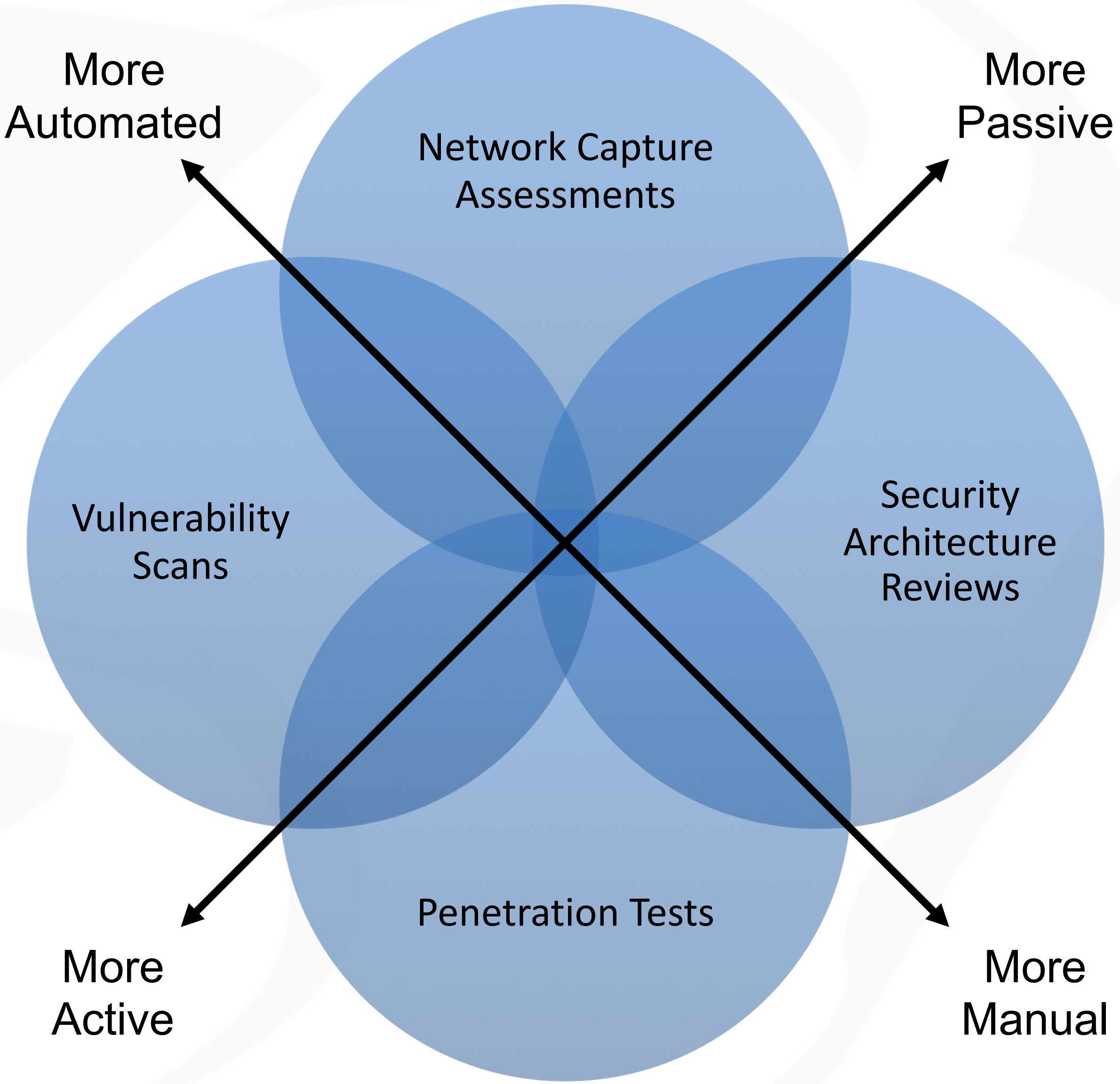
Scanning Highly Sensitive Networks

801-784-2052 // justin@controlthings.io

Types of Security Assessments

- We can perform many different types of security assessments to discover vulnerabilities in our systems and weaknesses in our defenses
- Each assessment type fills looks at the system from different perspectives and angles
- All types should be performed to gain a more complete picture
  - Some vulnerabilities might only be found using one type
  - Some tests increase system risk for increased visibility
  - Each type can be adapted to system and company needs



