Student Website Threat Model

Owner: Teacher
Reviewer: Diana Ibraheem
Contributors:
Date Generated: Wed Sep 11 2024

Executive Summary

High level system description

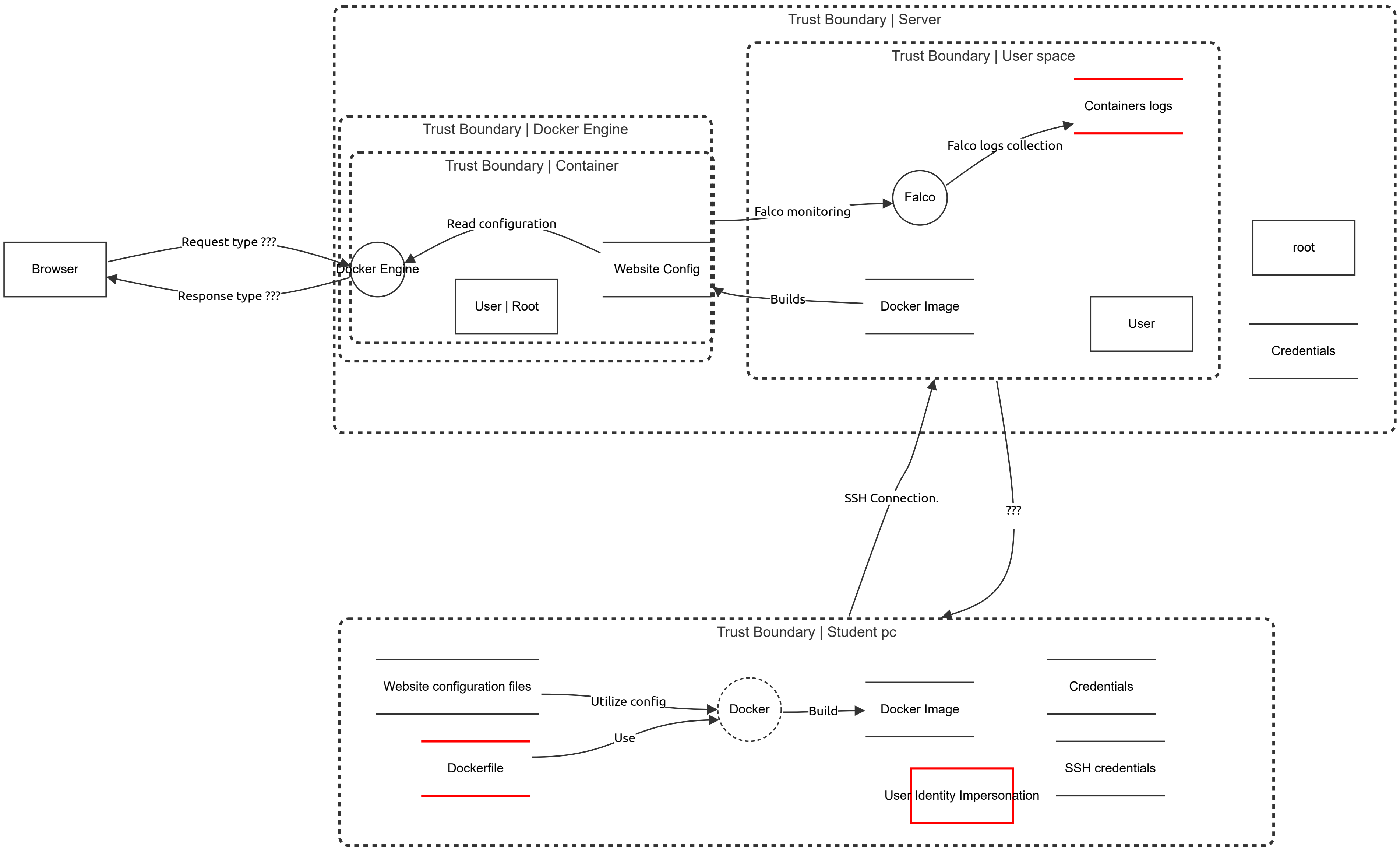
Whole system for a containerized website on cloud node.

Summary

Total Threats	9
Total Mitigated	6
Not Mitigated	3
Open / High Priority	1
Open / Medium Priority	2
Open / Low Priority	0
Open / Unknown Priority	0

System STRIDE

System includes: student's pc, cloud server and container.



System STRIDE

Browser (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Docker Engine (Process)

Engine

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Website Config (Store)

HTML and CSS for the website

Number	Title	Type	Priority	Status	Score	Description	Mitigations
10	Denial of Service (DoS) on Nginx Web Server	Denial of service	Medium	Mitigated		An attacker could overwhelm the Nginx web server with excessive traffic, causing it to become unresponsive or crash	DDoS protection, use the cloud provider’s built-in DDoS protection services to mitigate large-scale traffic attacks

Read configuration (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Response type ??? (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Request type ??? (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Builds (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Falco monitoring (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Falco logs collection (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Build (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Use (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Utilize config (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

???
(Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

SSH Connection. (Data Flow)

Dev env to server, used to copy image and update image.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
2	SSH Spoofing Threat	Information disclosure	High	Mitigated		Attackers could spoof SSH credentials to gain unauthorized access to the server	Implement multi-factor authentication (MFA) for SSH access

Docker Image (Store)

Ready made docker image

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Containers logs (Store)

Container monitoring via Falco

Number	Title	Type	Priority	Status	Score	Description	Mitigations
21	Exposure of Sensitive Information in Container Logs	Information disclosure	Medium	Open		If these logs are not properly secured, attackers could gain access to sensitive data by viewing log files	Provide remediation for this threat or a reason if status is N/A

Falco (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Website configuration files (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Dockerfile (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
22	nsecure Cloud Configuration Threat	Information disclosure	Medium	Open		The cloud server hosting the Docker container for the student's portfolio website could be improperly configured, allowing unauthorized access to critical services or sensitive data insecure access controls could expose the Docker container and other services to attackers	Provide remediation for this threat or a reason if status is N/A

Docker (Process) *- Out of Scope*

Builds docker image

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Docker Image (Store)

Includes website configuration files

Number	Title	Type	Priority	Status	Score	Description	Mitigations
16	Compromised Docker Image Configurations	Tampering	Medium	Mitigated		Attackers could tamper with the Docker images that are used to deploy the student's portfolio website. By modifying these images, attackers could inject malicious code, misconfigure the environment, or introduce vulnerabilities.	ensures that only verified and trusted images are pulled and deployed in the environment, preventing tampered images from being used
4	Tampering with Website HTML/CSS Files	Tampering	Medium	Mitigated		Attackers could modify the HTML or CSS files of the website, altering the content displayed to users	Implement file integrity monitoring (FIM) to detect unauthorized changes to website files and alert administrators of any tampering
6	Tampering with Docker Configuration	Tampering	Medium	Mitigated		Attackers could tamper with the Docker configuration files used to containerize and run the student portfolio website	Ensure that sensitive configurations, such as port mappings and environment variables Implement tools like Docker Bench for Security to regularly audit the Docker setup for insecure configurations or misconfigurations

SSH credentials (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
17	Weak SSH Key Management	Information disclosure	Medium	Mitigated		weak or improperly managed SSH keys could expose sensitive credentials	SSH keys need to be encrypted with strong password or passphrase

Credentials (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

root (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

User (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Credentials (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

User Identity Impersonation (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
18	User Identity Impersonation	Spoofing	High	Open		attacker could copy a legitimate user by stealing credentials or session tokens	Implement MFA for all users with sensitive access

User | Root (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations