

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:

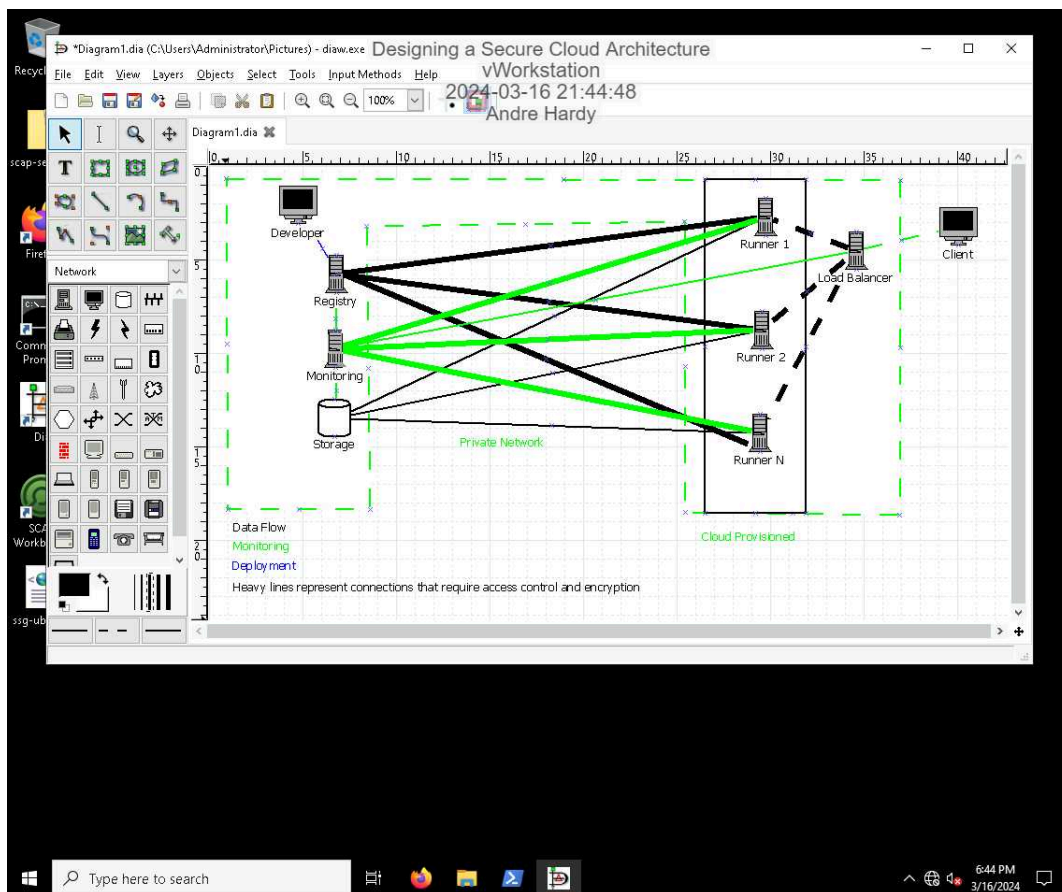
100%

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

Hands-On Demonstration

