



TEXAS
Health and Human
Services

Vulnerable at Vulnerability Management

Start small and aim big
A State Agency Case Study

V@VM

1. About Me / Disclaimer
2. In the Beginning ...
3. In the Middle ...
4. What about you?



TEXAS
Health and Human
Services

About Me / Disclaimer

1. HHSC Internal Audit
2. Very green....IT and Security
3. Not too much academic digression here.
4. Your mileage will vary.



TEXAS
Health and Human
Services

In the Beginning...

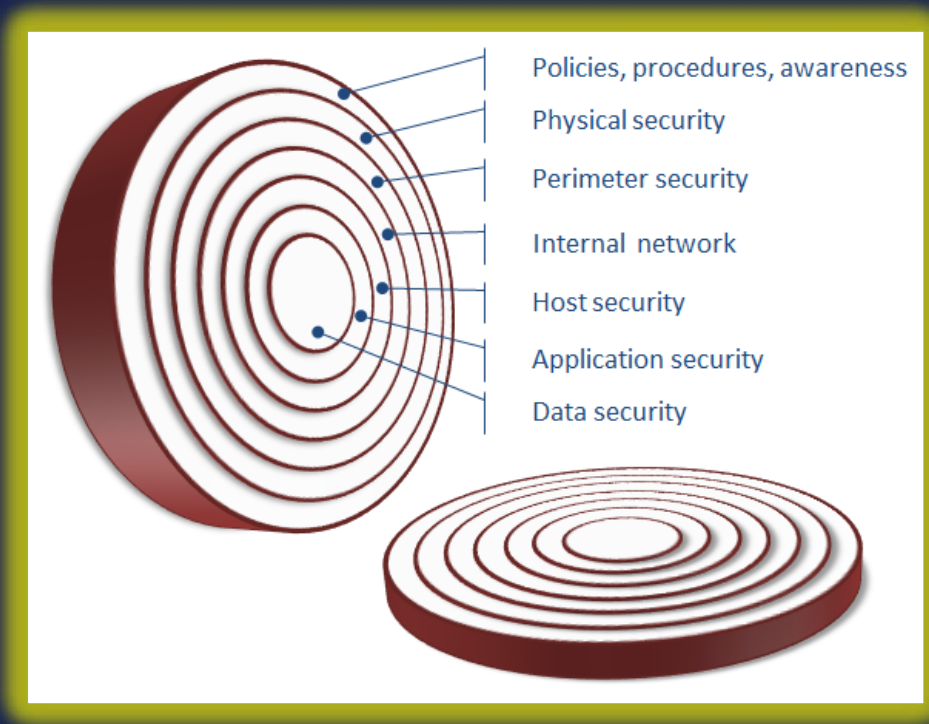
1. There was the worlds largest known honeypot on the internet.
2. Some say that this network was a hackers dream.
3. Penetration testing performed had limited value.
4. Passion as a motivational driver.



TEXAS
Health and Human
Services

Defense in Depth

So we got this onion.....how do we operationalize some processes to test HHS without tearing our eyes out?



Defense in Depth

How about part way.

Focus on Network layers and determine where the topology-

US → Austin, TX → DIR [via ISP's]

State to State → Agency Perimeter

Agency WAN → Agency Int. Gateway

Agency LAN



TEXAS
Health and Human
Services

Defense in Depth

Network Layers in various perspectives

Perspective 0

US → Austin, TX → DIR [ISP's]

