Building a Basic Cybersecurity Toolkit

Dain Couch
Chief Information Security Officer, Arkansas Administrative Office of the Courts

Josh Baugh
Chief Information Security Architect, Arkansas Administrative Office of the Courts

Special Agent Timothy Yee
FBI New Orleans
Hacked!

ERROR

./TheSilentKiller

TEAM_CC AKA CYBER COMMANDOS
Basic Cybersecurity Toolkit

Policy and Procedures
- National Institute of Standards and Technology (NIST) Publications
- CIS Controls

Technical Tools
- CIS Benchmarks
- CIS-CAT Pro Assessment Tool
- Multi-State Information Sharing & Analysis Center (MS-ISAC)
- NIST Checklist Program Repository

FBI Resources
Policy and Procedures
National Institute of Standards and Technology

https://www.nist.gov
Computer Security Resource Center

- [https://csrc.nist.gov/publications/sp800](https://csrc.nist.gov/publications/sp800)
- 169 Free Publications

NIST SP 800-53 Rev 4

Security Controls and Assessment Procedures for Federal Information Systems and Organizations
Security Controls applied based on Impact Baseline Assessment (level of information sensitivity)

- High (170)
- Moderate (159)
- Low (115)
AC - Access Control
• AU - Audit and Accountability
• AT - Awareness and Training
• CM - Configuration Management
• CP - Contingency Planning
• IA - Identification and Authentication
• IR - Incident Response
• MA – Maintenance
• MP - Media Protection

PS - Personnel Security
• PE - Physical and Environmental Protection
• PL – Planning
• RA - Risk Assessment
• CA - Security Assessment and Authorization
• SC - System and Communications Protection
• SI - System and Information Integrity
• SA - System and Services Acquisition
#CTC2019

Access Control Family

- 1<sup>st</sup> Control is Access Control Policy and Procedures
- Priority listed for each control
- Note: Subcontrols in parenthesis

## High Impact Controls

NIST Special Publication 800-53 (Rev. 4)
Security Controls and Assessment Procedures for Federal Information Systems and Organizations

