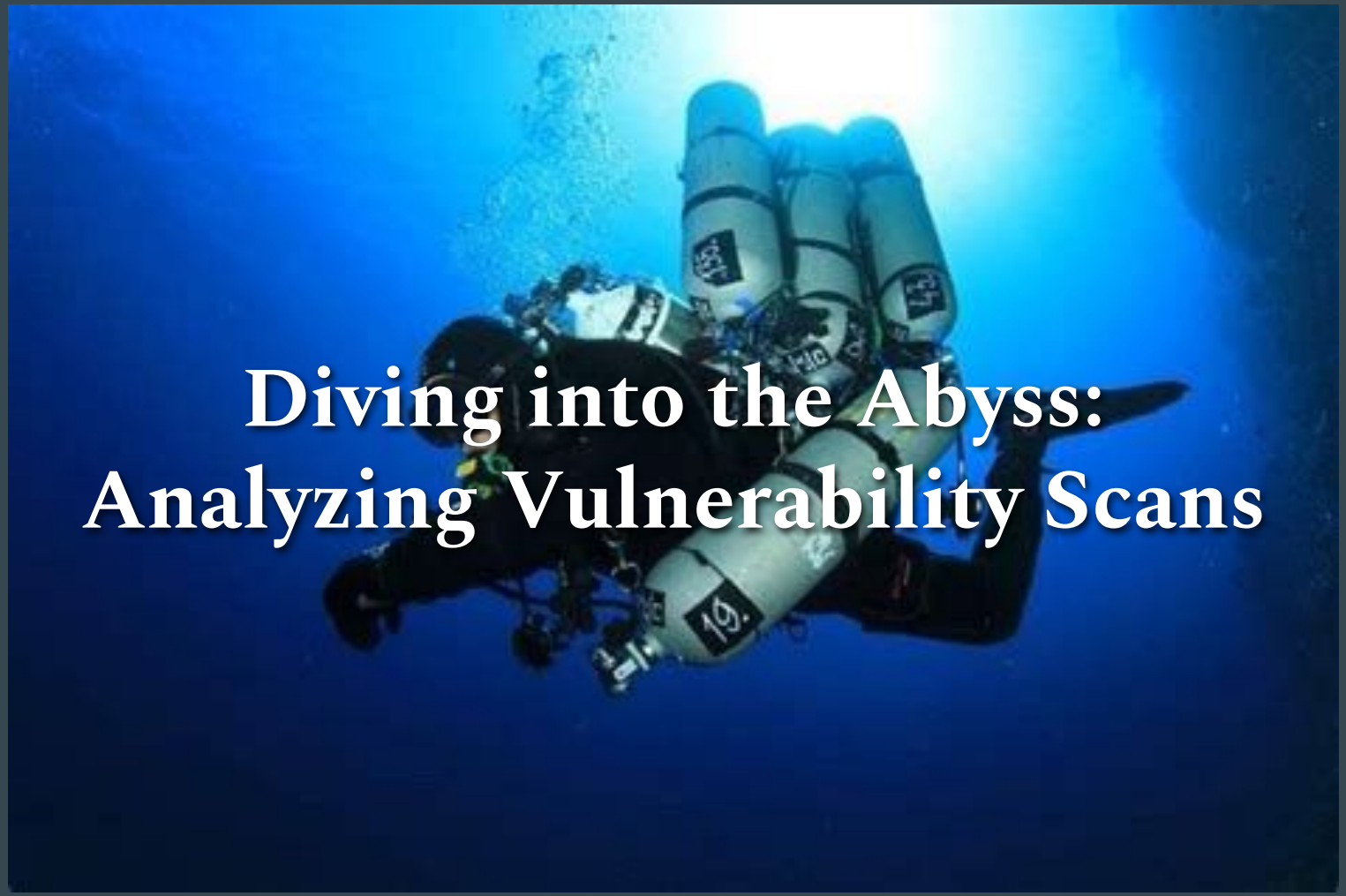


Diving into the Abyss: Analyzing Vulnerability Scans

BIO

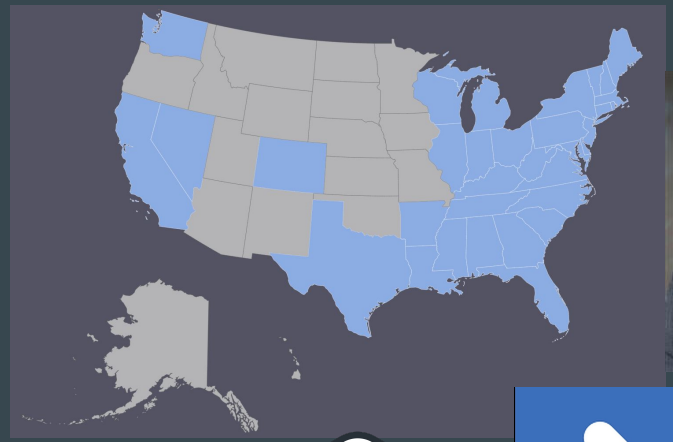
Joe Tegg

- Husband
- Father
- 25yr+ Security guy
- Recovering BOFH
- Technical Diver

BIO

Edwin Perez

- Avid Learner
- Enjoy Traveling
- Aspiring Pentester



Find this presentation online

https://github.com/avgjoesecurity

WARNING


MEMES
BECAUSE USING YOUR OWN WORDS IS JUST TOO MUCH WORK
imgflip.com

Agenda

01 **Gear Up**

- What is an infrastructure vulnerability scanner?
- Examples - Common Tools
- General Architecture

02 **Jump Off the Boat**

- Why Infrastructure Scan?
- Scan Process Review
- Target Identification
- Finger Printing - Is it a Mermaid or a Manatee?

!! BREAK !!

03 **Dive! Dive! Dive!**

- Verbose Scan Logs - Descend on the line
- Vulnerability Checks - Switch to your deep mix
- Custom Vulnerability Checks - Hit the wreck, swim around and return

04 **Decompress and Surface**

- Infrastructure VM Best Practices - Slow Ascent
- Informationals Matter Too - Safety Stop
- Questions - Surface and flag the boat

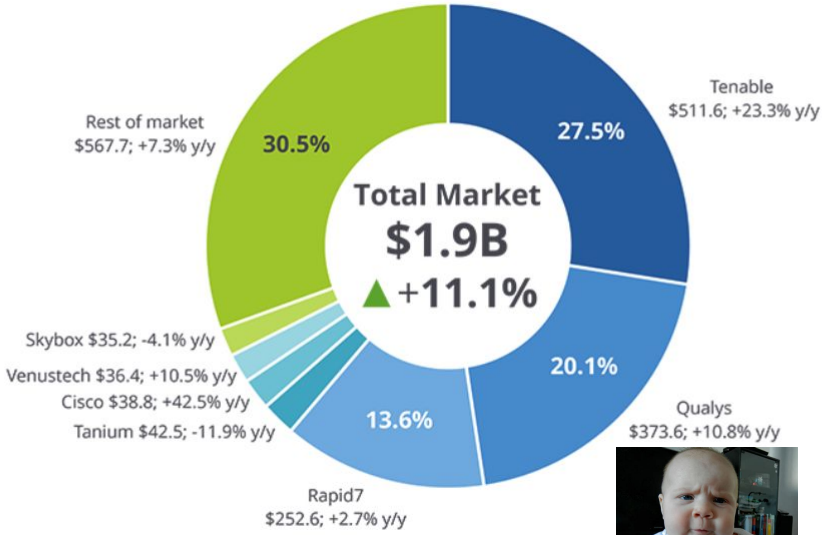
What is an Infrastructure Vulnerability Scanner?

NIST: (NISTIR 8011 Vol. 4)

“A network tool (hardware and/or software) that scans network devices to identify generally known and organization specific CVEs. It may do this based on a wide range of signature strategies.”

Vulnerability Scanners

Figure 1: **Worldwide Device Vulnerability Management 2021 Share Snapshot**

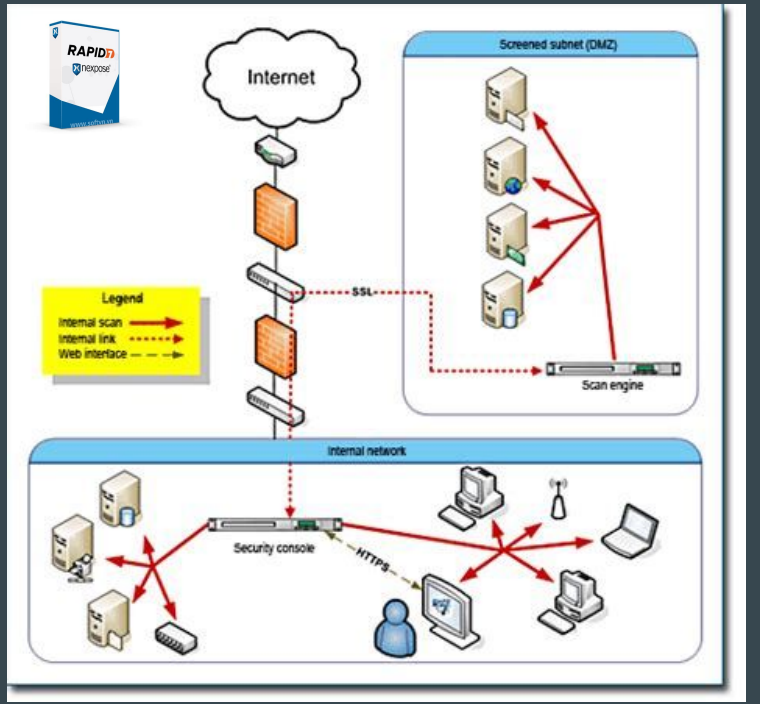


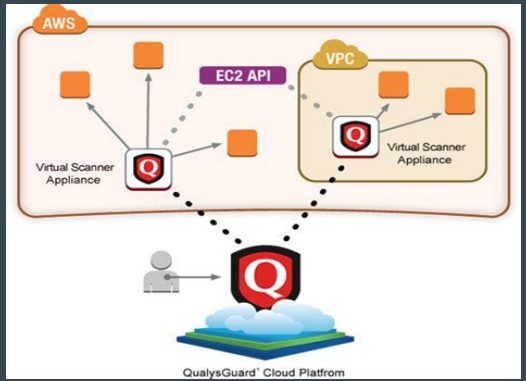
Note: 2021 Share (%), Revenue ($M), and Growth (%)
Source: IDC, 2022

Traditional Scanning:
OpenVAS
Reskins
NMAP

Nextgen Cloud:
Palo Prisma Cloud
Wiz
Aquasec

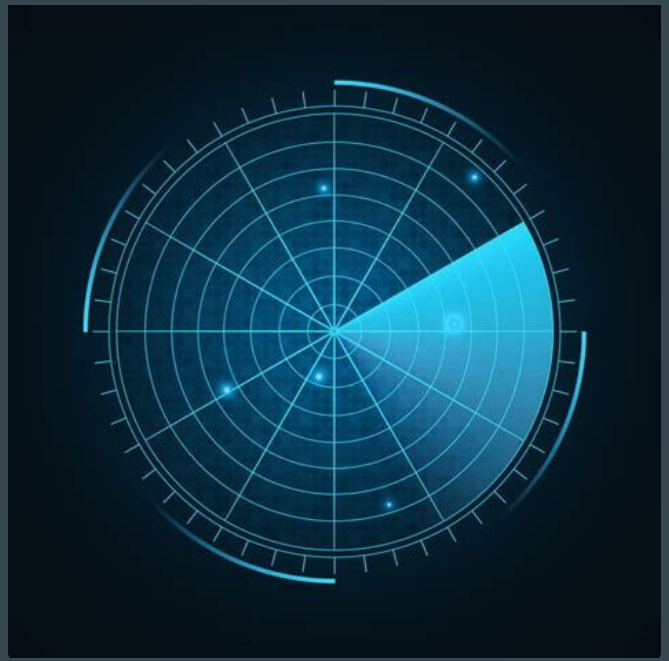
General Architecture





Why Infrastructure Scans?

- Network Enumeration
- Asset Identification
- Vulnerability Exposure Identification
- Compliance Verification (PCI, Baselines, etc)
- Attackers do.



Vulnerability Scanners - Just NMAP With a Wetsuit?

Vulnerability Scan Process Review

1. Target Identification - (NMAP)
2. Port Identification - (NMAP)
3. Service Identification - (NMAP)
4. Target Fingerprinting - (NMAP, Scanning Tool)
5. Service Fingerprinting - (NMAP, Scanning Tool)
6. Vulnerability Check Selection - (Scanning Tool)
7. Vulnerability Check Analysis - (Scanning Tool)
8. Collect / Store - (Scanning Tool)

Target Identification (Vulnerability Scanners)

- A combination of connection requests:
  - ARP
  - ICMP echo requests (pings)
  - TCP packets
  - UDP packets

Target Identification (NMAP)

- Going beyond just PING
- Identifying targets varies greatly depending on purpose (system admin, auditor, etc)
  - NMAP is extremely flexible and allows for multiple ways of scanning

- By default, if no host discovery options are given, nmap sends:
  - an ICMP echo request
  - a TCP SYN packet to port 443
  - a TCP ACK packet to port 80
  - an ICMP timestamp request
  - For IPv6, the ICMP timestamp request is omitted

- The flags -sn (no port scan, just host discovery) and -Pn (no ping, assume host is up) can also be used

Target Identification - Tenable Default Settings

- The four types of ping methods that Tenable uses are ARP, ICMP, TCP, and UDP
- These are ran in the following descending order
  - ARP (only when a scanner is on the same subnet as the target)
  - ICMP
  - TCP
  - UDP (if enabled in the scan)

