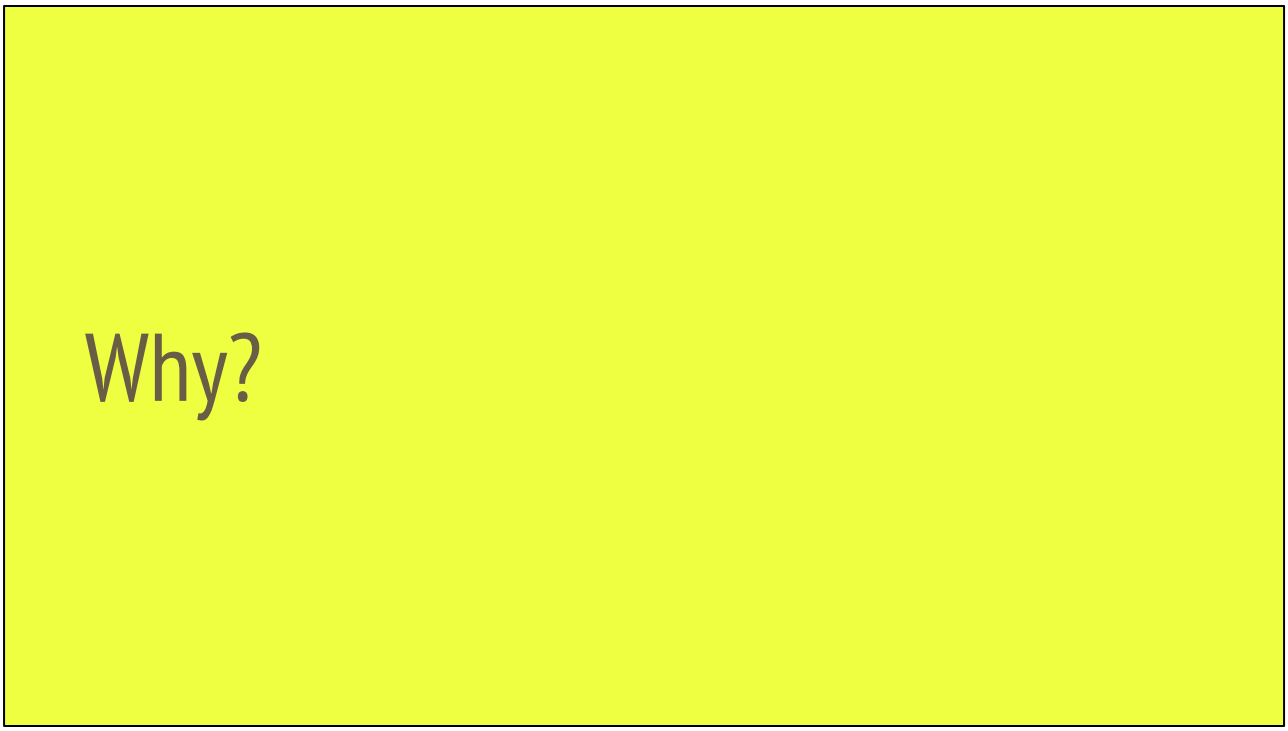
Security Baselines

Steve Miller
Gordon Food Service

1-2 minutes

- Brief introduction
  - Configuration using Security Baselines
  - Systems Administrator at Gordon Food Service.
  - Work with a lot of systems that fall under various compliance regimens. Just like most of you...
- Open up to asking current environment from attendees
  - Linux/Unix Server in environment
  - Windows Server (Maybe also ask about Hyper-V)
  - VMWare Server
  - Amazon EC2/Azure/other…



3-5 minute

Why?

- Carrot:
  - Good way to audit systems and ensure security best practices are being followed
- Stick:
  - Compliance requirements (PCI, SOX, HIPAA). Make your auditors happy...
    - PCI: Section 2.2
    - FISMA (NIST validated product for SCAP)
    - HIPAA, SOX, etc…
    - Generally have to have a way to ensure you are following best practices on all systems within scope.
  - Legal Requirements: FTC versus Wyndham….

