

Designing a Secure Cloud Architecture

Cloud Computing, Second Edition - Lab 04

Student:

Andre Hardy

Email:

ahardy754@email.porterchester.edu

Time on Task:

5 hours, 20 minutes

Progress:

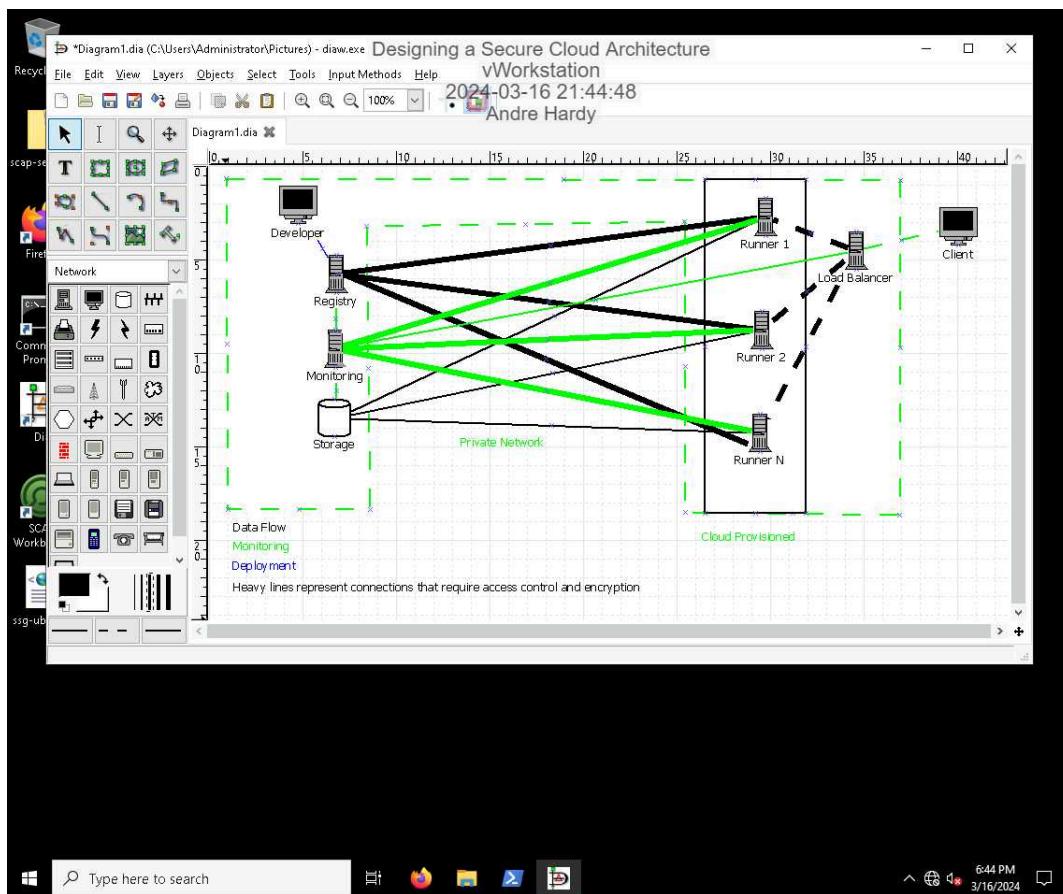
100%

Report Generated: Saturday, March 16, 2024 at 10:22 PM

Hands-On Demonstration

Part 1: Planning a Design

