Securing All the Things: CIS Benchmarks for the Win!

Rob VandenBrink
rob@coherentsecurity.com
whoami /all

- Rob VandenBrink
- Internet Storm Center Handler
- CIS Benchmark contributor / editor
- Consultant:
  - Security / Networking / Virtualization / AD / Automation
- https://www.coherentsecurity.com
- rob@coherentsecurity.com
CIS Benchmarks

• In this talk – we’ll cover off
  • What CIS Benchmarks are (and are not)
  • What platforms are covered
  • How the benchmarks are created
  • How they work in real life

• Most importantly
  • How you can get involved?
  • What the time commitments look like?
  • What do you get out of being involved?
CIS Benchmarks – What Are They?

• Security Guidance for specific platforms
• Specific Configuration Guidance
• “Navigate here, click there, type this”
• Written with automation and scripting in mind

• Authored by Volunteers
• Consensus driven
• Vendor independent (vendors have input but not control)
CIS Benchmarks are NOT:

- A Compliance Framework
  - ... though the benchmarks are used in many compliance frameworks (PCI DSS for one)
- “You must do everything on this list” set of guidelines
  - It’s not uncommon to see conflicting advice for different situations
- A “Now we are done” list
CIS – Operating Systems

- **LINUX:**
  - Amazon
  - CentOS
  - Debian
  - Distribution Independent
  - Oracle
  - Red Hat
  - SUSE
  - Ubuntu

- **Windows:**
  - Desktop
  - Server

- **UNIX:**
  - Apple OS
  - AIX
  - Solaris
CIS – Server Software

**Web Servers**
- Apache
- Tomcat
- IIS
- NGINX

**Virtualization**
- VMware
- Docker
- Kubernetes

**DataBase**
- Apache Cassandra
- DB2
- MS SQL
- PostgreSQL
- MongoDB
- Oracle

**Other:**
- BIND
- Kerberos
- Sharepoint
CIS – Cloud Providers

- Amazon
- Azure
- Google

- These are tougher to keep up to date
- It’s hard to get any of these CSP’s to commit to what they are at any given time
CIS – Network Devices

- Cisco
  - ASA / Switches / Routers / Wireless Controller
  - Multiple OS versions

- Juniper
  - JunOS

- Palo Alto
  - 6,7,8,9
CIS – Desktop Software

• Exchange
• MS Office
• Chrome
• IE
• Firefox
• Safari
CIS – Mobile Platforms / Other

- iOS
- Android

- Multifunction Printers
Wait – My Device / App / Thing isn’t on the list!

• With 140+ benchmarks out there, there’ll be something close.

• Use a benchmark for a similar platform to conduct your assessment or hardening exercise.

• If your platform is even semi-popular, consider volunteering to write a benchmark.

• Especially since you’ve already done half (or more) of the work!
So How Do They Get Built?

GREAT QUESTION,

I'M GLAD YOU ASKED.
Working with a Benchmark - Editor
Working with a Benchmark - Editor
## Working with a Benchmark - Editor

### Description

HTTP and Telnet options should not be enabled for device management.

### Rationale Statement

Management access over cleartext services such as HTTP or Telnet could result in a compromise of administrator credentials and other sensitive information related to device management. Theft of either administrative 

### Audit Procedure

Navigate to Device > Setup > Interfaces > Management.

### Remediation Procedure

Navigate to Device > Setup > Interfaces > Management.
Working with a Benchmark - Editor
Working with a Benchmark

• Once this is all done, a ticket is generated and sent out to all participants (also via email if you choose)

• Online and offline discussion often ensues, especially for more “controversial” things (DLP in this case was one)

• Weekly or Bi-weekly meetings are common, for “in person” discussions

• Editor(s) approve/finalize the wording
Working with a Benchmark

• After all that, what does this look like in the final document?
  • Cisco IOS Benchmark
  • Palo Alto Benchmark (editor, code)
  • VMware Benchmark (contributor, code)

  • https://github.com/robvandenbrink
Using Benchmarks in Real Life

- These documents are written with the goal of scripting and automation
  - CIS creates scripts in OVAL, these are used directly in CIS-CAT
  - OVAL scripts are also licensed by organizations such as Tenable (for use in Nessus and so on)
  - Community builds playbooks for orchestration / automation tools such as Ansible, Puppet, Chef or Salt

- Note that all of these are meant to be edited for your organization. **Implementing security guidance blindly never ends well!!**
Sounds Like Fun - How Do I Get Involved?

• Most importantly, how do you get involved?
• Volunteering is easy, when you create an account, you can volunteer for one or more benchmarks
• If you created an account just to download the benchmarks, you can always edit your profile and volunteer
• If you simply disagree with one recommendation in a benchmark, join the group and open a ticket!
• You can get more info at benchmarkinfo@cisecurity.org
Sounds Like Fun - How Do I Get Involved?

- Multiple roles (you are free to “mix and match”):
  - Technical and/or Security **Subject Matter Experts** to contribute or proof / verify content
  - **Technical Writer** – because it needs to be readable when completed. (Grammar and Spelling do matter!)
  - **Tester** – because after all is said and done, somebody needs to make sure that the guidance works
Finding time for all that?

- So once you’ve volunteered – how much time is involved? (maybe do this calculation first)
  - Figure on 2 hrs per month for meetings
  - Contributor - Budget 2-4 hrs per week (per benchmark) for actual work
  - Editor – hopefully budget a bit more –maybe 1.5-2 hrs per day(ish?)
  - If you’re doing a full run-through test, figure 4-8 hrs
- Of course, YMMV (Your Mileage May Vary)
What do I get Out of Volunteering?

• You get to learn that platform REALLY WELL.
• Influence security in a positive way for that platform industry-wide, not just for your organization
• Ammo for that same positive influence that you can use within your organization
• The opportunity to work with other security folks on the platform of your choice
• CPEs if you need them
• Your name in the final benchmark document
What do I get Out of Volunteering?

• It’s also a great reference if you’re interviewing 😊
Questions?

(Ok, any question except that one 😊 )