Getting Started

- What Tool(s) To Use
- How to Approach Usage
  - Existing Systems
  - New Systems

10-15 minutes

- Baseline Scanners
  - Toolbox Mentality. Every environment is different, so difficult for a “one size fits all” strategy.
  - Scanners
    - CIS and CIS-CAT (http://www.cisecurity.org/)
      - Standard PDFs are free. Scanner costs money
      - Multi-platform and multi-product (Apache, Tomcat, etc…)
    - OpenSCAP (along with OpenSCAP Scap Security Guide) (http://www.open-scap.org/page/Main_Page)
    - Lynis (https://cisofy.com/lynis/)
  - Remember, **don’t go into analysis paralysis**. Pick one that looks good enough as a starting point.
- Once you’ve decided on one
  - Existing systems.
    - Pick a “benchmark system”.
    - Run a scan.

        - Make judgement call on what to fix, and fix it across similar systems.
        - Rince and repeat. Use any type of risk profile you have as guide, or compliance requirements.
        - Hopefully you have a configuration management system of some sort...especially for continuous remediation and monitoring
    - New Systems
        - Baseline build standards. Should have automated OS buildout process!
        - VMWare ESXi: PXE boot, auto installation.
        - VMware, use templates for OS buildouts. Could also use cobbler.
        - For Bare Metal: Cobbler for Linux (and ESX). WAIK for Windows (or full on WDS install).
- Advanced Usage
    - Tagging CIS standards within configuration management tool...can prove to your auditors where enforcement occurs.
        - And if version controlled, history of changes.
    - Automated, continuous scanning…
        - TODO: Lookup CIS-CAT centralized tool…
        - Also discuss automated scans yourself...
    - Biggest idea, continuous scanning and detection/auto-correction of issues!

Using the Standards Effectively

10-15 minutes

Actually using the guidelines effectively

- Remember that the these standards are “guidelines”. There are very good reasons to deviate from them...just make sure they are justified and do not leave a hole open…
- For CIS, each item comes with a detailed description of “why”
- Examples of some of the configuration examples
  - Separate partitions on Linux/Unix systems
  - NTP time server on ESXi and Linux/Unix
  - Local Firewall
  - VMWare: Disconnect/remove Floppy and CD devices from VMs unless needed. At least force a reboot if they need to be reconnected (although newer versions allow hot-add of hard drives, so perhaps less then useful)
  - Windows/Linux/VMWare: Password complexity enforcement
- Some examples of exceptions you may need to consider
  - Example: VMWare Using active directory for AD authentication on ESXi...unless you don’t have Active directory….

    - Example: VMware ensure vSwitch is set to reject Promiscuous mode. Great for most instances, unless you are running any type of IDS collector within a VM
    - Example: CIS sshd “AllowedUsers” and pam_access configuration.
    - Example: X11 on SSHD
        - If you NEED X11, then this doesn’t help you
    - Example: SNMP complete shutdown...but what if custom software depends on it.
        - Mitigate...firewall off locally. However, scanner won’t be sophisticated enough to detect this mitigation.
    - Example: Linux auditd log configuration
        - Linux “audit” configuration will never rotate or delete, and will shut down the system when the audit log configuration is full.
- Items that guidelines might not detect automatically!
    - Password policies set on directory services (well, at least open source LDAP systems…)
- Non-scorable items on report(s)
    - A lot of items cannot be scanned by the report automatically, but still should be reviewed:
        - Example: VMWare: Ensure that port groups are not configured to VLAN values reserved by upstream physical switches
        - Example: VMWare: Prevent virtual machines from taking over resources

Considerations

5-10 minutes

- Items to worry about.
  - Monitoring of collected log files (in Linux, audit logs, as well as external syslog monitoring).
    i. Standards will have you collect logs, but if no one is watching, would you ever know of problems…
    ii. External logs still infinitely useful if compromised for post-mortum.
  - If system is compromised, can I trust output of locally run security scanner??
  - Does not replace SIEM/IDS/IPS, but properly configured systems can assist in early detection.

Streamlining

5-10 minutes

- Advance
  - Writing your own XCCDF/OVAL detection code…
  - Or perhaps something like ServerSpec for a Test Driven Development style configuration.
  - Integration of OS configuration and scans into a CI/CD framework of some type...

Questions