Autonomic Security Compliance Framework

Cihan Tunc and Salim Hariri
Cloud and Autonomic Computing Center at The University of Arizona
December 30, 2015, the U.S. Department of Defense (DoD) published a three-page interim rule with the deadline of December 31, 2017

- Implement all of the requirements of NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.

Current Supply chain security management techniques are

- Manual and labor intensive, and not flexible
- Infeasible to create a secure organization boundary

Project Overview

- Goal: Autonomic security compliance
  - Continuous monitor of computers, systems, devices, applications, etc.
  - Compliance requirements are met based on NIST SP-800-171
  - Create a compliance report and report the critical issues
  - Suggestions to fix the problems (automated/semi-automated actions)
Autonomic Cyber Security Framework

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
NIST SP 800-171

The security control requirements

Autonomic Security Compliance Engine

Server Systems

VM-1
 Apps
 vResource
 Operating System
 Hypervisor
 Physical Resource

VM-N
 Apps
 vResource

Supply Chain 1

Devices

Supply Chain 2
Autonomic Cyber Security Framework

NIST SP 800-171

1. Access Control
2. Awareness and Training
3. Audit and Accountability
5. Identification and Authentication
6. Incident Response
7. Maintenance
8. Media Protection
9. Personnel Security
10. Physical Protection
11. Risk Assessment
12. Security Assessment
13. System and Comm. Protection
14. System & Info. Integrity

United States Government Conf. Baseline (USGCB)

- Minimum password length (12 chars) → To make brute force password guessing attacks more difficult.
- Network security: Force logoff when logon hours expire → To prevent users from remaining connected after their logon hours have expired.
- Inbound connections (Block) → To minimize the risk of exploiting a vulnerable application with an inbound network port.

United States Government
Conf. Baseline (USGCB)

- Minimum password length (12 chars) → To make brute force password guessing attacks more difficult.
- Network security: Force logoff when logon hours expire → To prevent users from remaining connected after their logon hours have expired.
- Inbound connections (Block) → To minimize the risk of exploiting a vulnerable application with an inbound network port.

United States Government
Conf. Baseline (USGCB)

- Minimum password length (12 chars) → To make brute force password guessing attacks more difficult.
- Network security: Force logoff when logon hours expire → To prevent users from remaining connected after their logon hours have expired.
- Inbound connections (Block) → To minimize the risk of exploiting a vulnerable application with an inbound network port.

United States Government
Conf. Baseline (USGCB)

- Minimum password length (12 chars) → To make brute force password guessing attacks more difficult.
- Network security: Force logoff when logon hours expire → To prevent users from remaining connected after their logon hours have expired.
- Inbound connections (Block) → To minimize the risk of exploiting a vulnerable application with an inbound network port.

NIST SP 800-171 Security Control | Metric (0-1) | Report
--- | --- | ---
3.1 Access Control | 0.45 | Security controls do not pass
3.1.8 Limit unsuccessful logon attempts. | 0 | Failed the tests
3.1.9 Provide privacy and security notices consistent with applicable CUI rules. | 0.9 | 90% of the security tests passed
3.2 Awareness and Training | 1 | PASS
3.3 Audit and Accountability | 0.6 | Not all the security controls are effectively applied
3.3.4 Alert in the event of an audit process failure. | 0.3 | The tests failed mostly
3.4 Configuration Management | 0.55 | The tests failed
3.5 Identification and Authentication | 1 | PASS
3.6 Incident Response | 0.9 | PASS
3.7 Maintenance | 1 | PASS
3.8 Media Protection | 1 | PASS
3.9 Personnel Security | 0.4 | More work is needed
3.10 Physical Protection | 1 | PASS
3.11 Risk Assessment | 1 | PASS
3.12 Security Assessment | 1 | PASS
3.13 System and Comm. Protection | 0.7 | Not all the security controls are effectively applied
3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e. deny all, permit by exception). | 0.2 | Failed the tests
3.22 System & Info. Integrity | 0.99 | PASS
NIST SP 800-171

* 14 security categories
  • Access Control
  • Awareness and Training
  • Audit and Accountability
  • Configuration Management
  • Identification and Authentication
  • Incident Response
  • Maintenance
  • Media Protection
  • Personnel Security
  • Physical Protection
  • Risk Assessment
  • Security Assessment
  • System and Communications Protection
  • System and Information Integrity
Environment Information

- **3.1.8 – Limit unsuccessful logon attempts.**
  - Script name: check_login_attempts_SP800_171_3.1.8
  - Checks the auth.log to see if the number of unsuccessful attempts are beyond a limit

- **3.1.6 – Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).**
  - Script name: check_open_ports_SP800_171_3.13.6
  - Checks the open ports
  - It uses a given authorized port list to compare the ports
  - If there are any unauthorized ports, it gives a critical error to the admin.
Environment Information