65. Make a screen capture showing the network diagram for the system with the labels.

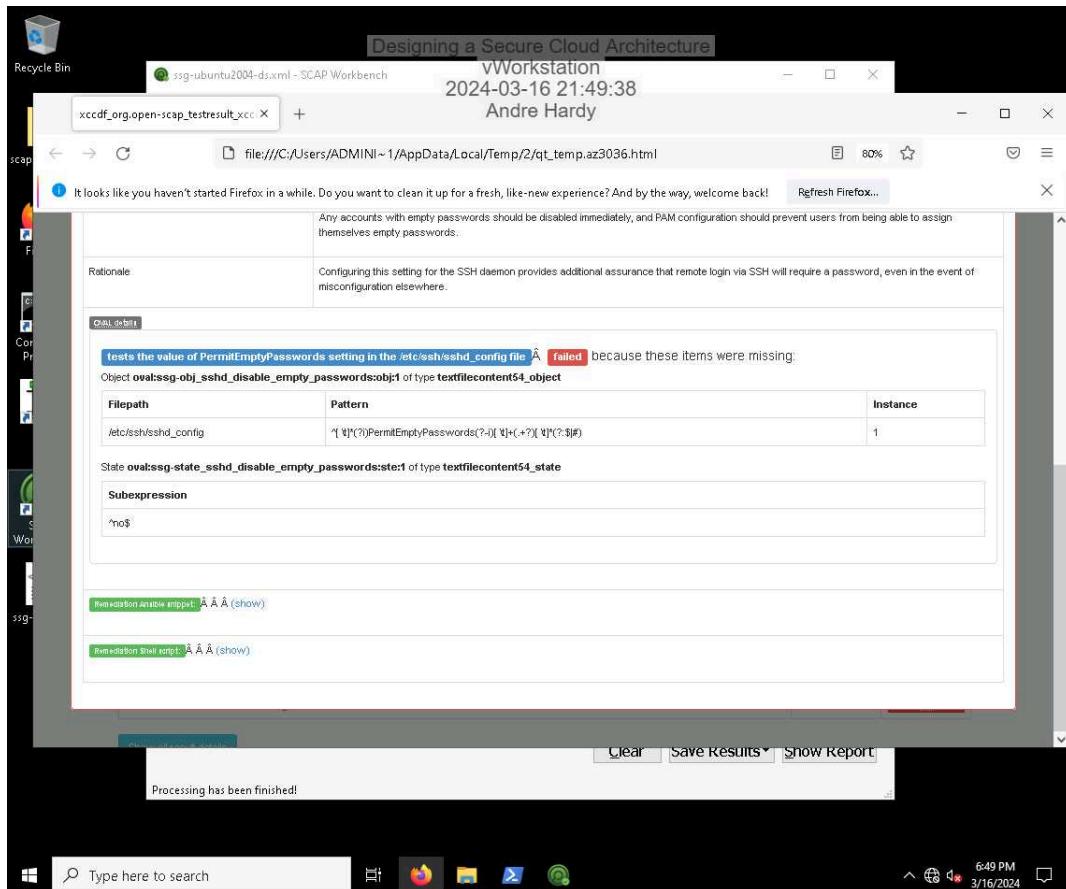


Part 2: Automating Security

Designing a Secure Cloud Architecture

Cloud Computing, Second Edition - Lab 04

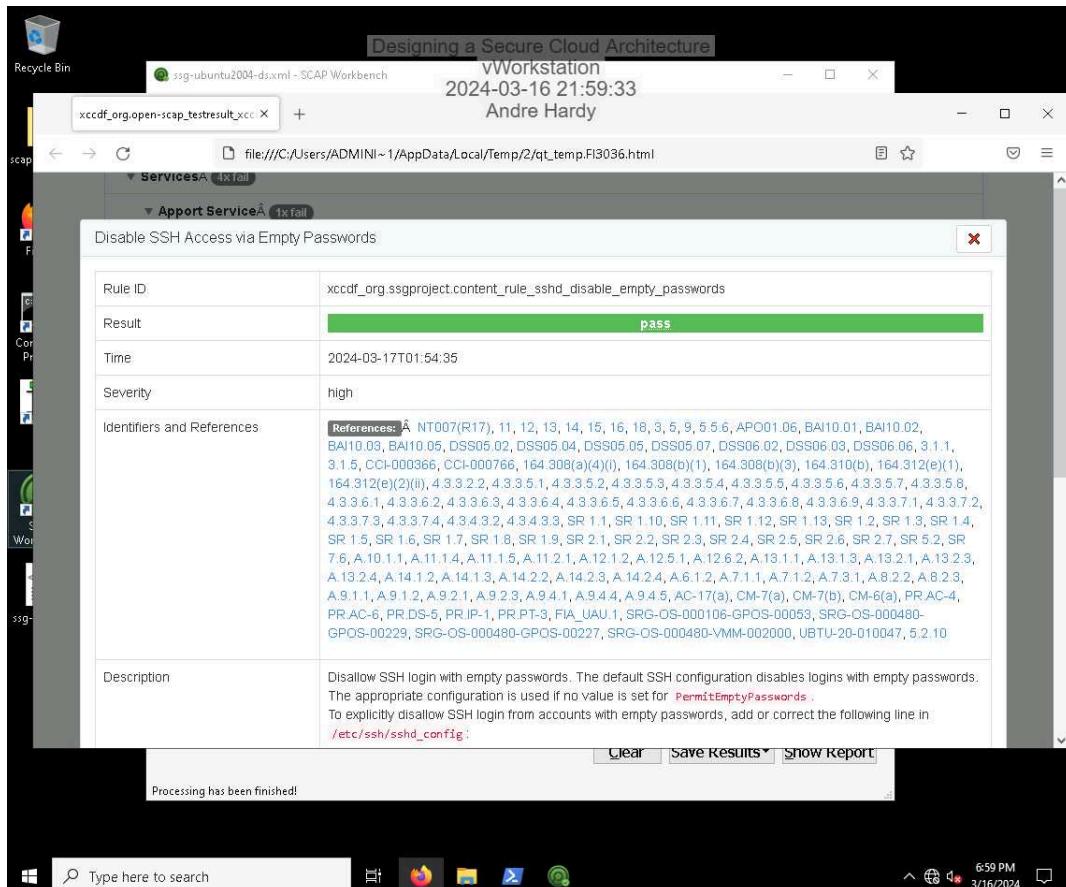
13. Make a screen capture showing the OVAL details of the PermitEmptyPasswords failure from the manual scan.



Designing a Secure Cloud Architecture

Cloud Computing, Second Edition - Lab 04

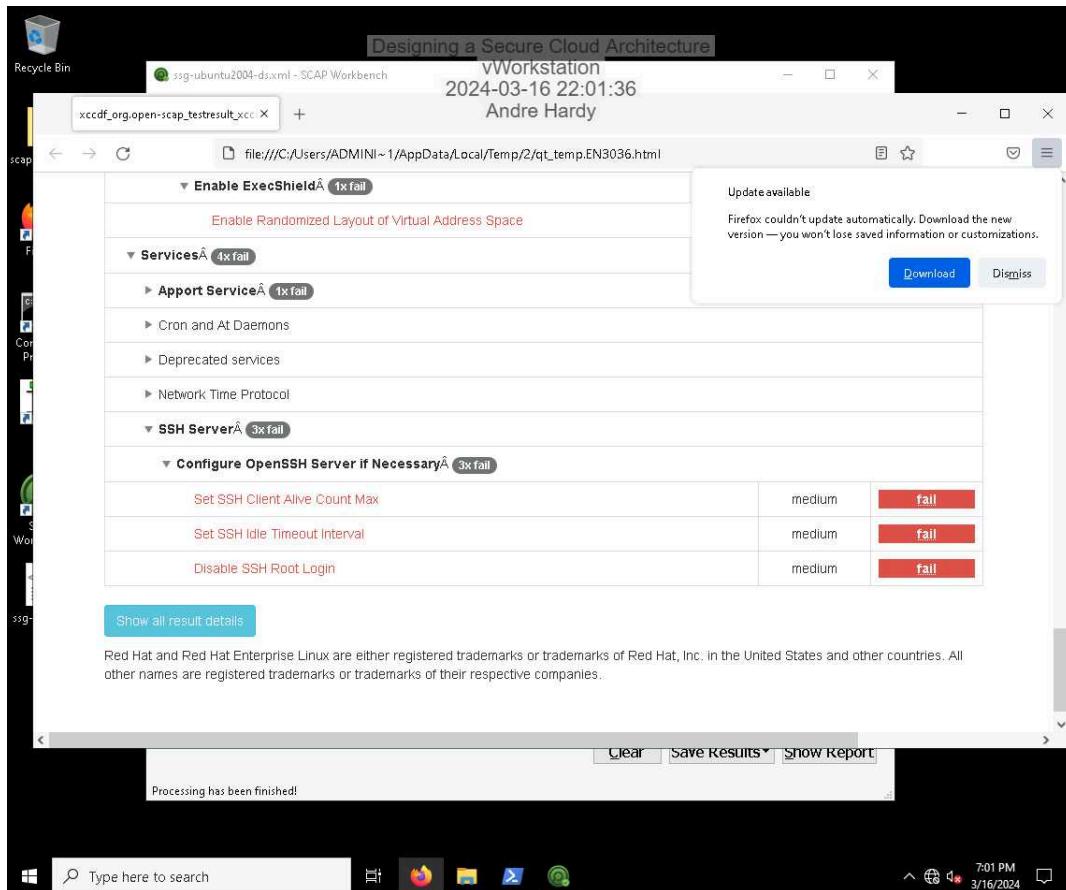
26. Make a screen capture showing that the Disable SSH Access via Empty Passwords test passed.



