Using the Right Tools for the Right Jobs

Sunia Laulile, Senior IT Security Specialist

C:\> WHOAMI

- Who: Sunia Laulile
- What: Support resource for IT Security Audits
- Where: Office of the Washington State Auditor
- Why: Worked in IT since 2005

Agenda

- Overview of Critical Security Controls (CSCs) and NIST 800-53

- In-depth look at methods used at assessing CSCs in Washington state

3 tiers of organizations

Policy

Plans/programs

Configurations, guides, checklists

Focus of NIST

- Heavily centered on governance and operational controls
- Risk assessments when changes are made to the environment

Nist 800-53 origins

- Electronic Government Act of 2002
- Federal Information Security Management Act (FISMA)
- National Institute of Standards and Technology (NIST) tasked with the creation of security standards and guidelines

Nist 800-53 related information

- **Federal Information Processing Standard (FIPS) 200**
  - Mandates federal agencies to meet security requirements
- **FIPS 199**
  - Provides guidance to categorize systems and information
- **NIST 800-53**
  - Provides a catalog of control families
- **NIST 800-60**
  - Provides detailed guidance on how to categorize systems and information
- **NIST 800-37**
  - Provides risk management framework

Control families, part 1

NIST 18 different control families

- Access Control
- Personnel Security
- Audit and Accountability
- Physical and Environmental Protection
- Awareness and Training
- Planning
- Contingency Planning
- Program Management
- Incident Response
- Risk Management
- Maintenance
- Security Assessment and Authorization
- Media Protection
- System and Communication Protection
- System and Services Acquisition
- System and Information Integrity

Control families, part 2

Technical	Operational	Management
Access Control	Training	Risk Assessment
System and Com Protections	Configuration management	Security Assessment and Authorization
Identification and Authentication	System and information integrity	System and Service Acquisition
Audit & Accountability	Contingency planning	Planning
	Maintenance	Program Management
	Media Protection	
	Physical protection	
	Personal security	
	Incident response	

In-depth look

Number	Control	Priority	Low risk	Moderate risk	High risk
AU-1	Audit and accountability policy and procedures	P1	AU-1	AU-1	AU-1
AU-2	Audit events	P1	AU-2	AU-2 (3)	AU-2 (3)
AU-3	Content of audit records	P1	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit storage capacity	P1	AU-4	AU-4	AU-4
AU-5	Response to audit processing failures	P1	AU-5	AC-5	AC-5 (1) (2)

AU control family

Look at handout Page 2

Workflow

- Categorize information and information systems
- Perform risk assessment
- Document and apply appropriate controls
- Monitor controls and revisit/reassess when appropriate

Focus of critical security controls (CSC)

- Heavily focused on operational and technical controls
- Controls directly tie to mitigating known attacks
- Less emphasis on documentation