- Scans only use the highest enabled ping method in the hierarchy
  - If the ARP scan is enabled, the ICMP and TCP scan will not run even if selected

- As a default, if a host does not respond to a ping, it will not be scanned and the scan will end

LOG REVIEW FOR TARGET IDENTIFICATION

```
163 2023-07-22T16:28:57 [INFO] [Thread: Scan 5] [Site: Test] NMAP: IPV4 ARGUMENTS: /opt/rapid7/nexpose/nse/nmap/nmap --privileged -n -PE -PS21-23,25,53,80,110-111,135,139,143,443,445,993,995,1723,3306,3389,5900,
    8080 -PU53,67-69,123,135,137-139,161-162,445,500,514,520,631,1434,1900,4500,5353,49152 -sS -sU -O --osscan-guess --max-os-tries 1 -p T:1-1040,1080,1098-1099,1125,1194,1214,1220,1352,1433,1500,1503,1521,1524,
    1526,1720,1723,1731,1812-1813,1818-1819,1895,1953,1959,1981,2000,2002,2030,2049,2100,2200,2222,2301,2375,2379,2381,2401,2433,2456,2500,2556,2745,3000-3001,3121,3127-3128,3230-3235,3268-3269,3306,3339,3389,
    3460,3527,4000,4045,4100,4242,4430,4443-4444,4505-4506,4661-4662,4711,4786,4848,5000,5010,5059-5061,5101,5180,5190-5193,5250,5432,5554-5555,5560,5566,5631,5678,5800-5803,5900-6009,6101,6106,6112,6346,6379,
    6565,6588,6777,7001-7002,7070,7100,7272,7510,7777-7778,7990,8000-8001,8004-8005,8008,8080-8083,8095,8098-8100,8153-8154,8180-8181,8282,8383-8384,8443-8444,8470-8480,8500,8787,8866,8888,9090,9100-9102,9292,
    9343,9443,9470-9476,9480,9495,9996,9999-10000,10025,10168,11211,12345-12346,13659,16080,18181-18185,18207-18208,18231-18232,18983,19190-19191,20034,21047,22226,27000-27010,27017,27374,27665,31337,32764,32771,
    33333,49152,49400,50000,51080,51443,54320,60000,60148,63148,U:7,9,11,13,17,19,37,53,67-69,88,111,123,135,137-139,161-162,177,213,259-260,445,464,500,514,520,523,623,631,749-751,1194,1434,1701,1812-1813,1900,
    2049,2746,3230-3235,3401,4045,4500,4665-4666,4672,5059-5061,5351,5353,5632,6429,7777,9100-9102,11211,17185,18233,23945,26000-26004,26198,27015-27030,27444,27960-27964,30720-30724,31337,31400,32771,34555,44400,
    47545,49152,54321 --max-retries 2 --min-rtt-timeout 500ms --max-rtt-timeout 1485ms --initial-rtt-timeout 500ms --defeat-rst-ratelimit --min-rate 3003 --max-rate 15000 --script-args=vulns.showall
    --script=mobileiron-sentry-detection.nse,ssh-hostkey.nse,ssh2-enum-algos.nse,codemeter-detection.nse,microsoft-exchange-server-detection.nse,pulse-connect-secure-detection.nse,kaseya-vsa-detection.nse,
    mobileiron-core-mult-vuln.nse,mobileiron-core-detection.nse,open-management-infrastructure-rce-vuln.nse,accellion-fta-detection.nse,kaseya-vsa-auth-bypass-vuln.nse,microsoft-exchange-server-mult-vuln.nse
    --script-timeout 180 --datadir /opt/rapid7/nexpose/plugins/nmap-config -oX - -v
164 2023-07-22T16:28:57 [INFO] [Thread: Scan 5] [Site: Test] NMAP: IPV6 ARGUMENTS: /opt/rapid7/nexpose/nse/nmap/nmap --privileged -n -PE -PS21-23,25,53,80,110-111,135,139,143,443,445,993,995,1723,3306,3389,5900,
    8080 -PU53,67-69,123,135,137-139,161-162,445,500,514,520,631,1434,1900,4500,5353,49152 -sS -sU -O --osscan-guess --max-os-tries 1 -p T:1-1040,1080,1098-1099,1125,1194,1214,1220,1352,1433,1500,1503,1521,1524,
    1526,1720,1723,1731,1812-1813,1818-1819,1895,1953,1959,1981,2000,2002,2030,2049,2100,2200,2222,2301,2375,2379,2381,2401,2433,2456,2500,2556,2745,3000-3001,3121,3127-3128,3230-3235,3268-3269,3306,3339,3389,
    3460,3527,4000,4045,4100,4242,4430,4443-4444,4505-4506,4661-4662,4711,4786,4848,5000,5010,5059-5061,5101,5180,5190-5193,5250,5432,5554-5555,5560,5566,5631,5678,5800-5803,5900-6009,6101,6106,6112,6346,6379,
    6565,6588,6777,7001-7002,7070,7100,7272,7510,7777-7778,7990,8000-8001,8004-8005,8008,8080-8083,8095,8098-8100,8153-8154,8180-8181,8282,8383-8384,8443-8444,8470-8480,8500,8787,8866,8888,9090,9100-9102,9292,
    9343,9443,9470-9476,9480,9495,9996,9999-10000,10025,10168,11211,12345-12346,13659,16080,18181-18185,18207-18208,18231-18232,18983,19190-19191,20034,21047,22226,27000-27010,27017,27374,27665,31337,32764,32771,
    33333,49152,49400,50000,51080,51443,54320,60000,60148,63148,U:7,9,11,13,17,19,37,53,67-69,88,111,123,135,137-139,161-162,177,213,259-260,445,464,500,514,520,523,623,631,749-751,1194,1434,1701,1812-1813,1900,
    2049,2746,3230-3235,3401,4045,4500,4665-4666,4672,5059-5061,5351,5353,5632,6429,7777,9100-9102,11211,17185,18233,23945,26000-26004,26198,27015-27030,27444,27960-27964,30720-30724,31337,31400,32771,34555,44400,
    47545,49152,54321 --max-retries 2 --min-rtt-timeout 500ms --max-rtt-timeout 1485ms --initial-rtt-timeout 500ms --defeat-rst-ratelimit --min-rate 3003 --max-rate 15000 --script-args=vulns.showall
    --script=mobileiron-sentry-detection.nse,ssh-hostkey.nse,ssh2-enum-algos.nse,codemeter-detection.nse,microsoft-exchange-server-detection.nse,pulse-connect-secure-detection.nse,kaseya-vsa-detection.nse,
    mobileiron-core-mult-vuln.nse,mobileiron-core-detection.nse,open-management-infrastructure-rce-vuln.nse,accellion-fta-detection.nse,kaseya-vsa-auth-bypass-vuln.nse,microsoft-exchange-server-mult-vuln.nse
    --script-timeout 180 --datadir /opt/rapid7/nexpose/plugins/nmap-config -oX - -v -6
```

LOG REVIEW FOR TARGET IDENTIFICATION

```
2023-07-21T20:49:26 [INFO] [Thread: Scan 2] [Site: Test] NMAP: IPV4 ARGUMENTS: /opt/rapid7/nexpose/nse/nmap/nmap --privileged -n -PE -PS21-23,25,53,80,110-111,135,139,143,443,445,993,995,1723,3306,3389,5900,8
2023-07-21T20:49:26 [INFO] [Thread: Scan 2] [Site: Test] NMAP: IPV6 ARGUMENTS: /opt/rapid7/nexpose/nse/nmap/nmap --privileged -n -PE -PS21-23,25,53,80,110-111,135,139,143,443,445,993,995,1723,3306,3389,5900,8
2023-07-21T20:49:26 [INFO] [Thread: Scan 2] [Site: Test] Nmap phase started.
2023-07-21T20:49:26 [INFO] [Thread: Scan 2] [Site: Test] Nmap will scan 65536 IP addresses at a time.
2023-07-21T20:49:26 [INFO] [Thread: Scan 2] [Site: Test] Nmap scan of 100 IP addresses starting.
2023-07-21T20:49:26 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] Nmap task NSE started.
2023-07-21T20:49:26 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] Nmap task NSE completed.
2023-07-21T20:49:26 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] Nmap task NSE started.
2023-07-21T20:49:26 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] Nmap task NSE completed.
2023-07-21T20:49:26 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] Nmap task ARP Ping Scan started.
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] Nmap task ARP Ping Scan completed.
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.40] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.41] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.42] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.43] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.44] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.46] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.47] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.32] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.33] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.34] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.35] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.36] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.37] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.38] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.39] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.56] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.57] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.58] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.59] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.60] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.61] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.62] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.63] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.48] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.49] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.51] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.52] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.53] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.54] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.8] DEAD (reason=no-response)
2023-07-21T20:49:28 [INFO] [Thread: Scan 2:nmap:stdin] [Site: Test] [192.168.0.12] DEAD (reason=no-response)
```

Port Identification (NMAP)

- At its simplest form, nmap will scan for 1,000 TCP ports

  nmap [TARGET]

- Nmap divides ports into six states
  - open
  - closed
  - filtered
  - unfiltered
  - open | filtered
  - closed | filtered

- Even though nmap can be ran with general user privileges, most of the scan types are only available to privileged users.

LOG REVIEW FOR PORT IDENTIFICATION

```
1473  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:789/TCP] CLOSED (reason=reset:TTL=64)
1474  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:2456/TCP] CLOSED (reason=reset:TTL=64)
1475  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:8098/TCP] CLOSED (reason=reset:TTL=64)
1476  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:218/TCP] CLOSED (reason=reset:TTL=64)
1477  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:494/TCP] CLOSED (reason=reset:TTL=64)
1478  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:727/TCP] CLOSED (reason=reset:TTL=64)
1479  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:71/TCP] CLOSED (reason=reset:TTL=64)
1480  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:197/TCP] CLOSED (reason=reset:TTL=64)
1481  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:248/TCP] CLOSED (reason=reset:TTL=64)
1482  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:259/UDP] FILTERED (reason=no-response:TTL=0)
1483  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:759/TCP] CLOSED (reason=reset:TTL=64)
1484  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:5250/TCP] CLOSED (reason=reset:TTL=64)
1485  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:8472/TCP] CLOSED (reason=reset:TTL=64)
1486  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:32/TCP] CLOSED (reason=reset:TTL=64)
1487  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:533/TCP] CLOSED (reason=reset:TTL=64)
1488  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:658/TCP] CLOSED (reason=reset:TTL=64)
1489  2023-07-22T16:09:37 [INFO] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:111/UDP] OPEN (reason=udp-response:TTL=64)
1490  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:426/TCP] CLOSED (reason=reset:TTL=64)
1491  2023-07-22T16:09:37 [INFO] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:443/TCP] OPEN (reason=syn-ack:TTL=64)
1492  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:4045/UDP] FILTERED (reason=no-response:TTL=0)
1493  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:640/TCP] CLOSED (reason=reset:TTL=64)
1494  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:140/TCP] CLOSED (reason=reset:TTL=64)
1495  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:706/TCP] CLOSED (reason=reset:TTL=64)
1496  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:924/TCP] CLOSED (reason=reset:TTL=64)
1497  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:7778/TCP] CLOSED (reason=reset:TTL=64)
1498  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:96/TCP] CLOSED (reason=reset:TTL=64)
1499  2023-07-22T16:09:37 [DEBUG] [Thread: Scan 4:nmap:stdin] [Site: Test] [192.168.0.200:8004/TCP] CLOSED (reason=reset:TTL=64)
```

Service Identification (NMAP)

- Nmap uses its nmap-services database, has about 2,200 well-known services
- Nmap also sends service-specific probes
- Miscellaneous information discovered about a service is collected in the “info” field. This is displayed in the VERSION column inside parentheses following the product name and version number.