Designing a Secure Cloud Architecture

Cloud Computing, Second Edition - Lab 04

35. Make a screen capture showing the three tests run under **Services > SSH Server > Configure OpenSSH Server if Necessary**.



Part 3: Continuous Monitoring

Designing a Secure Cloud Architecture

Cloud Computing, Second Edition - Lab 04

19. Make a screen capture showing an event in Wazuh for Disable SSH Access via Empty Passwords failing on the DockerRunner machine.

The screenshot shows a Windows desktop environment. On the left, there's a vertical taskbar with icons for Recycle Bin, scap-security..., Firefox, Command Prompt, Dia, SCAP Workbench, and ssg-ubuntu... In the center, a Firefox browser window is open, titled "Wazuh - Wazuh". The address bar shows the URL [https://172.30.0.10:3150/wazuh/api/v1/events?&g=\(filters:!0,refreshInterval:\(pause:!value\)\)](https://172.30.0.10:3150/wazuh/api/v1/events?&g=(filters:!0,refreshInterval:(pause:!value))). The main content of the browser is a table titled "wazuh. Modules Security events ⓘ". The table lists various audit findings from a DockerRunner machine. Most of the findings are related to OpenSCAP audits failing due to files being located on the same partition as /var/log or /tmp. One entry at the bottom states "OpenSCAP agent started". The browser status bar shows the date and time as 3/16/2024 7:08 PM.

Module	Date	Host	Description	Severity	ID
t data.oscap.check.description	Mar 16, 2024 @ 19:07:29.162	DockerServer	OpenSCAP: Ensure /var/log/audit Located On Separate Partition (not passed)	5	81529
t data.oscap.check.id	Mar 16, 2024 @ 19:07:29.109	DockerServer	OpenSCAP: Ensure /var/log Located On Separate Partition (not passed)	5	81529
t data.oscap.check.oval.id	Mar 16, 2024 @ 19:07:29.100	DockerServer	OpenSCAP: Ensure /var Located On Separate Partition (not passed)	5	81529
t data.oscap.check.rationale	Mar 16, 2024 @ 19:07:29.093	DockerServer	OpenSCAP: Ensure /tmp Located On Separate Partition (not passed)	5	81529
t data.oscap.check.references	Mar 16, 2024 @ 19:07:29.079	DockerServer	OpenSCAP: Ensure /home Located On Separate Partition (not passed)	5	81529
t data.oscap.check.result	Mar 16, 2024 @ 19:07:26.951	DockerRunner	OpenSCAP: Ensure the audit Subsystem is Installed (not passed)	7	81530
t data.oscap.check.severity	Mar 16, 2024 @ 19:07:25.892	DockerRunner	OpenSCAP: Ensure /var/log/audit Located On Separate Partition (not passed)	5	81529
t data.oscap.check.title	Mar 16, 2024 @ 19:07:25.871	DockerRunner	OpenSCAP: Ensure /var/log Located On Separate Partition (not passed)	5	81529
t data.oscap.scan.benchmark.id	Mar 16, 2024 @ 19:07:25.862	DockerRunner	OpenSCAP: Ensure /var Located On Separate Partition (not passed)	5	81529
t data.oscap.scan.content	Mar 16, 2024 @ 19:07:25.854	DockerRunner	OpenSCAP: Ensure /tmp Located On Separate Partition (not passed)	5	81529
t data.oscap.scan.id	Mar 16, 2024 @ 19:07:25.842	DockerRunner	OpenSCAP: Ensure /home Located On Separate Partition (not passed)	5	81529
	Mar 16, 2024 @ 19:06:21.461	DockerServer	OpenSCAP agent started	2	592

Designing a Secure Cloud Architecture

Cloud Computing, Second Edition - Lab 04

31. Make a screen capture showing an event about the alpine image being pulled.

The screenshot shows a Windows desktop environment with a taskbar at the bottom. The taskbar includes icons for File Explorer, Task View, Firefox, and others. A search bar says "Type here to search". The system tray shows the date as 3/16/2024 and the time as 7:11 PM.