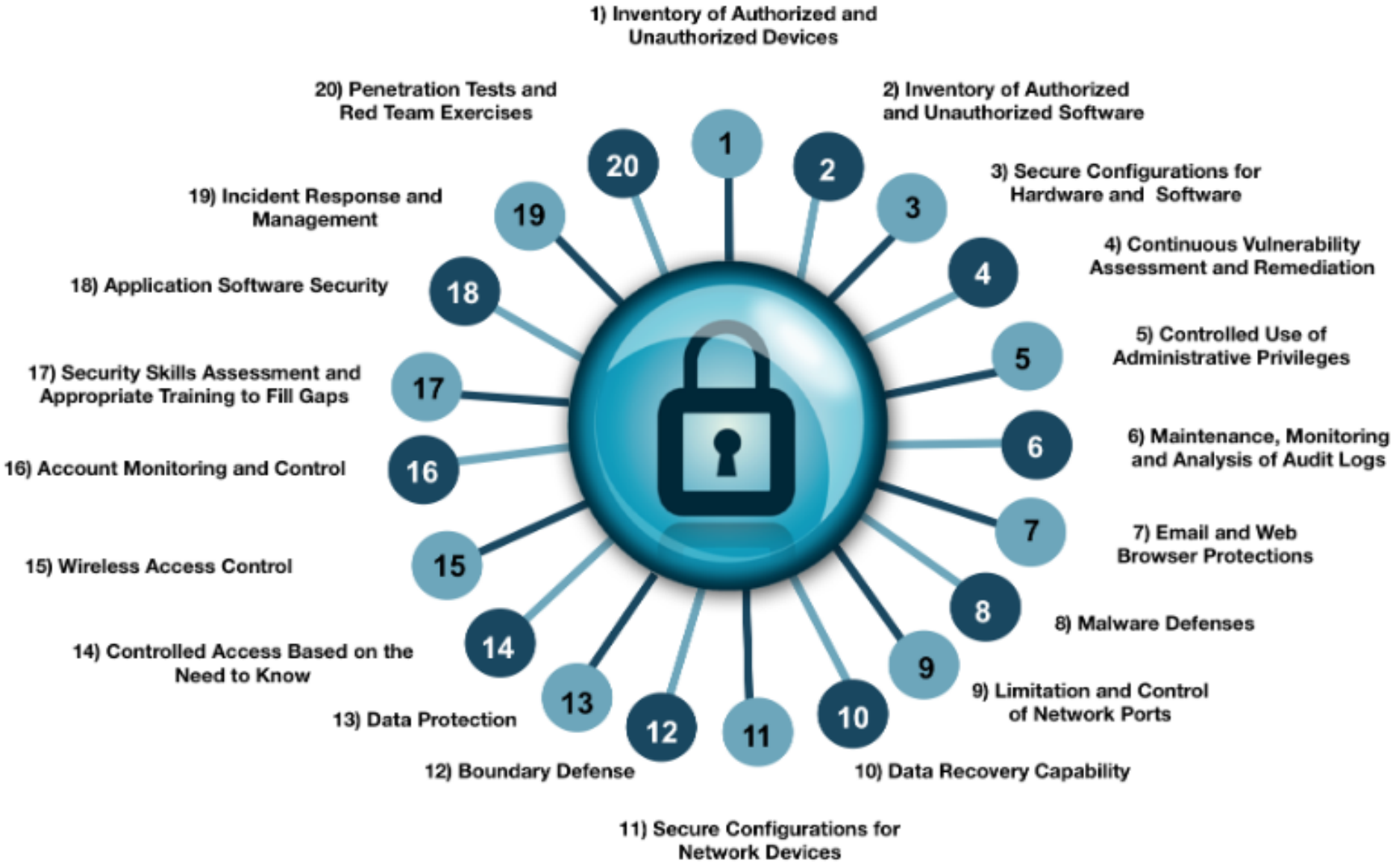
CSC history

- National Security Agency (NSA)
- SANS Institute
- Center for Internet Security (CIS)

Related information

- CIS-RAM (Risk Assessment Matrix)
- Measurement companion to the CIS controls

Control families



Overview

No.	Control title	Control details
1	Use 3 synchronized time sources	Use at least three synchronized time sources from which all servers and network devices retrieve time information regularly so timestamps in logs are consistent.
2	Activate audit logging	Ensure that local logging has been enabled on all systems and networking devices.
3	Enable detailed logging	Enable system logging to include detailed information such as event source, date, user, timestamp, source addresses, destination addresses and other useful elements.