Perspective 1

State to State → Agency Perimeter

Perspective 2

Agency WAN → Agency Int. Gateway

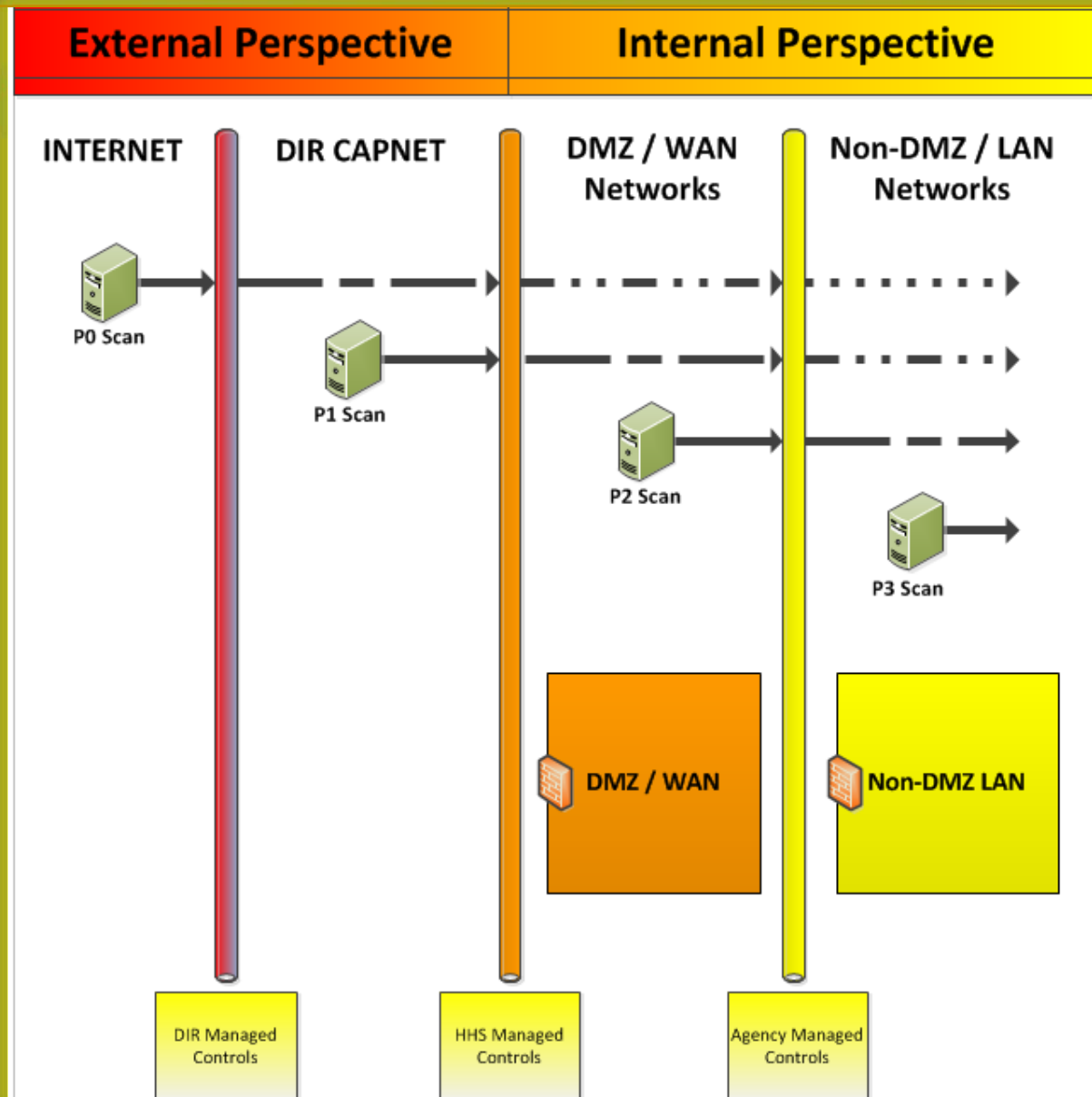
Perspective 3

Agency LAN



TEXAS
Health and Human
Services

Scan Engine Perspectives



TEXAS
Health and Human
Services

Defense in Depth: Observations

1. Perspective 0
 - a. Access -Firewall focus
 - b. Permit – IPS Vulnerability
2. Perspective 1
 - a. State Sharing at the Front Door
 - b. Removes DIR Controls (Eg. IPS)
3. Perspective 2
 - a. DMZ or Not
 - b. Soft gooey center
 - c. WAN access after pivot
4. Perspective 3
 - a. Hosts here accessed from outside....Yep ☹
 - b. LAN access after pivot ☹ ☹



TEXAS
Health and Human
Services

Defense in Depth: Observations

1. Effective Controls are representative
 - a. Intrusion Prevention Blocks.
 - b. Host Firewalls
 - c. Host intrusion prevention
2. Scan results are effectively residual risk.
3. The plan now:
 - a. Host enumeration for first pass
 - b. Vulnerability testing for second pass.



TEXAS
Health and Human
Services

Defense in Depth: Observations

1. Issues with "Scan all ip address space"
 - a. No ping. Used common port touches instead.
 - b. Licensing by address space.
2. Un-credentialed scans only.