The main window is titled "+ Designing a Secure Cloud Architecture vWorkstation 2024-03-16 22:11:09 Andre Hardy". It displays a "wazuh." dashboard with a "Security events" section. A log entry is shown:

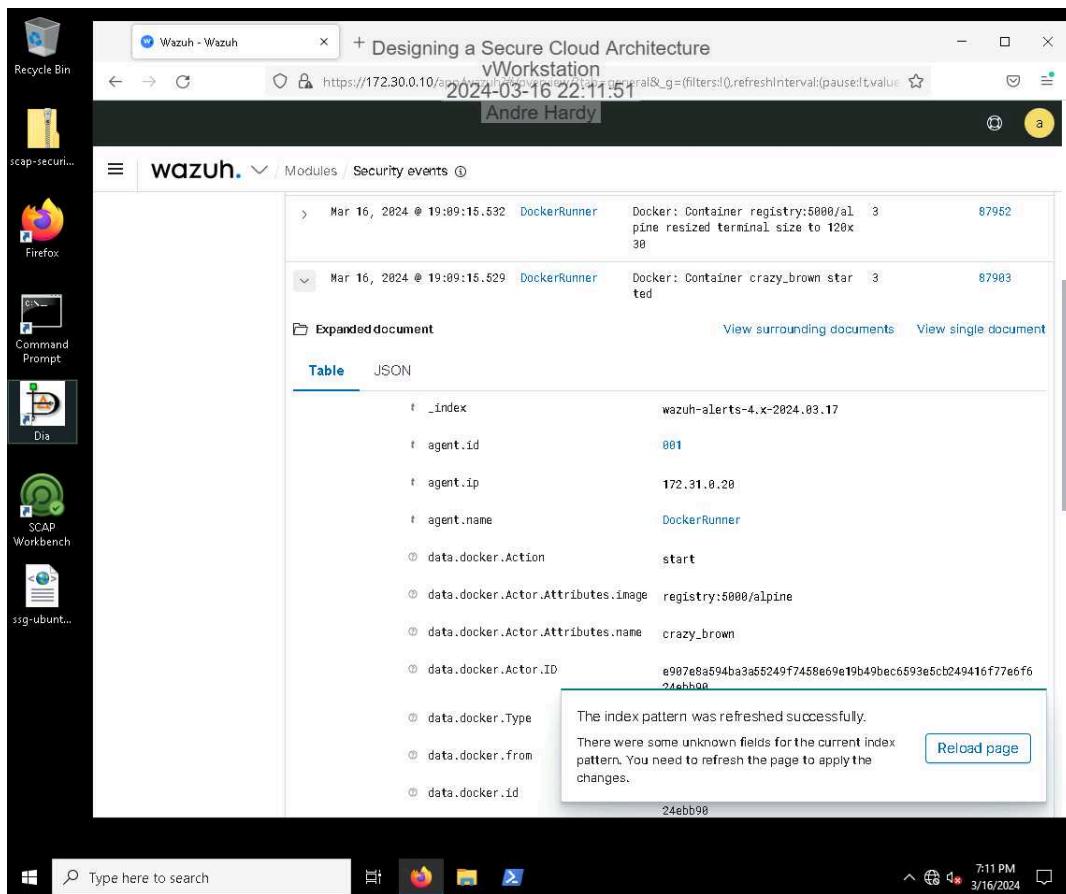
Mar 16, 2024 @ 19:09:00.685 DockerRunner Docker: Image or repository registered: registry:5000/alpine pulled 3 87932

The log is presented in both "Table" and "JSON" formats. A tooltip message in the JSON view states: "The index pattern was refreshed successfully. There were some unknown fields for the current index pattern. You need to refresh the page to apply the changes." A "Reload page" button is visible in the tooltip.