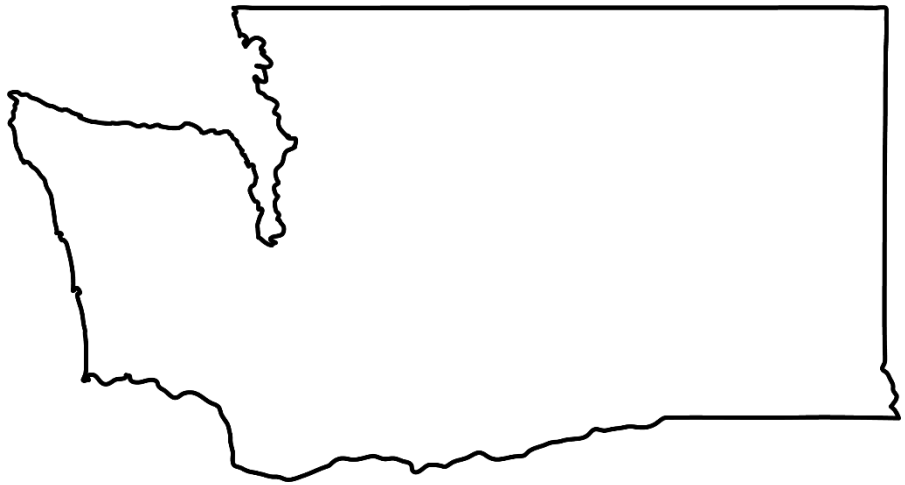
In-Depth look

Look at handout Page 3

Final thoughts on NIST, CSC

- NIST is not better than CSC, CSC is not better than NIST. They serve different functions.
- If the focus leans more toward governance, NIST might be the better metric.
- If the focus leans more toward effective defense, CSC might be the better metric.