Dangers of Port Scanning

- Port scanning can crash legacy embedded systems if not careful! Here are the most likely causes:
  - OS Fingerprinting
    - Don't use the `-O` or `-A` flags in nmap
    - By far the moly likely cause of crashed embedded systems
    - Can do ARP scans locally on each subnet and use MAC to ID devices
  - Scanning with SYN scans
    - Default when using nmap with sudo or running it as root
    - Not proper RFC behavior, so only mature ICP/IP stacks handles this properly
    - Always specify `-sT` in your scans to avoid this accident
  - Scanning too fast (yes, the defaults in nmap are too fast)
    - Use nmap's `-T2` setting sets this at 0.4 seconds
    - Or use nmap's `--scan-delay 0.1` or `--max-parallelism 1` to scan 1 port at a time per host
  - Scanning UDP ports with null payloads **(can affect ICS software on Windows and Linux too!!!)**
    - Don't use the `-sU` option in nmap
  - Service fingerprinting usually safe, but can occasionally cause problems
    - Use nmap's `-sV` selectively on new subnets
    - Or use nmap's `--script=banner`

nmap Suggestions

- Always run nmap with sudo with -sT
  - nmap rarely tells you its needed (only says it for `-O`)
  - Requirements vary from OS to OS
  - Required for all ICMP functions
  - Required for OS fingerprinting
  - Required for some NSE scripts
  - If you don't believe me, make and diff some pcaps
- Its always good practice to use `-v` when scanning

Low Risk Portscans

```
sudo nmap –n -PR -sn
```

- Risk = Almost None (only does ARP request (IP -> MAC) which is required by TCP)
- Value = retrieves MAC address if IP is live, which can be used to fingerprint
- Note = this must be done from the SAME subnet as the IP being scanned

```
sudo nmap -n -sn
```

- Risk = Very Low (only sends ICMP and TCP80/443 ping requests)
- Value = shows if IP address is responding to pings
- Note = if done on same subnet, will retrieve MAC address

```
sudo nmap -n -sT --scan-delay 0.1 --top-ports 100 ...
```

- Risk = Low (scans each host's TCP ports serially with 1 second delays)
- Value = Medium (tests for most common TCP servers...but not sensitive/proprietary protocols)

```
sudo nmap -n -sT --scan-delay 0.1 -p ??? ...
```

- Risk = Low (scans each host's TCP ports serially with 1 second delays)
- Value = Medium (tests for whatever services you specify)

Medium to High Risk Port Scans

```
sudo nmap –n -sT --max-parallelism 1 -p ??? ...
```

- Risk = Medium Low (scans each host's TCP ports serially as fast as possible)
- Value = Medium High (tests for whatever services you specify but quickly)

```
sudo nmap –n -sT --max-parallelism 1 -p- ...
```

- Risk = Medium (scans each host's TCP ports serially as fast as possible)
- Value = High (scans all possible TCP ports)

```
sudo nmap –n -sT --max-parallelism 1 -p- -sV ...
```

- Risk = Medium High (scans each host's TCP ports serially as fast as possible)
- Value = High (scans all possible TCP ports)

```
sudo nmap –n -sT -p- -A ...
```

- Risk = High (likely to crash most old gear and even some modern)
- Value = High (scans all possible ports, fingerprints everything, and runs NSE)

```
sudo nmap –n -sT -sU -p- -A ...
```

- Risk = Extremely High (likely to crash most old gear and even some modern)
- Value = High (scans all possible ports, fingerprints everything, and runs NSE)

How Vulnerability Scanners Work

- Network Port Scanning
  - basically like what nmap does WITHOUT as many options
- Service Fingerprinting
  - most vulnerabilities are identified this way
- Vulnerability Probing
  - only uses this technique to find some vulnerabilities
- Authenticated Scanning
  - logs in if credentials are provided
  - pulled patch levels
  - pulls listening ports via the netstat command
- Custom Audit Checks
  - script virtually any OS or application check desired

Low Risk Authenticated Scans with Nessus

- Decreases risk by removing TCP/UDP port scans and vulnerability probes
- To use Nessus audit checks:
  - In Nessus, create a new scan profile
  - Disable all Nessus TCP, SYN, UDP, and SNMP port scans
  - Leave Netstat and Ping port scans open
  - Disable all Nessus plugins except Windows/Linux compliance checks
  - In Preferences, configure the compliance checks to use any third party or custom made audit files (windows security policy or plain text file values)
- Create a new scan and tell it to use your new profile
- Some older scan profiles were made for ICS by Digital Bond
  - Part of their Bandolier Project
  - Nessus has changed their audit language, so they would need updating

Author Contact Information

Justin Searle

training and personal: justin@controlthings.io

consulting and testing: justin@inguardians.com

cell: 801-784-2052

twitter: @meeas

Facebook: www.facebook.com/m33as

LinkedIn: www.linkedin.com/in/meeas

GitHub: github.com/meeas