TEXAS
Health and Human
Services

Defense in Depth: Observations

1. Product expertise.
 - a. Black out periods
 - b. Scan templates.
 - c. What does web spidering do to scan time?
2. Exceptions- We asked but did not get much.



TEXAS
Health and Human
Services

Defense in Depth: Observations

1. Found some exceptions the hard way.
 - a. Mainframes are touchy
 - b. Log sensitivity set high → email alerts can be a Denial of service.
 - c. Angry Admins must be assuaged



TEXAS
Health and Human
Services

Defense in Depth: Observations

1. How long is this going to take?
 - a. No Web spidering!
 - b. Segment the Class B's
 - c. Enable parallel scanning
2. Host enumeration yielded ip addresses in data but no host names.
 - a. Allow Hostname and DNS into HHS environment from engines only
 - b. Hostnames! Yes. Reporting looks a bit clearer now.



TEXAS
Health and Human
Services

Defense in Depth: Observations

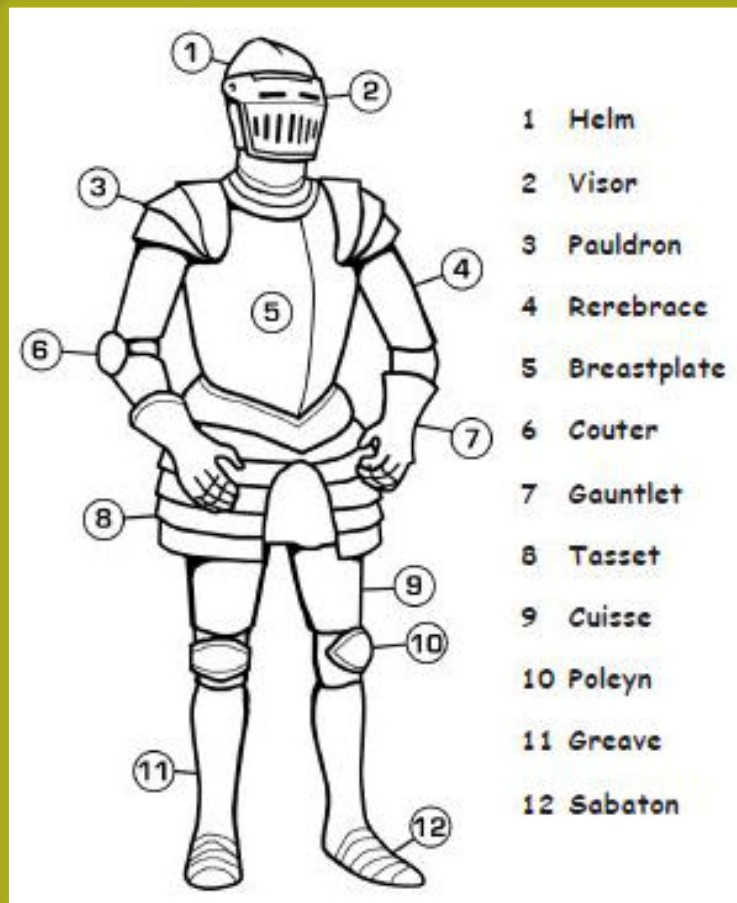
1. Why are we doing this again?
 - a. Controls testing in layers to determine effective controls.
 - b. That is do the controls in place really work.
 - c. How do you know?
 - d. What is your residual risk?
2. Ok. Just checking. Geez..