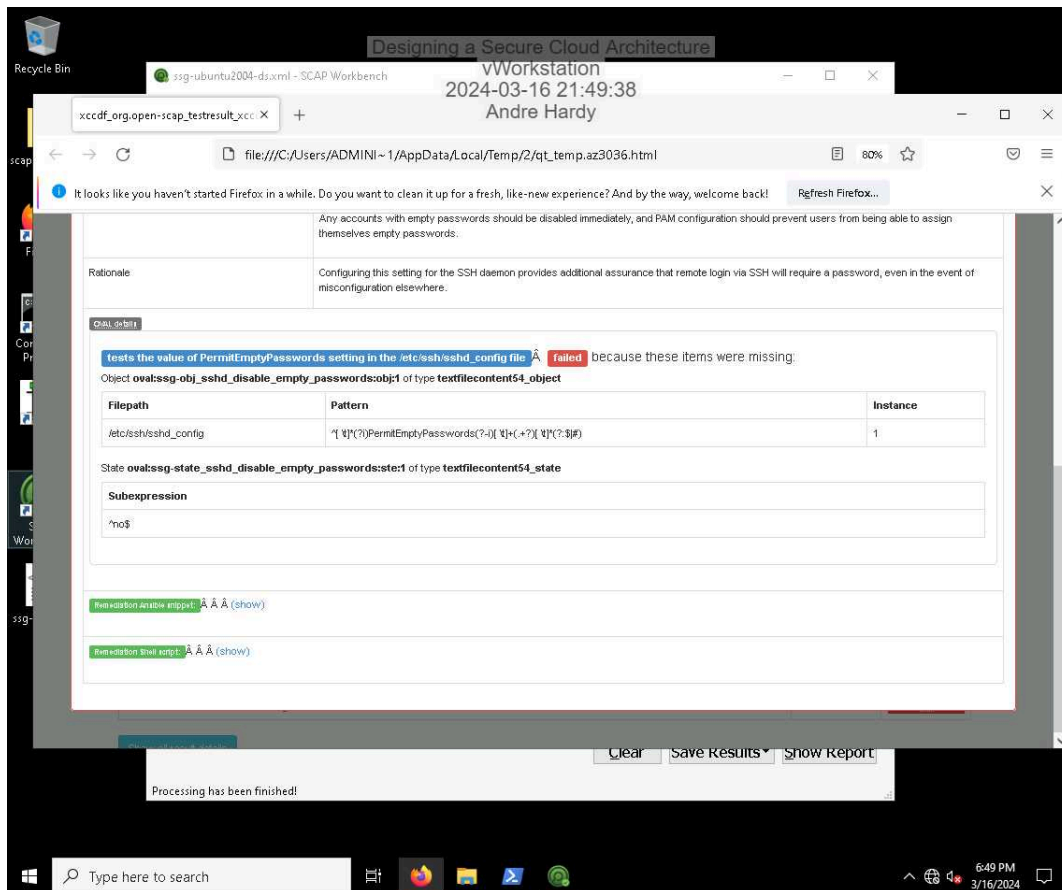
Part 1: Planning a Design

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

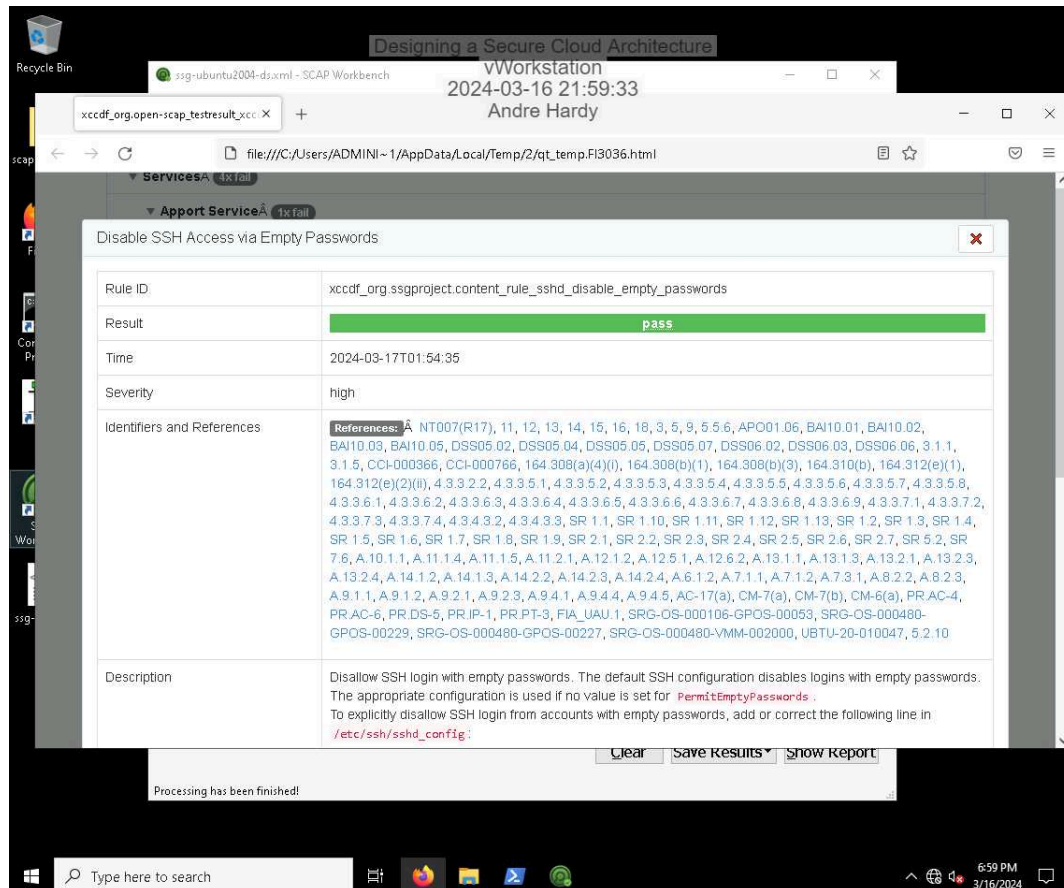