<table>
<thead>
<tr>
<th>No.</th>
<th>Control</th>
<th>Priority Low</th>
<th>Moderate</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-1</td>
<td>ACCESS CONTROL POLICY AND PROCEDURES</td>
<td>P1</td>
<td>AC-1</td>
<td>AC-1</td>
</tr>
<tr>
<td>AC-2</td>
<td>ACCOUNT MANAGEMENT</td>
<td>P1</td>
<td>AC-2</td>
<td>AC-2 (1) (2) (3) (4) AC-2 (1) (2) (3) (4) (5) (11) (12) (13)</td>
</tr>
<tr>
<td>AC-3</td>
<td>ACCESS ENFORCEMENT</td>
<td>P1</td>
<td>AC-3</td>
<td>AC-3</td>
</tr>
<tr>
<td>AC-4</td>
<td>INFORMATION FLOW ENFORCEMENT</td>
<td>P1</td>
<td>AC-4</td>
<td>AC-4</td>
</tr>
<tr>
<td>AC-5</td>
<td>SEPARATION OF DUTIES</td>
<td>P1</td>
<td>AC-5</td>
<td>AC-5</td>
</tr>
<tr>
<td>AC-6</td>
<td>LEAST PRIVILEGE</td>
<td>P1</td>
<td>AC-6 (1) (2) (3) (5) (9) (10)</td>
<td>AC-6 (1) (2) (3) (5) (9) (10)</td>
</tr>
<tr>
<td>AC-7</td>
<td>UNSUCCESSFUL LOGON ATTEMPTS</td>
<td>P2</td>
<td>AC-7</td>
<td>AC-7</td>
</tr>
<tr>
<td>AC-8</td>
<td>SYSTEM USE NOTIFICATION</td>
<td>P1</td>
<td>AC-8</td>
<td>AC-8</td>
</tr>
<tr>
<td>AC-10</td>
<td>CONCURRENT SESSION CONTROL</td>
<td>P3</td>
<td>AC-10</td>
<td></td>
</tr>
<tr>
<td>AC-11</td>
<td>SESSION LOCK</td>
<td>P3</td>
<td>AC-11 (1)</td>
<td>AC-11 (1)</td>
</tr>
<tr>
<td>AC-12</td>
<td>SESSION TERMINATION</td>
<td>P2</td>
<td>AC-12</td>
<td>AC-12</td>
</tr>
<tr>
<td>AC-14</td>
<td>PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION</td>
<td>P3</td>
<td>AC-14</td>
<td>AC-14</td>
</tr>
<tr>
<td>AC-17</td>
<td>REMOTE ACCESS</td>
<td>P1</td>
<td>AC-17 (1) (2) (3) (4)</td>
<td>AC-17 (1) (2) (3) (4)</td>
</tr>
<tr>
<td>AC-18</td>
<td>WIRELESS ACCESS</td>
<td>P1</td>
<td>AC-18 (1) (2) (3) (4)</td>
<td>AC-18 (1) (2) (3) (4)</td>
</tr>
<tr>
<td>AC-19</td>
<td>ACCESS CONTROL FOR MOBILE DEVICES</td>
<td>P1</td>
<td>AC-19 (1) (2) (3) (4)</td>
<td>AC-19 (1) (2) (3) (4)</td>
</tr>
<tr>
<td>AC-20</td>
<td>USE OF EXTERNAL INFORMATION SYSTEMS</td>
<td>P1</td>
<td>AC-20 (1) (2) (3) (4)</td>
<td>AC-20 (1) (2) (3) (4)</td>
</tr>
<tr>
<td>AC-21</td>
<td>INFORMATION SHARING</td>
<td>P2</td>
<td>AC-21</td>
<td>AC-21</td>
</tr>
<tr>
<td>AC-22</td>
<td>PUBLICLY ACCESSIBLE CONTENT</td>
<td>P3</td>
<td>AC-22</td>
<td>AC-22</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
<td>Subcategory</td>
<td>Informative References</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>
| IDENTIFY   | Asset Management (ID.AM): The data, personnel, devices, systems, and      | ID.AM-1: Physical devices and systems within the organization are inventoried  | CIS CSC 1  
               |                                           | systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy. | COBIT 5 BA109.01, BA109.02  
               |                                           |                                                                             | ISA 62443-2-1:2009 A.2.3.4  
               |                                           |                                                                             | ISA 62443-3-3:2013 SR 7.8  
               |                                           |                                                                             | ISO/IEC 27001:2013 A.8.1.1, A.8.1.2  
               |                                           |                                                                             | NIST SP 800-53 Rev. 4 CM-8, PM-5 |
|            |                                                                          | ID.AM-2: Software platforms and applications within the organization are     |                                                                                         |
|            |                                                                          | inventoried                                                                   |                                                                                         |
|            |                                                                          |                                                                             |                                                                                         |
|            |                                                                          | ID.AM-3: Organizational communication and data flows are mapped               |                                                                                         |
|            |                                                                          |                                                                             |                                                                                         |
|            |                                                                          |                                                                             |                                                                                         |
|            |                                                                          |                                                                             |                                                                                         |
That’s a big elephant to eat… I thought this was supposed to be about a Basic Toolkit??
FedRAMP

Federal Risk and Authorization Management Program

- Assessed, certified and continuously monitored cloud products and services
- Approval is by Impact Level (Low, Moderate, High)
- Examples: AWS GovCloud, Office 365, Google G Suite, etc.

NOTE: Approval is for specific services/editions
Cryptographic Module Validation Program


- Database of “validated modules” within the NIST Computer Security Resource Center

- Encrypted external hard drives, memory sticks, etc.
• CIS Controls V7.1

• 20 Prioritized Controls/Sub-controls
  • 6 Basic
  • 10 Foundational
  • 4 Organizational
Implementation Groups

Groups are based on resources and cybersecurity expertise, but data sensitivity is a factor too.
• Why Is This CIS Control Critical?
• Control Chart
• Procedures and Resources
## CIS Control 10: Data Recovery Capabilities

