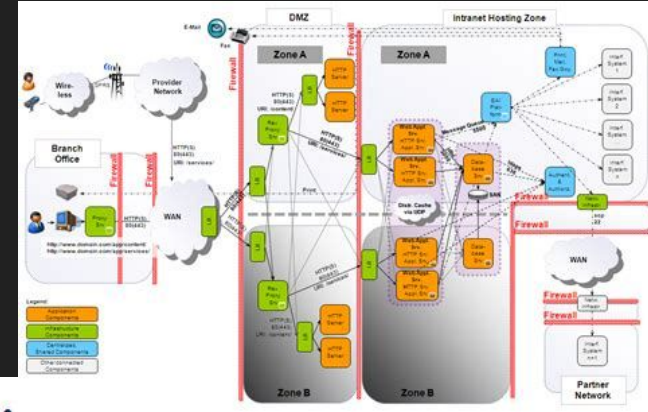
Auth failures, False Positives/Negatives, Asset misidentification

```
#tail -f nse.log
2023-07-22T16:29:12 [INFO] [Thread: 192.168.0.200:443/TCP] [Site: Test] Checking for SERVER match to: Apache
2023-07-22T16:29:12 [INFO] [Thread: 192.168.0.200:443/TCP] [Site: Test] [http_header.server] Matching against banner: Apache
2023-07-22T16:29:12 [INFO] [Thread: 192.168.0.200:443/TCP] [Site: Test] Creating ServiceFingerprint [[certainty=0.9][description=Apache HTTPD][family=Apache][product=HTTPD][protocol=HTTP]
TPS][vendor=Apache][version=null]]
2023-07-22T16:29:12 [INFO] [Thread: 192.168.0.200:443/TCP] [Site: Test] Checking for SERVER match to: Apache
2023-07-22T16:29:12 [INFO] [Thread: 192.168.0.200:443/TCP] [Site: Test] [http_header.server] Matching against banner: Apache
2023-07-22T16:29:12 [INFO] [Thread: 192.168.0.200:443/TCP] [Site: Test] Revoking ServiceFingerprint [[certainty=0.9][description=Apache HTTPD][family=Apache][product=HTTPD][protocol=HTTP]
TPS][vendor=Apache][version=null]]
2023-07-22T16:29:12 [INFO] [Thread: 192.168.0.200:443/TCP] [Site: Test] Creating ServiceFingerprint [[certainty=0.9][description=Apache HTTPD][family=Apache][product=HTTPD][protocol=HTTP]
TPS][vendor=Apache][version=null]]
2023-07-22T16:29:12 [INFO] [Thread: 192.168.0.200:443/TCP] [Site: Test] [favicon.md5] Matching against banner: 7b0d4bc0ca1659d54469e5013a08d240
2023-07-22T16:29:12 [INFO] [Thread: 192.168.0.200:443/TCP] [Site: Test] Creating SystemFingerprint [[architecture=null][certainty=0.5][description=Netgear Linux][deviceClass=null][family=null][product=Linux][vendor=Netgear][version=null]]
2023-07-22T16:29:12 [INFO] [Thread: 192.168.0.200:443/TCP] [Site: Test] Enumerating SSL/TLS protocol versions and cipher suites
2023-07-22T16:29:18 [INFO] [Thread: 192.168.0.200:5353/UDP] [Site: Test] Fingerprinting ran for 10 seconds.
2023-07-22T16:29:18 [INFO] [Thread: 192.168.0.200:5353/UDP] [Site: Test] Fingerprinted: mDNS
2023-07-22T16:29:18 [INFO] [Thread: 192.168.0.200:5353/UDP] [Site: Test] Fingerprinting thread complete...
2023-07-22T16:29:18 [INFO] [Thread: convert-open-udp-ports-to-services@192.168.0.200] [Site: Test] Protocol fingerprinting ran for 10 seconds.
2023-07-22T16:29:18 [INFO] [Thread: convert-open-udp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:111/udp] Running UDP service portmapper
2023-07-22T16:29:18 [INFO] [Thread: convert-open-udp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:5353/udp] Running UDP service mDNS
2023-07-22T16:29:18 [INFO] [Thread: convert-open-udp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200] SystemFingerprint [[architecture=PADRE][certainty=0.5][description=LINUX][deviceClass=null][family=null][product=LINUX][vendor=null][version=null]] source: mDNS
2023-07-22T16:29:18 [INFO] [Thread: convert-open-udp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200] mDNS name: NAS-BACKUP
2023-07-22T16:29:18 [INFO] [Thread: convert-open-udp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:111/tcp] Running TCP service portmapper
2023-07-22T16:29:18 [INFO] [Thread: convert-open-udp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:137/udp] Running UDP service CIFS Name Service
```

Important configuration settings / knowledge

Scanning groups / Asset Groups

- Configure scans for known assets (auth)
- Configure scans for network areas
- Configure scans for reporting types
- Agents (deployed)



How often should we run the scans?

1. What is the Policy requirement?
 - a. Asset Discovery cycles
 - b. Vulnerability Scan cycles
 - c. Compliance Scan cycles
2. What is the true remediation cycle?
 - a. How often does Engineering patch/remediate?
 - b. SLAs / OLAs?
3. Discovery / Improvement / Reporting cycles and processes
 - a. What are YOUR VM improvement cycles?
 - b. Leadership / Management reporting cycles (Board / Leadership presentations)
 - c. Remediation reporting cycles



We ran the scan, now what?

1. Report output types
 - a. PDF - High level, Metrics
 - b. CSV, XML - Detailed, Automation*
2. Review the data
 - a. Do the findings look right?
 - b. Scan failures?
3. Report the findings
 - a. Executives - High level metrics
 - b. Engineering - Engagement model, details
 - c. Compliance - Evidence of scans



Upleveling the vulnerability scanning processes

1. Run ALL IP / ALL Port scans*

- a. You'd be surprised what lurks beneath
- b. Find Shadow IT / OT

2. Review Asset / Network source information

- a. Trust but verify!
- b. Ask for access to management sources (System Management, Cloud infra, Network Architecture)

3. **Don't play whack-a-mole**

- a. Top 10 Vulnerability Root Causes
- b. Engineering Maturity Milestones (Engage with EA)
- c. Asset Baselines / Secure configurations

Questions?