Part 2: Automating Security

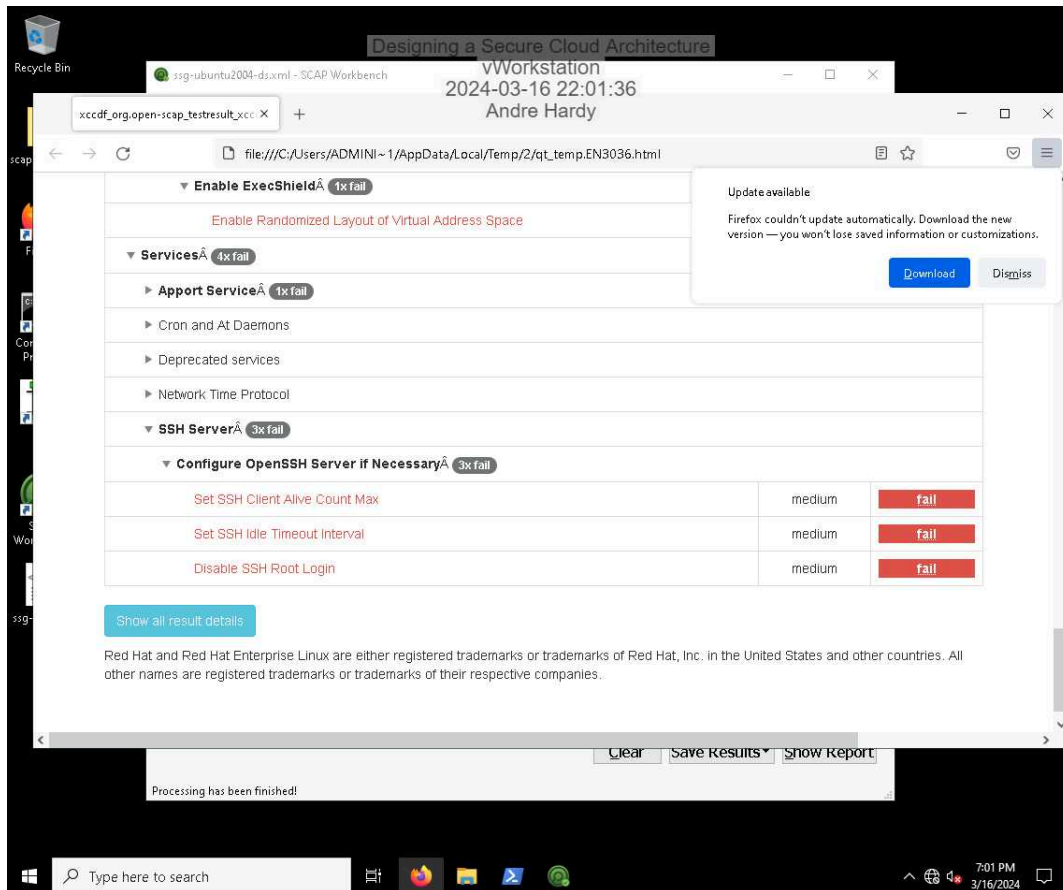
13. Make a screen capture showing the **OVAL** details of the **PermitEmptyPasswords** failure from the manual scan.