<table>
<thead>
<tr>
<th>Sub-Control</th>
<th>Asset Type</th>
<th>Security Function</th>
<th>Control Title</th>
<th>Control Descriptions</th>
<th>Implementation Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1</td>
<td>Data</td>
<td>Protect</td>
<td>Ensure Regular Automated Backups</td>
<td>Ensure that all system data is automatically backed up on a regular basis.</td>
<td>1</td>
</tr>
<tr>
<td>10.2</td>
<td>Data</td>
<td>Protect</td>
<td>Perform Complete System Backups</td>
<td>Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.</td>
<td>1</td>
</tr>
<tr>
<td>10.3</td>
<td>Data</td>
<td>Protect</td>
<td>Test Data on Backup Media</td>
<td>Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.</td>
<td>1</td>
</tr>
<tr>
<td>10.4</td>
<td>Data</td>
<td>Protect</td>
<td>Protect Backups</td>
<td>Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.</td>
<td>1</td>
</tr>
<tr>
<td>10.5</td>
<td>Data</td>
<td>Protect</td>
<td>Ensure All Backups Have at Least One Offline Backup Destination</td>
<td>Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.</td>
<td>1</td>
</tr>
</tbody>
</table>
There are only 11 Basic Implementation Group 1 Controls!

1. Maintain Detailed Asset Inventory
2. Address Unauthorized Assets
3. Maintain Inventory of Authorized Software
4. Ensure Software Is Supported by Vendor
5. Address Unapproved Software
6. Deploy Automated Operating System Patch Management Tools
7. Deploy Automated Software Patch Management Tools
8. Change Default Passwords
9. Ensure the Use of Dedicated Administrative Accounts
10. Establish Secure Configurations
11. Activate Audit Logging
• CIS Control 17: Implement a Security Awareness and Training Program

• CIS Control 19: Incident Response and Management
Password Reuse

• 73% of online accounts use duplicated passwords

• 54% use five or fewer passwords total
• Pwn – own; have power or mastery over someone; gain illegal access (through hacking)

• https://haveibeenpwned.com
Exactis – June 2018 – 340 million records

Compromised data: Credit status information, Dates of birth, Education levels, Email addresses, Ethnicities, Family structure, Financial investments, Genders, Home ownership statuses, Income levels, IP addresses, Marital statuses, Names, Net worths, Occupations, Personal interests, Phone numbers, Physical addresses, Religions, Spoken languages
dehashed.com
• Sampling of 192 attendee registered email addresses

• 104 involved in breaches (54%)

• 73 with passwords (38%) / 31 info only (16%)

• 17 passwords (9% of attendee sampling)
CTC2019 Attendee Passwords

- manbarq1
- broadie1
- n0=acc3ss
- zack33
- pms06226
- cl****
- newpassword
- cancun1
- baker9175
- Jackson8
- chipper1
- ba****
- 2meagan9
- Jimbob42
- njkfn646
- niemic
- Sn@M$60e
- random1234
- Lotte1
- myhome25377564
Policy and Procedure Basics

- NIST 800 series publications for reference
- CIS Controls for implementation/assessment
Technical Tools
https://www.cisecurity.org/
• Created by CIS and their global community of cybersecurity experts

• Over 140 configuration guidelines covering a wide range of technologies

• Provide IT staff and contractors a step-by-step guide to implement CIS Controls, which results in a compliant baseline configuration
CIS Benchmarks™

Cover most products used in the enterprise:

- Microsoft
- VMware
- Linux
- Apple
- Cisco
- Web Servers
- Database Servers
- Docker
- Mobile devices
- Application-specific
CIS-CAT Pro

- CIS-CAT is an assessment tool
- Can be run on technology assets locally or remotely to check compliance with benchmarks
- Provides easily digestible reports that detail rationale, impact, and remediation steps
- Can use the CIS Controls Assessment Module to measure your organization’s application of CIS Controls Implementation Group 1
## Summary