LOG REVIEW FOR SERVICE IDENTIFICATION

```
9427  2023-07-22T16:19:58 [INFO] [Thread: 192.168.0.200:50000/TCP] [Site: Test] Fingerprinting thread complete...
9428  2023-07-22T16:19:58 [INFO] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] Protocol fingerprinting ran for 10 minutes 20 seconds.
9429  2023-07-22T16:19:58 [INFO] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:548/tcp] Running TCP service AFP
9430  2023-07-22T16:19:58 [INFO] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:111/udp] Running UDP service portmapper
9431  2023-07-22T16:19:58 [DEBUG] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:111/udp] Asserting ServiceConfiguration: {port.discovered.from=tcp/111,
      program-number=100000, program-version=2}
9432  2023-07-22T16:19:58 [INFO] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:80/tcp] Running TCP service HTTP
9433  2023-07-22T16:19:58 [INFO] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:80/tcp] Service running: ServiceFingerprint [[certainty=0.9][description=Apache HTTPD]
      [family=Apache][product=HTTPD][protocol=HTTP][vendor=Apache][version=null]]
9434  2023-07-22T16:19:58 [DEBUG] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:80/tcp] Asserting ServiceConfiguration: {http.banner=Apache, http.banner.server=Apache}
9435  2023-07-22T16:19:58 [INFO] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:111/tcp] Running TCP service portmapper
9436  2023-07-22T16:19:58 [DEBUG] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:111/tcp] Asserting ServiceConfiguration: {port.discovered.from=tcp/111,
      program-number=100000, program-version=2}
9437  2023-07-22T16:19:58 [INFO] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:445/tcp] Running TCP service CIFS
9438  2023-07-22T16:19:58 [INFO] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:445/tcp] Service running: ServiceFingerprint [[certainty=1.0][description=Samba 3.5.22]
      [family=null][product=Samba][protocol=CIFS][vendor=null][version=3.5.22]]
9439  2023-07-22T16:19:58 [DEBUG] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:445/tcp] Asserting ServiceConfiguration: {domain=BACKUP, guest-login=enabled,
      password-mode=encrypt, security-mode=user, smb-signing=disabled, smb1-enabled=true}
9440  2023-07-22T16:19:58 [DEBUG] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200] Setting System Configuration: domain=BACKUP
9441  2023-07-22T16:19:58 [DEBUG] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200] Setting System Configuration: guest-login=enabled
9442  2023-07-22T16:19:58 [DEBUG] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200] Setting System Configuration: password-mode=encrypt
9443  2023-07-22T16:19:58 [DEBUG] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200] Setting System Configuration: security-mode=user
9444  2023-07-22T16:19:58 [DEBUG] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200] Setting System Configuration: smb-signing=disabled
9445  2023-07-22T16:19:58 [INFO] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:139/tcp] Running TCP service CIFS
9446  2023-07-22T16:19:58 [INFO] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:139/tcp] Service running: ServiceFingerprint [[certainty=1.0][description=Samba 3.5.22]
      [family=null][product=Samba][protocol=CIFS][vendor=null][version=3.5.22]]
9447  2023-07-22T16:19:58 [DEBUG] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:139/tcp] Asserting ServiceConfiguration: {domain=BACKUP, guest-login=enabled,
      password-mode=encrypt, security-mode=user, smb-signing=disabled, smb1-enabled=true}
9448  2023-07-22T16:19:58 [INFO] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:443/tcp] Running TCP service HTTPS
9449  2023-07-22T16:19:58 [INFO] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:443/tcp] Service running: ServiceFingerprint [[certainty=0.9][description=Apache HTTPD]
      [family=Apache][product=HTTPD][protocol=HTTPS][vendor=Apache][version=null]]
9450  2023-07-22T16:19:58 [DEBUG] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:443/tcp] Asserting ServiceConfiguration: {http.banner=Apache, http.banner.server=Apache,
      ssl=true, ssl.cert.chainerror=[Path does not chain with any of the trust anchors], ssl.cert.issuer.dn=CN=192.168.0.59, C=US, ssl.cert.key.alg.name=RSA, ssl.cert.key.rsa.modulusBits=1024, ssl.cert.not.valid.
      after=Mon, 18 Jan 2038 08:29:09 EST, ssl.cert.not.valid.before=Sat, 01 Oct 2016 09:29:09 EDT, ssl.cert.selfsigned=true, ssl.cert.serial.number=9965995117110924570, ssl.cert.sha1.
      fingerprint=9dcc9233cb4c35a3a3ee3e875e60728bd9076d64, ssl.cert.sig.alg.name=SHA1withRSA, ssl.cert.subject.dn=CN=192.168.0.59, C=US, ssl.cert.validchain=false, ssl.cert.validsignature=true, ssl.cert.version=1,
      ssl.dh.generator.1024=2, ssl.dh.prime.
      1024=d67de440cbbbdc1936d693d34afd0ad50c84d239a45f520bb88174cb98bce951849f912e639c72fb13b4b4d7177e16d55ac179ba420b2a29fe324a467a635e81ff5901377beddcfd33168a461aad3b72dae8860078045b07a7dbca7874087d1510ea9fcc9ddd
      330507dd62db88aeaa747de0f4d6e2bd68b0e7393e0f24218eb3, ssl.protocols=tlsv1_0, sslv2=false, sslv3=false, tlsv1_0=true, tlsv1_0.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize=1024, tlsv1_0.
      TLS_DHE_RSA_WITH_AES_256_CBC_SHA.dh.keysize=1024, tlsv1_0.ciphers=TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,
      TLS_RSA_WITH_3DES_EDE_CBC_SHA, tlsv1_0.extensions=RENEGOTIATION_INFO, tlsv1_1=false, tlsv1_2=false, tlsv1_3=false, verbs-1=GET, verbs-2=HEAD, verbs-3=OPTIONS, verbs-4=POST, verbs-count=4}
9451  2023-07-22T16:19:58 [INFO] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200] SystemFingerprint [[architecture=null][certainty=0.5][description=Netgear Linux]
      [deviceClass=null][family=null][product=Linux][vendor=Netgear][version=null]] source: HTTPS
9452  2023-07-22T16:19:58 [INFO] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:50000/tcp] Running TCP service HTTP
9453  2023-07-22T16:19:58 [INFO] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:631/tcp] Running TCP service HTTP
9454  2023-07-22T16:19:58 [INFO] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:631/tcp] Service running: ServiceFingerprint [[certainty=0.9][description=Apple CUPS 1.1]
      [family=CUPS][product=CUPS][protocol=HTTP][vendor=Apple][version=1.1]]
9455  2023-07-22T16:19:58 [DEBUG] [Thread: convert-open-tcp-ports-to-services@192.168.0.200] [Site: Test] [192.168.0.200:631/tcp] Asserting ServiceConfiguration: {http.banner=CUPS/1.1, http.banner.server=CUPS/1.1,
      verbs-1=GET, verbs-2=HEAD, verbs-3=OPTIONS, verbs-4=POST, verbs-5=PUT, verbs-count=5}
```

Target Fingerprinting - Is it a Mermaid or Manatee?

Target Fingerprinting (NMAP)

- Examining TCP/UDP/IP packets responses
- TCP ISN sampling
  - find patterns in the initial sequence numbers chosen by TCP implementations when responding to a connection request
- TCP options support and ordering
- IP ID sampling
  - Most operating systems increment a system-wide IPID value for each packet they send.
  - OpenBSD - uses a random IPID
  - Linux uses an IPID of 0 in many cases where the "Don't Fragment" bit is not set
  - Windows increments the IPID by 256 for each packet
- Window Size Check
  - window size on returned packets

Target Fingerprinting (NMAP)

- OS detection is more effective if at least one open and one closed TCP port are found.
- With the --osscan-limit option and Nmap will not even try OS detection against hosts which do not meet this criteria.
- This can save substantial time, particularly on -Pn scans against many hosts. You still need to enable OS detection with -O (or -A) for the --osscan-limit option to have any effect.
- If you specify the --osscan-guess option or the equivalent --fuzzy option, Nmap will guess more aggressively. Nmap still tells you when an imperfect match is found and display its confidence level percentage for each guess.
- When Nmap performs OS detection against a target and fails to find a perfect match, it usually repeats the attempt.
- By default, Nmap tries five times if conditions are favorable for OS fingerprint submission, and twice when conditions are not so good.
- The --max-os-tries option lets you change this maximum number of OS detection tries. Lowering it (usually to 1) speeds Nmap up, though you miss out on retries which could potentially identify the OS.