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



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



Part 3: Continuous Monitoring

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 the Wazuh Security Events dashboard. The left sidebar contains a list of modules, including 'data.oscap.check.description', 'data.oscap.check.id', 'data.oscap.check.oval.id', 'data.oscap.check.rationale', 'data.oscap.check.references', 'data.oscap.check.result', 'data.oscap.check.severity', 'data.oscap.check.title', 'data.oscap.scan.benchmark.id', 'data.oscap.scan.content', 'data.oscap.scan.id', and 'data.oscap.scan.profile.id'. The main panel displays a table of security events. The table has columns for 'Time', 'Source', 'Description', 'Score', and 'ID'. The events are filtered by 'Security events' and show a list of failed OpenSCAP checks on the DockerRunner machine.

Time	Source	Description	Score	ID
Mar 16, 2024 @ 19:07:29.162	DockerServer	OpenSCAP: Ensure /var/Log/audit Located On Separate Partition (not passed)	5	81529
Mar 16, 2024 @ 19:07:29.189	DockerServer	OpenSCAP: Ensure /var/Log Located On Separate Partition (not passed)	5	81529
Mar 16, 2024 @ 19:07:29.188	DockerServer	OpenSCAP: Ensure /var Located On Separate Partition (not passed)	5	81529
Mar 16, 2024 @ 19:07:29.093	DockerServer	OpenSCAP: Ensure /tmp Located On Separate Partition (not passed)	5	81529
Mar 16, 2024 @ 19:07:29.079	DockerServer	OpenSCAP: Ensure /home Located On Separate Partition (not passed)	5	81529
Mar 16, 2024 @ 19:07:26.951	DockerRunner	OpenSCAP: Ensure the audit Subsystem is Installed (not passed)	7	81530
Mar 16, 2024 @ 19:07:26.892	DockerRunner	OpenSCAP: Ensure /var/Log/audit Located On Separate Partition (not passed)	5	81529
Mar 16, 2024 @ 19:07:26.871	DockerRunner	OpenSCAP: Ensure /var/Log Located On Separate Partition (not passed)	5	81529
Mar 16, 2024 @ 19:07:26.862	DockerRunner	OpenSCAP: Ensure /var Located On Separate Partition (not passed)	5	81529
Mar 16, 2024 @ 19:07:26.854	DockerRunner	OpenSCAP: Ensure /tmp Located On Separate Partition (not passed)	5	81529
Mar 16, 2024 @ 19:07:26.842	DockerRunner	OpenSCAP: Ensure /home Located On Separate Partition (not passed)	5	81529

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

The screenshot shows a Windows desktop with a web browser displaying the Wazuh Security Events interface. The browser tab is titled "Wazuh - Wazuh" and the address bar shows the URL "https://172.30.0.10/wazuh-...". The interface displays a security event for a Docker image pull. The event details are as follows:

Time	Source	Destination	Event	Score
Mar 16, 2024 @ 19:09:00.685	DockerRunner	Docker: Image or repository registry:5000/alpine pulled	3	87932

The event details are expanded, showing the following JSON data:

```
{  "_index": "wazuh-alerts-4.x-2024.03.17",  "agent.id": "001",  "agent.ip": "172.31.0.20",  "agent.name": "DockerRunner",  "data.docker.Action": "pull",  "data.docker.Actor.Attributes.name": "registry:5000/alpine",  "data.docker.Actor.ID": "registry:5000/alpine:latest",  "data.docker.Type": "image",  "data.docker.id": "registry:5000/alpine:latest",  "data.docker.scope": "local",  "data.docker.status": "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.",  "data.docker.time": "2024-03-16 22:11:09",  "data.docker.timeNano": "1710711060000000000"}
```

A notification box at the bottom of the event details 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." with a "Reload page" button.

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

The screenshot shows a Windows desktop with a vWorkstation window displaying the Wazuh Security Events interface. The browser address bar shows the URL `https://172.30.0.10/wazuh-alerts-4.x-2024.03.17`. The interface displays a list of security events under the 'Security events' module. The selected event is from March 16, 2024, at 19:09:15.529, generated by the 'DockerRunner' agent. The event details show a Docker container named 'crazy_brown_star' being started. The 'Expanded document' section shows the event data in a table format.