Designing a Secure Cloud Architecture

Cloud Computing, Second Edition - Lab 04

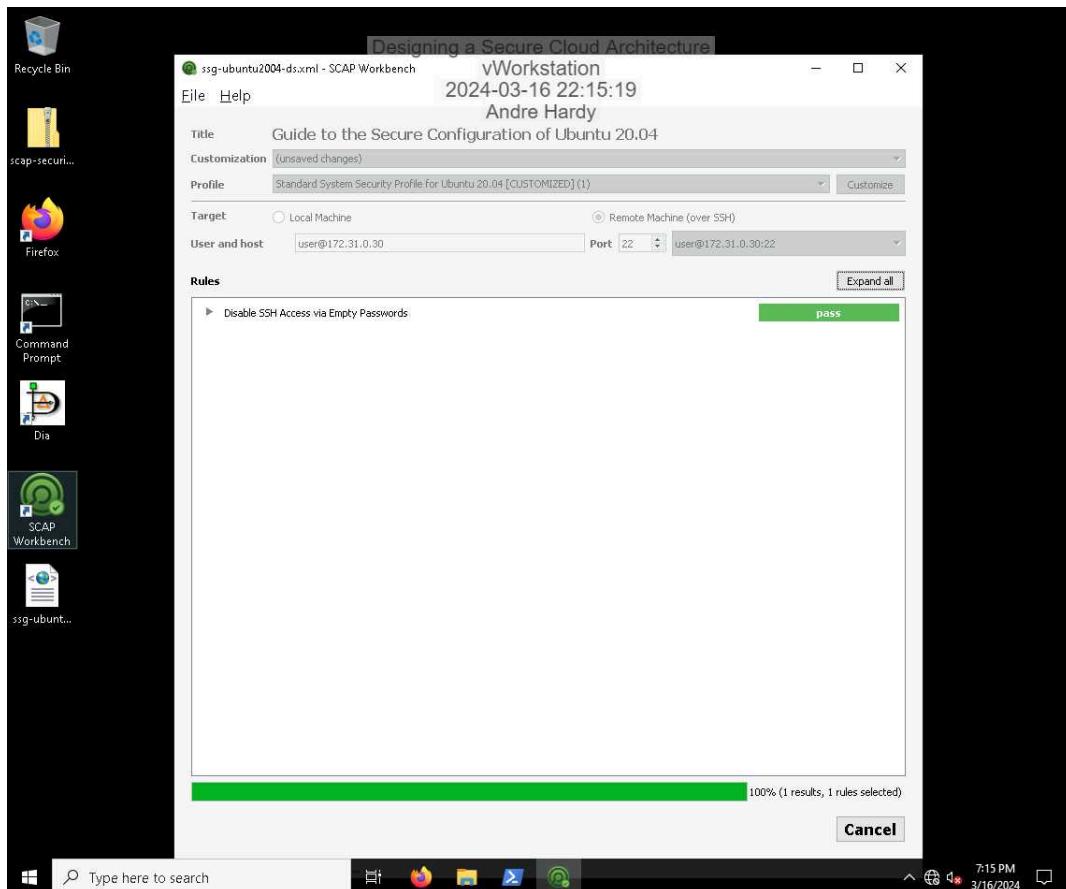
32. Make a screen capture showing an event about a container being started.



Challenge and Analysis

Part 1: Make a New SCAP Profile

Make a screen capture showing the results in OpenSCAP Workbench after using your new profile to scan DockerRunner.



Part 2: Update the Group Files to Use the New Profile

Designing a Secure Cloud Architecture

Cloud Computing, Second Edition - Lab 04

Make a screen capture showing the new group configuration file for the default group in Wazuh.

```
1 <agent_config>
2   <wodle name="open-scap">
3     <disabled>no</disabled>
4     <interval>1d</interval>
5     <scan-on-start>yes</scan-on-start>
6     <content type="xccdf" path="/var/ossec/etc/shared/default/ssg-ubuntu2004-ds-tailoring.xml">
7       <profile>xccdf_org.ssgproject.content_profile_standard</profile>
8     </content>
9   </wodle>
10  <wodle name="docker-listener">
11    <disabled>no</disabled>
12  </wodle>
13 </agent_config>
```