Improving Security while Reducing Toil with DevSecOps

Paul Czarkowski
@pczarkowski
I'M AN
DEVELOPER AVOCADO
Agenda

- Who I Am
- Compliance
- DevOps
- DevOps + Compliance
- Q+A
Compliance ?
What is Compliance?

Self Imposed
- CIS Controls / Benchmarks
- Security Technical Implementation Guide (STIG)
- Allowed opensource licenses

Regulatory
- PCI (US)
- HIPAA (US)
- Sarbanes-Oxley (US)
- EU GDPR
- NZ Information Security Manual (NZISM)
Verification
Validation of compliance based on Controls in place.

Checklists
Practice, Policy or Procedure established to meet compliance requirements.
- Spreadsheets
- Checklists
- Sharepoint Pages

Verification
Validation of compliance based on Controls in place.
- Checklists
- External Auditors
Example of Compliance Specifications

The SSH daemon must be configured to use only the SSHv2 protocol.

Overview

<table>
<thead>
<tr>
<th>Finding ID</th>
<th>Version</th>
<th>Rule ID</th>
<th>IA Controls</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>V-38607</td>
<td>RHEL-06-000227</td>
<td>SV-50408r1_rule</td>
<td></td>
<td>High</td>
</tr>
</tbody>
</table>

Description

SSH protocol version 1 suffers from design flaws that result in security vulnerabilities and should not be used.

Details

Check Text (C-46165r1_chk)

To check which SSH protocol version is allowed, run the following command:

```
# grep Protocol /etc/ssh/sshd_config
```

If configured properly, output should be

Protocol 2

If it is not, this is a finding.

Fix Text (F-43555r1_fix)

Only SSH protocol version 2 connections should be permitted. The default setting in “/etc/ssh/sshd_config” is correct, and can be verified by ensuring that the following line appears:

Protocol 2
Example of Compliance Specifications

## Implement Strong Access Control Measures

### Requirement 7: Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

“Need to know” is when access rights are granted to only the least amount of data and privileges needed to perform a job.

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
<th>Testing Procedures</th>
<th>Guidance</th>
</tr>
</thead>
</table>
| 7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. | 7.1 Examine written policy for access control, and verify that the policy incorporates 7.1.1 through 7.1.4 as follows:  
  - Defining access needs and privilege assignments for each role  
  - Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities  
  - Assignment of access based on individual personnel's job classification and function  
  - Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. | The more people who have access to cardholder data, the more risk there is that a user's account will be used maliciously. Limiting access to those with a legitimate business reason for the access helps an organization prevent mishandling of cardholder data through inexperience or malice. |
| 7.1.1 Define access needs for each role, including:  
  - System components and data resources that each role needs to access for their job function  
  - Level of privilege required (for example, user, administrator, etc.) for accessing resources. | 7.1.1 Select a sample of roles and verify access needs for each role are defined and include:  
  - System components and data resources that each role needs to access for their job function  
  - Identification of privilege necessary for each role to perform their job function. | In order to limit access to cardholder data to only those individuals who need such access, first it is necessary to define access needs for each role (for example, system administrator, call center personnel, store clerk), the systems/devices/data each role needs access to, and the level of privilege each role needs to effectively perform assigned tasks. Once roles and corresponding access needs are defined, individuals can be granted access accordingly. |
| 7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. | 7.1.2.a Interview personnel responsible for assigning access to verify that access to privileged user IDs is:  
  - Assigned only to roles that specifically require such privileged access  
  - Restricted to least privileges necessary to perform job responsibilities. | When assigning privileged IDs, it is important to assign individuals only the privileges they need to perform their job (the “least privileges”). For example, the database administrator or backup administrator should not be assigned the same privileges as the overall systems administrator.  
(Continued on next page) |
I want change!

Wall of Confusion

I want stability!

Development

Operations
Culture
- Focus on People
- Embrace Change & experimentation

Automation
- “Continuous Delivery”
- “Infrastructure as Code”

Lean
- Focus on producing value for the end-user
- Small batch sizes

Measurement
- Measure everything
- Show the improvement

Sharing
- Open information sharing
- Collaboration & Communication
Congrats Mark Miller (@EUSP) and John Willis (@botchagalupe) on launch of devsecopsdays.com #DevSecOps #devops #RSAC2018
Nobody gets in, nobody gets out
Rugged DevOps

DevSecOps

Secure DevOps
Implementing DevOps in a Regulated Environment

https://www.devsecopsdays.com/articles/its-just-a-name
Congrats Mark Miller (@EUSP) and John Willis (@botchagalupe) on launch of devsecopsdays.com #DevSecOps #devops #RSAC2018

5:08 PM - 15 Apr 2018

10 Retweets 6 Likes

Czarcloudski @pczarkowski · now
Replying to @conikeec @EUSP @botchagalupe
Awesome! It’s about time we empower security to be part of the devops revolution instead of actively depriving them from doing their jobs.
Culture
- Focus on People
- Embrace Change & experimentation

Automation
- “Continuous Delivery”
- “Infrastructure as Code”

Lean
- Focus on producing value for the end-user
- Small batch sizes

Measurement
- Measure everything
- Show the improvement

Sharing
- Open information sharing
- Collaboration & Communication
Culture
Organizational culture eats strategy for breakfast, lunch, and dinner.

- Culture
- Growth
- Change
- Performance
- Innovation
- Execution

Torben Rick www.torbenrick.eu
Adopting a DevOps culture

Despite varying approaches to describing high-performance teams there is a set of common characteristics that are recognised to lead to success.

- Participative leadership – using a democratic leadership style that involves and engages team members
- Effective decision-making – using a blend of rational and intuitive decision making methods, depending on that nature of the decision task
- Open and clear communication – ensuring that the team mutually constructs shared meaning, using effective communication methods and channels
- Valued diversity – valuing a diversity of experience and background in team, contributing to a diversity of viewpoints, leading to better decision making and solutions
- Mutual trust – trusting in other team members and trusting in the team as an entity
- Clear goals – goals that are developed using SMART criteria; also each goal must have personal meaning and resonance for each team member, building commitment and engagement
- Defined roles and responsibilities – each team member understands what they must do (and what they must not do) to demonstrate their commitment to the team and to support team success
- Positive atmosphere – an overall team culture that is open, transparent, positive, future-focused and able to deliver success

Value Stream Mapping Process

1. Define Product Family
   - Products (good or services) with common process steps

2. Document Current State
   - Foundation (the basis) for the future state; 70-80% accurate is acceptable (directionally correct)

3. Design Future State
   - Create flow by eliminating waste; it is now obvious from your current state map; typically 3-6 months out

4. Create Implementation Plan
   - Include accountability and timeframes for completion

Repeat

Implement!

The goal of mapping!

https://www.slideshare.net/KarenMartinGroup/value-stream-mapping-in-office-service-setttings
<table>
<thead>
<tr>
<th>Mappable Processes that include Security / Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Infrastructure Provisioning</strong></td>
</tr>
<tr>
<td>● OS Hardening</td>
</tr>
<tr>
<td>● Firewalling</td>
</tr>
<tr>
<td>● User Management</td>
</tr>
<tr>
<td>● Remote logging and auditing</td>
</tr>
<tr>
<td>● Intrusion Detection</td>
</tr>
<tr>
<td>● Vulnerability Scanning</td>
</tr>
<tr>
<td><strong>Application Release</strong></td>
</tr>
<tr>
<td>● Vulnerability Scanning</td>
</tr>
<tr>
<td>● Security Scanning (sql injection etc)</td>
</tr>
<tr>
<td>● License Scanning</td>
</tr>
<tr>
<td>● Attribution</td>
</tr>
<tr>
<td><strong>Compliance Audits</strong></td>
</tr>
<tr>
<td>● Vulnerability Scanning</td>
</tr>
<tr>
<td>● Security Scanning (sql injection etc)</td>
</tr>
<tr>
<td>● Package updates</td>
</tr>
<tr>
<td>● OS inspection</td>
</tr>
</tbody>
</table>
Value Stream map for Provisioning a New Server

Current State

Prepare Request 1-2 days
Network / VLANs 1-5 days
Launch VM / Install OS 1-5 days
Test Compliance 1-2 days
Deliver 1-5 days
Value Stream map for Provisioning a New Server