Target Fingerprinting (Scanning Tool)

- TCP/IP checks - not as reliable
  - OS guesses might be wrong and less of a chance of guessing the OS version correctly

- Other checks include: Banner grabs, Script injection, Analysis of SSL certificates, Queries of the protocols implemented on the host (Telnet, SinFP, etc), Structured ICMP pings, HTTP requests, Registry queries, Responses from authentication techniques (SMB, SSH, etc)

Target Fingerprinting (Scanning Tool)

- Tenable Plugin 11936
  - Various fingerprinting plugins give data back to this plugin and an overall score is compiled
  - Some of the fingerprint methods include: FTP, HTTP, LDAP, RDP, SMTP, SNMP, SSH and more

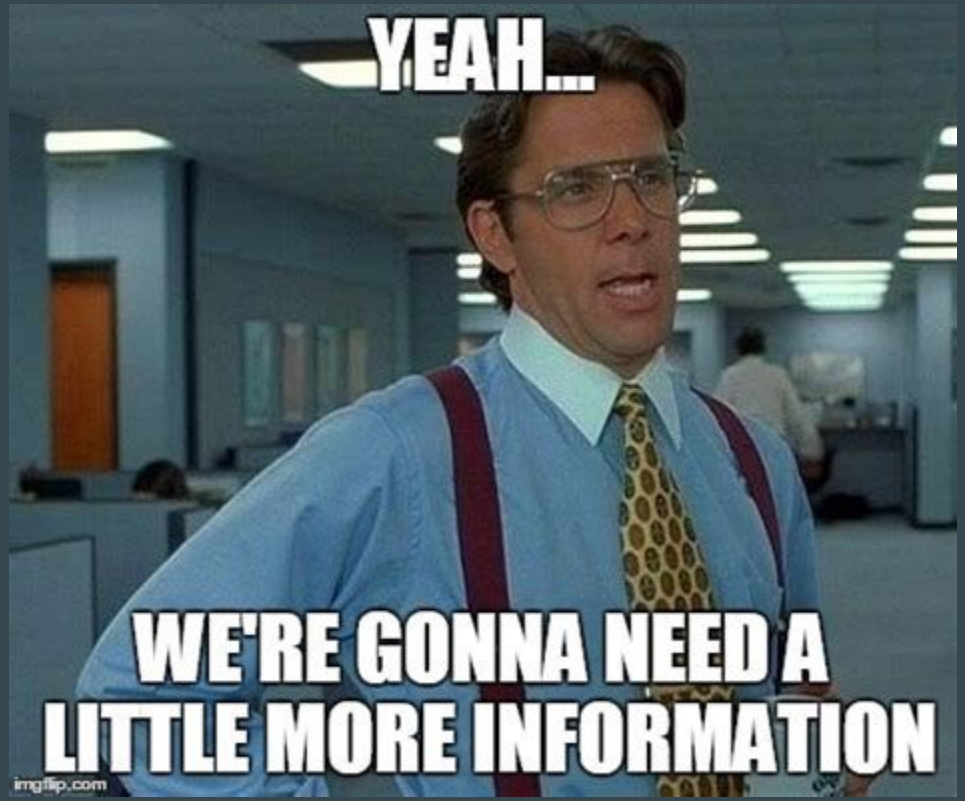
- It relies more on credential scans
  - OS fingerprints with higher confidence level percentages are based on querying the system after authentication

LOG REVIEW SYSTEM FINGERPRINT

```
870 2023-07-21T20:50:35 [INFO] [Thread: resolve-additional-dns-names@192.168.0.87] [Site: Test] [192.168.0.87] Finished resolving DNS records
871 2023-07-21T20:50:35 [INFO] [Thread: merge-system-fingerprints-thread@192.168.0.87] [Site: Test] [192.168.0.87] Promoting SystemFingerprint [[architecture=null][certainty=0.7][description=Linux 2.6.32 - 3.10]
    [deviceClass=General][family=Linux][product=LINUX 2.6.32 - 3.10][vendor=Linux][version=2.6.32]] source: IP stack analysis
872 2023-07-21T20:50:35 [INFO] [Thread: convert-open-tcp-ports-to-services@192.168.0.87] [Site: Test] Starting fingerprinting (is verbose)...
873 2023-07-21T20:50:35 [INFO] [Thread: 192.168.0.87:22/TCP] [Site: Test] Starting fingerprinting thread...
874 2023-07-21T20:50:35 [INFO] [Thread: 192.168.0.87:22/TCP] [Site: Test] [Preference: 1.0] Attempting handshake via SSH
875 2023-07-21T20:50:35 [INFO] [Thread: 192.168.0.87:22/TCP] [Site: Test] [ssh.banner] Matching against banner: dropbear_2020.81
876 2023-07-21T20:50:35 [INFO] [Thread: 192.168.0.87:22/TCP] [Site: Test] Creating ServiceFingerprint [[certainty=0.9][description=Dropbear SSH Project Dropbear SSH 2020.81][family=Dropbear][product=Dropbear SSH]
    [protocol=SSH][vendor=Dropbear SSH Project][version=2020.81]]
877 2023-07-21T20:50:35 [INFO] [Thread: 192.168.0.87:22/TCP] [Site: Test] Fingerprinting ran for 0 seconds.
878 2023-07-21T20:50:35 [INFO] [Thread: 192.168.0.87:22/TCP] [Site: Test] Fingerprinted: SSH
879 2023-07-21T20:50:35 [INFO] [Thread: 192.168.0.87:22/TCP] [Site: Test] Fingerprinting thread complete...
880 2023-07-21T20:50:35 [INFO] [Thread: convert-open-tcp-ports-to-services@192.168.0.87] [Site: Test] Protocol fingerprinting ran for 0 seconds.
881 2023-07-21T20:50:35 [INFO] [Thread: convert-open-tcp-ports-to-services@192.168.0.87] [Site: Test] [192.168.0.87:22/tcp] Running TCP service SSH
882 2023-07-21T20:50:35 [INFO] [Thread: convert-open-tcp-ports-to-services@192.168.0.87] [Site: Test] [192.168.0.87:22/tcp] Service running: ServiceFingerprint [[certainty=0.9][description=Dropbear SSH Project
    Dropbear SSH 2020.81][family=Dropbear][product=Dropbear SSH][protocol=SSH][vendor=Dropbear SSH Project][version=2020.81]]
883 2023-07-21T20:50:35 [INFO] [Thread: 192.168.0.11:161/UDP] [Site: Test] [snmp.sys_description] Matching against banner: HP ETHERNET MULTI-ENVIRONMENT,ROM none,JETDIRECT,JD137,EEPROM V.37.12,CIDATE 07/12/2010
884 2023-07-21T20:50:35 [INFO] [Thread: 192.168.0.11:161/UDP] [Site: Test] Creating SystemFingerprint [[architecture=null][certainty=0.8][description=HP JD137 none][deviceClass=Print Server][family=JetDirect]
    [product=JD137][vendor=HP][version=none]]
885 2023-07-21T20:50:35 [INFO] [Thread: 192.168.0.11:161/UDP] [Site: Test] [snmp.sys_object_id] Matching against banner: 1.3.6.1.4.1.11.2.3.9.1 HP ETHERNET MULTI-ENVIRONMENT,ROM none,JETDIRECT,JD137,EEPROM V.37.
    12,CIDATE 07/12/2010
886 2023-07-21T20:50:35 [INFO] [Thread: 192.168.0.11:161/UDP] [Site: Test] [snmp.sys_object_id] No matching fingerprint found for banner: 1.3.6.1.4.1.11.2.3.9.1 HP ETHERNET MULTI-ENVIRONMENT,ROM none,JETDIRECT,
    JD137,EEPROM V.37.12,CIDATE 07/12/2010
887 2023-07-21T20:50:35 [INFO] [Thread: 192.168.0.11:161/UDP] [Site: Test] No match found for SNMP banner: [sysObjectID: 1.3.6.1.4.1.11.2.3.9.1]
```