What our Office is doing in Washington

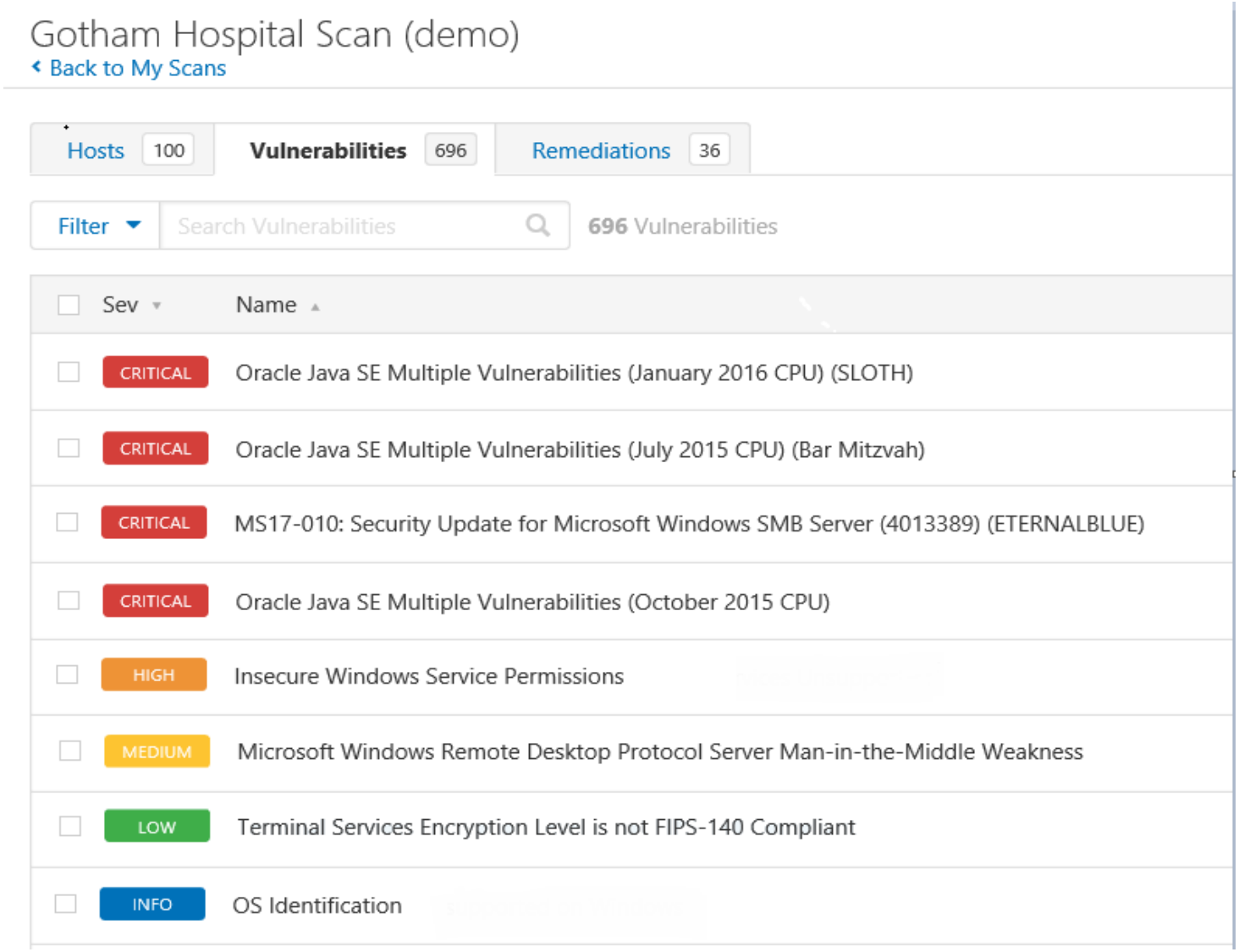


Validation tool #1: Scanning

Purpose:

- Identify vulnerabilities
- Perform security benchmark tests
- Assess maturity level of patch and vulnerability management
- Taking inventory of systems and software

Validation scanning tool: Nessus



Case 1

- **Inventory and Control of Software Assets, Control 2:** Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system

- **Analysis:** Compare authorized software list to software inventory

Case 2

- **Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers, Sub-Control 1:** Maintain documented, standard security configuration standards for all authorized operating systems and software

- **Note:** Use SCAP compliant tool with a benchmark to assess system configurations

Case 3

- **Controlled Use of Administrative Privileges, Sub-Control 1:** Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges

- **Analysis:** authorized privileged list to privileged inventory

Case 4

- **Continuous Vulnerability Management Control 3:** Deploy automated software update tools to ensure that the operating systems are running the most recent security updates provided by the software vendor

- **Analysis:** Scan the network and compare software to latest version

Validation tool #2: Scripting

Purpose: Help answer more-abstract questions

- Identify membership in default privilege groups
- Verify accounts follow security standards
  - Password requirement
  - Password age
  - Identifying abnormalities

Validation scripting tool: AD asset inventory

Domain Statistics

User Account Statistics	
Total User Accounts	685
Enabled	568
Disabled	117
Locked	5
Password Does Not Expire	171
Password Must Change	4

User Account Statistics	
Password Not Required	11
Dial-in Enabled	82
Control Access With NPS	603
Unconstrained Delegation	5
Not Trusted For Delegation	5
No Pre-Auth Required	0

Group Statistics	
Total Groups	926
Built-in	27
Universal Security	45
Universal Distribution	62
Global Security	779
Global Distribution	0
Domain Local Security	13
Domain Local Distribution	0

Validation scripting tool: AD asset inventory

Enterprise Administrators

A group that exists only at the forest level of domains. The group is authorized to make forest-wide changes in Active Directory, such as adding child domains. By default, the only member of the group is the Administrator account for the forest root domain.

Logon ID	Name	Pwd Age (Days)	Last Logged In	No Pwd Expiry	Pwd Reversable	Pwd Not Req.
Adam West	Adam West	1695	3/20/2016 2:59:45 AM	True	False	False
Dr.Pepper	Dr.Pepper	52	3/22/2016 3:07:35 AM	False	False	False
Dr.Dre	Dr.Dre	23	3/19/2016 12:15:58 AM	False	False	False
Dr.Doom	Dr.Doom	3	3/23/2016 1:10:26 AM	False	False	False

Schema Administrators

A group that exists only at the forest level of domains. The group is authorized to make schema changes in Active Directory. By default, the only member of the group is the Administrator account for the forest root domain. No other accounts should be in this group unless schema upgrades are being done.