TEXAS
Health and Human
Services

Armor testing

- Perspective 0
- Perspective 1
- Perspective 2
- Perspective 3



TEXAS
Health and Human
Services

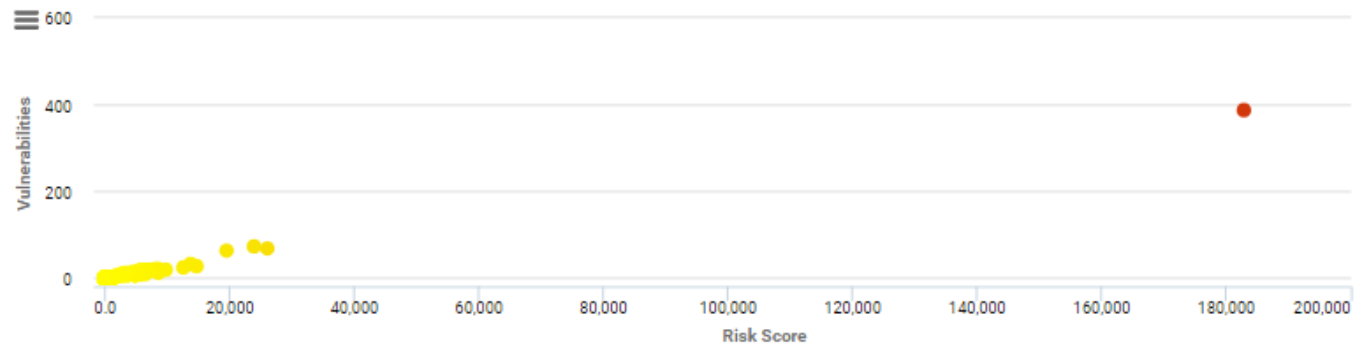
Now what? Start small!!

1. Having a plan avoids analysis paralysis.
2. Priorities first → Public Facing (P0/P1)
3. Actions: Triage → Isolate | Remediate
4. Emergencies to the top!



TEXAS
Health and Human
Services

ASSETS BY RISK AND VULNERABILITIES ?



Now what? Start small!!

1. Change Management Policy requires us to provide an assessment of risk for certain actions.
2. As such we needed a common and simple alert methodology that incorporated risk and controls.



TEXAS
Health and Human
Services

Alert Formula

1. CIS MS-ISAC Alert Level Formula

2. Severity =
(Criticality + Lethality) –
(System Countermeasures +
Network Countermeasures)



TEXAS
Health and Human
Services

Alert Formula

Criticality:

What is the target of the attack?



TEXAS
Health and Human
Services

Alert Formula: Criticality

5. Core services such as critical routers, firewalls, VPNs, IDS systems, DNS servers or authentication servers (e.g. LDAP)
4. E-mail, web, database and critical application servers.
3. Less critical application servers.
2. Business desktop systems.
1. Home users.



TEXAS
Health and Human
Services

Alert Formula: Criticality Observations

- We will spend significant time here.
- What does this host do? Does it do it actively?
- Lots of internal inquiries and time spent on this part for us.
- This is important for later for determining actions to take.
- So who owns this NT Sever Farm? Going once?



TEXAS
Health and Human
Services

Alert Formula

Lethality:

How likely will the attack do damage?



TEXAS
Health and Human
Services

Alert Formula: Lethality

5. Exploit exists.
Attacker could gain root or administrator privileges. Attacker could commit denial of service.
4. Exploit exists.
Attacker could gain user level access privileges. Attacker could commit denial of service.
3. No known exploit exists.
Attacker could gain root or administrator privileges. Attacker could commit degradation of service.
2. No known exploit exists.
Attacker could gain user level access privileges.
1. No known exploit exists.
Attacker could not gain access.



TEXAS
Health and Human
Services

Alert Formula: Lethality Observations

- Used Vulnerability Management tool for this.
- Metasploit exist?



TEXAS
Health and Human
Services

Alert Formula

System Counter-Measures:
What host-based preventative measures are in place?



TEXAS
Health and Human
Services

Alert Formula: System Counter-Measures

5. Current operating system with applicable patches applied. Server has been hardened and verified via vulnerability scan. Running host-based IDS or integrity checker. Anti-virus signature exists and has been applied to target systems.
4. Current operating system with applicable patches applied. Operating system has been hardened. Anti-virus signature exists and has been applied to target systems.
3. Current operating system with fairly up-to-date patches applied. Anti-virus signatures are current.
2. Current operating system but missing some applicable patches. Anti-virus signature either does not exist or has not been applied to target systems.
1. Older operating systems including Windows NT 3.51, Solaris 2.6, Windows 95/98/ME. No anti-virus software protection.



TEXAS
Health and Human
Services

Alert Formula: System Counter-Measures

- Some assumption declared here.
- Common configuration declared for some assets.



TEXAS
Health and Human
Services

Alert Formula

Network Counter-Measures:
What network-based preventative measures are in place?



