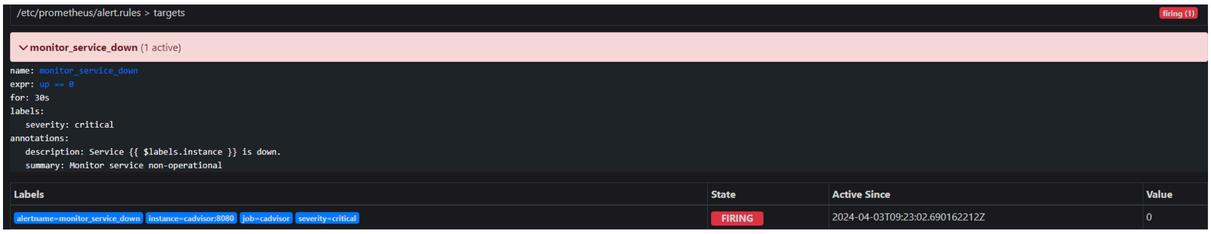
Security Incident Simulation: Cadvisor Service Down

Scenario:

An alert has been detected indicating that the cadvisor service, which is responsible for collecting metrics from containers, is not working.



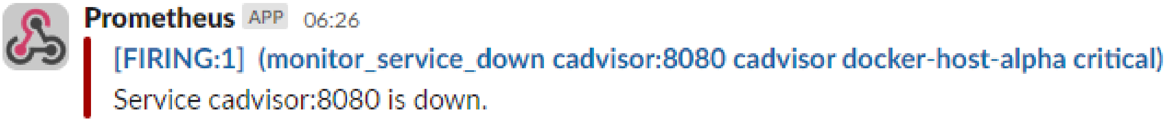
/etc/prometheus/alert.rules > targets

firing (1)

monitor_service_down (1 active)

```
name: monitor_service_down
expr: up == 0
for: 30s
labels:
   severity: critical
annotations:
   description: Service {{ $labels.instance }} is down.
   summary: Monitor service non-operational
```

Labels	State	Active Since	Value
alertname=monitor_service_down instance=cadvisor:8080 job=cadvisor severity=critical	FIRING	2024-04-03T09:23:02.690162212Z	0



Prometheus APP 06:26

[FIRING:1] (monitor_service_down cadvisor:8080 cadvisor docker-host-alpha critical)

Service cadvisor:8080 is down.

Incident Description:

- Date and time of the incident: 2023-11-14 17:45 UTC
- Type of attack: Attempted intrusion into a container
- Affected containers: cadvisor
- Impact of the incident: Loss of visibility into the state of the containers

Response Process:

1. Identification:

- A Prometheus alert was received indicating that the cadvisor service is not working.
- The cadvisor logs were reviewed to identify the cause of the problem.
- An attempted intrusion into the cadvisor container was identified.

2. Mitigation:

- The affected cadvisor container was stopped.
- The vulnerable container image was deleted.
- A new cadvisor image was deployed with the necessary security measures.
- The cadvisor service was restarted.

3. Post-Incident Analysis:

- The cause of the incident was an attack on the cadvisor container image that was being used.
- The attack was able to gain access to the container and execute malicious commands.
- The impact of the incident was limited to the loss of visibility into the state of the containers.

4. Reporting:

- The security team was informed about the incident.
- A report was created with the information of the incident and the measures taken.

5. Action Plan:

- Measures will be implemented to improve the security of container images.
- Regular penetration tests will be performed to identify and fix vulnerabilities in containers.
- An intrusion detection system (IDS) will be implemented to detect attacks in real time.

Conclusions:

The security incident on November 14, 2023 at 17:45 UTC highlights the importance of having robust security measures in place to protect containers. The quick response of the security team allowed the impact of the incident to be mitigated and prevented further damage.

Recommendations:

- Implement security measures for container images, such as using digital signatures and vulnerability scanning.
- Perform regular penetration tests to identify and fix vulnerabilities in containers.
- Implement an intrusion detection system (IDS) to detect attacks in real time.
- Have a well-defined security incident response plan.
- Inform the security team about any security incidents.
- Create a report with the information of the incident and the measures taken.