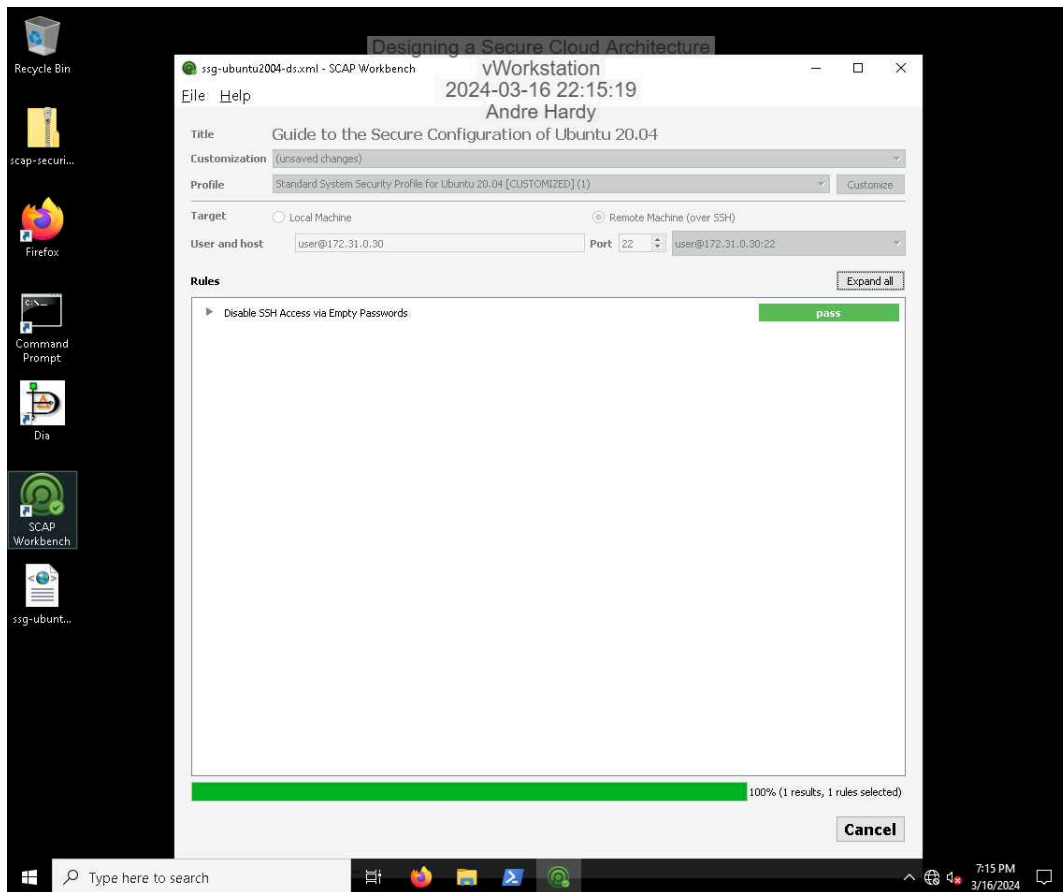
Field	Value
<code>_index</code>	<code>wazuh-alerts-4.x-2024.03.17</code>
<code>agent.id</code>	<code>001</code>
<code>agent.ip</code>	<code>172.31.0.20</code>
<code>agent.name</code>	<code>DockerRunner</code>
<code>data.docker.Action</code>	<code>start</code>
<code>data.docker.Actor.Attributes.Image</code>	<code>registry:5000/alpine</code>
<code>data.docker.Actor.Attributes.name</code>	<code>crazy_brown</code>
<code>data.docker.Actor.ID</code>	<code>e907e8a594ba3a55249f7458e69e19b49bec6593e5cb249416f77e6f624ebb00</code>
<code>data.docker.Type</code>	<code>24ebb98</code>
<code>data.docker.from</code>	
<code>data.docker_id</code>	

A notification message is displayed over the table, stating: '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 next to the message.

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

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