Future State

Deploy VM 1-2 hours

Configure VM 1-5 days

Test Compliance 1-5 days

Deliver 1-2 Hours

Pivotal
Value Stream map for Provisioning a New Server

Future State

Push Button
Receive Bacon
| Feature ID | Feature Title | Feature Description | Feature Details | Feature Status | Feature Priority | Feature Release Date | Feature Notes |
|------------|---------------|---------------------|----------------|---------------|-----------------|---------------------|----------------|----------------|
| 1          | 123.1.2       | Logging             | The feature allows for logging of events and activities. | Done           | Medium          | 2023-04-01          | Needs review   |
| 2          | 123.2.1       | Security           | The feature enhances security measures and access controls. | In progress     | High            | 2023-05-01          | Under review   |
| 3          | 123.3.1       | Performance        | The feature optimizes performance and increases system efficiency. | Done           | Low             | 2023-06-01          | No comments    |
| 4          | 123.4.1       | Usability          | The feature improves user experience and interface usability. | In progress     | Medium          | 2023-07-01          | Needs review   |
| 5          | 123.5.1       | Maintainability    | The feature enhances maintainability and support for the system. | Done           | High            | 2023-08-01          | No comments    |
| 6          | 123.6.1       | Scalability        | The feature ensures scalability and ability to handle increased load. | In progress     | Medium          | 2023-09-01          | Needs review   |
| 7          | 123.7.1       | Reliability        | The feature enhances reliability and reduces downtime. | Done           | Low             | 2023-10-01          | No comments    |
| 8          | 123.8.1       | Compatibility      | The feature improves compatibility with other systems and software. | In progress     | Medium          | 2023-11-01          | Needs review   |
| 9          | 123.9.1       | Customization      | The feature allows for customization and tailoring to user needs. | Done           | High            | 2023-12-01          | No comments    |
| 10         | 123.10.1      | Accessibility      | The feature enhances accessibility for users with disabilities. | In progress     | Medium          | 2024-01-01          | Needs review   |
| 11         | 123.11.1      | Interoperability   | The feature improves interoperability with external systems and applications. | Done           | Low             | 2024-02-01          | No comments    |

**Notes:**
- Feature 123.1.2 requires additional review before implementation.
- Feature 123.4.1 is currently undergoing user testing.
- Feature 123.6.1 faces scalability challenges during peak hours.
- Feature 123.9.1 is receiving positive feedback from users.
● Implements STIG controls via Ansible playbooks
● Opensource project started at Rackspace
● Plays well with existing config management
● Easily override problematic controls

● Extends RSPEC for Compliance testing
● Similar to Serverspec, but better.
● Easy to go from serverspec to inspec
● Inspec-STIG is all of STIG already written into inspec tests.
Example of Compliance Specifications

*The SSH daemon must be configured to use only the SSHv2 protocol.*

### Overview

<table>
<thead>
<tr>
<th>Finding ID</th>
<th>Version</th>
<th>Rule ID</th>
<th>IA Controls</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>V-38607</td>
<td>RHEL-06-000227</td>
<td>SV-50408r1_rule</td>
<td></td>
<td>High</td>
</tr>
</tbody>
</table>

### Description

SSH protocol version 1 suffers from design flaws that result in security vulnerabilities and should not be used.

### STIG

- **STIG:** Red Hat Enterprise Linux 6 Security Technical Implementation Guide
- **Date:** 2017-03-01

### Details

**Check Text ( C-46165r1 chk )**

To check which SSH protocol version is allowed, run the following command:

```
# grep Protocol /etc/ssh/sshd_config
```

If configured properly, output should be Protocol 2

If it is not, this is a finding.

**Fix Text ( F-43555r1_fix )**

Only SSH protocol version 2 connections should be permitted. The default setting in `/etc/ssh/sshd_config` is correct, and can be verified by ensuring that the following line appears:

```
Protocol 2
```
title 'V-38607 - The SSH daemon must be configured to use only the SSHv2 protocol.'

control 'V-38607' do
  impact 1.0
  title 'The SSH daemon must be configured to use only the SSHv2 protocol.'
  desc 'SSH protocol version 1 suffers from design flaws that result in security vulnerabilities.'
  tag 'stig','V-38607'
  tag severity: 'high'
  tag fixtext: 'Only SSH protocol version 2 connections should be permitted. The default is version 2.'
  tag checktext: 'To check which SSH protocol version is allowed, run the following command.'