BREAK

Verbose Logging



Enabling Verbose Logging Overall

- Easiest way to understand what checks are being ran in a particular scan
- It is pretty verbose (in the magnitude of a few 100k lines per scan for a basic scan)
- Recommended to only use **as needed**

Where do logs live? - Nessus

The nessusd.messages file can be found in these directories

Windows

C:\ProgramData\Tenable\Nessus\nessus\logs\nessusd.messages

Linux

/opt/nessus/var/nessus/logs/nessusd.messages

MacOS

/Library/Nessus/run/var/nessus/logs/nessusd.messages

Where do logs live? - Nexpose

	Console	Scan Engine
Linux	/opt/rapid7/nexpose/nsc/logs/	/opt/rapid7/nexpose/nse/logs/
Windows	C:\Program Files\rapid7\nexpose\nsc\logs	C:\Program Files\rapid7\nexpose\nse\logs

Where do logs live? - Qualys

Windows Agent

C:\Program Data\Qualys\QualysAgent

Linux/BSD/Mac OS Agent

/var/log/qualys/

Enabling Verbose Logging for Nessus Part 1

- For all options ensure that you restart the service after changes are made

- Nessus GUI
  - Log into Nessus
  - In the top navigation, click Settings
  - In the left navigation, click Advanced
  - Click the Logging tab
  - Change the value for log_details to Yes
  - Change the value for log_whole_attack to Yes

Command Line Options per OS

Windows

"C:\Program Files\Tenable\Nessus\nessuscli.exe" fix --set log_details=true
"C:\Program Files\Tenable\Nessus\nessuscli.exe" fix --set log_whole_attack=true

Enabling Verbose Logging for Nessus Part 2

Linux

/opt/nessus/sbin/nessuscli fix --set log_details=true
/opt/nessus/sbin/nessuscli fix --set log_whole_attack=true

MacOS

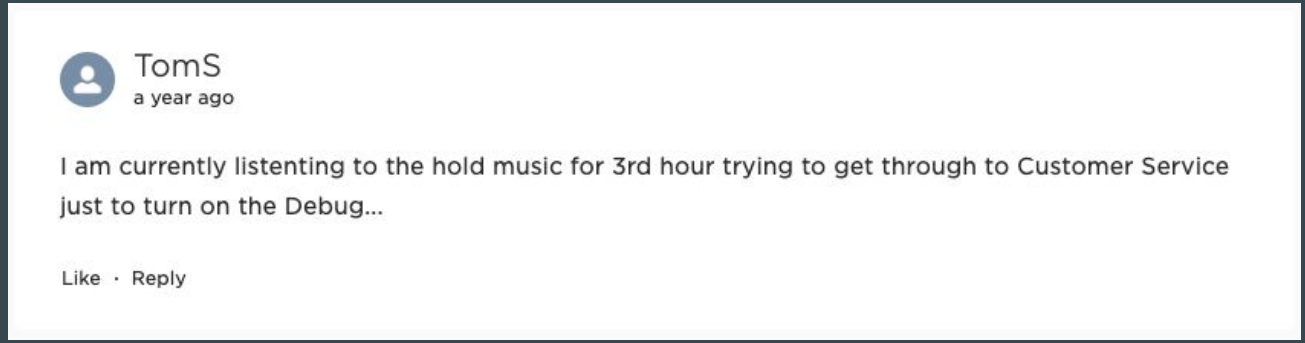
/Library/NessusAgent/run/sbin/nessuscli fix --set log_details=true
/Library/NessusAgent/run/sbin/nessuscli fix --set log_whole_attack=true

Enabling Verbose Logging for Nexpose

Enable Enhanced logging in a custom scan template

1. On the Administration page, click Scans > Templates.
2. In the configuration of the new template, click the Logging tab.
3. Select the Enhanced logging check box to enable Enhanced logging.
4. Configure the rest of the template as desired and save it.

Enabling Verbose Logging for Qualys



As of April 2023, Qualys introduced Debug Scan for VM Internal Scanner, though it needs to be enabled for the subscription first.

Launch the Debug Scan feature from the Setup UI
Select the "Enable Debug Scan" & click "Save"

Enabling Verbose Logging for Qualys

Launching a Debug Scan

1) Go to VM/VMDR > Scans > Scans > New > Debug Scan

2) Provide General Information (Name of scan, Scanner Debug Mode, Scanner Appliance)

3) Provide Launch Debug Information (IP Address/FQDN)

4) Launch

After completing the Debug Scans, the Scanner Appliance will automatically revert to normal. Still has a component where the Qualys Support Team may need to be involved

The pain of log verbosity (mainly comes from Qualys)

Vulnerability Checks

References:

Coding for Penetration Testers: Building Better Tools 2nd Edition - Jason Andress, Ryan Linn