<table>
<thead>
<tr>
<th>Description</th>
<th>Pass</th>
<th>Fail</th>
<th>Error</th>
<th>Unkn.</th>
<th>Score</th>
<th>Max</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Initial Setup</td>
<td>11</td>
<td>21</td>
<td>0</td>
<td>0</td>
<td>11.0</td>
<td>32.0</td>
<td>34%</td>
</tr>
<tr>
<td>1.1 Filesystem Configuration</td>
<td>4</td>
<td>15</td>
<td>0</td>
<td>0</td>
<td>4.0</td>
<td>19.0</td>
<td>21%</td>
</tr>
<tr>
<td>1.1.1 Disable unused filesystems</td>
<td>0</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
<td>7.0</td>
<td>0%</td>
</tr>
<tr>
<td>1.2 Configure Software Updates</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
<td>1.0</td>
<td>0%</td>
</tr>
<tr>
<td>1.3 Filesystem Integrity Checking</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1.0</td>
<td>2.0</td>
<td>50%</td>
</tr>
<tr>
<td>1.4 Secure Boot Settings</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1.0</td>
<td>3.0</td>
<td>33%</td>
</tr>
<tr>
<td>1.5 Additional Process Hardening</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1.0</td>
<td>3.0</td>
<td>33%</td>
</tr>
<tr>
<td>1.6 Mandatory Access Control</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
<td>0.0</td>
<td>0%</td>
</tr>
<tr>
<td>1.6.1 Configure SELinux</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
<td>0.0</td>
<td>0%</td>
</tr>
<tr>
<td>1.7 Warning Banners</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3.0</td>
<td>3.0</td>
<td>100%</td>
</tr>
<tr>
<td>1.7.1 Command Line Warning Banners</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2.0</td>
<td>2.0</td>
<td>100%</td>
</tr>
<tr>
<td>2 Services</td>
<td>32</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>32.0</td>
<td>34.0</td>
<td>94%</td>
</tr>
</tbody>
</table>
The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.

Membership is free for SLTT government organizations.

MS-ISAC membership provides a free CIS SecureSuite membership.
Free Services

- Advisories
- Threat Notification
- Vulnerability Assessment
- Incident Response
- Malicious Code Analysis Platform

- Vulnerability Management Program
- Information Sharing, Cybersecurity Awareness, and Education
- DHS Initiatives
- CIS SecureSuite Membership
MS-ISAC®
Multi-State Information Sharing & Analysis Center®

TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2019-015

DATE(S) ISSUED:
02/05/2019

SUBJECT:
Multiple Vulnerabilities in Google Android OS Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in the Google Android operating system (OS), the most severe of which could allow for arbitrary code execution. Android is an
Advisories

Quarterly Cyber Threat Actor Review

[INFO]

United States Secret Service

January 24, 2019

[INFO] Information Only Alert – GIOC Reference #19-001-I
TLP Green

Newest Trends in Business Email Compromise Matters
The National Checklist Program is the US government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications.

https://checklists.nist.gov
Basic Cybersecurity Toolkit

Policy and Procedures
- National Institute of Standards and Technology (NIST) Publications
- CIS Controls

Technical Tools
- CIS Benchmarks
- CIS-CAT Pro Assessment Tool
- Multi-State Information Sharing & Analysis Center (MS-ISAC)
- NIST Checklist Program Repository

FBI Resources
Benefits of Working with the FBI

• Resources
  • 56 Field Offices
  • 20 International Sites
  • Part of the Intelligence Community
  • Internet Crime and Complaint Center (IC3)
  • NCIJTF CyWatch 24/7 Command Center

• Trusted Point of Contact
  • Will work with/around victim’s consent
  • Avoid unwanted disclosure of info

• Support
  • Incident response - Guidance and intelligence for your IT team
    • Ransomware decryption keys
    • Recover fraudulent funds
  • Investigation, Attribution, and Potential Prosecution
Who’s Doing the Hacking?

- Hacktivism
- Insider
- Terrorism
- Crime
  - Email Account Compromises
  - Ransomware
  - IP/Sensitive Info
- Espionage
- Warfare
How do I report a Cyber Intrusion?

FBI

• Internet Crime & Complaint Center – www.ic3.gov
• FBI Field Office - http://www.fbi.gov/contact-us/field

Local Police

State Police

U.S. Secret Service
Internet Crime and Complaint Center (IC3)

- [www.ic3.gov](http://www.ic3.gov)

- Core Functions
  - Collection – central point for victims to report and alert criminal internet activity
  - Analysis – review and analyze data submitted to highlight emerging threats and new trends
  - Public Awareness – Public service announcements, scam alerts, etc.
  - Referrals – Forwards complaints to the appropriate law enforcement authorities
What to provide LE investigators?

- Identify and preserve system log files
- Collect digital forensic evidence of targeted/infected systems
- Maintain records of ongoing incident response activities (timeline)
- Provide information related to historical intrusions and audits
- Network topology
Questions?