Logon ID	Name	Pwd Age (Days)	Last Logged In	No Pwd Expiry	Pwd Reversable	Pwd Not Req.
Adam West	Adam West	1695	3/20/2016 2:59:45 AM	True	False	False
Dr.Pepper	Dr.Pepper	52	3/22/2016 3:07:35 AM	False	False	False
Dr.Dre	Dr.Dre	23	3/19/2016 12:15:58 AM	False	False	False
Dr.Doom	Dr.Doom	3	3/23/2016 1:10:26 AM	False	False	False

Domain Administrators

Members are authorized to administer the domain. By default, the Domain Admins group is a member of the Administrators group on all computers that have joined a domain, including the domain controllers. Domain Admins is the default owner of any object that is created in the domain's Active Directory by any member of the group. If members of the group create other objects, such as files, the default owner is the Administrators group.

Logon ID	Name	Pwd Age (Days)	Last Logged In	No Pwd Expiry	Pwd Reversable	Pwd Not Req.
Bruce.Wayne	Bruce.Wayne	1695	3/20/2016 1:14:39 PM	True	False	False
Adam West	Adam West	1695	3/20/2016 2:59:45 AM	True	False	False
svc.SQL.GH	svc.SQL.GH	588	3/20/2016 7:40:17 PM	True	False	False
svc.backup.GH	svc.backup.GH	367	3/14/2016 7:39:37 AM	True	False	False
Dr.Pepper	Dr.Pepper	52	3/22/2016 3:07:35 AM	False	False	False
lucius.fox_Admin	Lucius.fox.Admin	43	3/22/2016 7:15:02 AM	False	False	False
Dr.Dre	Dr.Dre	23	3/19/2016 12:15:58 AM	False	False	False
barbara.gordon_admin	barbara.gordon_admin	10	3/14/2016 8:50:05 AM	False	False	False

Case 1

- **Controlled Use of Administrative Privileges, Sub-Control 1:** Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges

- **Analysis:** Authorized privileged list to privileged inventory

Case 2

- **Account Monitoring and Control, Sub-Control:**
  - **6:** Maintain an inventory of all accounts organized by authentication system.
  - **8:** Disable any account that cannot be associated with a business process or business owner.
  - **9:** Automatically disable dormant accounts after a set period of inactivity.
  - **10:** Ensure that all accounts have an expiration date that is monitored and enforced.
- **Analysis:** Compare policy to user account inventory.

Validation tool #3: Experimental

Purpose: Help answer more-abstract questions

- Network discovery tool
- Big Data
- Phishing

Questions?

Sunia Laulile
Senior IT Security Specialist
(360) 725-5636
lauliles@sao.wa.gov

Website: www.sao.wa.gov

Twitter: www.twitter.com/WAStateAuditor

Tools used in our audits

- **Nessus:** https://www.tenable.com/products/nessus/select-your-operating-system
  - Gain awareness of patch levels
  - Check systems against known benchmarks
  - Gain awareness of privileged accounts
- **Lynis:** https://cisofy.com/lynis
  - Free audit tool for Linux, Unix, and Apple systems.
- **AdAssetInventory.PS1:** https://gallery.technet.microsoft.com/office/Active-Directory-Audit-7754a877
  - PowerShell script that identifies privileged accounts in AD and provides insight

More tools used in our audits

- **NetBrain:** https://www.netbraintech.com
  - Maps networks for situational awareness
  - Generates network diagram
  - Assists in configuration review
- **Nipper:** https://www.titania.com/products/nipper-studio
  - Networking auditing tool
- **CIS-CAT:** https://learn.cisecurity.org/cis-cat-landing-page
  - Center of Internet Security tool for checking CIS benchmarks