Tenable

https://www.tenable.com/blog/using-the-nasl-nessus-command-line-tool

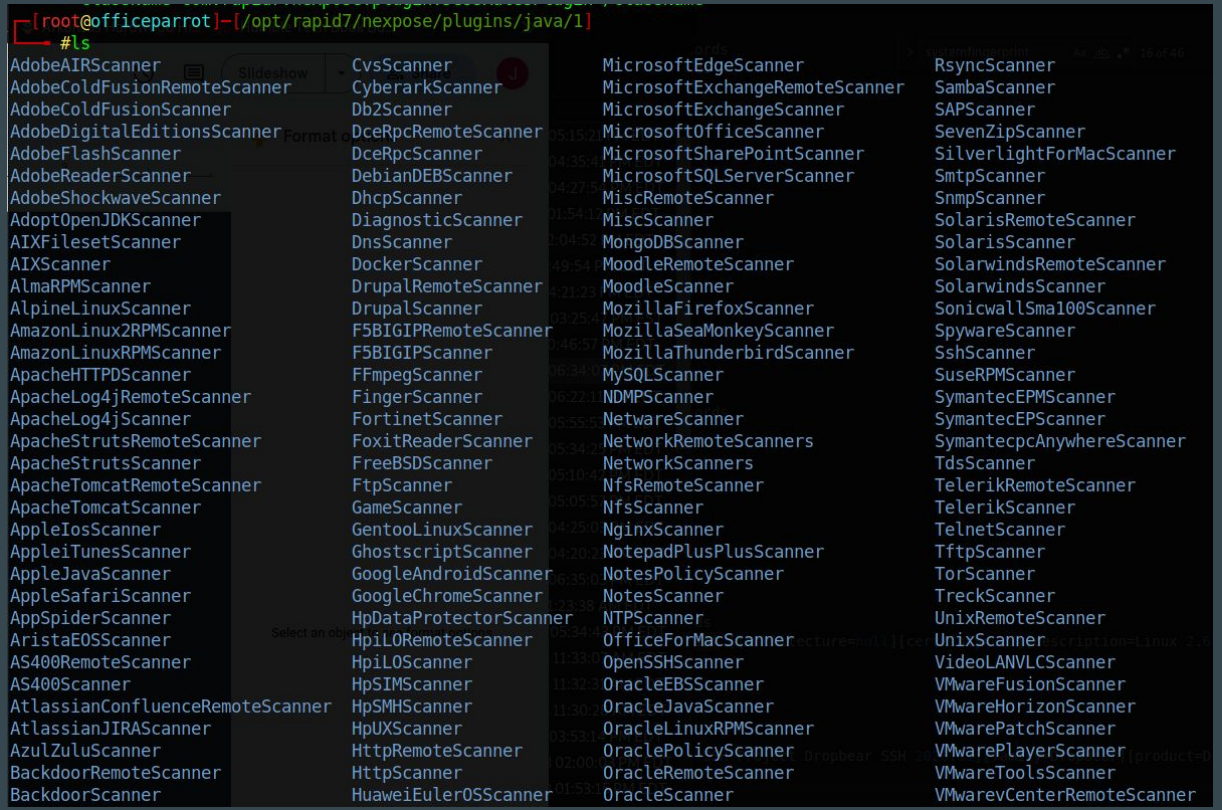
Rapid7

https://docs.rapid7.com/insightvm/writing-vulnerability-checks/

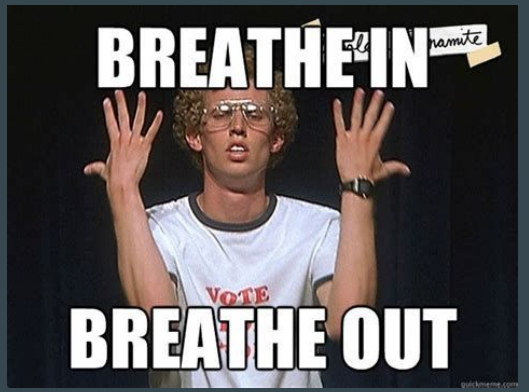
Qualys

https://www.qualys.com/docs/qualys-custom-vulnerability-checks-user-guide.pdf

Vulnerability Checks Deep Dive



Come up slowly...



Infrastructure Vulnerability Management - Best Practices

Asset Inventory

Patch Management

Risk Management

Compliance

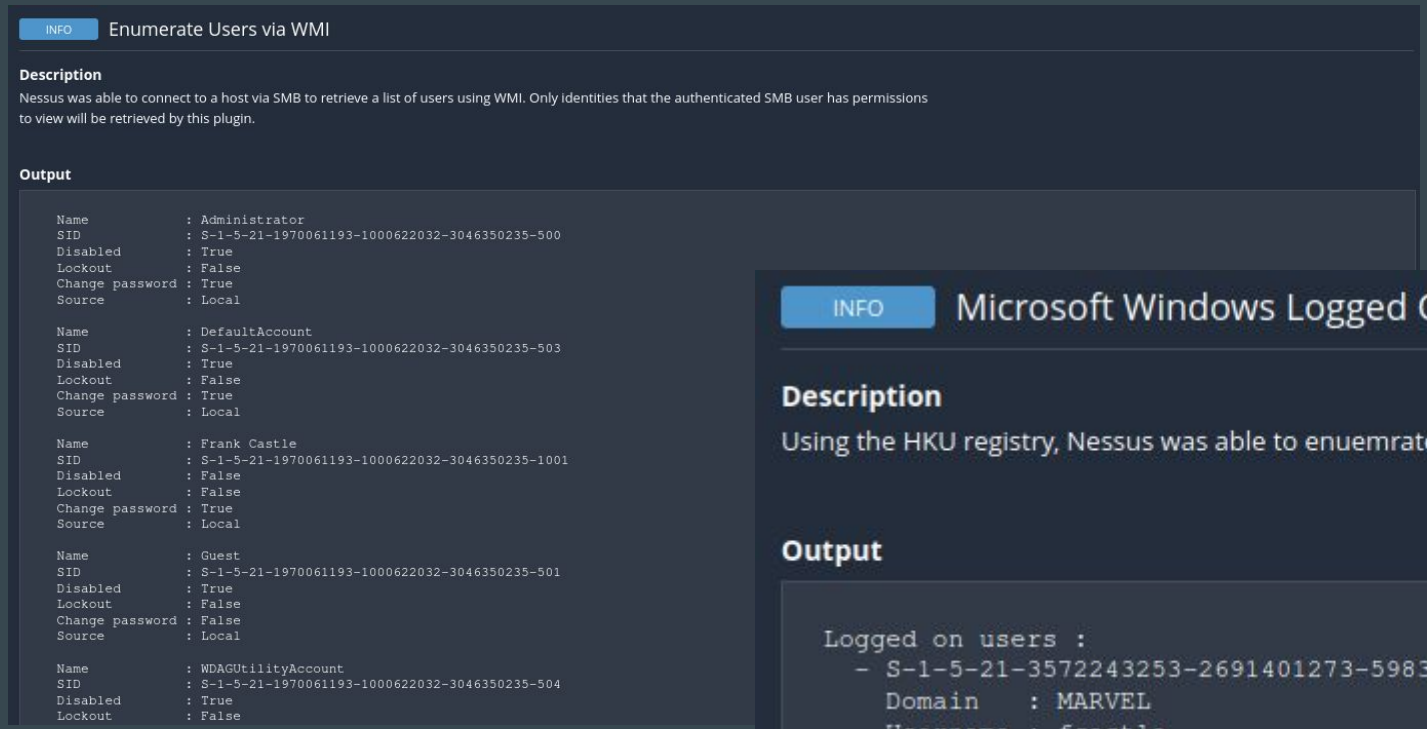
Automation

Continuous Monitoring

When does Vulnerability Management End?

The Often Forgotten Informationals

The Often Forgotten Informationals



Surface


NOT SURE IF THEY'RE CLAPPING FOR MY PRESENTATION
OR BECAUSE ITS FINISHED

Appendix

After this slide, there are a bunch of info slides in no specific order