TEXAS
Health and Human
Services

Common Indicator Bits: Network Counter-Measures

5. Restrictive (i.e. deny all except what is allowed) firewall. Firewall rules have been validated by penetration testing. All external connections including VPNs go through (not around) the firewall Network-based IDS is implemented. E-mail gateway filters attachments used by this virus.
4. Restrictive firewall. External connections (VPNs, Wireless, Internet, Business partners, etc) are protected by a firewall. E-mail gateway filters attachments used by this virus.
3. Restrictive firewall. E-mail gateway filters common executable attachments.
2. Permissive firewall (i.e. "accept all but") or allowed service (e.g. HTTP, SMTP, etc) E-mail gateway does not filter all attachments used by this virus.
1. No firewall implemented. E-mail gateway does not filter any attachments.



TEXAS
Health and Human
Services

Common Indicator Bits: Network Counter-Measures

- Familiar with the applicable controls after the network layers exercise.
- Most items were the same with some outliers.



TEXAS
Health and Human
Services

Alert Level for Perimeter

1. Alert Indicator Level - Severity

- a. Green - Low : -8 to -5
- b. Blue - Guarded : -4 to -2
- c. Yellow - Elevated : -1 to +2
- d. Orange - High : +3 to +5
- e. Red - Severe : +6 to +8

2. Emphasis on controls understanding and infrastructure knowledge gained and documented.



TEXAS
Health and Human
Services

Alert Level and Criticality

1. Triage Planning
→ Isolate | Remediate
2. Cannot isolate Critical Assets.
 - a. Compensating controls
 - b. Remediation planning
3. All others isolate.



TEXAS
Health and Human
Services

Priority ranking

1. Raw risk scores totals from Vulnerability Management Scans also used as a priority measure for a given triage group.
2. Higher number of Critical and Severe Vulnerabilities and Exploits identified then the higher the priority.



TEXAS
Health and Human
Services

Action:

Isolate | Remediate

Core issue notices for Isolation or Remediation.

- a. Hosts are public facing and are not intended for this purpose.
- b. Hosts are not fully patched and have readily exploitable vulnerabilities.



TEXAS
Health and Human
Services

Action: Isolate

1. Core isolation notices
2. Change Rules apply
3. Firewall Monitoring needed.
 - a. FW reviews rare.
 - b. ACL's do not retire.
4. Scan continuously to determine if fixed. Proof is needed.
Eg. Patches applied but still vulnerable. A reboot is in needed!



TEXAS
Health and Human
Services

Action: Remediate by IPS

1. Core vulnerability notices.
2. Upgrade and patch requests.
3. Deadlines for urgency.
4. Change rules apply.
5. IPS filters for known vulnerabilities and exploits applied as soon as possible.
6. Security to IT reduce your ~~Attack~~ patch surface.



TEXAS
Health and Human
Services

In the Middle...

1. The honeypot takedown successful and significant isolation completed.
2. Vulnerability Testing occurs continuously. Remediation can be slow.
3. Started small via P0/P1 to get operationalized.



TEXAS
Health and Human
Services

In the Middle...

1. Aim BIG with the P2/P3 data set
2. Analyze footprint
 - a. Common OS w/ pervasive vulnerabilities that can patched in a sweep.
3. High security but low IT effort critical items
 - a. Telnet
 - b. Credentialed web services w/o HTTPS



TEXAS
Health and Human
Services

What about you?

- Perspective 0, 1, 2, and 3?
One server bro...How does this help me?
→ Strongly worded policies can help.
Feel that TAC 202 protection!
- Outside and inside
→ Focus on the inside
VPN is cheap.
Throttle your scan through that.
- Talk it out...DIR Monthly Meetings.
- DCS now has Tenable. Ask for scans and HIPS. Pilot PIM



TEXAS
Health and Human
Services

Resources

- MS ISAC Cyber Alert Indicator
<https://msisac.cisecurity.org/alert-level/>
- Vulnerability Policy
Self written- Shared upon request
- Firewall Management and Monitoring
<https://www.firemon.com/>
- Rapid 7 Nexpose Vulnerability Mgt.
<https://www.rapid7.com/>
- DIR (NSOC)
- DCS (ATOS and Capgemini)
- MS-ISAC



TEXAS
Health and Human
Services



TEXAS
Health and Human
Services

Questions?



TEXAS
Health and Human
Services

Thank you

joseph.alma@hhsc.state.tx.us