  describe ssd_config do
    | its('Protocol') { should eq '2' }
  end
end
control 'MYSQL005' do
  impact 1.0
  title 'Strict permissions for my.cnf to prevent unauthorized'
  desc 'strict permissions(644) and ownership (root user and group'
  tag 'production', 'development'
  tag 'mysql'
  tag remediation: 'ansible-playbook site.yml --tags=MYSQL005'
  tag documentation: 'http://e.corp/MYSQL005'
  if File.file?('/etc/my.cnf')
    describe file('/etc/my.cnf') do
      its('mode') { should cmp '0644' }
      its('group') { should eq 'root' }
      its('owner') { should eq 'root' }
    end
  end
end
<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>create</td>
</tr>
<tr>
<td>auto_resolve</td>
<td>true</td>
</tr>
<tr>
<td>command</td>
<td>sudo /etc/sensu/plugins/check-serverspec.rb -d /etc/serverspec -s warning</td>
</tr>
<tr>
<td>duration</td>
<td>4.744</td>
</tr>
<tr>
<td>executed</td>
<td>2016-10-14 15:22:20</td>
</tr>
<tr>
<td>handle</td>
<td>true</td>
</tr>
<tr>
<td>handlers</td>
<td>default</td>
</tr>
<tr>
<td>history</td>
<td>1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1</td>
</tr>
<tr>
<td>interval</td>
<td>3600</td>
</tr>
<tr>
<td>issued</td>
<td>2016-10-14 15:22:20</td>
</tr>
<tr>
<td>name</td>
<td>serverspec-check</td>
</tr>
<tr>
<td>occurrences</td>
<td>1920</td>
</tr>
<tr>
<td>output</td>
<td>CheckServerspec WARNING: 286 examples, 1 failure</td>
</tr>
<tr>
<td>standalone</td>
<td>true</td>
</tr>
<tr>
<td>status</td>
<td>1</td>
</tr>
<tr>
<td>total_state_change</td>
<td>0</td>
</tr>
<tr>
<td>type</td>
<td>standard</td>
</tr>
</tbody>
</table>
- name: Adjust ssh server configuration based on STIG requirements
  blockinfile:
    dest: /etc/ssh/sshd_config
    state: present
    marker: "# {mark} MANAGED BY ANSIBLE-HARDENING"
    insertbefore: "BOF"
    validate: '/usr/sbin/sshd -T -f %s'
    block: "{{ lookup('template', 'sshd_config_block.j2') }}"
  notify:
    - restart ssh
  tags:
    - high
    - sshd
    - V-38607
Pivotal.
Measurement
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>create</td>
</tr>
<tr>
<td>auto_resolve</td>
<td>true</td>
</tr>
<tr>
<td>command</td>
<td>sudo /etc/sensu/plugins/check-serverspec.rb -d /etc/serverspec -s warning</td>
</tr>
<tr>
<td>duration</td>
<td>4.744</td>
</tr>
<tr>
<td>executed</td>
<td>2016-10-14 15:22:20</td>
</tr>
<tr>
<td>handle</td>
<td>true</td>
</tr>
<tr>
<td>handlers</td>
<td>default</td>
</tr>
<tr>
<td>history</td>
<td>1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1</td>
</tr>
<tr>
<td>interval</td>
<td>3600</td>
</tr>
<tr>
<td>issued</td>
<td>2016-10-14 15:22:20</td>
</tr>
<tr>
<td>name</td>
<td>serverspec-check</td>
</tr>
<tr>
<td>occurrences</td>
<td>1920</td>
</tr>
<tr>
<td>output</td>
<td>CheckServerspec WARNING: 286 examples, 1 failure</td>
</tr>
<tr>
<td>standalone</td>
<td>true</td>
</tr>
<tr>
<td>status</td>
<td>1</td>
</tr>
<tr>
<td>total_state_change</td>
<td>0</td>
</tr>
<tr>
<td>type</td>
<td>standard</td>
</tr>
</tbody>
</table>

FAILED: os_spec.rb:42, File /etc/adduser.conf should contain ^DIR_MODE=700
What’s Next?
Other Security / Compliance tools

- Gauntlt (Security Testing Framework)
- Metasploit (Penetration Testing)
- Syntribos (API security testing)
- Pivotal LicenseFinder (Scanning licenses of dependencies)
- Snort (Intrusion Detection)
- Fossology (license compliance)
- OpenVAS (vulnerability scanning)
- OSSEC (Intrusion Detection)