Supply Chain Management Dashboard

Monitored System Statuses

<table>
<thead>
<tr>
<th>System Name</th>
<th>IP Address</th>
<th>Operating System</th>
<th>Compliance Status</th>
<th>View Usage Graphs</th>
<th>View System Compliance Status</th>
<th>View NHIDS Logs</th>
<th>View SBIDS Logs</th>
<th>Delete from Monitor List</th>
</tr>
</thead>
<tbody>
<tr>
<td>aim-scm</td>
<td>127.0.0.1</td>
<td></td>
<td>Compliant</td>
<td>View</td>
<td>View</td>
<td>View</td>
<td>View</td>
<td>Delete</td>
</tr>
<tr>
<td>scm-client-1</td>
<td>10.5.253.216</td>
<td></td>
<td>Compliant</td>
<td>View</td>
<td>View</td>
<td>View</td>
<td>View</td>
<td>Delete</td>
</tr>
<tr>
<td>scm-client-2</td>
<td>10.5.253.215</td>
<td></td>
<td>Compliant</td>
<td>View</td>
<td>View</td>
<td>View</td>
<td>View</td>
<td>Delete</td>
</tr>
</tbody>
</table>

Network Usage Information

Public Network Information
Access Control

![Access Control Interface](image)

### Compliance Status for System 'scm-client-1'

#### Summarized Status

<table>
<thead>
<tr>
<th>CUI Security Control</th>
<th>Compliance Status</th>
<th>Compliance Score</th>
<th>Details</th>
<th>Automatic Fix Available?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logged In Users</td>
<td>OK</td>
<td>1.00</td>
<td>USERS OK - 1 users currently logged in</td>
<td>No</td>
</tr>
<tr>
<td>Open Ports</td>
<td>OK</td>
<td>1.00</td>
<td>OK - 1 open</td>
<td>No</td>
</tr>
<tr>
<td>System Load Average</td>
<td>OK</td>
<td>1.00</td>
<td>OK- Client Load Average: 0.00, 0.01, 0.00</td>
<td>No</td>
</tr>
<tr>
<td>Unsuccessful Log in Attempt Limit</td>
<td>UNKNOWN</td>
<td>0.00</td>
<td>3 - Not defined</td>
<td>No</td>
</tr>
<tr>
<td>Unsuccessful Log in Attempts</td>
<td>OK</td>
<td>1.00</td>
<td>0 - Acceptable</td>
<td>No</td>
</tr>
</tbody>
</table>
# Access Control

![Access Control Diagram](image)

## CUI Security Control Details: SCM-CLIENT-1

**Details for CUI Security Control: Logged In Users**

<table>
<thead>
<tr>
<th>Name</th>
<th>Unsuccessful Log in Attempt Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>scm-client-1</td>
</tr>
<tr>
<td>Current State</td>
<td>UNKNOWN</td>
</tr>
<tr>
<td>Execution Time</td>
<td>0.022 sec</td>
</tr>
<tr>
<td>Latency Time</td>
<td>0.211 sec</td>
</tr>
<tr>
<td>Log Output</td>
<td>3 - Not defined</td>
</tr>
<tr>
<td>Performance Data</td>
<td>Limit not defined</td>
</tr>
<tr>
<td>Last Check</td>
<td>2017-04-18 05:28:02</td>
</tr>
<tr>
<td>Next Check</td>
<td>2017-04-18 05:30:03</td>
</tr>
</tbody>
</table>

**Details for CUI Security Control: Unsuccessful Log in Attempt Limit**

- **Name:** Unknown
- **Hostname:** Unknown
- **Current State:** Unknown
- **Execution Time:** Unknown
- **Latency Time:** Unknown
- **Log Output:** Unknown
- **Performance Data:** Unknown
- **Last Check:** Unknown
- **Next Check:** Unknown
Vulnerability Analysis

Scan Report

April 18, 2017

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “SCM Client 1 Scan”. The scan started at Tue Apr 18 14:40:15 2017 UTC and ended at Tue Apr 18 11:57:54 2017 UTC. The report first summarizes the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview ........................................... 2

2 Results per Host ........................................ 2

2.1 10.5.253.216 ........................................... 2

2.1.1 Log general/tcp ..................................... 2

2.1.2 Log general/tcp ..................................... 3

2.1.3 Log general/icmp .................................... 5

2.1.4 Log 22/tcp .......................................... 6

2.1.5 Log general/CPE-T ................................. 9

2.1.6 Log 80/tcp .......................................... 9

Log (CVSS: 0.0)  
NVT: Traceroute

Summary

A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result

Here is the route from 10.5.253.217 to 10.5.253.216:

10.5.253.217
10.5.253.216

Solution

Block unwanted packets from escaping your network.

Log Method

Details: Traceroute

OID: 1.3.6.1.4.1.25623.1.0.51662

Version used: $Revision: 5390$
Deliverables and Benefits

- Autonomic security control framework
  - Implementing security controls on individual systems for supply chain
  - Monitoring the systems 24x7
    - Security → Continuous monitoring
  - Built a proof-of-concept testbed
Please take a moment to fill out your L.I.F.E. forms.

http://www.iucrc.com
Select “Cloud and Autonomic Computing Center”
then select “IAB” role.

What do you like about this project?
What would you change?
(Please include all relevant feedback.)